MANUAL DE INFORMÁTICA FORENSE

(Prueba Indiciaria Informático Forense)

Bases Metodológicas: Científica, Sistémica, Criminalística, Tecnológica-Pericial y Marco Legal



INCLUYE ACTUALIZACIÓN ON-LINE

María Elena Darahuge
Luis E. Arellano González

Prólogo del Dr. Ricardo Guibourg

ERREPAR

María Elena Darahuge
Luis E. Arellano González

MANUAL DE INFORMÁTICA FORENSE

(Prueba Indiciaria Informático Forense)

Bases metodológicas:
científica, sistémica, criminalística,
tecnológica-pericial y marco legal

ERREPAR

Darahuge, María Elena

Manual de informática forense : prueba indiciaria informático forense / María Elena Darahuge y Luis Enrique Arellano González. - 1a ed. - Ciudad Autónoma de Buenos Aires : Errepar, 2014.

E-Book.

ISBN 978-987-01-1681-3

1. Informática. I. Arellano González, Luis Enrique II. Título CDD 001.5

Manual de informática forense Primera edición

ERREPAR S.A.

Paraná 725 (1017) - Buenos Aires - República Argentina Tel.: 4370-2002

Internet: www.errepar.com

E-mail: clientes@errepar.com

ISBN: 978-987-01-1681-3

Nos interesan sus comentarios sobre la presente obra: editorial@errepar.com

© 2014 ERREPAR S.A.

Queda hecho el depósito que marca la ley 11.723

No se permite la reproducción parcial o total, el almacenamiento,

el alquiler, la transmisión o la transformación de este libro, en cualquier forma o por cualquier medio, sea electrónico o mecánico, mediante fotocopias, digitalización u

otros métodos, sin el permiso previo y escrito del editor. Su infracción está penada por las leyes 11.723 y 25.446.

ACTUALIZACIÓN ON-LINE



El contenido del presente libro se actualiza por Internet a través de nuestra página web. Deberá ingresar a www.errepar.com/libros.



Seleccione la presente obra presionando el botón Ingresar, visualizará la siguiente pantalla:

La primera vez que intente consultar el material tendrá que registrarse como usuario, para lo cual se le pedirá que ingrese la clave de de acceso (22462691) y que complete una serie de datos personales.

Tenga presente que es muy importante que ingrese correctamente su dirección de correo electrónico, debido a que allí se le enviará su usuario y contraseña para acceder a los servicios asociados al libro.

Finalmente, presionando el icono correspondiente, tendrá acceso a las actualizaciones de esta obra.

LOS AUTORES

Prof. Ing. María Elena Darahuge

Licenciada e Ingeniera en Informática.

Profesora Universitaria en Ingeniería en Informática, UCSA.

Secretaria Académica del Curso de Experto en Informática Forense, FRA (UTN). Profesora Asociada de la materia Sistemas Operativos, UAJFK.

Prof. Ing. Luis Enrique Arellano González

Abogado con orientación Penal, UBA. Licenciado e Ingeniero en Informática.

Profesor Universitario en Ingeniería en Informática y en Criminalística, UCSA.

Licenciado en Criminalística.

Perito en Documentología, Balística y Papiloscopía, IUPFA. Director del Curso de Experto en Informática Forense, FRA (UTN). Profesor Asociado de la materia Sistemas Operativos, UAJFK.

PRÓLOGO

Hacia 1970, cuando empecé a interesarme en ella, la Informática era casi un tema de ficción científica. En las películas aparecían enormes máquinas llenas de luces intermitentes y carretes de cinta de movimiento espasmódico, a las que se atribuían poderes enormes, a ratos divinos, a menudo diabólicos. Vincular esas máquinas con el derecho era un verdadero desafío; no tanto técnico informático, sino técnico jurídico. En efecto, las computadoras siempre pudieron dar de sí mucho más que lo que los hombres de derecho fuimos capaces de pedirles. La persistente brecha entre estas dos variables obedeció a varios factores: uno, la aversión que la mayoría de los abogados sienten por las matemáticas y el temor de que un día las máquinas lleguen a reemplazarlos, utopía negativa que suelen comentar en términos de excelsitud del hombre, libre albedrío, irracionalidad de lo inanimado y otras referencias metafísicas. Otro factor consiste en el retraso epistemológico que afecta al conocimiento jurídico que –más allá de la evolución de sus contenidos– nunca tuvo su revolución copernicana y se encuentra hoy casi en el mismo punto donde lo dejó el emperador Justiniano en el siglo VI de nuestra era.

El desafío, pues, no giraba entonces en torno de la programación sino del modo de representar aquello que pudiera llamarse realidad jurídica. Era un tema apropiado para la filosofía del derecho y, al tratar de encararlo racionalmente, trabé relación y amistad con especialistas que se aproximaban también desde la elaboración de *software*, desde la recopilación de datos y desde la administración de justicia, pero también desde lo que aparecía como una nueva rama del derecho: el derecho informático, que muchos confundían entonces con la informática jurídica. Yo trataba de distinguirlos: una cosa –decía– es ser el abogado de un psicoanalista y otra distinta ser el psicoanalista de un abogado.

Todo aquello ha quedado en la historia de una época que –con escasa autocrítica– se me antoja heroica. La informática jurídica avanzó mucho en sus aspectos documentales y de gestión, pero sigue retrasada (por los motivos ya apuntados) en el ámbito decisorio, que es el más fascinante. Sin embargo, gracias a la difusión de computadoras personales y portátiles, en los últimos veinte años la Informática pasó a formar parte imprescindible de la vida de cualquiera y las computadoras se convirtieron en eficaces máquinas de pensar auxiliares, acopladas a nuestros cerebros por medio de teclados, ratones y monitores.

El hecho de que las computadoras formen parte de la vida cotidiana trajo consigo que, como los automóviles, los teléfonos y las armas de fuego, sirvieran también para

cometer delitos o para contener indicios de actos ilícitos cometidos en cualquier rama de la actividad humana. Y, así como los médicos legistas escudriñan los cadáveres, los expertos en balística examinan las estrías de los proyectiles o anónimos funcionarios controlan las comunicaciones telefónicas de los sospechosos, aparecieron los peritos informáticos, capaces de buscar información en una computadora secuestrada, restaurar archivos borrados de un disco duro o verificar la autenticidad de un intercambio de correos electrónicos.

Esta nueva especialidad de la criminalística, que se ha vuelto indispensable para el procedimiento judicial, no es cosa sencilla. Requiere un profundo conocimiento de los elementos técnicos materiales e inmateriales, ingenio para extraer de ellos la información requerida venciendo disfraces y disimulos, una cuidadosa revisión de las condiciones que permitan preservar el valor probatorio de esa información y un certero modo de vincular toda esta actividad con las necesidades legales del proceso que las requiera.

Todo esto está presente en el preciso y completo manual que han preparado mis amigos María Elena Darahuge y Luis Enrique Arellano González, expresado en nuestro idioma y con la claridad que es la cortesía del intelecto. Aunque muchas de las precisiones técnicas que contiene son ajenas a mi propia experiencia, considero un honor presentar el libro como un valioso instrumento para la investigación de los hechos a partir de los vestigios informáticos.

Ricardo A. Guibourg

Buenos Aires, marzo de 2011

"Dicere etiam solebat nullum esse librum tam malum

Ut non aliqua parte prodesset".[1]

Plinio el Joven (Epístolas III)

1 "Se dice que no hay libro malo donde no se halle alguno bueno..."

PREFACIO

Cuando a principios del año 2004 comenzamos a reunir información para iniciar el dictado de un Curso de Informática Forense, con carácter informativo, para todo tipo de profesionales, en la Regional Avellaneda de la Universidad Tecnológica Nacional, advertimos una serie de eventos que finalizaría en la planificación y redacción de este manual. Las circunstancias que nos llevaron a ello pueden sintetizarse en:

La mayoría de la bibliografía consultada era de origen estadounidense o europeo, casi en su totalidad en inglés, en menor cantidad en otros idiomas y escasamente en castellano.

Las obras referidas consistían en descripciones generales de las técnicas relacionadas con la Informática Forense, obras anecdóticas con algún sentido práctico, o descripciones de operación de algunas herramientas específicas (con su correspondiente origen y marca registrada), que las convertían en manuales de dichas herramientas.

No aparecían obras orientadas a generar un análisis conceptual, metodológico, formal y estricto de la Informática Forense como especialidad de las Ciencias Criminalísticas.

Por otra parte aparecía una gran cantidad de herramientas sin clasificación ni orden aparente, entre los programas ofrecidos al respecto por la comunidad de Software Libre (entorno Linux).

Se tornaba evidente la necesidad de efectuar una recopilación ordenada y sistemática de los distintos componentes detectables en la comunidad pericial, a efectos de aportar entidad metodológica, científica, criminalística, informática y legal a la nueva disciplina surgida de hecho y aún no formalizada de derecho.

En nuestro país, se han producido diversos intentos para normar la conducta delictiva informática, representada por las leyes 25.506, de Firma Digital y 26.388 de Delitos Informáticos. Sin embargo es muy poco lo que se ha avanzado desde aquel momento citado hasta la fecha, en lo que hace al Derecho Procesal. Algunas jurisdicciones han evolucionado más que otras integrando nuevas formas de notificación y consulta de expedientes, avanzando hacia el expediente digital (sueño de todo operador del derecho). Muy poco es lo que se puede encontrar en el Derecho Internacional, en particular en el Derecho Privado, a pesar de que muchos contratos

entre exportadores e importadores de productos en especial regionales, se celebran por medio de intercambio de mensajes de correo electrónico, lo que se está haciendo extensivo al área comercial de las autopartes y otros emprendimientos similares. En cuanto al tratamiento específico de la Prueba Documental Informática, su confirmación por medio de la Prueba de Informes y su revisión por la Prueba Pericial Informático Forense, la disciplina se encuentra muy lejos de estar adecuadamente inserta en el Sistema Judicial y convenientemente normalizada mediante el uso de protocolos claros, fáciles de implementar y útiles en el apoyo a la decisión judicial (objetivo principal de toda prueba pericial).

Recordando que en un momento crítico de nuestra formación profesional hemos recurrido a obras simples, integradoras, pero sumamente esclarecedoras, como el *Manual de Criminalística* de Roberto Albarracín, que tan útil nos fuera en nuestra aproximación a la investigación del delito. Aproximación que luego debíamos orientar con obras específicas como *El ABC del Dactilóscopo* de Ricardo Rosset y Pedro Lago. Pensamos que era necesario conformar un texto de apoyo al perito informático forense que le permitiera actuar de manera profesional, unificando los perfiles mínimos pretendidos para esta actividad en apoyo de la investigación delictiva. Sus componentes principales debían incluir:

Un Marco Científico, que le facilite realizar sus investigaciones y experiencias, apoyado estrictamente en el método científico. Asimismo debería aportarle las estructuras lógicas necesarias para justificar sus fundamentaciones de manera estricta e irrebatible, más allá de la fluidez argumentativa propia de cada profesional.

Un Marco Criminalístico, a partir del cual pueda interrelacionarse con los restantes especialistas del área, interactuar con éstos, trabajar en forma mancomunada y en lo posible arribar a conclusiones coherentes desde todas las visiones específicas. De la misma forma en que la Medicina Legal es una especialidad de la Medicina imbuida de un amplio contenido Criminalístico y Legal (especialmente desde el Derecho Procesal), la Informática Forense es una disciplina Informática con las mismas características propias.

Un Marco Informático general, a partir de las metodologías de Análisis de Sistemas, que le permitan utilizar aquellas herramientas de uso general que se adapten a las actividades periciales informáticas. En ese sentido, las etapas de relevamiento de información y desarrollo de un modelo coherente de análisis, se evidencian como instrumentos adecuados para brindar soporte metodológico a la actividad del experto en Informática Forense.

Un Marco Informático específico, en relación con las herramientas propias del

tratamiento de la prueba indiciaria informático forense. Al respecto es dable destacar que éstas deben ser abordadas desde los dos ambientes más frecuentes en uso en nuestra sociedad, el de *software libre* y el de *software propietario*, más allá de sus características de pago o gratuito.

Un Marco Legal abarcativo de las distintas actividades periciales a desarrollar. Esto implica la inserción legal del accionar pericial al concurrir al lugar del hecho (a requerimiento de un Tribunal, o de un cliente, con orden judicial que lo avale o sin ella), al realizar una inspección ocular, al documentar y secuestrar elementos probatorios, su responsabilidad respecto de la prueba indiciaria que se le ha confiado en custodia, los cumplimientos de los plazos legales, su condición de testigo experto, los artículos de los códigos de fondo y de forma que lo protegen o lo limitan y la interacción resultante de su presentación ante los distintos Fueros Judiciales.

Los puntos anteriores, se verían reflejados en un informe pericial:

Científicamente fundamentado.

Criminalísticamente interrelacionado.

Modelado mediante técnicas propias del Análisis de Sistemas.

Investigado con las mejores herramientas disponibles.

Inserto en el marco legal correspondiente.

No obstante y teniendo en cuenta la actual tendencia judicial hacia la metodología de juicio oral, no es suficiente con una fundamentación técnica adecuadamente implementada para defender un informe pericial. Hacen falta técnicas de argumentación, redacción y oratoria contundentes, precisas e irrebatibles. De ahí la necesidad de recomendar la capacitación del profesional en el arte de la redacción y la oratoria que le permitan realizar una adecuada defensa oral y escrita de sus resultados periciales, ante posibles impugnaciones o pedidos de aclaración.

Estamos seguros de no haber podido realizar una obra adecuada a las pretensiones anteriores, pero también podemos asegurar que se trata de un punto de partida, disperso, con fallas, criticable y perfectible, pero punto de partida al fin.

"Criminalística es la metodología integradora multidisciplinaria que proveela información tendiente al esclarecimiento del hecho,a partir de los indicios recolectados (prueba indiciaria)."

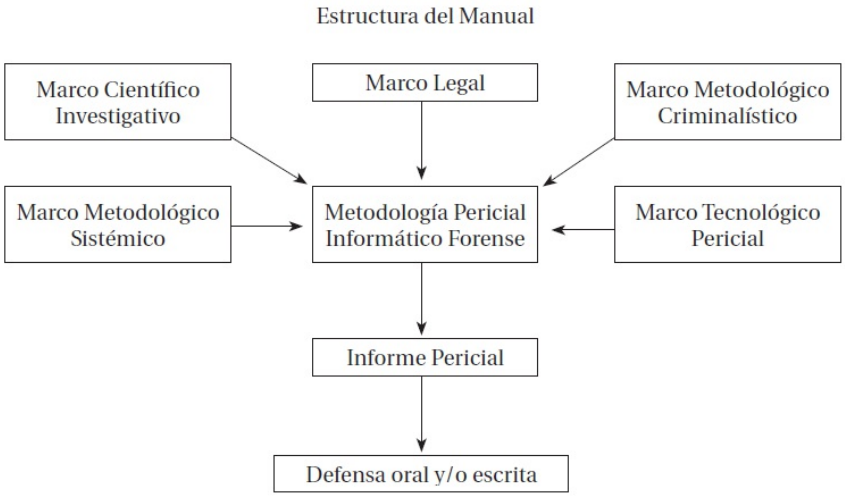
“Prueba indiciaria es la prueba integrada por el conjunto de elementos físicos y virtuales, que obran en un lugar determinado, necesarios y suficientes para efectuar una reconstrucción lógica, científica,

tecnológica y técnica de los hechos investigados, por medio del correspondiente análisis pericial forense.”

“Informática Forense es el conjunto muldisciplinario de teorías, técnicas y métodos de análisis, que brindan soporte conceptual y procedimental, a la investigación

de la prueba indiciaria informática.”

CAPÍTULO 1
ESTRUCTURA GENERAL



Este trabajo ha sido planificado y desarrollado con el objeto de aportar al perito informático forense una guía de referencias y consultas rápida, sencilla y fundamentada especialmente en la inter y transdisciplinariedad que este tipo de tareas implica.

Pese a lo novedoso de esta especialidad, es indudable que los fundamentos que la sustentan ya existían con anterioridad a su implementación práctica. La Metodología Pericial Informático Forense es alimentada, soportada y justificada por otras ciencias y técnicas precedentes, que aportan a la tarea pericial distintos entornos específicos entre los que debemos destacar:

Marco Científico Investigativo: El método científico se constituye en una herramienta fundamental de análisis para toda tarea tecnológica de investigación.

Marco Metodológico Sistémico: El Análisis de Sistemas nos aporta los elementos necesarios para realizar un análisis de la información estructurado y estricto, relacionado con las estructuras de datos analizadas y las arquitecturas involucradas.

Marco Metodológico Criminalístico: La prueba indiciaria como fundamento de la investigación criminal ha sido identificada como la reina de las pruebas y se ha

utilizado de manera sistemática durante la totalidad del siglo pasado. Su eficiencia ha sido harto probada, sus defectos detectados y corregidos. Constituye la base indiscutible de la tarea pericial, incluyendo a la pericia informática forense entre sus disciplinas derivadas y determinando las relaciones interdisciplinarias derivadas de la interacción pericial en el lugar del hecho (real o virtual, propio o impropio) o la gestión y análisis de la prueba involucrada.

Marco Tecnológico Pericial: Si bien la pericia informática forense se encuentra integrada, respaldada y justificada en la investigación criminalística en general, debe su existencia individual a una metodología específica y diferente de las demás. Se apoya en herramientas, métodos y técnicas propios y actúa sobre una prueba indiciaria, que posee características particulares que la diferencian notoriamente de las restantes pruebas indiciarias, analizadas por otras disciplinas criminalísticas.

Marco Legal: La pericia informática forense, por su orientación específica a la investigación reconstructiva, de transgresiones que pueden o no constituir ilícitos de diferente naturaleza (penal, civil, comercial, contractual, particular), involucra una enorme gama de actores y relaciones de todo tipo. Es inevitable el análisis metodológico ordenado y estricto de la legislación relacionada con ésta en cada caso particular, no es posible describirlos a todos en una obra como la presente, de ahí la necesidad del perito de acomodar su tarea a la jurisdicción y competencia en la cual debe actuar.

Hemos intentado integrar los marcos descriptos con anterioridad a efectos de constituir una Metodología Pericial Informático Forense estricta y científicamente fundamentada. Por supuesto esta metodología no tendría una razón de ser si no es volcada en un informe pericial. El análisis de las características propias de este informe pericial específico constituye una parte destacada de este manual.

A partir de la realización del informe pericial surge un compás de espera para el perito, hasta que llega la tan frecuente impugnación éste es llamado a realizar aclaraciones ante el Juzgado Interventor en la etapa de instrucción o debe concurrir ante el tribunal de oral que dictará sentencia.

En este punto se produce una división estricta en el accionar del perito como testigo. Esta división surge de la naturaleza federal de nuestro país, que implica diferentes códigos de procedimientos para las provincias que lo conforman, por una parte, y del tipo de pericia realizada (ámbito penal, civil, comercial, etc.), lo que determina diferentes entornos de testificación. No obstante estos entornos, desde la práctica se pueden resumir en dos tipos de defensa pericial: la defensa escrita y la defensa oral.

La defensa escrita, no tiene más implicancias que las analizadas en este manual y

éstas, en general, se refieren a la oportunidad y formalidad de las presentaciones. En cambio, la defensa oral implica un cambio notorio en el escenario y grado de participación de los actores involucrados en el estudio pericial. Es necesario que el perito se capacite en las características que rodean al acto referido y las diferentes técnicas que pueden ser utilizadas en apoyo de su argumentación pericial. En la vida en general y en el discurso en particular, no siempre el que tiene la razón logra demostrarla.

Orientación para la lectura del manual

A poco de iniciar nuestra tarea, notamos que era una obra de notable extensión. Sabemos que una obra extensa tiende a cansar al lector y a dispersarlo de las ideas fundamentales de la misma. *Lo bueno, si breve, dos veces bueno* y nosotros queremos agregar: ¡y *lo malo… también!* Por lo tanto preferimos reducir la obra a los componentes esenciales de ésta.

No obstante, el propósito de este trabajo no es sólo confeccionar una guía para el perito informático forense, sino servir de consulta y fuente de información para otros profesionales que lo requieran. Tal el caso de abogados, ingenieros o licenciados en sistemas, informática o computación, licenciados en criminalística, médicos legistas, criminólogos, licenciados en administración de empresas, empresarios y toda otra persona que se interese por el tema.

Hemos intentado reunir en el texto todos los elementos necesarios para el experto y los conocimientos ampliatorios se distribuyen a lo largo de una serie de apéndices y anexos. En los apéndices el lector encontrará profundizados ciertos temas que se dan por conocidos en el cuerpo principal de la obra (la lógica, la prueba indiciaria, la inspección ocular, etc.) y en los anexos, todos aquellos instrumentos que puedan facilitarle su labor pericial (modelos de actas, de informes, de listas de control, etcétera).

Pensamos que la mejor manera de acercarse a la obra es realizar una lectura detallada del cuerpo principal. Para quienes lo necesiten o simplemente sientan curiosidad, se agregan los apéndices y para facilitar la tarea de los peritos se incluyeron los anexos. Todos estos documentos y algunos anexos suplementarios, como fuentes de consulta, se encuentran disponibles en su versión digital, para uso de quienes los necesiten y los consideren pertinentes.

CAPÍTULO 2
LA PROBLEMÁTICA DE LA INFORMÁTICA FORENSE

La inserción dentro de la sociedad de la Informática, como herramienta de gestión de la información, ha sido un proceso que se inicia a mediados del siglo pasado y que se ha caracterizado por su expansión incremental.

Los cambios tecnológicos y metodológicos han impulsado el desarrollo de la Informática de manera constante. A diferencia de lo que históricamente ha ocurrido en otras ciencias, que luego de un descubrimiento teórico extraordinario han sido necesarios largos períodos para desarrollar los instrumentos asociados con la misma en Informática, en contrapartida la aceleración del descubrimiento-implementación ha sido tan exponencial que actualmente no llega a difundirse un cambio sustancial en los equipos y su forma de empleo, cuando ya se está construyendo una nueva generación teórica y tecnológica que cambia totalmente las reglas de juego para profesionales y usuarios.

A principios del siglo pasado Albert Einstein proponía como resultado de sus investigaciones sobre la naturaleza y comportamiento de la luz, la existencia de un haz coherente con ciertos comportamientos particulares. Fue necesario que transcurriera prácticamente medio siglo, para que se implementara el primer láser operativo. Hoy habiendo transcurrido un período de tiempo similar, esta tecnología forma parte de nuestra vida y se ha incorporado a ella como un componente tan usual como la telefonía móvil.

En lo que hace a la Informática, ésta ha invadido la mayoría de las sociedades humanas, sin distinciones políticas, sociales, ni religiosas. Afecta la vida de todos los habitantes del mundo, de una u otra manera y con mayor o menor intensidad. Ha llegado a introducirse efectivamente en millones de hogares en las más diversas latitudes y longitudes y amenaza con dividir al mundo en dos grandes grupos principales: los que tienen acceso a la información y los que carecen de ella. Ha surgido un nuevo tipo de pobres que difícilmente puedan superar esta dificultad.

Los problemas derivados del atentado a las Torres Gemelas impusieron un gran respeto por la seguridad de las cosas y las personas. Como la mayoría de las personas pretende conservar su vida, el riesgo de los viajes se hizo evidente. Esto motivó a muchos productores regionales (jugo de arándanos, miel, dulces regionales, carnes exóticas a pequeña escala) a formalizar sus contratos de exportación e importación, por medio de mensajes de correo electrónico. A esto se suma que los procesos de

integración en que nos encontramos insertos, avanzan en lo comercial, pero son mucho más conservadores en lo normativo. Esta realidad provoca litigios que generalmente se resuelven por medios alternativos de resolución de conflictos (mediación, conciliación, arbitraje, etc.), algunos de los cuales finalizan radicados ante la jurisdicción correspondiente (tema sumamente complejo de resolver, por la multiplicidad de normas nacionales, bilaterales, multilaterales y de integración que afectan a los países involucrados). La preservación de la prueba documental informática en estos casos requiere de protocolos con validez internacional, los que aún están en vías de desarrollo y en nuestro país ni siquiera en ciernes (a pesar de los esfuerzos del Arcert).

Progresivamente el mercado real, se fue trasladando paulatinamente al mercado virtual. En estos momentos las salas comunes de los mercados de valores se parecen más a un centro de cómputos atestado que a un lugar de intercambio de acciones personalizado.

La integración de los componentes de procesamiento y almacenamiento de la información con las redes de comunicaciones, asimilando estas últimas al proceso de gestión de los datos, ha trascendido las fronteras y en este momento los negocios en todos sus niveles son parcialmente realizados utilizando estos medios disponibles. Si recordamos la arquitectura de una central telegráfica o telefónica de la primera mitad del siglo pasado, veremos que estaba constituida por una enorme cantidad de material eléctrico operado manualmente. Desde mediados de dicho siglo, este material fue paulatinamente sustituido por elementos electrónicos. Pero al avanzar el siglo XX, los elementos electrónicos fueron adquiriendo cada vez más complejidad lógica asociada y en estos momentos el *hardware* (equipos eléctricos y electrónicos) es mínimo respecto del *software* (programas con su lógica asociada.

Las redes han llegado no sólo a los centros de investigación, universidades, centros comerciales, banca financiera y área de negocios, sino que actualmente permiten relaciones de comercio al por menor dentro y fuera de la casa. Es posible adquirir desde libros, hasta componentes electrónicos por medio de Internet, las relaciones humanas se amplían, los idiomas se simplifican (no siempre para bien del idioma original, pero claro está facilitando la comunicación), la gente se relaciona.

Sin embargo esta aparente panacea informática es en muchos casos falsa. Por la red no sólo se intercambian bienes y servicios que facilitan la vida diaria, también se adquieren drogas ilegales, armas y pornografía infantil entre otros productos nocivos para la sociedad humana.

Es imposible entender estos procesos sin analizar la problemática consustancial con

la naturaleza humana. Sólo la firme convicción en la inocuidad ética y moral de los desarrollos humanos, permite asimilar esta disparidad de conductas y sus resultados. El instrumento (la computadora y la red), no son buenos, ni malos en sí mismos.

De la misma manera que la tecnología nuclear ha permitido destruir ciertos tipos de cáncer y las ciudades Hiroshima y Nagasaki, sin que se viera afectada su inocuidad moral intrínseca (y al parecer tampoco la de quienes lanzaron las bombas), la red puede emplearse para enviar fotografías y diagramas de una técnica novedosa de intervención quirúrgica, fotos de nuestro hijo recién nacido, para nuestros parientes en el otro extremo del mundo, las órdenes y plan de ejecución de un ataque terrorista o la seducción con fines sexuales de niños/as. El fenómeno de la sustitución de identidad se ha integrado a los males sociales modernos, en especial desde la aparición de las redes sociales y los perfiles virtuales (en la red, nada es lo que parece).

Entender esta naturaleza disociada entre tecnología, ética y normativa vigente es una tarea esencial para el perito informático forense. Sólo de esta manera podrá alcanzar el imprescindible grado de asepsia, objetividad y compromiso profesional con la tarea que le toca realizar. Los instrumentos, las tecnologías, los animales en general, no son bondadosos ni malvados, altruistas ni egoístas, son y/o actúan acorde con su naturaleza. Los conceptos éticos y morales son propios del hombre, de ninguna manera son universales y mucho menos compartidos por dos hombres diferentes (a poco de conversar con nuestro vecino, nuestro padre o nuestro hermano, podremos detectar dichas diferencias). Por lo tanto deben ser expuestos, propuestos, consensuados y normatizados (generalmente mediante leyes, reglamentos y disposiciones formales y coactivas; la ley sin castigo no parece ser una ley muy eficiente y hasta las leyes religiosas recurren a premios y castigos).

El perito informático forense es un auxiliar del aparato judicial, representado por el tribunal interventor. De ninguna manera es un auxiliar de la Justicia. La Justicia es un elemento tan indefinible, incomprensible e inmensurable como el amor, el bien, la superioridad racial, o el compromiso social de los políticos en general y de los nuestros en particular.

El perito debe cumplir su labor de asesoramiento en carácter de testigo, respecto del tribunal que ha requerido sus servicios. No es un investigador privado, no es el responsable de juzgar a las partes que intervienen en la causa y por supuesto no es quien va a decidir sobre la culpabilidad o inocencia de una persona. Esta tarea está reservada al tribunal y no nos concierne. Debemos actuar según nuestras capacidades profesionales, acorde con nuestras convicciones técnicas y separando dichas tareas de nuestras opiniones personales y prejuicios. ¿Es posible actuar de esta manera? ¿Existen los seres humanos objetivos y desprejuiciados? No estamos en condiciones

de afirmarlo, probablemente no, pero como sabemos de la existencia de aves sin alas y de mamíferos sin patas, no podemos negar la probabilidad de descubrir alguno. Esta objetividad del perito es tal vez una meta, tan inalcanzable e indeterminada como la Justicia, pero sin lugar a dudas, debe ser nuestra meta.

El surgimiento de la Informática Forense, su inserción social, judicial y tecnológica

Como decíamos, la Informática Forense se desprende directamente de una serie de sucesos que han afectado a la sociedad globalizada e informatizada de fines del siglo XX y principios del XXI.

Entre ellos podemos destacar:

El surgimiento de una serie de agresiones delictivas, utilizando medios informáticos, para concluir en delitos informáticos propios e impropios.

Estas agresiones son capaces de interactuar directa o indirectamente con gran parte de la normativa penal vigente.

Sin embargo la legislación específica vigente es escasa o se encuentra en vías de análisis para su implementación.

En el momento de producirse un hecho delictivo por medios informáticos, las acciones legales determinadas por los Códigos de Procedimientos (Legislación de Forma), no incluyen ni prevén los mecanismos necesarios para accionar contra este tipo de delitos. Ni siquiera establecen con claridad los límites legales de dichas investigaciones. Los derechos a la verdad material, al debido proceso y a la privacidad, se intersecan e invaden mutuamente, cada vez que hay que secuestrar y preservar elementos probatorios, en particular en la prueba documental informática.

La jurisprudencia es incipiente y depende más de la opinión, la formación profesional y la buena voluntad del juez, que de un accionar legislativo consensuado y fundamentado científicamente en un entorno multidisciplinario.

Como consecuencia de lo expresado y en razón del enorme auge de este tipo de delitos, han resultado afectadas diferentes áreas de la sociedad en general y de la comunidad científica, educativa y política en particular.

Desde el ambiente profesional de la Informática, de la abogacía, de la administración de empresas y de la criminalística se han iniciado una serie de

acciones tendientes a reunir información multidisciplinaria acerca del delito informático, su "modus operandi", los métodos informáticos involucrados en la comisión del delito y las carencias legales que los facilitan. Sobre la base de dicha información es necesario generar:

Nueva legislación de fondo que defina con claridad el delito informático, separando sus especies. La legislación vigente se ocupa en particular del delito informático impropio, pero muy poco del delito informático propio (que afecta a la información, por ejemplo, el robo de identidad y la falsedad de datos propietarios).[2]

Nueva legislación de forma para dar soporte legal a los métodos de investigación, sin afectar la confidencialidad asegurada a cada ciudadano sobre sus actos privados.

Nuevas formas de auditoría informática para la detección de intrusiones a los sistemas de información en uso.

Nuevos métodos informáticos de análisis y recuperación de la información.

Nuevas reglas gerenciales de protección de la información para asegurar la privacidad de las empresas y evitar los daños resultantes del espionaje industrial y/o comercial.

Nuevas técnicas criminalísticas que aseguren la detección, certificación, resguardo, preservación, traslado y análisis de la prueba indiciaria informático forense.

En el sentido de lo expresado la Informática Forense está inserta y/o es abarcativa de la totalidad de las acciones detalladas.

El conocimiento sobre sus alcances, desarrollo y posible evolución, permitirán al profesional (independientemente del área de origen), tener una visión clara y científicamente sustentada que le asegure una opinión certera e idónea al respecto.

Esta opinión, le será de suma utilidad, ya sea en el desarrollo de sus acciones profesionales particulares o en la interacción multidisciplinaria que nos conducirá hacia una legislación e investigación eficientes, efectivas y eficaces del delito informático y sus consecuentes.

El permanente crecimiento y difusión del uso de las computadoras y de los servicios que ofrece el trabajo en redes de comunicaciones por parte de los seres humanos, provoca inexorablemente el surgimiento de diversas actitudes hacia este tipo de entorno de trabajo o entretenimiento. Por consiguiente al estar involucrado el ser humano, aparecen diversas conductas relacionadas con el uso de las computadoras. La

actitud delictiva del ser humano es inevitable y se encuentra reflejada de diversas formas, una de las que afecta al resto de los integrantes de este entorno de trabajo es el delito cibernético.

La computadora puede ser utilizada como elemento para cometer un delito o la computadora en sí misma es el objetivo del delito. Por ejemplo los delitos relacionados con la pornografía infantil, amenazas a través mensajes electrónicos, fraudes, robo de la propiedad intelectual, pueden dejar huellas digitalizadas (para evitar llamarlas digitales, ya que suelen confundirse con dactilares) cuando la computadora es utilizada para cometer un delito. En estos casos se intenta investigar aquellas computadoras de las cuales se sospecha que están involucradas en un delito. Por medio de la búsqueda de palabras claves específicas, análisis de registros de eventos para verificar qué ocurrió en determinado horario y fecha y del análisis de información almacenada en dispositivos volátiles o no volátiles, se podría obtener evidencia de que alguna persona cometió un delito específico o no.

Cuando una computadora es una víctima en sí misma se la relaciona con una respuesta a un incidente, por ejemplo, el análisis y reconocimiento de sistemas que han sido atacados en forma remota. Estos ataques durante los años ochenta eran propios de los sistemas conectados por líneas telefónicas a través de módems, pero actualmente se encuentran en su mayor parte en Internet. Los ataques remotos se encuentran facilitados por las propias vulnerabilidades de los sistemas operativos, aplicaciones y servicios de red que se encuentran en las computadoras conectadas a una red área local, amplia o en Internet. De esta forma surgen distintos tipos de equipos que trabajan para responder a estos incidentes, entre ellos el CERT –Coordination Center– (www.cert.org), el Forum of Incident Response and Security Teams (www.first.org), el AR-CERT –Coordinación de Emergencias en Redes Teleinformáticas– (www.arcert.gov.ar).

Por lo tanto, las técnicas de detección y análisis de los delitos informáticos deben actualizarse permanente para responder a la variada gama de ataques y nuevos delitos que surgen en el entorno cibernético, merced a la aguda creatividad de los seres humanos que lo componen. Este proceso debe ser acompañado por la acción legislativa prospectiva, la vieja frase “el derecho siempre llega tarde”, nunca fue tan pertinente como en estos casos.

Concepto de Informática Forense

Si bien uno de los propósitos de la Informática Forense consiste en determinar los responsables de los delitos informáticos, también permite esclarecer la causa original de un ilícito o evento particular para asegurarse de que no vuelva a repetirse. La

Informática Forense es aplicable tanto en los casos llevados a juicio como en investigaciones particulares solicitadas por empresas u organismos privados. Podemos decir que:

La informática forense es un método probatorio consistente en la revisión científica, tecnológica y técnica, con fines periciales, de una colección de evidencias digitalizadas para fines de investigación o legales.

Cada caso específico debe ser analizado como si fuera a juicio, de esta manera cualquier investigación en Informática Forense puede soportar un escrutinio legal.

Resumiendo, entendemos por Informática Forense al conjunto multidisciplinario de teorías, técnicas y métodos de análisis que brindan soporte conceptual y procedimental a la investigación de la prueba indiciaria informática.[3]

2 Nada tiene de extraño que un caballero o una dama, al llenar sus datos personales en una red social, modifique su fecha de nacimiento u optimice su fotografía, para hacerlo más atractivo a las personas con las que quiere relacionarse. Este hecho no es nuevo y por esa razón en las entrevistas laborales, luego de analizar el currículum, se pide que presente los certificados correspondientes a la capacitación académica atribuida (para evitar los falsos doctores, ingenieros y licenciados). Esta acción hasta suena simpática y no tiene más consecuencia que la decepción de la primera cita. Sin embargo, cuando quien cambia su edad es un adulto, que se hace pasar por un niño, para interactuar con otros niños e intentar sus fines ilegítimos, el tema se vuelve complejo. Establecer los límites entre el derecho a publicar sus propios datos modificados con fines de relación adulta o con fines de violación infantil, es una tarea ímproba y difícil, pero que en algún momento debe ser legislada.

3 Desde la Criminalística, consideramos como “prueba indiciaria” al conjunto de huellas (“testigos mudos”), de cualquier tipo y naturaleza, que se hayan producido como resultado de una acción cualquiera y que al ser metodológicamente investigados, permitan reconstruir los hechos acaecidos. En general, pero no de manera excluyente, se relacionan con actos delictivos.

CAPÍTULO 3
IMPLANTACIÓN PERICIAL CRIMINALÍSTICA

La Criminalística es la disciplina que se encarga de brindar soporte a la investigación judicial. Se inicia aportando criterios científicos, tecnológicos y técnicos al análisis *a posteriori* de los hechos criminales, se orienta al derecho penal. Surge como una respuesta metodológica racional, con pretensiones de sustituir a los restantes métodos probatorios clásicos. Es la conclusión evidente de un proceso evolutivo, que desde lo judicial, se evidencia en la venganza privada, la ley del Talión y los sistemas normativos. Abandona la prueba divina, las pruebas corporales y sus sucesores, la prueba confesional con sus resabios de tortura integrados y la prueba testimonial, con sus problemas de subjetividad, coerción y cohecho. Aparece como una pócima dorada, aportada por y para la sociedad industrializada de fines del siglo XIX. Conceptualmente se basa en el estudio de los indicios ("testigos mudos") que obran en la escena del crimen, con fines reconstructivos. Esta nueva prueba que se agrega a las clásicas, es genéricamente llamada "prueba indiciaria" y también entres sus precursores: "la reina de las pruebas". Su objetivo final es *la reconstrucción del hecho*, a partir de la prueba indiciaria, que se identifica, recolecta, certifica y resguarda en la escena del crimen, da lugar a la entonces llamada "inspección ocular", hoy renombrada inspección judicial. A continuación intentaremos describir sus principales características.

Criminalística: Es la disciplina auxiliar de la investigación judicial que aplica los conocimientos, métodos y técnicas de investigación de las ciencias naturales en el examen del material sensible significativo relacionado con un presunto hecho delictivo o no, con el fin de determinar su existencia, o bien reconstruirlo, para señalar y precisar la intervención de uno o varios sujetos, llegando así a la verdad histórica o material del hecho. Su objeto de estudio es la prueba indiciaria.

Objetivos:

Investigar técnicamente y demostrar científicamente la existencia de un hecho en particular, que probablemente sea delictivo.

Reconstruir los hechos acaecidos, determinando los fenómenos ocurridos y los mecanismos utilizados, señalando los instrumentos u objetos de ejecución, sus manifestaciones y las acciones que se pusieron en juego para realizarlo.

Aportar evidencias, coordinar técnicas y sistemas para la identificación de la

víctima.

Aportar evidencias para la identificación del o los presuntos autores.

Aportar pruebas indiciarias para probar el grado de participación del o los presuntos autores y demás involucrados.

Características destacables en la disciplina:

Indicios (testigos mudos): Todo objeto, instrumento, huella, marca, rastro, señal o vestigio, que se produce como resultado de la ejecución de un hecho, independientemente de su naturaleza y condiciones particulares. Su estudio nos puede ayudar a establecer relaciones respecto de la sucesión de acontecimientos que lo generó, los instrumentos utilizados y/o los actores involucrados, puede o no corresponder a actos ilegítimos o ilegales. Es importante destacar que todo indicio está formado de signos y en algunos casos de símbolos, cuyo sentido e interpretación dependerán del entorno y el objetivo de nuestra labor reconstructiva. Sólo reconstruyendo se pueden realizar predicciones objetivas y con probabilidad de acierto.[4]

Identidad: Un indicio es idéntico a sí mismo y diferenciable de sus copias y modelos representativos.

Intercambio: Es el que observa los fenómenos que se desprenden de la interacción, deliberada o inadvertida, que existe entre el criminal, la víctima y la escena del crimen en un hecho delictivo.

Correspondencia o identificación comparativa: Establece la relación de los indicios entre sí y eventualmente con una persona.[5] Por ejemplo: si dos huellas dactilares corresponden a la misma persona, si dos proyectiles fueron disparados por la misma arma, etcétera.

Reconstrucción de hechos: Permite deducir, generar y proponer una secuencia de ejecución de acciones, a partir de los indicios localizados en el lugar del hecho, establecer sus relaciones y proponer una situación originaria, una serie de hechos y una situación resultado, coherente, metodológica y lógicamente válida, soportada en medios de investigación científicos, tecnológicos y técnicos de validez reconocida y reproducción asegurada, como propuesta sobre la manera en que pudieron ocurrir los hechos que los generaron.

Probabilidad: Determina la probabilidad de ocurrencia de un fenómeno sobre la

base del número de características verificadas durante un cotejo. Puede ir desde la certeza metodológica, lógica e instrumental, hasta un grado muy bajo de probabilidad. En todos los casos, puede resultar pertinente y conducente a la investigación judicial.

Clasificación por su relación con el lugar del hecho:

Indicios determinados: Son aquellos que requieren solamente un análisis minucioso a simple vista o con lentes de aumento y que guarden relación directa con el objeto o persona que los produce. Pueden subclasificarse acorde con su naturaleza física, por ejemplo, en armas, huellas dactilares e instrumentos.

Indicios indeterminados: Son aquellos que requieren de un análisis completo para el conocimiento de su composición y estructura de acuerdo con su naturaleza física, pues de otra forma no estaríamos en la posibilidad de definirlos. Son, por ejemplo: pelos, fibras, semen, orina, vómito, manchas o huellas de sangre y pastillas desconocidas con envoltura o sin ella. Entre ellos y en razón de nuestro estudio en particular, se deben destacar especialmente los indicios que conforman la prueba indiciaria informático forense.

Indicios asociativos: Los que corroboran y guardan relación directa con el hecho que se investiga.

Indicios no asociativos: Se localizan en el lugar del hecho o del hallazgo, pero no están relacionados íntimamente con el caso que se investiga.

Indicios microscópicos: Son aquellos que por su naturaleza exigen el empleo de algún instrumento óptico (de amplificación macro o microscópica) para su observación (pelos y fibras). También requieren el empleo de otras técnicas de análisis de micropartículas, como la activación neutrónica, la espectrofotometría de acción de masas o la resonancia nuclear magnética.

Indicios macroscópicos: Los que se observan a simple vista (manchas, armas, etc.).

Indicios trasladables: Son aquellos que por su naturaleza, forma, volumen, peso o cualidades inherentes, se pueden sacar del lugar de investigación y se pueden preservar de forma adecuada para trasladarse al laboratorio y realizar el estudio pericial respectivo (armas, fibras, datos codificados en soportes magnéticos, ópticos, etc.).

Indicios no trasladables. Son aquellos que por su naturaleza, forma, volumen, peso o cualidades inherentes, no pueden moverse del lugar de investigación ya que alterarían

sus condiciones originales (huellas de efracción en paredes, muros, redes de cableado para interconexión digital, antenas de comunicaciones, etc.).

Indicios virtuales. Son aquellos que se obtienen a partir de la investigación informático forense, pueden o no constituirse en prueba documental informática (LHVP Lugar del hecho virtual propio).

Resguardo de indicios: Son las técnicas de manejo y conservación adecuadas para guardar, inmovilizar y proteger un indicio de acuerdo a la naturaleza de éste, con el objeto de mantener su integridad para su posterior estudio y análisis. Cada indicio se empaqueta por separado, etiquetándolo con los datos administrativos correspondientes (número de averiguación previa, llamado, características del indicio, clase, fecha y nombre del criminalista) y una cadena de custodia asociada. (Prueba documental informática[6]).

Recolección de indicios: Es la acción de orden técnico que tiene como objetivo la recolección de los indicios localizados en el lugar de investigación, sin contaminar, transformar o modificar la naturaleza de éstos, con el objeto de mantener su integridad para su posterior estudio y análisis. (Gestión de la Prueba Documental Informática, normalmente como medida procesal previa o preliminar, a veces *"in audita altera pars".*)

Lugar del hallazgo: Corresponde a un espacio en donde encontramos los indicios que puedan estar relacionados con algún hecho –por ejemplo el hallazgo de un cadáver–, no necesariamente se corresponde con el lugar del hecho delictuoso. En algunos casos ni siquiera es posible establecer el lugar de comisión del hecho, como en los supuestos de delitos informáticos propios o impropios cometidos en lugares del hecho virtuales propios, este tema se tratará oportunamente con mayor profundidad en esta misma obra.

Causas de alteración del lugar del hecho:

Intencionales: Suele ser cometida por los actores involucrados en la acción analizada (responsables, familiares, terceros interesados).

No intencionales: Suele ser consecuencia culposa de la intromisión de personas extrañas a la investigación (periodistas y curiosos).

Por causas naturales: (meteoros, fuegos, terremotos).

Por desconocimiento, impericia o inexperiencia del propio investigador o los

participantes (otros expertos, miembros de Fuerzas de Seguridad, bomberos, equipos de emergencia sanitaria).

Desde la visión puramente deductiva y privada de un Sherlock Holmes, hasta las normalizaciones de procedimientos efectuadas por Scotland Yard y difundidas por INTERPOL, se crea un mundo nuevo. La investigación seria y científicamente soportada ha llegado para quedarse. Algunos de nuestros compatriotas hicieron enormes aporte a ésta, basta con recordar la sistematización que Vucetich aportó a la sociedad, conformando un auténtico sistema de identificación masivo, efectivo, eficiente y eficaz (el Sistema Dactiloscópico Argentino). Se trata de artes y técnicas relacionadas exclusivamente con el accionar de las Fuerzas de Seguridad en apoyo jurisdiccional directo. Desde la Policía de la Capital se conforman soluciones a partir de iniciativas particulares, soluciones que lentamente llevarán hasta la creación de la Scopometría y sus primeras divisiones en especialidades técnicas. Aún está muy lejos la concepción de una Policía Judicial, de la que se constituye en pionera la Morgue Judicial. El antiguo asesor del juez, el médico legista, se destaca en este proceso, es la voz autorizada de un profesional de la medicina, con capacitación específica en técnicas forenses (investigación causal de la muerte) y su respuesta pericial constituye un aporte indispensable a la hora de dictar sentencia.

En fin uno de los grandes maestros de la Criminalística, el inspector general Roberto Albarracín, a principios de los años setenta, en su obra Manual de Criminalística y en sus clases, solía decirnos respecto de esta denominación: “ha sido llamada: Policía Científica y Técnica Policial, Ciencia de la Policía Judicial, Arte de la Policía Judicial, Policía Científica, Técnica Policial, Policía Técnica, Policía científica o técnica (Reiss), Criminalística (Locard a partir de la Escuela Alemana representada por Hans Gro*ss). Determinado que la más exacta y adecuada denominación de nuestra materia es actualmente la de Criminalística, diremos que ella encierra el estudio de l*as técnicas del crimen. En este sentido brinda una extraordinaria colaboración al proceso penal, ya que su fundamento es encontrar la verdad para que el hecho delictuoso no quede impune”. (pp. 24 y 25).

A partir de las afirmaciones anteriores, podemos descubrir ciertos detalles destacables:

Nuestro referido y dilecto maestro (a principios de los setenta) utilizaba con ambigüedad los términos crimen y delictuoso (delito en definitiva), utilizándolos en relación con el proceso penal.[7]

Asignaba a la Criminalística un valor puro de soporte al proceso penal (algo inherente seguramente a su profunda formación policial), dejando de lado el aporte

que la misma pudiera realizar a los restantes fueros judiciales (comercial, civil, laboral, etc.).

Aunque en primera instancia parecería la panacea de la investigación del delito, en la práctica no resulta tal cosa, ni mucho menos. En efecto su método estrictamente comparativo, termina relacionando objetos con otros objetos o con determinados hechos, pero muy rara vez con el autor de dichos hechos. Se limita a comparar elementos provenientes de la prueba indiciaria, ya sea con otros objetos similares o con tablas y fórmulas estadísticas preestablecidas, sólo excepcionalmente podrá brindar información precisa respecto de la participación de una persona determinada en los hechos investigados. Esto se hace evidente en el caso de las cámaras ocultas y su pertinencia probatoria. La prueba indiciaria sólo podrá ser evaluada por el juez, en el marco de la normativa procesal vigente y a partir de su propia concepción e interpretación, como elemento pertinente y conducente en la investigación del hecho particular que debe analizar, juzgar y sentenciar (*iura novit curia*).[8]

Si bien la medicina legal se ha ganado su lugar por medios propios, no pasa lo mismo con otras áreas de la Criminalística, que lentamente se van separando de la integralidad originaria. Un perito es un experto, pero difícilmente pueda ser "experto en todo", por ese proceso natural de selección, basado en las necesidades e intereses de cada profesional, se separan las primeras disciplinas criminalísticas: Laboratorio Pericial, Balística, Documentología, Fotografía, Dactiloscopia, Rastros. Sin embargo, no todas las necesidades periciales son sustentadas a partir de estas divisiones originarias, por ejemplo, puede ser necesario que el tribunal sea asesorado respecto de la autenticidad de un cuadro u otra obra de arte, algo excepcional pero no improbable. En ese caso será necesario consultar a un experto en el tema, que brindará su informe, en lo posible, con las mismas condiciones metodológicas que el resto de las áreas independientes ya consolidadas. A esto se agrega que desde el Derecho Civil se requieren actividades semejantes, es necesario realizar pericias contables, determinar superficies de inmuebles, identificar textos manuscritos y mecanografiados, establecer los daños de un vehículo siniestrado, es decir, realizar las mismas tareas que aparecían como propias de la Criminalística en soporte del Derecho Penal. A este conjunto de especialidades permanentes y ocasionales se lo denomina Ciencias Forenses.

Entre estas Ciencias Forenses ha aparecido una nueva disciplina, proveniente de la Informática, pero con sustento científico clásico, metodológico criminalístico y probatorio judicial. Esta nueva disciplina ya tiene nombre propio: *Informática Forense*. Se incluye, integra, complementa y es complementada por las restantes Ciencias Forenses, se constituye en herramienta de análisis de todas ellas y se relaciona de manera similar con todos los métodos probatorios aceptados por el Derecho Procesal, cualquiera sea el fuero considerado. Su visión particular se orienta

hacia la prueba indiciaria informática, es decir a los testigos mudos que quedan como resultado de operaciones lícitas e ilícitas sobre activos informáticos, con fines reconstructivos orientados en particular, pero no exclusivamente a la investigación judicial.

Concepto: *Se denomina Informática Forense al conjunto multidisciplinario de teorías, técnicas y métodos de análisis que brindan soporte conceptual y procedimental a la investigación de la prueba indiciaria informática.*

Sintetizando podríamos decir que:

La Informática Forense es a la Informática lo que la Medicina Legal es a la Medicina.

Como toda disciplina forense, tiene sus particularidades, que justifican su diferenciación inclusiva en las mismas. Forma parte de la Informática en general y de la Seguridad Informática en particular.

Objeto: La prueba indiciaria informática.[9]

Método: Desarrollar mecanismos de análisis criminalístico, con soporte científico, tecnológico y técnico, sobre la prueba indiciaria informática.[10]

Tipicidad: Aunque se trata de una construcción transdisciplinaria, posee características propias derivadas de sus diferencias conceptuales con las restantes ciencias forenses.[11]

Especificidad: Su empleo, desde el punto de vista metodológico, puede clasificarse en:

Análisis Pericial de la Prueba Indiciaria Informática.

Gestión Integral de la Prueba Documental Informática.[12]

Auditoría Informática Forense.

4 Aunque en su sentido forense, la Criminalística se asocia con la reconstrucción del hecho delictivo y sus indicios son particularmente característicos, por ejemplo, la

identificación y resguardo de vainas servidas en un lugar del hecho correspondiente con un homicidio *criminis causa*, no son exclusivos de esta actividad. Si llegamos a nuestro hogar y encontramos la cocina encendida y la comida hirviendo a fuego lento, puede ser un indicio de la presencia de otros miembros de la familia en el hogar. Aunque existan otras razones que pueden provocar dicha situación, nos parece una respuesta razonable y nos permite reconstruir varias acciones relacionadas, incluso si unimos este hecho a otros que consideramos relevantes, nos pueden preparar para el encuentro con la persona que suponemos desarrolló la tarea previa de preparar la comida. El uso de indicios forma parte de la vida diaria, coexiste con nosotros en todo momento y nos permite interactuar con la naturaleza y la sociedad. Las huellas de pisadas en el barro pueden significar para el cazador la presencia de una presa o de un predador.

5 Es imprescindible destacar que la determinación de la autoría de un hecho delictivo no forma parte de la tarea criminalística. Es una potestad exclusiva, insustituible e irrenunciable del juez, del cual la criminalística es una herramienta más de apoyo a la decisión que finalizará en la correspondiente norma particular a generar como resultado del proceso (sentencia).

6 Se trata de una especie del género Prueba Documental Clásica, la que ya fuera subdividida hace tiempo en bibliográfica (texto), foliográfica (gráficos, mapas, esquemas, etc.) y pictográfica (figuras, fotografías, películas, etc.).

7 Fuente: www.rae.es.
Crimen: (Del lat. *crimen*). 1. m. Delito grave.
m. Acción indebida o reprensible.
m. Acción voluntaria de matar o herir gravemente a alguien.
Delito: (De *delicto, delinquere*).1. m. Culpa, quebrantamiento de la ley.
m. Acción o cosa reprobable. *Comer tanto es un delito. Es un delito gastar tanto en un traje.*
m. *Der.* Acción u omisión voluntaria o imprudente penada por la ley.
Queda clara la división conceptual entre crimen (en general delitos graves o de sangre) como especie del género delito (contravención normativa, generalmente asociada al delito penal, aunque también existe el delito civil), esta división no es universal, ni mucho menos, es una particularidad regional, no aceptada por muchos autores.

El delito, en sentido estricto, es definido como una conducta, acción u omisión típica (tipificada por la ley), antijurídica (contraria a Derecho), culpable y punible. Supone una conducta infraccional del Derecho penal, es decir, una acción u omisión tipificada y penada por la ley. La palabra delito deriva del verbo latino *delinquere*, que significa abandonar, apartarse del buen camino, alejarse del sendero señalado por la ley. La definición de delito ha diferido y difiere todavía hoy entre escuelas criminológicas. Se reduce a ciertos tipos de comportamiento que una sociedad, en un determinado momento, decide punir. Así se pretende liberar al concepto de paradojas y diferencias culturales que dificultan una definición universal.

Delito penal y delito civil: En algunos sistemas jurídicos, como en el de Derecho Romano, el de Argentina, el de Chile, o el de España (y, en general, en varios sistemas de la familia del Derecho continental), se distingue entre "delito civil" y "delito penal". El "delito civil" es el acto ilícito, ejecutado con intención de dañar a otros, mientras que constituye "cuasidelito civil" el acto negligente que causa daño. Los actos considerados como "delitos civiles" y "cuasidelitos civiles" pueden constituir también un "delito penal" si se encuentran tipificados y sancionados por la ley penal. Un "delito penal" no será, a la vez, "delito civil", si no ha causado daño; como tampoco un "delito civil" será, a la vez, "delito penal", si la conducta ilícita no está tipificada penalmente.

Crimen y delito: Crimen y delito son términos equivalentes. Su diferencia radica en que "delito" es genérico, y por "crimen" se entiende un delito más grave o, en ciertos países, un delito ofensivo en contra de las personas. Tanto el delito como el crimen son categorías presentadas habitualmente como universales; sin embargo los delitos y los crímenes son definidos por los distintos ordenamientos jurídicos vigentes en un territorio o en un intervalo de tiempo.

Crear delitos, crímenes y castigos son facultades soberanas de quienes están a la cabeza de un sistema normativo (principio de legalidad penal). Eso explica las diferencias entre los distintos sistemas penales aplicados en Singapur, Chile o Argentina, con las complejidades que estas diferencias implican.

Clasificación de los delitos (no exhaustiva, ni exclusiva, sólo a modo de ejemplo):

Doloso: Individualizan acciones por la incorporación del resultado al programa causal finalmente dominado por el agente. El autor ha querido la realización del hecho típico. Hay coincidencia entre lo que el autor hizo y lo que quiso.

Culposo: El autor no ha querido la realización del hecho típico. El resultado no es producto de su voluntad, sino del incumplimiento del deber de cuidado.

Por comisión: Surgen de la acción del autor. Cuando la norma prohíbe realizar una determinada conducta y el actor la realiza.

Por omisión: Son abstenciones, se fundamentan en normas que ordenan hacer algo. El delito se considera realizado en el momento en que debió realizarse la acción omitida. (Por omisión propia: Están establecidos en el Código Penal. Los puede realizar cualquier persona, basta con omitir la conducta a la que la norma obliga.)

8 Desde las pericias mecanográficas, es posible establecer con qué máquina de escribir se realizó un texto mecanografiado, mediante el cotejo del documento dubitado y el correspondiente cuerpo de

escritura empleado en la comparación, pero difícilmente establecer quién fue el dactilógrafo. Desde la balística es posible identificar dos proyectiles (incriminado y testigo) y atribuirles su pasaje a través del cañón de una misma arma de fuego, pero esto está muy lejos de determinar al autor del disparo. En el mismo sentido, puede establecerse que una persona ha disparado un arma (por los restos de antimonio y bario presentes en su mano), pero de ahí a decir que efectuó "ese disparo en particular que acabó con la vida de la víctima", hay un trecho muy largo y sumamente conjetural. La utilidad de la prueba indiciaria siempre será relativa a las demás circunstancias del hecho analizado, el juez deberá determinar la pertinencia e importancia de la misma en relación con las restantes pruebas obrantes en el caso en particular.

9 Subsidiariamente brindar soporte científico, tecnológico y técnico a la Prueba Documental Informática.

10 Estos mecanismos se hacen extensivos a la Prueba Documental Informática, constituyendo las herramientas de análisis de la misma.

11 Si bien este tema será ampliado en los capítulos siguientes, basta con tener en cuenta que el principio de identidad, no rige para los archivos informáticos, ya que un bit es idéntico a otro bit, cualquiera sea su forma de almacenamiento y es imposible, en este sentido, establecer cuál es el original y cuál la copia, sin recurrir a métodos externos anteriores, posteriores y contemporáneos a la realización de la referida copia.

12 Véase la prueba documental informática: una variación de la prueba documental clásica (bibliográfica o foliográfica), que difiere de ésta en el soporte (papel vs. digital).

CAPÍTULO 4
IMPLANTACIÓN INFORMÁTICA

Toda disciplina nueva genera conflictos, desde su ubicación dentro de las demás, su objeto, su método y en particular los límites de su accionar. Éste es un problema particularmente destacado dentro de las denominadas Disciplinas Informáticas. Ellas incluyen una gran variedad de formaciones académicas y profesionales, desde el conocido "Computador Científico", hasta el actual "Ingeniero en Informática", pasando por títulos que hacen referencias a los "Sistemas" en general, a los "Sistemas de Información" en particular, a la "Computación" y toda otra idea que haga referenciar cierta o presunta a la gestión de los activos informáticos.

Si recurrimos a un mecanismo de desambiguación típico podríamos separar estos conceptos en:

Informática: Disciplina que estudia la gestión de la información, generalmente, pero no de manera exclusiva por medio de elementos computacionales. No obstante su aplicación como herramienta es abarcativa de toda la ciencia humana, cualquiera sea la teoría del conocimiento que se considere cierta.

Sistemas de Información: Estudia la gestión de la información, sistematizada en aplicaciones específicas. Se orienta especialmente al conocimiento, reconocimiento, planificación y desarrollo de aplicaciones informáticas, mediante el empleo de medios computacionales y con una metodología propia: el "Análisis de Sistemas". Esta metodología se ha expandido a la investigación, en general, por medio del "Método Sistémico", complementario de los métodos clásicos.

Computación: Es el empleo particular pero no exclusivo de la computación de datos, como instrumento de gestión de los activos informáticos. No obstante es más un medio que una disciplina propia. La tecnología computacional con soporte en silicio es sólo una manera de representar, codificar y analizar los datos. Actualmente coexiste con otros medios tan idóneos como el referido, por ejemplo, la computación cuántica, la computación con base en ADN o proteínas, etc. Nada podemos decir respecto del futuro, hoy es la herramienta de análisis de información más utilizada y difundida, lo que vendrá a continuación es sólo motivo de especulación. Su ámbito de aplicación suele intersecarse con el de los mecanismos empleados por los Servicios de Información, las Auditorías Contables, Financieras y la llamada Guerra de la Información. La computadora forma parte del mundo y sin ella sería prácticamente imposible su funcionamiento organizado, tal y como lo conocemos.

Nos resta destacar que, para complicar aún más las cosas, no está muy claro el nivel académico de sus profesionales. Por ejemplo, si analizamos una de sus ramas, la Informática Forense considerada respecto de su homóloga de la Ciencia Médica, la Medicina Legal, nos encontramos con las siguientes características propias de esta última:

Título de grado originario (médico).

Matrícula Profesional (Colegios Médicos)

Título de Post Grado específico (Especialización en Medicina Legal).[13] En contrapartida, las listas de peritos judiciales informáticos incluyen:

Ingenieros y licenciados en Informática (Carreras de Grado).

Técnicos superiores y analistas de sistemas (Carreras Terciarias).

Carreras de Post Grado (especializaciones, maestrías y doctorados específicos).

Incumbencias de otras disciplinas (por ejemplo, de la carrera de ingeniero electrónico o industrial, contador o administrador de empresas).

Esta colección de carreras, títulos profesionales de diferente nivel académico y listados particulares en los distintos fueros, genera un ambiente de confusión y desorden que actúa en detrimento de la Informática como herramienta de análisis probatorio judicial. Por el contrario, en la ciencia médica no se duda un instante en el momento de solicitar una pericia médico forense. El profesional del derecho laboral, por ejemplo, ante cualquier controversia en el grado de incapacidad de su cliente, recurrirá sin dudarlo al Cuerpo Médico Legista, integrado curiosamente por médicos legistas. Si se trata de un abogado dedicado al derecho penal, optará por la solución que le brinda la Morgue Judicial, para requerir una necropsia, también en manos de médicos legistas. Ningún operador del derecho necesitaría fundar y justificar esta decisión.

¿En qué razones, fundamentos o criterios, debería basarse un operador del derecho al momento de solicitar un informe pericial informático forense? Debido a las clásicas deficiencias de formación de que adolece nuestro sistema universitario, el egresado no ha recibido formación criminalística en particular, llevando a los abogados noveles a confundir los términos criminalística y criminología en el peor de los casos o a no tener clara la pertinencia de la prueba indiciaria en el mejor de ellos. Para generar los puntos de pericia, que deben ser conducentes y pertinentes a la argumentación planificada, debería asesorarse con un experto en el tema, pero

¿cómo elegirlo? Si ni siquiera dentro de la Informática los profesionales se ponen de acuerdo respecto la incumbencia particular de cada título, más allá de la visión de conveniencia que cada Facultad aporta al suyo propio, intentado que sea lo más abarcativo posible, para competir en nuestro ya saturadísimo mercado educativo.

¿Cómo solucionar este problema? Nuevamente podemos basarnos en la experiencia de la Medicina. Si hacemos una comparación con su evolución hasta su arribo a la Medicina Legal podemos decir:

La Medicina se origina con los sangradores y cirujanos, hasta llegar en nuestro caso al histórico Protomedicato. Sin embargo, ya en esta etapa se diferencia del hechicero, del brujo y del curandero. La Informática aún no lo ha hecho, ante la falta de normativa que la regule, permite la interacción de cualquier "idóneo", aunque su capacidad computacional se limite al parentesco de quien acepta su asesoramiento y lo da por válido.

Luego del Protomedicato se constituye en disciplina autónoma y regulada. Surge la carrera de médico, claramente diferenciada de la odontología, de la enfermería y de las ciencias auxiliares de la medicina. En nuestro caso aún no tenemos muy clara la diferencia entre una carrera de grado, de entre las múltiples que se ofrecen y una carrera terciaria. El Colegio Médico nunca matricularía como médico a una persona con formación terciaria en una carrera auxiliar de la medicina. Sin embargo los diversos y variados Colegios Profesionales que se atribuyen potestades matriculantes sobre las ciencias informáticas, matriculan indistintamente ingenieros, licenciados y analistas de sistemas, llegando a incluir estudiantes secundarios egresados de escuelas técnicas. Por supuesto, previo pago del arancel correspondiente que los acredita como peritos para actuar ante el Poder Judicial.

A partir de la Especialización en Medicina, que actualmente es obligatoria para cualquier profesional del área que pretenda ejercer, se separan la pediatría, la cirugía, la medicina interna, la psiquiatría y en lo que nos interesa la Medicina Legal. En contrapartida la Informática se encuentra aún en la etapa anterior. Si bien aparecen especializaciones y maestrías en Seguridad Informática, ninguno de ellos se orienta hacia la Informática Forense, al menos en nuestro país y a la fecha.

Disciplinas Informáticas: Considerando como disciplina principal a la Informática[14] y como partes de la misma, necesarias pero no suficientes, a la Computación y los Sistemas de Información, podemos subdividir sus especializaciones principales en:

Computación.

Equipos informáticos.

Métodos de cómputo.

Servicios de generación, almacenamiento, procesamiento y análisis estadístico de datos.

Herramientas de apoyo (oficina virtual, soporte a la decisión).

Sistemas de información.

Análisis y diseño de sistemas de información.

Programación.

Gestión de sistemas operativos.

Gestión de Aplicaciones.

Gestión de Bases de Datos.

Redes de Datos.

Diseño e implementación de redes:

De área Local (LAN).

De área Metropolitana (MAN).

De área Amplia (WAN).

Gestión de operaciones y servicios remotos (Internet, transferencia de activos, comercio electrónico “E-commerce”).

Aplicaciones interactivas de comunicaciones (Correo Electrónico “E-mail”, conversación en línea “chat”, videoconferencia).

Aplicaciones educativas (Educación no presencial, local y/o a distancia, “E-learning”).

Seguridad Informática.

Protección de activos informáticos.

Auditoría Informática.

Ingeniería Inversa (Técnica y social).

Guerra Informática ("Warfare").

Informática Forense.

En este último caso, se trata de una especialización crítica, ya que es transdisciplinaria en por lo menos dos sentidos principales:

En sentido intrínseco porque abarca métodos y técnicas de todas las otras divisiones de la Informática (desde la simulación y análisis de redes físicas o virtuales, hasta la ingeniería inversa).

En sentido extrínseco, complementa, suplementa y se nutre de diversas áreas del Derecho y de la Criminalística.

Retomando nuestra definición: *Se denomina Informática Forense al conjunto multidisciplinario de teorías, técnicas y métodos de análisis, que brindan soporte conceptual y procedimental, a la investigación de la prueba indiciaria informática.* Desde esta delimitación podemos distinguirla del resto de las especialidades informáticas:

La Informática Forense y la auditoría informática o contable: Al respecto, esta última tiene fines de supervisión sobre la gestión de los activos informáticos de una persona física o jurídica, aunque en general se refiere a esta última en el formato de empresas de muy diversa índole. Si bien la informática forense actúa en soporte de dicha auditoría, ésta trasciende a la primera, ya que las herramientas informático forenses brindarán los elementos necesarios para su ejecución práctica, pero no aportarán datos referidos a la legalidad o legitimidad de los resultados obtenidos. Quien informa sobre los resultados de la auditoría es el auditor, cualquiera fuere su nivel de representatividad legal, mientras que la Informática Forense le brinda la capacidad técnica para realizar el análisis de los activos informáticos y sus relaciones, exclusivamente.

La Informática Forense, como instrumento de análisis de la realidad: Por su propia naturaleza, la Informática Forense tiende a generar un modelo de comportamiento racional con soporte científico, tecnológico y técnico respecto de la prueba indiciaria disponible en un determinado lugar. Este modelo de comportamiento, incluyendo sus consideraciones sociales, criminológicas y criminalísticas, instrumentado por medios idóneos, como, por ejemplo, la realidad

virtual, se constituye en una auténtica reconstrucción del hecho virtual. De ahí que su utilidad se expanda más allá del ámbito jurídico y judicial. Es una forma particular y específica de analizar, reconstruir y modelar la realidad.3 En definitiva puede ser utilizada en toda circunstancia que lo requiera, tanto en los distintos fueros judiciales, como en la labor diaria de organismos oficiales y privados y hasta en ámbito particular propio de una persona determinada y su grupo de pertenencia.

Requiere de la participación activa de un experto en la materia. Esa posibilidad implica la necesidad de exigir un perfil muy especial al profesional que la desempeña. Debe evidenciar las características de inteligencia racional y memoria procedimental que distinguen al criminalista en general y a este tipo de peritos en particular. Al respecto es conveniente recordar que la inteligencia (según la obra de L. Campbell, B. Campbell y D. Dickenson, *Inteligencias Múltiples*, Editorial Troquel, Buenos Aires, Argentina, 2000), tiene distintas formas de evidenciarse: verballingüística, lógico-matemática, cinestésica, visual-espacial, musical, interpersonal, intrapersonal y naturalista. En cuanto a la memoria (según Francis Eustache y Beatrice Desgranges, *Hacia un modelo unificado de la memoria*, Mente y Cerebro 43/2010, pp. 48 y ss.) también puede dividirse en: episódica, semántica, perceptiva, operativa y procedimental. Aunque sería ideal contar con la suma de las inteligencias y las memorias, eso es imposible para un ser humano, de ahí la necesidad de suplir por medios tecnológicos las deficiencias naturales de cada profesional que desempeña la labor pericial.

13 Que incluye la formación específica en Criminalística para actuar de manera transdisciplinaria y mancomunada con los restantes expertos de las Ciencias Forenses y formación específica en Derecho Procesal para evitar los errores procesales que pudieran anular a ésta a los fines judiciales.

14 Si bien esta concepción es una visión particular de los autores, sumamente discutible y discutida, las razones para adoptarla no parecen ser caprichosas: el siglo XXI es llamado el siglo de la información, la herramienta de análisis de información es la Informática, si bien los sistemas de información constituyen el modelo clasificatorio y operacional más vigente, son una forma de interactuar con los mismos, pero no la única. De la misma manera, la computación es la herramienta en uso y en boga desde fines del siglo pasado, se integra en la sociedad de la misma forma en que lo hizo el fuego, la rueda, la imprenta o el bolígrafo. Pero ambas componentes integradas no son suficientes para brindar solución a la totalidad de los problemas que la gestión de información genera. De ahí su importancia radical para nuestra visión específica, dejamos librado al lector la aceptación o descarte de ésta.

CAPÍTULO 5
IMPLANTACIÓN JUDICIAL

Es necesario tener en cuenta que la prueba procesal no implica necesariamente la comprobación de la verdad material[15] respecto de los hechos acaecidos. Este aserto se hace evidente por varias razones:

El significado de las palabra probar y prueba establecido por el Diccionario de la Real Academia Española, resulta como todo concepto: vago, ambiguo y multívoco.1 Si intentamos desambiguarlo, recurriendo a la etimología de la palabra probar, también ésta se demuestra compleja.[16] Podríamos inferir, aunque no de manera absoluta que lo que resulta probado, es bueno, es concreto, o sea, que es auténtico: conforma una verificación o demostración de autenticidad.

No se prueban los hechos, pues éstos ya no existen, se intenta reconstruirlos y establecer su cronología pretérita. Lo que se intenta demostrar son las afirmaciones que aportan las partes durante el proceso, para asegurar sus pretensiones.

El juez es quien constata, comprueba o verifica si las referidas afirmaciones coinciden con la argumentación expuesta por las partes, salvaguardando sus propias facultades ordenadoras e instructoras para esclarecer la verdad procesal de los hechos controvertidos alegados en un proceso.

La prueba documental informática, es un medio probatorio, tan válido como cualquier otro. Se encuadra en el marco general de la prueba documental clásica, difiriendo de ésta sólo en el soporte (papel en la clásica, digital en la Informática). Su tratamiento es analógico a la antes citada, con algunas características propias y se encuentra respaldada por el artículo 378 del Código Procesal Civil y Comercial de la Nación.[17]

La primera consideración respecto de su pertinencia y ubicación entre los mecanismos probatorios judiciales, se refiere a la naturaleza complementaria de ésta. Obtenidos los resultados, a partir de la prueba documental informática disponible, en general es necesario corroborarlos mediante la realización de una prueba de informes o de una pericia informático forense. Es necesario destacar que la Prueba Documental Informática es una especie dentro del género de la Prueba Indiciaria Informática.

Resumiendo, toda documental informática es una prueba indiciaria, pero no toda

prueba indiciaria informática es una prueba documental. Esta característica debe ser tenida especialmente en cuenta por el operador del derecho, a la hora de establecer los puntos de pericia, ya que los mismos pueden incluirse en la documental informática o no y seguramente la trascienden a la hora de formularlos.

El delito informático propio e impropio

Al analizar el elemento informático en la producción de delitos, nos encontramos ante dos situaciones distintas que debemos destacar:

Delitos informáticos propios: Son aquellos delitos que atentan contra un bien protegido específico: "la información". En general afectan al derecho a la privacidad.[18]

Delitos informáticos impropios: Son los que se producen mediante la violación de normas jurídicas ya establecidas, con anterioridad al empleo de esta modalidad, por ejemplo daño, estafa, utilizando para cometerlos herramientas informáticas.[19]

Como toda clasificación, admite las formas mixtas, ya que es imposible delimitar exactamente las zonas grises, por mucho que el lenguaje técnico se esfuerce en hacerlo. De ahí que algunas figuras gocen de ambas particularidades, por ejemplo: en la sustitución de identidad, se procuran los datos filiatorios (sensibles) propios de la persona a sustituir y luego mediante esta información se realizan todo tipo de actividades lícitas e ilícitas en su nombre y por su cuenta. En esta tarea es de rigor analizar la Cadena Causal Propia que une los eventos considerados.

La reconstrucción del hecho

En razón de su naturaleza, toda prueba indiciaria tiene como fin principal o subsidiario, contribuir a la reconstrucción de los hechos acaecidos en un momento espacio temporal histórico. Esta reconstrucción metodológicamente hablando, consiste en el desarrollo de un guión factible, a partir de la prueba indiciaria recolectada. Este guión supone una situación inicial, con sus componentes físicos y humanos, una trama que concatene los hechos supuestos realizados por cada uno de los protagonistas y un desenlace que se produce como consecuencia de los hechos anteriores. La relación de causa efecto debería ser estricta. No obstante existen diversos factores que concurren a dificultar esta tarea, entre ellos:

Cadena Causal Propia: Sucesión de eventos entre los cuales el precedente (antecedente) es causa necesaria y suficiente para la producción del siguiente (consecuente). *Cadena Causal Impropia:* Cuando a la relación precedente siguiente le

falta una o ambas características de la Cadena Causal Propia (causa necesaria y suficiente).

Todo modelo es una interpretación y por lo tanto dependerá directamente de la subjetividad de quien lo realiza.

Todo testimonio es también una interpretación y aunque contemos con todos los protagonistas y pongan su mayor interés y celo en relatar los acontecimientos, seguirán apareciendo inconsistencias entre las distintas versiones aportadas por cada uno de ellos.[20]

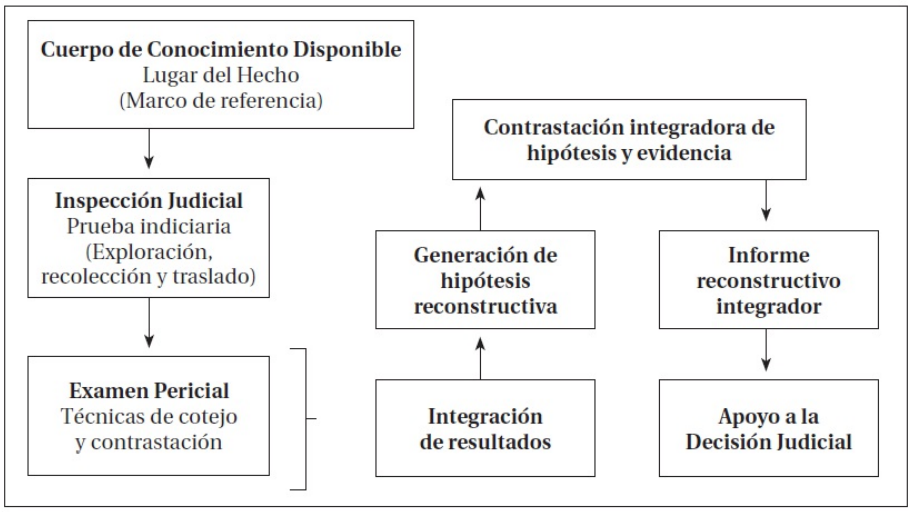
Los agentes externos (naturales, artificiales y humanos), interactúan con la prueba indiciaria, modificándola total o parcialmente. Esta modificación es tanto mayor cuanto más tiempo transcurre desde los hechos hasta su investigación reconstructiva.[21] La posibilidad de separar los componentes originales de sus modificaciones es una tarea ardua y que en general sólo produce resultados parciales.[22]

Los expertos que participan en la reconstrucción tienen sus propias "visiones profesionales" y analizan la situación desde su campo de competencia. Esto produce luchas internas, fundadas en las diferentes capacidades e idoneidades involucradas y especialmente en el innato sentido de antagonismo y contienda humanos, especialmente en lo profesional. La opinión personal suele primar por sobre la convicción profesional, especialmente a los fines retóricos. Fines estos inescindibles de la naturaleza humana.

Tal vez, una opción posible para reducir estas dificultades, podría provenir de las mismas incumbencias académico-profesionales que obran en nuestra sociedad. Nuestro país cuenta con una carrera de formación adecuada para esta tarea, se trata de la figura del "Licenciado en Criminalística". Su visión generalizadora e integradora podría realizar la tarea de reunir los resultados de los informes periciales, efectuados por los restantes expertos y conformar diversas alternativas técnica y metodológicamente coherentes, para ofrecerlas al Tribunal Interventor. De esta manera se reducen las distintas disidencias periciales parciales a la interpretación de un solo experto (un único guionista), resultando más objetiva ya que no ha estado en contacto con la prueba indiciaria, sino que analiza los resultados periciales, intentando conformar un modelo ajustado a la pretendida verdad material de los hechos acaecidos. Esta herramienta podría constituir un elemento de soporte a la decisión judicial, sumamente útil y especialmente confiable. Si agregamos que el modelo

reconstruido puede utilizar técnicas de inteligencia artificial y realidad virtual, las posibilidades reales de su empleo aparecen como sumamente positivas. Por el momento esto no es más que una expresión de deseo, la realidad política, social, jurídica y especialmente económica de nuestro país impide el surgimiento de este rol protagónico en la investigación criminal.

La tarea de reconstrucción de los hechos ocurridos se realiza a partir de un marco de referencias, soportado por el marco teórico de quien la efectúa y a partir de las variables involucradas (situación original → hechos → nueva situación). No escapa al marco general de una investigación formal, a partir de cualquier disciplina del conocimiento:



Como podemos observar en el gráfico anterior, el punto de partida es el lugar del hecho a partir del cual se realizan todas las tareas reconstructivas y de cuya integridad dependen los resultados posteriores. Es por esa razón que dedicaremos un párrafo en particular para analizarlo.

La reconstrucción metodológica del hecho

La reconstrucción del hecho es una tarea sumamente compleja y que implica el análisis de un conjunto de elementos cuyo origen es claramente multidisciplinario. Depende principalmente de la inteligencia, experiencia y sentido común del investigador. Estas características se pueden inducir, estimular y optimizar, pero en general forman parte de la naturaleza intrínseca y de la personalidad del perito. Aunque parezca mentira, el sentido común no es el más común de los sentidos y

mucho más si existen intereses particulares de por medio. Podemos sugerir que:

Realice un análisis previo de los elementos probatorios con que cuenta, sin considerar los restantes hechos colaterales involucrados. Fórmese una opinión respecto de la naturaleza de dichos elementos y sus relaciones posibles. Analice dicha prueba minuciosamente y extraiga conclusiones *a priori* .

Lea concienzuda y profundamente los documentos relacionados con el hecho investigado:

Causa, cuadernos de pruebas, otras pericias, documentos sobre políticas de seguridad y sus implementaciones, documentos de desarrollos de aplicaciones, documentos de otras áreas relacionados con la pericia en desarrollo (aunque sean de contaduría, recursos humanos o ventas).

Construya esquemas y organigramas asociados a los elementos dubitados y a su posible origen. Muchas veces la solución a un problema depende de la detección de un interés particular en un área determinada, antes que del área específica de trabajo.

Busque motivos por parte de los actores involucrados (incluyendo testigos, colaboradores, jefes, subordinados, transacciones, etc.).

Analice los restantes informes periciales en profundidad, busque coincidencias y discrepancias, no sólo de su especialidad, sino también entre ellos.

Genere un modelo de comportamiento, que avale una determinada reconstrucción de los hechos acaecidos.

Realice un cotejo minucioso entre las conclusiones obtenidas. Busque integrar lógicamente ambas conclusiones. De no ser posible, retroalimente el sistema y comience de nuevo. Evite dejar cabos sueltos.

De ser necesario solicite autorización del tribunal para realizar consultas interdisciplinarias, nada impide que como parte de una pericia se integren estudios realizados por otros profesionales de la misma o de diferentes especialidades, pero siempre bajo la supervisión del juez.

Tenga en cuenta que la labor detallada tiene como fin analizar objetivamente la prueba y sus connotaciones, de ninguna manera pretende sustituir la labor del juez. Todo el trabajo anterior pretende arribar a conclusiones periciales científicamente fundamentadas, metodológicamente comprobadas, eficientes, eficaces y efectivas para asesorar al tribunal, no pierda de vista esta circunstancia. Usted no debe sugerir al juez

quién es el culpable, debe limitarse a presentar sus conclusiones periciales a partir del estudio de la prueba (pero siempre en una labor multidisciplinaria, integradora y estrictamente lógica).

El lugar del hecho virtual propio e impropio

En Criminalística, como en toda disciplina del saber, el problema lingüístico de los términos empleados en una definición técnica es prácticamente insuperable. Todo concepto tiene imbuido en sí mismo las características propias de la lengua en cada región geográfica considerada. Los modismos afectan el lenguaje hablado y modifican el sentido propio de las oraciones expresadas (ni hablemos de las nuevas formas de comunicación en los mensajes de texto). Esto se transfiere a lo técnico y todo se vuelve más difícil para alcanzar una comunicación efectiva, eficiente y eficaz.

Si nos ponemos a hilar fino y acordamos que lugar del hecho es precisamente y con claridad *"el lugar donde ocurrieron el o los hechos"*, entonces nos independizamos del Hecho Criminal (aunque por supuesto un buen abogado podría interpretar exactamente lo contrario a lo que quiero expresar). Entonces una cosa es investigar el lugar del hecho y otra la escena del crimen. Bueno, pero la cosa no es tan simple, por ejemplo en nuestro entorno cultural tendemos a identificar como crímenes aquellos que implican hechos de sangre graves, como el homicidio, dejando para el resto de las infracciones penales la palabra delito. Entonces el vocablo "crimen" tendría una relación de especie a género con el vocablo "delito". Entonces y sólo para esta concepción, la escena del crimen sería únicamente aquella donde ha ocurrido un homicidio (y algunos pocos delitos más).

Está claro que la Criminalística de ninguna manera pretende esto. Si tomamos la consideración regional expresada, una denominación aproximada de esta actividad podría ser denominada como "Investigación Técnica del Delito". Ahora bien, no toda investigación realizada por peritos o expertos es exclusivamente delictiva, muchas veces, se limita a la comprobación de hechos con fines comerciales, contables, financieros o simplemente administrativos (como en el caso de las auditorías, contables, financieras, etc.). Pero esto no las extrae del entorno criminalístico, ya que para realizarlas se requiere: un marco legal (conforme a derecho), un marco criminalístico (metodología de investigación) y un marco técnico propio del tema a analizar (técnica específica), todo esto reflejado en un informe que reúna todas las características del Informe Pericial. Por lo tanto en nada difiere de una pericia criminalística típica.

Por esa razón preferimos identificar la Criminalística con la investigación del lugar del hecho (se trate de una escena criminal, delictiva o no).[23] Lo que percibimos y complica bastante el tema es que el lugar del hecho real (el lugar físico donde ocurrieron los hechos investigados) en general estaba restringido a un espació físico limitado y que con escasas excepciones (las aeronaves, las embajadas, los océanos, las vías navegables internacionales), podía circunscribirse, delimitarse y establecer con claridad la jurisdicción y competencias correspondientes (de esto dependerá el derecho procesal a aplicar y la validez e inserción legal de la prueba pericial a implementar). Pero con el auge de las comunicaciones las circunstancias han cambiado, se producen delitos informáticos propios (ataque a la información) e impropios (delitos comunes utilizando herramientas y métodos informáticos, pero en un entorno geográficamente distribuido y no siempre posible de delimitar.

A partir de ahí derivamos la concepción y representación de un lugar del hecho virtual (propio cuando se trata de delitos realizados por medios informáticos distribuidos geográficamente e impropio cuando sólo se emplea para modelar mediante herramientas de simulación, inteligencia artificial y redes neuronales, un lugar del hecho real clásico). Este lugar del hecho virtual no deja de ser un lugar del hecho con características particulares. Es un lugar delimitado o delimitable, donde ha ocurrido un hecho o un conjunto de hechos íntimamente relacionados, que deben ser utilizados para comprender e integrar la trama investigada. No debemos olvidar que la reconstrucción del hecho no es otra cosa que la representación posible del orden sucesivo en que se supone ocurrieron los acontecimientos cuestionados, a partir de los "testigos mudos"; obrantes en la escena analizada (sea ésta criminal, delictiva o no), una especie de trama con soporte argumental lógico y respaldo científico, tecnológico y técnico específicos.

Hasta mediados del siglo pasado, el lugar del hecho se evidenciaba como un lugar físico, geográficamente determinado. A partir del surgimiento de la computación, que llevaría gradualmente al desarrollo de una nueva disciplina "la Informática", aparece el criterio de virtualidad.

La virtualidad no es otra cosa que un modelo representativo de una realidad contrastable o meramente imaginaria. No es sólo un mecanismo computacional, ya que se evidencia en el fenómeno más importante de dicha época "la televisión", que a partir de su precursor el cine, complementa la diaria cotidianidad, con mundos virtuales donde las cosas tienden a ser mejores para el observador. En todos los casos se trata de una realidad informática, porque parte de la información y genera información.

Como toda herramienta humana, esta posibilidad de representar mundos, aunada al

crecimiento exponencial de las comunicaciones, concurrió en ayuda de las actividades humanas y como contrapartida permitió generar nuevas formas delictivas aprovechando su potencial de distribución masiva y su incorporación directa a los hogares. Surge entonces el delito informático propio e impropio, que ya analizamos en esta misma obra. A partir de dicha forma delictiva se construye una nueva forma de interpretar la realidad reconstructiva y aparece el lugar del hecho virtual. Este modelo adquiere por lo menos dos formas distintas:

Lugar del Hecho Virtual Impropio: Consiste en el modelo virtual, realizado por medio informáticos, del Lugar del Hecho Real. Por supuesto es contrastable con la realidad y cuenta con el soporte tecnológico de la Realidad Virtual y la Inteligencia Artificial. Es básicamente una simulación interactiva, que pretende ofrecer alternativas consistentes a partir de las cuales realizar una reconstrucción de los hechos sucedidos.

Lugar del Hecho Virtual Propio: En este caso no existe el Lugar del Hecho Real. Se trata de reconstruir situaciones puramente virtuales a partir de la prueba indiciaria informática.[24] En este caso el lugar del hecho no es estrictamente determinable y puede llegar a abarcar diversas situaciones geográficas, jurisdicciones y competencias.[25]

Ciberespacio: Es necesario evitar la confusión entre el denominado lugar del hecho virtual propio, y el ciberespacio. El ciberespacio o ciberinfinito es una concepción imaginaria a partir de la realidad virtual que se encuentra de manera inmaterial en las computadoras y redes del mundo. Es decir no se trata de un espacio en el sentido propio y material que se podría definir a partir de una concepción física determinada (como la Mecánica de Newton, la Teoría de la Relatividad de Einstein o la Mecánica Cuántica de Planck), es un concepto tan subjetivo, como el Infierno del Dante, el inframundo, la Tierra de Oz o el País de las Maravillas. Algunos profesionales en su afán de definir, clarificar y explicar la idea del delito informático, lo suponen establecido en dicho espacio. Esta concepción no tiene entidad física alguna y por lo tanto no puede ser objeto de análisis a partir de la Informática Forense.

Para la Informática Forense se trata de datos, en unos de los tres estados posibles: almacenado, en tránsito o en procesamiento, lo que dichos datos representan, no son razón de análisis de la misma, más allá de la reconstrucción física y lógica de ésos. Quien debe interpretar si son conducentes o pertinentes a la investigación en curso es el juez, de ahí la necesidad de recomendar a los expertos en Informática Forense la mayor discreción posible al expresarse al respecto para evitar un resultado que eluda a la ciencia y se transforme en ciencia ficción. Recordemos que no todo lo concebible existe y no todo lo imaginable es posible.

El ciberespacio es un tema recurrente en la ciencia ficción, fue popularizado por la novela *Neuromante* de William Gibson (1984), a partir del relato del mismo autor denominado *Johnny Mnemonic* (1981). El 8 de febrero de 1996, en Davos, Suiza, John Perry Barlow escribió la *Declaración de Independencia del Ciberespacio* en la que exhortaba a los gobiernos a no ejercer soberanía sobre el ciberespacio, definido por éste como "el nuevo hogar de la Mente".

Tampoco debemos confundir al ciberespacio con Internet, el término se refiere a menudo a los objetos e identidades que existen dentro de la misma red informática, hablando metafóricamente una página web "se encuentra en el ciberespacio". Según esta interpretación, los acontecimientos que tienen lugar en Internet no están ocurriendo en los países donde los participantes o los servidores se encuentran físicamente, sino "en el ciberespacio".

Sin embargo sabemos que una página web se encuentra almacenada en un servidor determinado, con su correspondiente almacenamiento secundario (disco magnético u óptico) que la contiene, la visión expresada en el párrafo anterior es propia de la ciencia ficción, esta última es la que debe utilizar el perito.

Nuestra profesión, para bien o para mal, se encuentra siempre caminando por la fina división existente entre la ciencia y la ciencia ficción, para evitar las caídas hacia uno u otro lado, la única solución es mantenerse actualizado de manera permanente en los avances científicos, tecnológicos y técnicos. En nuestra disciplina (al igual que en Medicina), una desactualización de tres meses implica simplemente haber quedado fuera del sistema.

La confección de modelos a partir del Lugar del Hecho Real, no trae grandes dificultades, es nada más que una herramienta puesta al servicio de la investigación judicial. Herramienta sumamente útil, porque facilita el intercambio de información entre los participantes que pueden interactuar por medios virtuales, adecuar sus tiempos a las necesidades particulares de cada actor y evitar las complicaciones derivadas de la concurrencia en un momento y lugar determinado de la totalidad de los actores necesarios para realizar una inspección judicial. Por otra parte admite las posibilidades de revisión, reconsideración y reformulación de propuestas, sin abandonar el lugar de trabajo. Una inspección judicial normalmente trae aparejadas una serie de tareas complementarias en las que los artífices de la misma deben reunirse (ajustar sus agendas en el mejor de los casos, concurrir a citaciones en la mayoría) para intercambiar información, esto se vuelve innecesario utilizando medios reconstructivos a partir de un modelo virtual de lugar del hecho.

Desde el surgimiento del litigio judicial en la antigua Roma, se presenta el problema

de la multiplicidad de jurisdicciones y competencias, ante las cuales es posible litigar. Esto se hace evidente al decidir si vamos a demandar ante la jurisdicción comercial o civil, si por la penal o la civil, si por la justicia nacional o la local, si pedimos la excarcelación al juez de Feria o esperamos a que finalice la misma. En este sentido la informática y las comunicaciones permiten el intercambio de bienes y servicios reales, por medios virtuales y también de bienes y servicios virtuales por medios virtuales. Es posible adquirir libros, contratar empleados, descargar archivos de música o video, acceder a un servicio de soporte legal, disponer de jurisprudencia *on line*, conocer personas, establecer amistades, entablar relaciones (con concreción real o puramente virtuales), crear nuestra propia imagen virtual. En definitiva, interactuar con nuestros congéneres y con la sociedad a partir de estas herramientas virtuales. Por supuesto todas estas relaciones son factibles de derivar en conflictos jurídicos, que requieran intervención jurisdiccional. Establecer la misma se vuelve sumamente complejo, no sólo a la hora de lograr el cumplimiento efectivo de la sentencia judicial recaída, sino a partir del momento de seleccionar (de ser esto posible) la jurisdicción ante la cual presentar la batalla legal.

En lo que se refiere al Lugar del Hecho Virtual Propio, la problemática está aún lejos de ser comprendida en su totalidad, en su consideración intervienen factores extraños a la ciencia y a la tecnología, relacionados con la situación política de un país determinado y sus normas de Derecho Internacional Privado y Derecho Internacional Público, como ser:

Tratados Internacionales de Integración: Debería constituir el caso más sencillo; los países conforman bloques económicos y/o políticos a partir de los cuales compatibilizan sus normas jurídicas, o al menos tienden a hacerlo. Pero se trata de una solución sumamente parcial, ya que se refiere únicamente al caso en que uno o varios delitos informáticos propios y/o impropios trasciendan las fronteras, pero restringidos al marco del bloque de integración considerado. La mayoría de los tratados de integración admite las relaciones en bloque con los países externos al mismo, pero también permiten las relaciones individuales de cada país en particular a los mismos efectos. Por lo tanto una defraudación cometida por un delincuente desde Argentina, sobre un Banco de Brasil, pero cuyos servidores se encuentran en EE.UU., utilizando como herramienta una página comercial de ventas por Internet situada en Uruguay, escapa a la estructura normalizadora del bloque (Mercosur) y permite una amplia variedad de planteos, legalmente fundables e internacionalmente convalidables, referidos a la competencia y jurisdicción involucradas.

Relaciones Internacionales bilaterales: En este caso, la complejidad aumenta, ya que depende de la naturaleza, extensión y detalle de los Tratados Internacionales existentes entre dos países. Como ya vimos los delitos informáticos propios e

impropios pueden involucrar a más de dos países, lo que nos refiere a la situación planteada en el párrafo anterior *in fine*. En algunos casos la existencia de Tratados de Adhesión multilaterales, que sin llegar a constituirse en Tratados e Integración, al menos establecen pautas rectoras generales para los adherentes, quienes suelen concurrir en ayuda del Poder Judicial. No obstante son muchos los países que no han adherido a los mismos, no forman parte del bloque de integración propio y con los cuales no existen tratados de asistencia recíproca judicial alguna.

En la mejor situación imaginable, existen normas internacionales que regulan el proceso judicial de forma similar. Pero en la realidad diaria, las incompatibilidades son tales que aún en el derecho penal mínimo se observan diferencias e incompatibilidades, llegando al caso de que hechos que resultan punibles en un país no lo son en otro. Esta ocurrencia restringe directamente la tipicidad delictiva, anulando de cuajo la acción penal pretendida.

Por último podemos utilizar la simulación reconstructiva por medios informáticos, del lugar del hecho virtual propio, tratándolo como si fuera un lugar del hecho real. Es ésta una asignatura transdisciplinaria pendiente, donde deberían integrarse las visiones de los operadores del derecho, los criminalistas y los informáticos, ya que ninguna solución parcial aparece como factible de implementación. La normalización jurídica global, por el momento, ni siquiera alcanza el grado de posibilidad en el Derecho Internacional Público y apenas está formulada en algunos aspectos del Derecho Internacional Privado.[26]

A partir de las razones expuestas inferimos la necesidad de realizar una tarea transdisciplinaria. La labor del experto solitario ha quedado en el tiempo. El experto debería ser un actor más dentro de la estructura judicial, integrado en equipos de trabajo, cuya dirección supongo en manos de licenciados en Criminalística (intentando compatibilizar e integrar los distintos informes producidos) y cuya interacción debería ser permanente en condiciones de soporte técnico mutuo (físico o virtual).

Prueba documental clásica (bibliográfica, foliográfica y pictográfica) e Informática

La prueba documental ha sido desde la invención de la escritura, el principal aliado de la investigación judicial. Actúa como respaldo de la mayoría de los procesos. Ni siquiera la oralidad procedimental la ha podido desplazar, el documento forma parte de nuestra forma de ser y de nuestra sociedad, podemos “despapelizar” los procedimientos, pero no prescindir de los documentos soportados en papel.[27]

Esta prueba, no requiere de más explicaciones, se conoce y se emplea como

complemento procesal, se evalúa acorde a su pertinencia y a su carácter conducente en el desarrollo del proceso. Se relaciona directa o indirectamente con los hechos a probar y en especial con la pretensión del litigante. Tal vez no siempre se identifique con claridad su clasificación técnica:

Prueba documental bibliográfica: Se refiere a la prueba consistente mayoritariamente en textos, a partir de un lenguaje determinado.

Prueba documental foliográfica: Se integra mediante diversos modelos o representaciones (gráficos, esquemas, planos, cuadros estadísticos).

Prueba documental pictográfica: Se conforma a partir de imágenes fijas o en movimiento (fotografías, diapositivas, películas).

Nuevamente debemos destacar que esta división no es estricta respecto de la realidad observable la forma mixta es muy común y se realiza principalmente con fines de estimación de los mecanismos de análisis periciales a utilizar.[28] Si bien es una división que ha caído en desuetudo, se agrega a este trabajo para demostrar que a los fines clasificatorios a partir de un género (prueba documental), es posible establecer especies (bibliográfica, foliográfica, pictográfica), sin desnaturalizar el género originario.

En este sentido es necesario agregar una nueva especie a la documental, se trata de la Prueba Documental Informática, que complementa pero no sustituye, suplanta, ni reemplaza a la prueba Documental Clásica y que sólo difiere de ésta en el soporte. A los efectos descriptivos podemos asimilar la palabra documento con la palabra archivo. Todo documento está almacenado en alguna parte, si es papel entonces éste será su soporte, por lo tanto está “archivado en papel”. Se archiva con fines de preservación y permanencia en el tiempo. Lo mismo ocurre con un archivo informático resguardado mediante herramientas computacionales. Aquí debemos agregar una consideración técnica específica: *Desde el punto de vista informático, toda información es información almacenada.* Ya sea que se encuentre almacenada en un soporte físico (cintas, discos magnéticos u ópticos), en procesamiento (registros, memoria volátil, ALU) o en tránsito (redes alámbricas e inalámbricas). Un documento puede obrar en un archivo de computadora o ser impreso y transformarse en prueba documental clásica.

Sentado este concepto, el tratamiento que se debe implementar para procesar la Prueba Documental Informática, es judicialmente similar al que se aplica a sus homólogas bibliográfica, foliográfica o pictográfica. Por supuesto desde el punto de vista técnico, requiere el empleo de ciertos protocolos que aseguren su validez

probatoria, tema que presentaremos un poco más adelante en este volumen.

Elemento probatorio pertinente y conducente

Los códigos de procedimientos establecen un lugar especial para la prueba documental, otro para la prueba de informes y otro para la pericial. En este caso la Informática Forense se relaciona con todos ellos. La estructura más sencilla para entender este mecanismo es la siguiente:

La prueba documental informática es una especie del género Prueba Documental, junto con las ya conocidas documental bibliográfica, foliográfica y pictográfica, difiriendo de éstas únicamente en el soporte que la contiene, en el caso clásico papel o similar (pergaminos, papiros, telas, etc.) y en el que nos ocupa soporte digital (magnético, óptico, ADN[29], proteínas, etc.).

Los resultados obtenidos mediante el análisis informático forense frecuentemente deben ser confirmados por una prueba de informes. Por ejemplo, establecido que fuere el origen, el destino y la hora GMT de un mensaje de correo electrónico, por métodos informáticoforenses, dicho resultado debería ser validado mediante la producción de una prueba de informes dirigida al ISP[30] que corresponda.

A partir de la identificación, preservación, certificación, resguardo y presentación ante el tribunal de la Prueba Documental Informática, es muy probable que se generen puntos controvertidos, que deberán ser resueltos mediante una pericia informático forense.

Prueba pericial informático forense

Relacionando las pruebas documentales y de manera analógica a las concepciones periciales documentológicas, podemos decir que:

La prueba documental informática, es a la Pericia Informática-Forense,

lo que la prueba documental clásica, es a la pericia documentológica.

Establecida la utilidad de la prueba documental informática, se ha mostrado evidente la necesidad de su revisión pericial estricta y metodológica. Esta necesidad

afecta no sólo al derecho como disciplina autónoma, sino que provoca cambios en la Informática, al requerir de especialistas en la temática que puedan desarrollar y utilizar herramientas para dicha tarea (detección, recolección, identificación, clasificación, resguardo, certificación y traslado de la prueba indiciaria informático forense). Por otra parte genera una nueva especialidad criminalística, orientada a la gestión de la mencionada prueba indiciaria informático forense, su inclusión dentro de la disciplina y sus relaciones con las restantes Ciencias Forenses. A esta especialidad la denominamos Informática Forense.

Relaciones con otras disciplinas

Medicina Legal: Soporte informático a los conocimientos y procedimientos médicos aplicados a las cuestiones de interés forense. Un elemento destacable en estas relaciones es la confección de las llamadas Historias Clínicas Virtuales.

Criminología: Esta disciplina estudia de las razones que provocan la comisión de delitos, su posible prevención y la reinserción del delincuente en la sociedad (naturaleza causal, psicológica, objetivos preventivos y de recuperación social). Generalmente se inserta e identifica con alguna de las doctrinas penales "no retributivas", es decir en las distintas modalidades de prevención.[31] Se constituye en un soporte imprescindible a la hora de intentar realizar la reconstrucción virtual del hecho, el factor humano es uno de los elementos más complejos de determinar en dicha reconstrucción. Desde antaño hemos oído hablar del *modus operandi,* que pretende establecer conductas típicas en la forma de actuar delictiva y relacionarlas con determinada persona o determinado perfil psicológico.

Criminalística: Concebida como el conjunto de conocimientos técnico-científicos, aplicados a la resolución de los interrogantes indiciarios procesales, mantiene con la Informática Forense una estricta relación de género (Criminalística) a especie (Informática Forense).

Disciplinas periciales integradoras: Se constituyen en soporte mutuo e instrumento de cada disciplina específica. La labor pericial es una labor transdisciplinaria de ahí su pertinencia relacionante (Fotografía Pericial, Planimetría, Medicina Legal, Papiloscopía, Identificación Humana, Rastros, Laboratorio pericial, Documentología, entre otras).

A esta altura del desarrollo argumental se hace necesario recordar la definición de esta nueva disciplina:

Se denomina Informática Forense al conjunto multidisciplinario de teorías,

técnicas y métodos de análisis, que brindan soporte conceptual y procedimental, a la investigación de la prueba indiciaria informática.

Como toda disciplina en ciernes, requiere de una definición y de ciertos principios que la delimiten (marco de referencias y variables normativas), los que describiremos en el siguiente capítulo.

15 Probar: (Del lat. *proba−re*).

tr. Hacer examen y experimento de las cualidades de alguien o algo.

tr. Examinar si algo está arreglado a la medida, muestra o proporción de otra cosa a que se debe ajustar. U. t.

c. prnl.

tr. Justificar, manifestar y hacer patente la certeza de un hecho o la verdad de algo con razones, instrumentos o testigos.

tr. Gustar una pequeña porción de una comida o bebida. *Probé la sopa para asegurarme de que tenía sal.*

tr. Comer o beber algo. U. m. con neg. *Desde el año pasado no prueba el alcohol.*

tr. ant. aprobar (dar por bueno).

intr. Hacer prueba, experimentar o intentar algo. *Probó a levantarse y no pudo.*

intr. Dicho de una cosa: Ser a propósito o convenir, o producir el efecto que se necesita. *El calor me prueba bien; el frío me prueba mal.*

Prueba.

f. Acción y efecto de probar.

f. Razón, argumento, instrumento u otro medio con que se pretende mostrar y hacer patente la verdad o falsedad de algo.

f. Indicio, señal o muestra que se da de algo.

f. Ensayo o experimento que se hace de algo, para saber cómo resultará en su forma definitiva.

f. Análisis médico.

f. Muestra, cantidad pequeña de un alimento destinada a examinar su calidad.

f. Examen que se hace para demostrar o comprobar los conocimientos o aptitudes de alguien.

f. En algunos deportes, competición.

f. Muestra del grabado y de la fotografía.

f. Reproducción en papel de una imagen fotográfica.

f. *Der.* Justificación de la verdad de los hechos controvertidos en un juicio, hecha por los medios que autoriza y reconoce por eficaces la ley.

f. *Impr.* Muestra de la composición tipográfica, que se saca en papel ordinario para corregir y apuntar en ella las erratas que tiene, antes de la impresión definitiva. U. m. en pl.

f. *Mat.* Operación que se ejecuta para comprobar que otra ya hecha es correcta.

f. pl. *Der.* Probanzas, y con especialidad las que se hacen de la limpieza o nobleza del linaje de alguien. Prueba antes de la letra. f. prueba tirada por vía de ensayo, cuando aún no se le ha puesto la inscripción que dice lo que el grabado representa.

Prueba de fuego. f. La comprometida y decisiva, en la que es necesario demostrar que se está a la altura de lo esperado.

Prueba de indicios, o indiciaria. f. *Der.* La que se obtiene de los indicios más o menos vehementes relacionados con un hecho, generalmente criminal, que se pretende esclarecer.

Prueba negativa. f. *Fotogr.* Imagen que se obtiene de la cámara oscura como primera parte de la operación fotográfica, donde los claros y los oscuros salen invertidos.

Prueba positiva. f. *Fotogr.* Última parte de la operación fotográfica, que consiste en invertir los claros y los oscuros de la prueba negativa, obteniendo así sobre papel, cristal o metal las imágenes con sus verdaderas luces y sombras. Prueba semiplena. f.

Der. prueba imperfecta o media prueba, como la que resulta de la declaración de un solo testigo, siendo éste de toda excepción.

Prueba tasada. f. *Der.* La que, por diferencia de la regla de su libre estimación por el juez, la ley exige específicamente para poder acreditar un hecho determinado. Ver libres convicciones y sana crítica (libres convicciones razonada).

A prueba: loc. adj. Dicho de un empleado: Que durante un tiempo tiene que demostrar su valía para poder confirmar su puesto de trabajo mediante un contrato.

loc. adv. Denota que algo está hecho a toda ley, con perfección.

loc. adv. Entre vendedores, u. para dar a entender que el comprador puede probar o experimentar aquello que se le vende, antes de efectuar la compra.

Prueba de agua, de bomba. locs. advs. U. para referirse a lo que por su perfecta construcción, firmeza y solidez, es capaz de resistir al agua, a las bombas, etc.

Prueba de. loc. adj. Adecuado para probar el límite de la resistencia de alguien. loc. adj. desus. Que tiene la consistencia o firmeza de una cosa en lo físico o en lo moral.

En prueba de. loc. prepos. Como muestra o señal de algo.

Poner a prueba. a alguien o algo. loc. verb. Someterlo a determinadas situaciones para averiguar o comprobar sus cualidades, comportamientos, etc.

Recibir a prueba. loc. verb. Der. Abrir el período del juicio en que los interesados han de proponer y practicar sus justificaciones o probanzas.

Referido virtualmente en: http://www.rae.es.

16 Probar: del lat. *Proba−re*, probar, ensayar, aprobar, comprobar. De uso general en todas las épocas y común a todos los romances de occidente. La grafía medieval era *provar*… Corriente en la Edad Media era la acción intransitiva "resultar ser" o "resultar ser cierto", *"todos a él vinién consejo demandar: / lo que lis él dizié faziégelo provar"*…Un resto de la misma es la alocución probar bien o mal, por convenir, sentar bien o mal, hablando especialmente del clima, muy usual desde el siglo XVII y hasta hoy, aunque actualmente en castellano tiende a sustituirse por sentar. Cuando probar en calidad de verbo modal se combina con un infinitivo con el valor de intentar o hacer prueba, se ha construido, sobre todo en la Edad Media, con el auxilio de la proposición "de"… Aprobar, nótese que en la Edad Media no se distingue semánticamente de probar, los primeros testimonios de la acción moderna se hallan en el siglo XV, *Celestina, Seguro de Tordesillas,*…-var: probo, aprobo, *compprobo, de approbare;* aprobable, aprobaión, aprobador, aprobante, aprobanza, aprobativo, aprobatorio.

Comprobar, tomado de comprobare id.; comprobable, comprobacion comprobante, comprobatorio. Improbar: raro. Reprobar, tomado de reprobare, reprobable, reprobación, reprobador, reprobatorio, reprueba. *Probo,* tomado de *probus,* probidad, de *probitas –atis,* improbo, de improbus improbidad, réprobo de *reprobus id.* En realidad *reprobare* sólo en apariencia deriva de *probare* (ver reproche). Referido en: Corominas Joan, Pascual Juan. *Diccionario Crítico Etimológico Castellano e Hispánico*. Editorial Gredos, Madrid, 1981, pp. 657 y 658.

17 Medios de prueba. Art. 378. "La prueba deberá producirse por los medios previstos expresamente por la ley y por los que el juez disponga, a pedido de parte o de oficio, siempre que no afecten la moral, la libertad personal delos litigantes o de terceros, o no estén expresamente prohibidos para el caso. *Los medios de prueba no previstos se diligenciarán aplicando por analogía las disposiciones de los que sean semejantes o, en su defecto, en la forma que establezca el juez."*

18 Como ejemplo típico podemos destacar los accesos indebidos a los datos sensibles de una persona física o jurídica.

19 Como ejemplo, podemos señalar el uso de herramientas de análisis y decodificación de claves para acceder a una institución bancaria y realizar una transferencia de fondos ilegal.

20 Esta circunstancia se hace evidente en las declaraciones testimoniales, donde frecuentemente es necesario recurrir al careo para intentar desambiguar una situación, técnica ésta que no siempre permite alcanzar resultados positivos (una parte "convence" a la otra, una parte "se acomoda" a los dichos de la otra, "vieron" cosas distintas, los focos de atención y perspectivas no coinciden, no se ponen de acuerdo, etc.).

21 Esta dificultad se hace evidente en los análisis históricos, cuanto mayor es la distancia a los hechos relatados, más difícil es interpretar y relatar los mismos. Entre otras cosas porque menores son las fuentes de información disponibles para realizar el relevamiento de la información necesaria. Por otra parte cuando los hechos son muy recientes, están afectados por la subjetividad del intérprete, que también los condiciona; el análisis de nuestro pasado reciente como Nación es un fiel reflejo de esta circunstancia.

22 No se obtienen los mismos resultados si se realiza la autopsia de un cadáver preservado de manera adecuada, ocho horas después de fallecido, que si éste ha estado expuesto a la intemperie durante un mes.

23 En sentido similar, aunque no idéntico, la define el doctor Pablo A. Rodríguez Regalado en su artículo "Nuevo Enfoque en la definición de la ciencia criminalística". *"Criminalística es la ciencia mediante la cual se procede al examen de indicios o evidencias de diverso origen y naturaleza, por parte de expertos forenses, con el objeto de plasmar la información obtenida en un pronunciamiento pericial que sirva de ilustración para un proceso judicial, administrativo o de* índole *particular".*Obviamente, que esta definición propuesta amerita una argumentación, la que de inmediato paso a exponer : *Primero:* Definitivamente, no podemos negar que la Criminalística sea ciencia, es tema ampliamente dilucidado, pues ésta se encuentra comprendida dentro de las ciencias "factuales" (que estudia hechos que ocurren en el mundo y del tipo "mixto", porque hace suyos temas que corresponden a las Ciencias Naturales y a las Ciencias Sociales, constituyéndose en una Ciencia Técnica, como corresponde al planteamiento hecho por Kedrov y Spirkin.. *Segundo:* El empleo de las

ciencias, técnicas y artes que comprende a la Criminalística, permite justamente el examen de indicios o evidencias.

Tercero: Que estos indicios o evidencias puedan ser de diverso origen (corpóreos o extracorpóreos) y naturaleza (sólidos, líquidos, pastosos, gaseosos).

Cuarto: El examen obviamente estará a cargo de expertos forenses, ello en razón de que deben ser profesionales o técnicos debidamente calificados en alguna de las áreas que comprende a la Criminalística, ya que ésta responsabilidad no se la podríamos adjudicar a la persona no idónea para este tipo de análisis.

Quinto: El resultado del análisis o examen realizado debe de estar debidamente protocolizado en un informe que tenga una metodología particular, la misma que tiene calidad de "pronunciamiento pericial".

Sexto: El informe resultante y la información contenida en él puede ser ilustrativa tanto en una investigación policial, proceso administrativo, judicial o interés particular.

Fuente: "Nuevo enfoque en la definición de la ciencia criminalística", Dr. Pablo A. Rodríguez Regalado Abogado – Perito Criminalístico Doctor en Ciencias Forenses y Criminalística por la Universidad Nacional de San Agustín de Arequipa.

24 Un ejemplo de esta tarea sería la modelización, con fines reconstructivos del Lugar del Hecho Virtual, a partir del cual se ha realizado una sustitución de identidad con fines delictivos.

25 Pensemos en un delincuente ubicado en Chile, que mediante el empleo de herramientas informáticas disponibles en Irán, decodifica una clave de acceso a una cuenta en Suiza, a partir de la información disponible en una Banca Informática Francesa, realizando una transferencia de fondos a un banco de las Islas Caimán. No sólo involucra lugares geográficos determinables (por la situación de cada servidor de datos y procesos) sino que interviene la conectividad de la red (Internet), que pasa por muchos y muy diversos países, comunicación que forma parte indiscutible de la cadena causal, al momento de analizar el delito cometido. Por ejemplo un mensaje de correo electrónico, enviado desde Buenos Aires (Argentina), hacia Montevideo (Uruguay), puede realizar su recorrido por distintos enrutadores situados en EEUU y Europa, lo que es fácilmente comprobable al realizar un trazado de la ruta seguida, empleando las herramientas disponibles en Internet.

26 Una muestra de esta integración la constituye el derecho de navegación comercial, donde son muchas las normas aceptadas por la comunidad internacional. De todas formas está lejos de contemplar la totalidad de las situaciones previsibles (de lo contrario no sería necesaria la acción protectora de Greenpeace, frente al conflicto ballenero).

27 Aunque se admitan los resguardos electrónicos y en algún momento se llegue a una efectiva implementación de los mecanismos de firma digital y el derecho notarial evolucione, difícilmente se llegará al punto de eliminar los protocolos de los escribanos y sustituir los Instrumentos Públicos escritos.

28 Las máquinas de escribir mecánicas sólo aportaban caracteres de texto (los gráficos se limitaban a algunas líneas de subrayado), las máquinas de escribir electromecánicas aportaron nuevos elementos gráficos que se desarrollaron especialmente en las máquinas de escribir electrónicas. Al llegar las impresoras, las primeras de matriz de puntos tenían dos formas de trabajar, una en textos y otra en gráficos, ahí surge esta división en particular. Actualmente este tema ha quedado prácticamente obsoleto. En cuanto a la redaccion caligráfica, en general, se limita a textos y cuando obran dibujos suelen requerirse los servicios de otros profesionales ajenos a la documentología (expertos en dibujo, pintura, arte, etc.) Suponiendo el caso de un testamento ológrafo, que incluyera planos, representaciones y/o dibujos manuscritos u otras representaciones gráficas, el análisis pericial de esta prueba tal vez no estaría completo con la participación exclusiva de un perito en documentología.

29 Computación por ADN propia, ya que la misma suele ser simulada por medios convencionales.

30 ISP (Internet Service Provider), el proveedor del servicio (p.e., google, yahoo, hotmail, etc.).

31 Prevención General (Positiva o Negativa) y Prevención Especial (Positiva o Negativa).

CAPÍTULO 6
INFORMÁTICA FORENSE LA PRUEBA DOCUMENTAL INFORMÁTICA

Principios y relaciones periciales informático forenses

Principio de entidad pericial propia: El empleo de los medios informáticos como instrumentos de conformación de prueba indiciaria informático forense. Prueba que si bien constituye una parte de la Criminalística y en lo formal no difiere de cualquier otra prueba pericial, se integra con metodología propia, que permite asegurar la detección, identificación, documentación, preservación y traslado de la evidencia obtenida, con técnicas e instrumentos propios e inéditos para las Ciencias Criminalísticas. En este sentido, la prueba indiciaria informático forense, requiere de cuidados específicos que la diferencian de otras pruebas periciales.

Principio de protección y preservación: Cadena de custodia estricta y con certificación unívoca comprobable.

Principio de identidad impropio (de Copias): Del original, ya que cuando se duplica un archivo informático la copia no es igual a la original sino idéntica (un bit no difiere de otro bit y entre sí son inidentificables unívocamente).

Principio tecnológico transdisciplinario: Se requieren conocimientos específicos por parte de todos los involucrados en la prueba indiciaria informático forense:

jueces para evaluar correctamente la prueba;

fiscales y abogados para efectuar la requisitoria de manera adecuada y oportuna;

profesionales de la Criminalística y otros peritos, para no contaminar dicha prueba durante sus propias tareas periciales, contribuyendo a su preservación;

funcionarios judiciales y policiales, a efectos de proteger y mantener la cadena de custodia establecida.

Principio de oportunidad: Debido a su facilidad de destrucción normalmente requiere de tareas complementarias que aseguren su recolección (medidas preliminares, inspecciones o reconocimientos judiciales, órdenes de allanamiento o de intercepción judiciales).

Principio de compatibilización legislativa internacional: Gran parte de los contratos particulares celebrados en el marco del Derecho Internacional Privado se realizan mediante comunicaciones digitales (instrumentadas en correo electrónico en claro o cifrado y certificadas por medio de claves criptográficas o firmas digitales). Estas actividades no sólo devienen en demandas civiles, comerciales y laborales internacionales, sino que en muchas oportunidades constituyen delitos tipificados en la legislación de fondo de cada país. Diversos contratos de trabajo se proponen, establecen y ejecutan por medios informáticos. Sin embargo la pertinencia y utilidad de la prueba informática será siempre relativa a las definiciones que la ley de fondo y forma de cada país establece en particular y las que regulan los tratados internacionales.

Principio de vinculación estricta: La prueba indiciaria informático forense puede estar relacionada con múltiples actividades delictivas dentro de la legislación internacional o el derecho interno, algo que si bien es propio de toda prueba pericial, se vuelve crítico respecto de esta disciplina por su relación vinculante directa (como medio de ejecución e indicio probatorio), entre otras: actividades de espionaje industrial y comercial, trata de personas, tráfico de órganos, blanqueo de capitales, terrorismo (político, delictivo, ideológico, narcoterrorismo), prostitución y pornografía infantil.

La prueba documental informática

El marco de inserción de la prueba documental informática es indiscutiblemente transdisciplinario, este hecho se constituye y evidencia por pertenecer simultáneamente a las siguientes disciplinas:

El derecho: Se incluye entre los métodos probatorios procesalmente aceptados, en este sentido forma parte de la prueba documental, es factible de confirmación mediante prueba de informes y de verificación mediante la prueba pericial informático forense.

La Informática: Constituyendo una especie de la misma. Su inserción respectiva se corresponde con la clasificación: Informática → Seguridad Informática → Informática Forense.

La Criminalística: Es también una especie conformada por una nueva disciplina dentro de este conjunto de técnicas periciales, coexistiendo de manera interdisciplinaria con las restantes (Balística, Documentología, Papiloscopía, Laboratorio pericial, Fotografía, Rastros, entre otras).

Definición y relaciones

La prueba documental informática es una especie de la prueba documental clásica (bibliográfica, foliográfica o pictográfica) que difiere de ésta en el soporte que la contiene.

Si bien se relaciona con toda la estructura probatoria, integrando los indicios conducentes y pertinentes a la investigación y la argumentación procesal pretendida, tiene especialidad afinidad con:

La prueba de informes: En la mayoría de los casos la prueba recolectada debe ser confirmada por organismos públicos o privados, nacionales o internacionales que la convaliden.

La prueba pericial: A partir de la prueba documental informática recolectada se deben obtener conclusiones periciales, pertinentes y conducentes para sustentar la argumentación planificada.

La simple exposición de la documental muy pocas veces es suficiente para probar los hechos invocados. Por esta razón es necesario confeccionar el pedido de informes y los puntos de pericia juntamente con las actividades de preservación de la documental informática, conformando entonces un cuerpo probatorio interdependiente y autosuficiente.

Inteligencia estratégica

Como todo proceso destinado orientado a un fin y destinado a cumplir objetivos, debe ser dividido en etapas:

Entrevista con el consultante:

Puesta en común de la pretensión, su argumentación y la prueba requerida (en este caso orientada a la documental informática, de informes y pericial).

Determinación de los elementos probatorios públicos y privados y su posible alojamiento físico (local, remoto, en poder de nuestro patrocinado, de la contraparte o de terceros).

Consulta con el experto en Informática Forense, para establecer un cronograma de acciones de recolección. En el mismo acto coordinar las agendas del abogado, el experto, el escribano y el cliente, para efectuar la recolección a la brevedad. Toda

pérdida de tiempo en estas tareas pone en riesgo la disponibilidad de los elementos probatorios a recolectar, ya sea por acciones dolosas propias o de la contraparte procesal.

Ejecución metodológica de la recolección.

Inicio formal del pleito ante la Jurisdicción, o métodos alternativos de resolución de conflictos.

La entrevista

Aunque esta actividad ya ha sido tratada por múltiples autores del derecho procesal de manera extensa, exhaustiva y a nuestro entender sumamente completa, utilizaremos en principio ciertos principios fijados por el doctor Genaro Carrió, en un libro elemental, breve, sencillo, pero sumamente práctico: ¿Cómo *estudiar y cómo argumentar un caso?* (Abeledo Perrot, Buenos Aires, 2009):

"Una persona C (el cliente), que se encuentra en las circunstancias H (un conjunto de hechos) desea obtener un resultado R (un cierto estado de cosas)." p. 22.

"El conjunto de medios que permiten llegar a R partiendo de H, constituyen la solución (S)."

p. 23.

"En relación con R. a) Averiguar bien qué es lo que realmente quiere C y por qué lo quiere… Ver si eso se puede alcanzar a partir de H." p. 35.

"En relación con H… formarse una opinión propia e independiente acerca de H." p. 36.

Estas reglas prácticas y sencillas permiten en primera instancia conformar una estructura inicial (marco de referencias) a partir del cual seleccionar las variables de interés para nuestra "S" *a priori*. Pero en el caso que nos ocupa, la selección de variables para construir la documental informática implica tener en cuenta ciertas características propias diferenciativas, que no pueden ser olvidadas al momento de planificar la estrategia argumental.

Aunque en ciertos casos particulares la capacidad argumental y oratoria forman parte consustancial con el operador del derecho que las utiliza, deviene de su propia naturaleza (*"le viene desde la cuna"*), no es ésta la regla general sino la excepción. Pero al igual que la capacidad docente, lo que no se tiene, se puede adquirir (con más

o menos esfuerzo). De ahí que la argumentación debe ser planificada en dos sentidos: estratégico y táctico. Esta tarea está implícita en las reglas que nos aporta Carrió, pero en cuanto a la documental informática forense, por su naturaleza novedosa y poco conocida, consideramos que debe ser explicitada. Consideraciones generales a tener en cuenta al seleccionar la prueba documental informática: La única prueba documental informática que puede ser recolectada sin autorización judicial previa es la que obra en poder de nuestro cliente o constituye información pública de libre acceso. Incluye toda la información de la que es propietario. Almacenada en los equipos informáticos de su propiedad y la que obre en lugares de almacenamiento remoto sometidos a su dominio por cualquier relación jurídica legalmente establecida (por ejemplo alquiler de espacio de almacenamiento).

En relación con la restante prueba que podamos considerar necesaria, la misma puede hallarse en poder de un tercero (persona física o jurídica, organismo oficial o privado, artículo 389 del Código Procesal Civil y Comercial de la Nación) o en poder de la contraparte. Si no contamos con la autorización expresa del tercero y siempre en el caso de la contraparte, deberemos requerir una autorización al Juzgado Interventor para acceder a la misma, por los medios que dicha autoridad establezca (autorización de intercepción de comunicaciones, acceso remoto o orden de allanamiento con las debidas y específicas autorizaciones de recolección de información). Por la naturaleza de esta prueba es de difícil aplicación lo establecido en el artículo 388 del Código precitado, ya que si la contraparte es notificada, fácilmente podrá destruir o modificar la información que tiene en su poder, tarea que si es adecuadamente realizada, no dejará rastro digital alguno para que sea posteriormente relevado. Por esta razón, se solicita realizar la recolección *in audita altera pars*, como medida previa o preliminar a la instrucción del proceso formal. Artículos 323, 325 y subsiguientes del antes citado cuerpo legal.[32]

La documental informática, es sólo una prueba documental más. Todos los aportes probatorios que nuestro consultante puede acercar a la causa y que permitan sustituirla, deben ser requeridos y utilizados. Nunca es conveniente utilizar un medio probatorio poco conocido y sobre el cual la mayoría de los profesionales cree tener “la verdad”, cuando existen otros medios de prueba más conocidos y fáciles de implementar (por ejemplo, la documental clásica). Se debe recurrir a la documental informática en forma complementaria o cuando no existen otros medios más idóneos de prueba. Esta subsidiariedad de la documental informática irá migrando lentamente hacia una posición prioritaria, a medida que la tecnología y las herramientas (especialmente comerciales) se popularicen y sean aceptadas como hechos normales entre la sociedad y en particular entre los operadores del derecho.

La documental informática debe estar respaldada por la prueba de informes y la

prueba pericial informático forense, constituyendo un único cuerpo probatorio interrelacionado y autosuficiente, en soporte de nuestra argumentación planificada.

No todo lo que se puede imaginar se puede probar, es ésta una regla aplicable a cualquier argumentación y en relación con cualquier prueba. Sin embargo, se vuelve especialmente crítica respecto de la documental informática. En nuestra planificación, no todo lo que se pretende recolectar es factible de recolección, ya sea por restricciones legales, procedimentales (criminalísticas) y/u operativas (informáticas). Se hace necesario, trabajar de manera transdisciplinaria con el experto en informática forense.[33] De ahí que para seleccionar la documental informática se debe determinar la factibilidad de comprobarla por medio de una prueba de informes o de una pericia informático forense, descartando los elementos superfluos, inconducentes, irrelevantes, redundantes y sobreabundantes. Esta tarea le resultará sumamente fácil a un abogado en lo que hace a la preparación de la prueba documental clásica, pero no es una tarea tan sencilla en cuanto a la documental informática.[34] Es mejor asesorarse antes que fracasar más tarde o lo que es peor ser atacado con nuestras propias evidencias (ya sea para impugnar o para contra-argumentar).

La verdad procesal no siempre coincide con la verdad material. La selección de los elementos probatorios útiles a nuestra estrategia argumental no es una tarea equitativa, la posición del abogado de la parte (sin caer en actitudes antiéticas, ni delictivas) es por supuesto tendenciosa por naturaleza. Si nuestro abogado no está de nuestra parte, entonces, ¿quién podrá defendernos? Pero esto no significa que se recolecten sólo las evidencias a nuestro favor y se ignoren los elementos que puedan contradecirnos. Partimos de lo que nuestro cliente nos dice y ¿quién podría ser más tendencioso, que nuestro cliente, respecto de temas judiciables, que le afectan directamente (vital, liberal o patrimonialmente)?, ¿acaso no somos los mejores para justificar nuestros propios fracasos y atribuirlos siempre a razones exógenas, que casi siempre involucran directa o indirectamente a otros actores? Una buena estrategia argumentativa debe incluir la mayoría de las situaciones posibles, si sabemos cómo atacar y defendernos es bueno, pero si sabemos cómo nos atacará y se defenderá la contraparte es mucho mejor. En lo técnico esta información nos tiene que ser proporcionada por el experto consultado, no sólo desde lo pura y estrictamente relacionado con nuestra pretensión, sino también con aquellos elementos probatorios que puedan ser utilizados en nuestra contra. Como sugerencias generales, podemos decir:

Respecto de los operadores del derecho: planifiquen más, busquen asesoramiento técnico especializado, pregunten detallada y claramente al experto, entiendan, atiendan, comprenda y asimilen; intenten resumir e integrar los puntos periciales a lo estrictamente imprescindible;

Para los peritos: están efectuando una tarea de asesoramiento, no una labor pericial, comprometerse con la causa no implica trasgresión ética alguna: *"estamos asesorando, no concluyendo un informe pericial"*, todo profesional debe ser capaz de adaptarse a los diferentes roles que sus clientes le requieran. Están en libertad de decidir no asesorar, de la misma forma en que un abogado puede decidir no participar de un pleito legal (por la razón que sea), pero si aceptamos asesorar, entonces asesoremos de manera integral y completa, utilizando el máximo de nuestra aptitudes y capacidades.[35]

era integral. Aproveche las herramientas informáticas en tal sentido. Existen varias aplicaciones que le permitirán construir un modelo de los hechos controvertidos y relacionarla con las pretensiones de su cliente. En general todos requieren de la determinación clara del punto de partida (marco de referencias), las variables involucradas (elementos probatorios seleccionados) y el fin pretendido (objetivo a alcanzar). La lógica no es su enemiga, debería ser su aliada, el uso de tablas y árboles de decisión es común en otras disciplinas, ¿por qué debemos tercamente negarle esta utilidad dentro del derecho? Complementar nuestra planificación con diagramas sencillos y de fácil utilización como ser Pert y Gantt, puede ser una medida concurrente a organizar nuestra tarea. Si sirven para planificar una construcción, una fabricación, un proyecto administrativo, ¿por qué no usarlo en nuestra tarea profesional diaria? Lo usan hasta los estudiantes secundarios. ¿Qué otra cosa nos limita, más que nuestros propios prejuicios? Compruebe metódica y sistemáticamente las relaciones entre las tres pruebas informática principales (documental, de informes, pericial), luego de comprobar, complete o depure hasta obtener una línea de demostración argumental, clara, precisa, específica y conducente.

Consideraciones particulares a tener en cuenta al recolectar la prueba documental informática:

Exprese al experto sus necesidades y requerimientos en lenguaje sencillo. Uno de los problemas principales en la comunicación transdisciplinaria es la diversidad de lenguajes, una auténtica torre de Babel construida y destruida por los mismos actores que participan de en dicho diálogo. A esto se agrega la innata necesidad de figurar y aparecer como docto e incomprensible (una especie de Heráclito de la respectiva profesión). Sin embargo, en casi todos los casos, tenemos un lenguaje en común, que la mayoría manejamos en mayor o menor medida, nos referimos al castellano. Si a veces somos capaces de entendernos con nuestros hijos utilizando dicho ingenio, ¿por qué no usarlo con los profesionales de otra disciplina? Basta con bajar el nivel técnico y aumentar el nivel de castellano para que siempre se pueda llegar a una comprensión aceptable.[36]

Para que el diálogo llegue a buen término, requiere por supuesto que la contraparte dialogal haga un esfuerzo por entender lo que el requirente pretende decirle. Es común escuchar por parte de informáticos experimentados la frase *"el cliente nunca sabe lo que quiere"*, en realidad lo más probable es que quien escucha no lo esté haciendo, que no ponga el suficiente interés en lo que pretenden decirle, que no tenga los conocimientos técnicos propios necesarios para dar respuesta a la requisitoria o que simplemente carezca de las aptitudes y actitudes necesarias para comunicarse con los demás. Un profesional de la Informática debe estar capacitado para realizar un relevamiento completo y exhaustivo de una situación real en funcionamiento. A partir de dicho relevamiento, se podrá generar un modelo de aplicación que resuelva las necesidades del sistema evaluado. Luego el análisis de modelo confeccionado permitirá determinar si éste es o no computable. En nuestro caso estamos ante una especie del género prueba documental, prueba que funciona adecuadamente hace siglos, representarla adecuadamente, desde el punto de vista informático, es sólo un problema más a digitalizar, a partir de un modelo de comportamiento, que debe generar el profesional informático cualquiera sea el tenor del mismo y la cultura informática del cliente que lo solicita. Si ni siquiera podemos modelar la situación, el problema ya no está en la realidad, sino en nuestra idoneidad profesional.[37]

Asuma el rol de intermediario entre el experto y su cliente (siempre debe estar presente, ya que es quien puede decir dónde está situada la información pertinente para nuestro caso), de esta interacción tripartita y de la puesta en común de sus ideas, depende el éxito de su plan de pleito. Ocupe su rol mediador, conciliador; componer las cosas en ese momento es evitar disgustos más tarde.

Al seleccionar la prueba documental a recolectar utilice el criterio más estricto posible para reducir la misma a lo estrictamente necesario para fundar su pretensión. Aunque la sobreabundancia no debería producir efectos negativos, siempre otorga más posibilidad de generar mecanismos dilatantes en la contraparte. *"Somos dueños de los silencios y esclavo de las palabras."* La selección debe tener como objetivo brindar soporte a la argumentación y relacionarse directamente con las pruebas de informes y pericial.

Luego de la recolección y preferentemente en el mismo acto, debe preparar un borrador con las solicitudes de certificación por informes y los puntos de pericia a presentar junto con la documental informática.

Al momento de interactuar con el experto, el abogado debe tener en cuenta que éste no siempre posee la formación legal necesaria y suficiente para actuar de manera adecuada en preservación de la prueba recolectada, en especial desde el punto de vista procesal. Dependiendo de la formación académica del mismo, los conocimientos

procesales pueden ser realmente escasos (algo similar pasa con los conocimientos criminalísticos de los abogados), de ahí la importancia de la interacción mutua. El abogado debe asegurarse de que el experto entienda y asimile la importancia en el cumplimiento de plazos y citaciones, desde el momento de la recolección de prueba en adelante y hasta la finalización del proceso. Por ejemplo y no taxativamente, se lo debe instruir respecto de su carácter general de "testigo experto", por lo que no deja de soportar los requisitos, prevenciones y exigencias de otros testigos, aunque su responsabilidad resulte mayor. También debe conocer la importancia y seriedad de su tarea, especialmente en lo que se refiere al falso testimonio y a las diferentes formas de confesión, aceptadas por el Derecho Procesal, incluidas las responsabilidades legales y patrimoniales, que podría generar una incomparencia injustificada:

Confesión expresa: La más simple de todas, la contraparte se aviene a nuestra pretensión y *"a confesión de parte relevo de prueba"*. En lo referente al experto reconocimiento expreso de un error de apreciación técnica, injustificado, puede conllevar el procesamiento por falso testimonio determinado en el artículo 449 del Código Procesal Civil y Comercial de la Nación.[38]

Confesión ficta:[39] La forma canónica, expresada en el artículo 417 del texto jurídico citado *ut supra*.[40] En lo referido a la incomparencia requiere tres condiciones:

Notificación previa.

Intimación a considerarlo confeso en caso de incomparencia.

Incomparencia injustificada.

Confesión tácita: Se conforman analógicamente mediante formas irregulares de la confección ficta, establecidas en los artículos 413, 414, 437 del antes citado cuerpo legal.

Confesión extrajudicial: Aunque no debería constituir ninguna preocupación dentro del mecanismo que se está implementando, lo cierto es que las afirmaciones ciertas, pero situadas fuera de contexto, pueden ser sumamente perjudiciales para nuestro plan y constituirse en elementos dilatorios, muchas veces imposibles de revertir. De ahí la necesidad de mantener la más absoluta reserva respecto de las acciones iniciadas por parte de todos los participantes en la tarea (abogado, escribano, perito, partes presentes), despejando momentáneamente el lugar de todas aquellas personas que no sean imprescindibles para la tarea (otros empleados, amigos, familiares, colaboradores innecesarios, etc.).[41]

Recuerde:

La certificación por escribano público. La cadena de custodia estricta.

32 “CAPÍTULO II DILIGENCIAS PRELIMINARES ENUMERACIÓN. CADUCIDAD, Art. 323. El proceso de conocimiento podrá prepararse pidiendo el que pretenda demandar, o quien, con fundamento prevea que será demandado:…Salvo en los casos de los incisos 9, 10 y 11, y del artículo 326, no podrán invocarse las diligencias decretadas a pedido de quien pretende demandar, si no se dedujere la demanda dentro de los TREINTA (30) días de su realización…

”TRÁMITE DE LA EXHIBICIÓN DE COSAS E INSTRUMENTOS, Art. 325. La exhibición o presentación de cosas o instrumentos se hará en el tiempo, modo y lugar que determine el juez, atendiendo a las circunstancias. Cuando el requerido no los tuviere en su poder deberá indicar, si lo conoce, el lugar en que se encuentre o quién los tiene. ”PRUEBA ANTICIPADA Art. 326. Los que sean o vayan a ser parte en un proceso de conocimiento y tuvieren motivos justificados para temer que la producción de sus pruebas pudiera resultar imposible o muy dificultosa en el período de prueba, podrán solicitar que se produzcan anticipadamente las siguientes: …2) Reconocimiento judicial o dictamen pericial para hacer constar la existencia de documentos, o el estado, calidad o condición de cosas o de lugares. 3) Pedido de informes. 4) La exhibición, resguardo o secuestro de documentos concernientes al objeto de la pretensión, conforme lo dispuesto por el artículo 325…

”PEDIDO DE MEDIDAS PRELIMINARES, RESOLUCIÓN Y DILIGENCIAMIENTO, Art. 327. En el escrito en que se

solicitaren medidas preliminares se indicará el nombre de la futura parte contraria, su domicilio si fuere conocido y los fundamentos de la petición. El juez accederá a las pretensiones si estimare justas las causas en que se funda, repeliéndolas de oficio en caso contrario. La resolución será apelable únicamente cuando denegare la diligencia. Si hubiese de practicarse la prueba se citará a la contraria, salvo cuando resultare imposible por razón de urgencia, en cuyo caso intervendrá el defensor oficial. El diligenciamiento se hará en la forma establecida para cada clase de prueba, salvo en el caso de la pericial, que estará a cargo de un perito único, nombrado de oficio. PRODUCCIÓN DE PRUEBA ANTICIPADA DESPUÉS DE TRABADA LA LITIS, Art. 328. Después de trabada la litis, la producción anticipada de prueba sólo tendrá lugar por las razones de urgencia indicadas en el artículo 326, salvo la atribución conferida al juez por el artículo 36, inciso 4).

”RESPONSABILIDAD POR INCUMPLIMIENTO, Art. 329. Cuando sin justa causa el interpelado no cumpliere la la orden del juez en el plazo fijado, o diere informaciones falsas o que pudieren inducir a error o destruyere u ocultare los instrumentos o cosas cuya exhibición o presentación se hubiere requerido, se le aplicará una multa que no podrá ser menor de PESOS CUARENTA MIL ($ 40.000) ni mayor de PESOS SIETE MILLONES ($ 7.000 000) sin perjuicio de las demás responsabilidades en que hubiere incurrido. La orden de exhibición o presentación de instrumento o cosa mueble, que no fuere cumplida, se hará efectiva mediante secuestro y allanamiento de lugares, si resultare necesario. Cuando la diligencia preliminar consistiere en la citación para el reconocimiento de labligación de rendir cuentas y el citado no compareciere, se tendrá por admitida dicha obligación y la cuestión tramitará por el procedimiento de los incidentes. Si comparece y niega que deba rendir cuentas, pero en el juicio a que se refiere el artículo 652 se declarare que la rendición corresponde, el juez impondrá al demandado una multa que no podrá ser menor de PESOS CINCUENTA MIL ($ 50.000) ni mayor de PESOS OCHOCIENTOS MIL ($ 800.000) cuando la negativa hubiere sido maliciosa. Si correspondiere, por la naturaleza de la medida preparatoria y la conducta observada por el requerido, los jueces y tribunales podrán imponer sanciones conminatorias, en los términos del artículo 37.”

33 Un lugar común en la jerga especializada es; *“somos peritos, no hacemos magia y aunque no lo crean el sentido común aún está vigente”.*

34 Por ejemplo,establecer la dirección IP, asociada a una cuenta de correo electrónico en un determinado momento, es una tarea factible en general,

determinar la dirección física (MAC) de la máquina relacionada, ya es más complejo (la mayoría de las empresas y también muchas casas particulares reciben sus servicios en una entrada general, a partir de la cual se coloca un enturador muchas veces inalámbrico y se distribuye la señal en todos los locales necesarios) y

comprobar quién fue el operador que creó el mensaje cuestionado no es un punto pericial informático forense, ya que depende de otras circunstancias imposibles de determinar por estos medios. Pensemos en una máquina compartida por toda una familia, donde la clave del correo electrónico también es conocida por varios de sus integrantes. En el peor de los casos, ¿estamos seguros cuando mantenemos una comunicación en línea (chat), que la otra persona es quien dice ser?, ¿sabemos si está actuando en pleno uso de sus facultades y libertades?, ¿nos consta que no está siendo víctima de un secuestro u otra forma de coerción? (reiteramos lo dicho en la referencia de la nota al pie anterior).

35 Estamos ante una situación sumamente complicada. El folklore profesional ha creado una concepción que no siempre se ajusta a la verdad (material, lógica, procesal o la que fuere): *“cuando un*

abogado te llama, es porque está intentando corromperte (o aumentar tu corrupción)". Lo cierto es que la corrupción no es el género, sino la especie y no todos forman parte de esta especie (aunque la experiencia diaria parezca negarlo). Una cosa es actuar como perito oficial o de oficio, en una causa, donde la objetividad científica, tecnológica y técnica, deben ser en lo posible absolutas, otra distinta es actuar como perito de parte (o asesor técnico), las tareas son disímiles, los objetivos son distintos, las pretensiones son diferentes. Cuando nos llaman para impugnar una pericia, es improbable analizar el tema de manera absolutamente imparcial y objetiva (algo que por otra parte es imposible para la naturaleza humana, conformada particularmente de subjetividad). La solución a esta situación dicotómica no se debe buscar únicamente en la desconfianza, sino que debe partir de un claro entendimiento y una profunda comprensión del derecho que nos atañe, nos limita y nos faculta (falso testimonio, carácter testimonial de la pericia, razones de excusación y recusación, normas procesales aplicables al caso en particular etc.).*El comedido siempre sale mal:* Se produce la absurda situación en la cual asesoramos mejor a un familiar, amigo o compañero de trabajo, que al profesional que nos consulta de manera onerosa. El experto suele llegar al extremo en que gratuita y cándidamente, explica cómo decodificar una tabla de contraseñas (SAM), o cómo acceder a un Sistema Operativo con privilegios de administrador utilizando la herramienta adecuada, sin detenerse a considerar que este asesoramiento lo puede convertir en partícipe primario (necesario) de un delito efectuado utilizando los procedimientos que recomendamos. Determinada la cadena causal por el juez o el fiscal que intervienen comprueban que el delincuente no pudo lograr su cometido sin nuestros datos técnicos. ¿Qué deben pensar ante el hecho anterior? ¿Cómo les explicamos *a posteriori* y desde el interior de la celda, que lo hicimos de *"puro comedidos nomás"*? Si no ocurren más procesamientos por este tema, es más por la benevolencia de los jueces y fiscales, que por falta de oportunidades comprobables. Adoptamos una posición desconfiada y prejuiciosa respecto de todo y de todos (en particular hacia los abogados), al menos seamos equitativos y asesoremos al que nos paga con el mismo interés y compromiso que lo hacemos con nuestros allegados a título gratuito. Ser íntegros como profesionales, ser éticos como tales, implica asesorar de manera adecuada y completa, informar sobre datos no percibidos por el requirente, destacar peligros en la selección de la prueba, no conlleva delinquir, para saber ¿cuándo estamos transgrediendo la ley?, ¿cuándo estamos excediendo nuestra responsabilidad como asesores,para entrar en el terreno de la complicidad?, basta con recurrir al derecho vigente (estudiar, normalmente no daña al que estudia).

36 Usted le dice a sus hijos que *"junten los juguetes"*, sin embargo ante un colega habla de la teoría de *"conglobación por instituciones"*, es mejor adecuar su lenguaje al que usa con sus hijos y ser entendido y comprendido, que hablar técnicamente pero sólo para usted mismo. Recordemos que muchas veces el tantas veces referido lenguaje técnico, o no lo es tal o se da directamente de patadas con el lenguaje natural (a partir del cual, nos guste o no, se construyó nuestra sociedad y se desarrolló nuestra civilización. Por ejemplo, nos referimos a *"penas privativas de la libertad".* Desde el lenguaje natural privar es impedir absolutamente, quitar de cuajo, erradicar y libertad se refiere a todo tipo de libertad (caminar, respirar, comer, dormir, pensar entre otras especies del referido género). Por lo tanto esta pena sólo puede ejecutarse mediante la inducción de un coma profundo en el cuerpo del condenado, única manera de impedirles todos los grados de libertad de que dispone (tal vez por razones humanitarias, deberíamos optar por un coma farmacológico, que resulta menos cruento que otras formas más efectivas e inmediatas). Otra solución consistiría en matarlo, pero únicamente para los casos de prisión o reclusión perpetua, ya que es una medida irreversible e imposible de limitar temporalmente (dificultando la reinserción social posterior, para los que creen en una segunda oportunidad). Por supuesto que esto no es lo que se pretende afirmar, sería un absurdo desde todo punto de vista. Se corrige fácilmente utilizando el lenguaje natural, estamos en presencia de una *"pena restrictiva de la libertad ambulatoria",* ya que ni siquiera en este caso es privativa, acaso ¿pretendemos

que permanezca inmovil?, como en el caso de la ilegal, pero no absolutamente derogada pena del "plantón" (representada para los menos jóvenes, en su versión hogareña, por la venerable penitencia), de ninguna manera. Pese a lo evidente de este error lingüístico, analizado desde el lenguaje en uso y empleando el más liso y llano sentido común, no pretendemos cambiar los usos y costumbres, sino lograr un equilibrio adecuado a las necesidades de comunicación y participación que una labor interdisciplinaria requiere. Esta misma recomendación es válida para los criminalísticas e informáticos que tienen tendencias similares.

37 Las consecuencias de esta falta de cooperación mutua interdisciplinaria se hacen evidentes al momento de interactuar en grupos de asesoramiento con fines legislativos. El supuesto diálogo colaborativo termina siendo un "diálogo de sordos contra mudos". No hay forma de lograr que los abogados se callen y dejen de discutir toda afirmación que se realice (especialmente entre ellos) y tampoco de estimular a los informáticos para que hablen (al parecer un estigma profesional, que les impide comunicarse con cualquier elemento que no esté constituido por silicio o plástico). De ahí que se escindan en dos universos antagónicos y luego intercambien artículos legales, logrando que la norma generada resulte naturalmente equívoca, jurídicamente redundante o escasa, socialmente irrelevante, individualmente de cumplimiento improbable y, lo peor de todo contradicatoria para quienes deben hacerla cumplir.La redundancia aparece clara y distinta en normas como la Ley 26388: "*Art. 1°.Incorpóranse como* últimos *párrafos del artículo 77 del Código Penal, los siguientes: El término 'documento' comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión."* Nos gustaría que algún doctrinario del derecho nos explique ¿en qué caso un acto no es un hecho?, ya que el primero es una especie del segundo (algo así como decir "toda representación de mujeres o seres humanos". En fin, complejidades del famoso "lenguaje técnico jurídico", incomprensibles para los legos).

En la ley 25.326, podemos apreciar: *"Art 2° (Definiciones). A los fines de la presente ley se entiende por:…Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso. Art. 21. (Registro de archivos de datos. Inscripción). 1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control… Art. 24. (Archivos, registros o bancos de datos privados). Los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal deberán registrarse conforme lo previsto en el artículo 21."* Por lo tanto la agenda de tapas duras, que obra en mi escritorio. donde anoto los teléfonos, direcciones, matrícula profesional, fecha de cumpleaños, aniversario de casamiento y otros datos sensibles de mis colegas y que comparto con mi esposa, reúne todas las características establecidas en la ley: *es un archivo, no electrónico, formado, almacenado y organizado a mi gusto, accesible por los dos y de uso compartido (no exclusivamente personal).* Estoy entonces obligado a registrarla, junto con los imanes adheridos a nuestra heladera. Sintetizando: *dura lex, sed lex.*

38 *"La confesión expresa, prestada en juicio, constituye en principio plena prueba de la verdad de los*

hechos que han sido materia de ella y no es susceptible de destruirse mediante prueba en contrario, aunque pueda revocarse en el caso de resultar acreditado que fue prestado por error, dolo o violencia." Palacios, Lino. *Manual de Derecho Procesal Civil,* Lexis Nexis, Buenos Aires, 2004, p. 464.

39 *"La confesión ficta produce los mismos efectos que la confesión expresa en cuanto hace a la admisión de los hechos contenidos en la posición o posiciones de que se trate, pero a diferencia de aquélla, es susceptible de desvirtuarse mediante prueba en contrario",* ídem, p. 466.

40 Fallo Banco de la Nación Argentina c/Bellizzi SA. 30/11/76, Cámara Comercial: A Barrancos y Vedia Etcheverry – Silva. Constituye jurisprudencia reiterada, considerar que la confesión ficta tiene pleno valor y priva sobre la negativa en la contestacion de la demanda, siempre que no aparezca desvirtuada por prueba en contrario. (En igual sentido: Sala A, 3.4.64, "Midland comercial sa c/ Bizzotti y cia."; Sala B, 3.9.69, "Santamarina c/ Lorusso"; Sala C, 11.6.71, "Gran Rolado c/La Universal Propaganda SRL"; Sala A, 13.4.78, "González c/ Edgardo Bennati"; Sala A, 10.7.70, "Vita c/ Viviendas Tarzán SA"; Sala C, 7.7.89, "Gimeza Cía. Financiera c/ Iriarte"; Sala A, 22.8.84, "SA para la elab., import. y expor t. y ventas de vermouth... Francesco Cinzano c/ Noemi Zappa de Bono"; Sala A, 19.11.82, "Abaco c/ Marta Martorano".

41 Código Procesal Civil y Comercial de la Nación: "Confesión Extrajudicial. Art. 425. La confesión hecha fuera del juicio, por escrito o verbalmente, frente a la parte contraria o a quien la represente, obliga en el juicio siempre que esté acreditada por los medios de prueba establecidos por la ley. Quedará excluida la testimonial, cuando no hubiere principio de prueba por escrito. La confesión hecha fuera de juicio a un tercero, constituirá fuente de presunción simple." "Un padre que da consejos, / más que padre es un amigo; / ansi como tal les digo; / que vivan con precaución / naides sabe en qué rincón; / se oculta el que es su enemigo." Hernández, José. *La vuelta de Martín Fierro.* Ediciones Argentinas SA Buenos Aires, 1978, Canto 32, verso 1.150, p. 283.

CAPÍTULO 7
INSERCIÓN LEGAL DEL PERITO EN INFORMÁTICA FORENSE LA INSPECCIÓN JUDICIAL

Generalidades

Si bien el derecho es una disciplina que tiende a permanecer estable durante periodos considerables de tiempo, especialmente en lo que se refiere a legislación de fondo y forma, basando su evolución para acompañar a los cambios sociales y culturales lógicos de la estructura de convivencia humana, en la jurisprudencia, la legislación que afecta a las pericias informáticas y al delito informático que las genera, son tan novedosas que se encuentran en estado de planificación o con una implementación en sus primeras etapas.

En este sentido, es muy probable que cuando el lector analice esta descripción legal se hayan producido cambios profundos al respecto. Por lo tanto recomendamos que se efectúe una lectura del texto y una posterior reunión de información actualizada por los medios disponibles en Internet (a tal efectos les adjuntamos una serie de direcciones útiles para efectuar este tipo de consultas) y que dicha actitud se convierte en una norma de acción permanente, mientras practiquen la profesión. Los cambios en la legislación relacionada con los delitos informáticos constituyen la norma y no la excepción a principios del siglo XXI.

A las circunstancias anteriores se suma un elemento más que complica la seguridad jurídica pretendida por todo profesional de las pericias y especialmente por quienes realizan pericias informáticas, este elemento es el carácter federal de nuestro país. Si bien la Ley de Fondo (Código Penal, Civil, Comercial, etc.) son de aplicación a todo el ámbito de nuestro país, facilitando el análisis y control de las acciones necesarias para evitar contravenir sus artículos, por el contrario los Códigos de Forma (Códigos de Procedimientos en lo Penal, Civil, etc.) son jurisdiccionales respecto de cada provincia (salvo en los delitos federales). Estas diferencias imprimen un carácter especial al accionar pericial, dependiendo el mismo de la provincia en que se actúe.

Por otra parte, cada juez en particular estampa en el Juzgado a su cargo alguna nota especial, propia de su forma de trabajar. Esto hace que todos los Juzgados Civiles, sean similares pero no idénticos en su accionar y en las formas de proceder, especialmente respecto de las formalidades de control de los expedientes y de cesión de los elementos probatorios a ser peritados.

Los elementos antes mencionados llevan consigo algunas recomendaciones generales para los peritos:

Profundice sus conocimientos del derecho argentino, en la misma medida en que profundiza sus conocimientos informáticos específicos. Su libertad, la validez de la prueba y la mayor o menor facilidad para que le impugnen un informe pericial, dependen de su conocimiento de la ley.

Cuando haya alcanzado el nivel de conocimientos legales necesario para realizar su labor, mantenga una actitud de permanente consulta en busca de cambios en la legislación relacionada con su labor. Al respecto la participación en grupos de difusión, discusión o consulta profesional, no sólo en el ámbito informático forense, sino también en los Colegios de Abogados y en los Foros de Criminalística le permitirá mantenerse actualizado y reducirá la tasa de errores en su accionar pericial.

Participe activamente de los foros específicos informáticos forenses nacionales e internacionales. Esta actitud le permitirá prever las tendencias en la evolución de la profesión y también el desarrollo legal paralelo a la evolución del delito informático.

El presente desarrollo legal es sumamente breve, pero requerirá más esfuerzo respecto del profesional que desee mantenerse actualizado en materia legal y contar con la protección de la ley en todo momento. Si bien el perito informático forense no necesariamente debe ser un abogado, es preciso recordar que muchas pericias se arruinan, por errores en la requisitoria pericial, por lo que no es imprescindible que un abogado conozca en profundidad sobre criminalística, pero es conveniente. De la misma manera, cuanto más sepa usted de leyes, menos probabilidades tiene de ser procesado y más probabilidades de realizar un informe pericial sólido y contundente, evitando o reduciendo la posibilidad de impugnación. Por lo tanto es necesario tener en cuenta:

Diferencias entre dolo, culpa y preterintencionalidad: Si consideramos ciertos delitos como el homicidio y las lesiones vemos que tienen distintos artículos que agravan o disminuyen la pena para cada caso específico, es así que:

El homicidio simple es tipificado en el artículo 79 del CPN y las lesiones en el 89 del CPN.

El homicidio agravado en el artículo 81, el artículo 90 las lesiones graves y el artículo 91 las lesiones gravísimas.

El artículo 84 para el homicidio y el 94 para las lesiones definen el delito en grado de culpa: ambos artículos coinciden en *“el que por imprudencia, negligencia,*

impericia en su arte o profesión o inobservancia de los reglamentos o de los deberes de su cargo…" Evidentemente exige que el delincuente no haya tenido intención de matar o lesionar y que lo haya hecho por error, descuido, ineptitud o inobservancia en el cumplimiento de las normas a respetar.

El artículo 81 define el caso del homicidio en estado de emoción violenta y del homicidio preterintencional: *"Al que con el propósito de causar un daño en el cuerpo o en la salud, produjere la muerte de alguna persona, cuando el medio empleado no debía razonablemente ocasionar la muerte".*

Tengamos en cuenta entonces que un delito puede ser doloso (intencional), o culposo (sin intención) con algunas figuras marginales como es el caso de la preterintencionalidad. Los delitos que admiten la figura culposa están detallados en el Código Penal, para cada caso en particular (por ejemplo, el homicidio o las lesiones). Sin embargo esto no es aplicable al falso testimonio, los artículos 275 y 276 del CPN, implican dolo. Llevan implícita la intención de mentir, de ninguna manera pueden ser cometidos mediante culpa. Si el perito por inepto, por tonto o simplemente por interpretar mal los datos comete un error y afirma algo que resulta no ser verdadero, no está cometiendo falso testimonio. De ahí que el criterio general de los informáticos que supone que no es lo mismo equivocarse por ineptitud o error de interpretación de los datos que por negligencia es erróneo, que un perito sea negligente, no implica obligatoriamente que sea falaz (ya que la falacia implica la intención de mentir). El perito negligente podrá ser sancionado administrativamente o hasta suspendido, pero nunca procesado por falso testimonio. Sin embargo, es importante tener en cuenta que la determinación de la intencionalidad en la falacia es un problema probatorio y de interpretación del juez, por lo tanto no es conveniente arriesgarse.

En cambio respecto de la participación criminal, el tema es mucho más peligroso. El artículo 45 del CPN dice: *"Los que tomasen parte en la ejecución del hecho o prestasen al autor o autores un auxilio o cooperación sin los cuales no habría podido cometerse, tendrán la pena establecida para el delito…"* Si usted asesora a una persona sobre cómo ingresar a la cuenta del Banco Central y efectuar una transferencia ilegal de fondos, evidentemente no podrá escapar a este artículo. Pero si usted asesora a alguien sobre cómo ingresar a este tipo de cuenta para que se proteja de los ataques y el usuario termina realizando un delito, la prueba sobre su intención de facilitar el delito o no, se vuelve tan sutil, que seguramente aunque no sea condenado, dejará una mancha de duda sobre su prestigio, imposible de eliminar. Sea responsable profesionalmente, no sea partícipe necesario accidentalmente. Si usted decide transgredir la ley, es una opción personal y tiene posibilidades de hacerlo de manera impune o de ser castigado, en este último caso por delinquir; no permita que por ineptitud o excesiva locuacidad termine delinquiendo a partir de su impericia,

imprudencia, inoperancia o simple deseo de figuración. El delinquir es una decisión ética, que ha sido consustancial con el ser humano desde la imposición de las leyes, en cambio la tontería es muy anterior a los códigos y seguramente trascenderá a los marcos legales, sea cuidadoso con sus conocimientos, respetuoso de su profesión y todo lo reservado que su carácter le permita.

Legalidad de la requisitoria pericial

En este sentido podemos considerar a la pericia informático forense como originada en uno de estos dos entornos:

Como resultado de una requisitoria pericial específica, legal y formalmente realizada por un Juzgado en particular.

Como resultado de una acción extrajudicial, originada en una empresa o en un particular que requiere nuestros servicios.

Entorno legal del perito

El accionar del perito está regido por el Código Penal, por los Códigos de Procedimientos, por las legislaciones complementarias y en el mejor de los casos por la supervisión del colegio profesional correspondiente.

Un poco más adelante consideraremos en particular cada caso, sin embargo, es necesario tener en cuenta que toda actividad pericial es una actividad que debe realizar en un determinado marco legal. La Constitución nos protege en nuestra actividad particular y profesional, recordemos que:

Art. 19 de la Constitución Nacional: "[…] Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe".

Este aserto legal, es llamado el "principio de clausura" y pretende convertir al Sistema Jurídico vigente en un sistema cerrado. Para un orden jurídico determinado es imposible normar todas las conductas imaginables en la sociedad a partir del comportamiento de sus individuos. En los distintos universos legales concebibles, se podría optar por establecer normas permisivas, normas prohibitivas y normas facultativas. Nuestro país ha optado por establecer normas prohibitivas en lo referente al derecho penal. Estas normas tipifican infracciones legales, denominadas delitos. El Código Penal y las leyes complementarias tipifican los delitos. Pero ¿qué pasa con el resto de las conductas humanas?, ¿es necesario permitirlas específicamente o está implícito que están permitidas? A esto se refiere el artículo 19 cuando pretende

clausurar el sistema, autorizando a hacer todo lo que no está prohibido. Si se trata de un principio válido y útil, es toda una controversia doctrinaria, que no tiene razón de ser en esta obra. Para quien desee ampliar el tema se sugiere la lectura de la obra *Introducción a la metodología de las ciencias jurídicas y sociales* de Carlos Alchourrón y Eugenio Bulygin (Editorial Astrea, Buenos Aires, 2006), sumamente esclarecedora al respecto. Esta afirmación, además de asegurar la libertad, implica la sujeción a la ley, ya que por el contrario si la ley lo manda se debe cumplir, haciendo o dejando de hacer ciertas cosas, que en definitiva restringen la libertad pero aseguran la convivencia. Para ampliar esta temática y en especial la inserción de la lógica deóntica en la estructura lógica proposicional, se ha agregado un apéndice sintético al finalizar esta obra.

Por lo tanto, tener clara conciencia que cualquier acto que realicemos es susceptible de revisión legal, es la meta a alcanzar y para eso es necesario conocer en profundidad la ley que nos restringe y nos protege. El perito no puede ni debe ignorar el marco de inserción legal de su profesión. La ignorancia no es excusa ante la ley. Nuestras armas están formadas básicamente por la idoneidad profesional, la tecnología disponible y el marco legal en que actuamos. Actúe según sus criterios éticos, pero nunca ignore la ley.

Por otra parte, el perito se encuentra sometido a las disposiciones particulares de cada Código de Procedimientos en particular. Sería imposible en este libro desarrollar todas las diferencias y matices en el acto judicial formal, impuestas por cada jurisdicción. Hemos agregado a este libro los Códigos de Procedimientos de materia penal, de la mayoría de las provincias, cada profesional deberá analizar en profundidad los contenidos de los mismos que acoten su accionar pericial y tener en cuenta que ciertas formas de actuar en un lugar no son exactamente compatibles con las que se utilizan en un lugar próximo geográficamente pero dependiente de otra jurisdicción.

Formalidades de la aceptación del cargo

Esta actividad depende directamente del fuero en que actuemos y de las características propias de la jurisdicción analizada, pero podemos sintetizarla en:

El perito oficial, prácticamente no requiere de esta diligencia. Su propio cargo y actividad profesional, implican que una solicitud pericial, tiene carácter mandatorio y es irrenunciable.

En el caso de actuar como perito de oficio (inscripto como perito, incluido en la lista y preferentemente matriculado), la aceptación del cargo es un requisito legal

ineludible que, con distintas formas y matices, deberá ser realizada en un tiempo limitado y detallado en la cédula de notificación correspondiente.

Respecto de los peritos de partes, normalmente el abogado de la parte que solicita nuestros servicios, se encarga de realizar el pedido correspondiente al Juzgado y de tramitar la cédula de notificación que nos designa, no obstante estamos restringidos formal y temporalmente a las mismas condiciones que el perito de oficio (debemos aceptar el cargo en tiempo y forma).

Diligencias previas en el Juzgado

La pericia informática forense es un caso muy particular de actividad pericial, ya que:

Para realizar una adecuada interpretación de la prueba indiciaria disponible es prácticamente imprescindible contar con un relevamiento adecuado de entorno informático relacionado con dichos indicios.

Si somos designados como peritos oficiales, la estructura que nos rodea seguramente nos proveerá de los elementos necesarios para realizar las diligencias previas al análisis pericial específico. Esto puede implicar entrevistas, relevamiento de áreas de sistemas, inspección judicial, secuestro y traslado de elementos probatorios. Todas estas tareas deben efectuarse con autorización expresa del tribunal interventor.

Si actuamos como peritos de oficio, no contaremos con la estructura que acompaña al perito oficial, por lo que tendremos que solicitar todas aquellas medidas que consideremos pertinentes para analizar metodológicamente los elementos *sub peritia*. La mayoría de los peritos realiza algunos contactos con el Juzgado interventor, sobre todo para pedir adelanto de honorarios en conceptos de gastos periciales, sin embargo, ésta no es la única actividad que se puede realizar con el Juzgado que nos ha designado. A partir del momento de la designación el perito forma parte de la causa, es un testigo de la misma (testigo calificado, pero testigo al fin), en tal sentido es también un colaborador en la investigación del delito, por lo tanto puede interactuar perfectamente con el tribunal. Si bien es cierto que para reclamar honorarios impagos es necesario contar con un abogado que nos represente, lo es también que podemos pedir las medidas necesarias para realizar la pericia. Uno de los ejemplos más comunes es la solicitud por parte de los peritos en documentología, de audiencia para formar cuerpo de escritura a una persona determinada. Esta facilidad debe ser aprovechada por el perito para solicitar todas aquellas medidas previas al análisis real de los datos y que permitan facilitar la tarea (pedido de autorización para efectuar relevamientos o detección de pruebas, en un área de sistemas específica, con el auxilio

de la fuerza pública si es necesario). Siempre teniendo en cuenta que las medidas previas o preliminares de recolección de documental informática son una potestad exclusiva de las futuras partes en el proceso y que el perito sólo puede actuar como asesor al respecto, los trámites de las mismas deben ser realizados por los interesados ante la jurisdicción correspondiente.

Los miembros del tribunal no son expertos en Informática Forense, por lo tanto es nuestra obligación indicarles las medidas necesarias para el mejor desempeño pericial. Por una cuestión de antigüedad de la metodología y de práctica frecuente, ningún empleado de un Juzgado se asombra cuando un perito en documentología solicita formar cuerpo de escritura para realizar su labor, sin embargo, no están acostumbrados a recibir solicitudes relacionadas con la investigación informático forense, es una necesidad para el desarrollo de la profesión ejercer la difusión necesaria que nos permita actuar con la misma naturalidad y aceptación que los documentólogos.

Si actuamos como peritos de parte o consultores técnicos, la situación puede variar acorde con la naturaleza de la pericia, el objeto de la misma y qué parte la solicite. Si la parte que requiere el estudio es la que dispone de los sistemas informáticos realizados, la tarea se facilita sobremanera, si por el contrario los elementos corresponden a la otra parte, deberemos ajustarnos estrictamente a lo expresado en el punto anterior.

Sobre todas las cosas debemos actuar estrictamente dentro del marco legal establecido.

Toda diligencia a practicar debe estar en conocimiento del Juzgado interventor, haber sido autorizada por éste y dichas circunstancias obrar en autos. Respecto de las autorizaciones particulares para ingresar a determinado lugar, efectuadas por las partes, deben ser siempre formales, por escrito y con copia al Juzgado. Muchas veces las relaciones cambian a partir de los resultados periciales y podemos tener un problema serio si actuamos basados en autorizaciones verbales o en manifestaciones de intención. Los seres humanos nos movemos sobre la base de intereses particulares y éstos son altamente mutables témporo-espacialmente. Todos somos confiables y honestos en alguna medida, pero establecer esa medida no es algo tan fácil de realizar, aun para el interesado. *"Si tengo que optar entre que llore tu mamá o que llore la mía, prefiero que llore la tuya".*

Requisitos legales y formales de la inspección judicial

Reiteramos la dificultad de definir estrictamente estos aspectos, ya que se relacionan

con la jurisdicción analizada, el Código de Forma vigente en el lugar, las legislaciones particulares asociadas y la idiosincrasia del aparato judicial concomitante. Pero a modo de ejemplo, les aportamos algunos temas específicos relacionados con la actividad pericial dentro de la Ciudad Autónoma de Buenos Aires, en materia penal. Cada profesional deberá realizar un cotejo entre estos elementos y los que corresponde a su zona de trabajo:

Artículos pertinentes del Código de Procedimientos Penal de la Nación (CPPN)

Actas. Regla General. Art. 138.

Contenido y formalidades. Art. 139.

Nulidad. Art. 140.

Testigos de actuación. Art. 141.

Atribuciones, deberes y limitaciones. Art. 184. Inspección Judicial. Art. 216.

Ausencia de rastros. Art. 217.

Inspección corporal y mental. Art. 218.

Facultades coercitivas. Art. 219.

Identificación de cadáveres. Art. 220.

Reconstrucción del hecho. Art. 221.

Operaciones técnicas. Art. 222.

Registro domiciliario y requisa personal. Art. 224.

Allanamiento de morada. Art. 225.

Allanamiento de otros locales. Art. 226.

Allanamiento sin orden. Art. 227.

Formalidades para el allanamiento. Art. 228.

Autorización del registro. Art. 229.

Requisa personal. Art. 230, Art. 230 bis.

Secuestro Orden de Secuestro. Art. 231.

Orden de presentación. Art. 232.

Custodia del objeto secuestrado. Art. 233 (Sumamente importante para el accionar pericial sobre los elementos secuestrados o sus copias.)

Interceptación de correspondencia. Art. 234.

Apertura y examen de correspondencia. Secuestro. Art. 235.

Intervención de comunicaciones telefónicas. Art. 236 (Muy importante para el perito por las posibles intercepciones de comunicaciones o transferencias de datos digitales.)

Documentos excluidos de secuestro. Art. 237 (Ídem anterior.)

Devolución. Art. 238.

Testigos. Deber de interrogar. Art. 239.

Obligación de testificar. Art. 240. (El perito es un testigo experto.)

Capacidad de atestiguar apreciación. Art. 241. (Valoración del testimonio por la sana crítica.)

Prohibición de declarar. Art. 242. (Es también una causa de excusación para el perito.)

Facultad de abstención. Art. 243. (Ídem anterior.)

Deber de abstención. Art. 244. (Ídem anterior, hay que tener cuidado con la facultad del juez de liberar al experto de su deber de guardar secreto.)

Compulsión. Art. 247.

Peritos. Facultad de ordenar pericias. Art. 253

Calidad habilitante. Art. 254. (Los peritos deberán tener título de tales en la materia a que pertenezca el punto sobre el que han de expedirse…)

Incapacidad o incompatibilidad. Art. 255.

Excusación o recusación. Art. 256. (Sin perjuicio de lo dispuesto en el artículo anterior, son causas legales de excusación o recusación de los peritos las establecidas para los jueces).

Obligatoriedad del cargo. Art. 257. (Art. 154.)

Nombramiento y notificación. Art. 258.

Facultad de proponer. Art. 259. (Peritos de parte.)

Directivas. Art. 260.

Conservación de objetos. Art. 261. (Preservar para permitir repetir las experiencias, autorización judicial para destruir la prueba como consecuencia de las experiencias sobre la misma.)

Ejecución. Peritos nuevos. Art. 262.

Dictamen de apreciación. Art. 263. (Informe pericial o constancia en acta.)

Autopsia necesaria. Art. 264.

Cotejo de documentos. Art. 265.

Reserva y sanciones. Art. 266.

Honorarios. Art. 267.

Artículos referidos en el artículo 184

Incomunicación. Art. 205.

Allanamiento sin orden. Art. 227.

Requisa personal. Art. 230. Art. 230 bis.

Secuestro Orden de Secuestro. Art. 231.

Arresto. Art. 281.

Flagrancia. Art. 285.

Derecho del imputado. Art. 104.

Defensor y domicilio. Art. 197.

Asistencia. Art. 295.

Libertad de declarar. Art. 296.

Formalidades previas. Art. 298.

Fin artículos referidos en el artículo 184.

En este punto es necesario considerar un tema en particular: el acceso a la correspondencia de una persona en especial, debemos recordar al respecto que por sobre todas las leyes de la Nación se encuentra la Constitución y que nos dice:

Art. 18 de la CN: "[…] El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación…"

Si bien el correo electrónico no es epistolar y el mismo puede constituir un servicio particular específico de la empresa contratante, limitado específicamente por una relación contractual, al uso interno y específicamente laboral en la empresa, existen otros correos que son particulares de cada persona y que cuyo acceso no ha sido autorizado por su propietario. Existe amplia jurisprudencia que equipara el Correo Electrónico al Correo Epistolar. Para estos casos el CPPN, nos dice:

"Secuestro de correspondencia: prohibición. Art. 185. Los funcionarios de la policía y fuerzas de seguridad no podrán abrir la correspondencia que secuestren, sino que la remitirán intacta a la autoridad judicial competente; sin embargo, en los casos urgentes, podrán ocurrir a la más inmediata, la que autorizará la apertura si lo creyere oportuno."

Para su accionar particular considere los siguientes principios generales:

Si el correo electrónico a vulnerar es propietario de la empresa y ha sido entregado a los empleados con fines específicamente laborales, dicha circunstancia debe obrar en el contrato del empleado, pero aun así puede ser cuestionado por el empleado que fue obligado a firmar el contrato o que debió firmarlo para acceder al empleo *(in dubio pro operario)*. Exija ver ese contrario y actúen en consecuencia. No dé por sentado que todo correo electrónico propietario de una empresa implica la facultad de violarlo por parte de dicha empresa.

Nunca (salvo que disponga de orden judicial escrita) proceda a la lectura de correos electrónicos obrantes en servicios externos a la empresa (aunque se trate de empresas subsidiarias o asociadas), pida siempre la correspondiente autorización legal.

Lea en profundidad el artículo 234 del CPPN.

Responsabilidad legal del perito informático forense: posesión, protección, análisis, preservación y devolución de la prueba

Consideramos innecesario destacar la responsabilidad directa del perito durante la posesión de los elementos probatorios que le fueran entregados en custodia. Especialmente es necesario tener en cuenta:

La prueba indiciaria informático forense generalmente se encuentra alojada en soportes de información magnéticos u ópticos.

Los soportes magnéticos son altamente sensibles a los campos electromagnéticos y juntamente con los ópticos a los cambios bruscos de temperatura o exposiciones directas a los agentes ambientales. Por ejemplo, muchos hemos comprobado lo que puede pasarle a un disquete o a un CD si lo dejamos bajo la luneta trasera de un vehículo, en una playa descubierta, una tarde de verano.

Los puntos anteriores implican que debemos tomar precauciones especiales para proteger la prueba. Pero dichas protecciones no superan las que debemos tener como profesionales para proteger la información propia o de nuestros clientes.

Por otra parte siempre existe el riesgo de que la prueba sea accedida por personas que no deberían tener acceso a la misma. En este sentido los únicos autorizados a tener contacto con la prueba son el perito y sus colaboradores periciales obrantes en el informe pericial.

La prueba informático forense es fácil de destruir, copiar o modificar, contando con elementos adecuados, fáciles de obtener y conocidos por cualquier persona con una formación computacional adecuada.

Sin embargo, tiene una ventaja particular: se puede copiar estrictamente. Es decir se puede generar un clon idéntico al original. Esta circunstancia que es peligrosa desde el punto de vista del acceso de terceros, juega en nuestro favor en esta oportunidad.

Para eludir responsabilidades innecesaria, lo ideal es:

realizar un *hash* de la prueba ofrecida en el juzgado,

efectuar una copia bit a bit de la prueba,

realizar un *hash* de la copia,

comparar que sean idénticos,

devolver la prueba original,

trabajar sobre la copia.

Las diligencias expresadas en el punto anterior deben ser informadas al Juzgado. Es conveniente concurrir a aceptar el cargo y en el mismo momento presentar un escrito solicitando autorización para actuar de la manera descripta. Esta solicitud debe ser adecuadamente fundamentada, ya que no sólo facilita nuestra tarea, sino que lentamente difunde entre los neófitos la naturaleza especial de la prueba informática y facilita el análisis de la misma (ya sea con fines periciales, o con fines de evaluación judicial, si quien debe juzgar sabe más, indudablemente juzga mejor).

En el caso en que secuestre elementos probatorios en el lugar del hecho, cambie comodidad por seguridad. Sugiera la conveniencia de trasladar la prueba al juzgado y no a su laboratorio y luego ejecute las acciones recomendadas. Es cierto que agregará un paso más a la labor, pero su responsabilidad con la protección de la prueba será mínima.

Legislación de fondo, el perito como testigo y el falso testimonio

El perito no es otra cosa que un testigo y como tal se encuentra limitado en su accionar por el Código Penal en lo que se refiere al falso testimonio:

Art. 275 del CPN: “Será reprimido con prisión de un mes a cuatro años, el testigo, perito o intérprete que afirmare una falsedad o negare o callare la verdad, en todo o en parte, en su deposición, informe, traducción o interpretación, hecha ante la autoridad competente.

”Si el falso testimonio se cometiere en una causa criminal en perjuicio del inculpado, la pena será de uno a diez años de reclusión o prisión.

”En todos los casos se impondrá al reo, además, inhabilitación absoluta por doble tiempo del de la condena.”

Art. 276 del CPN: “La pena del testigo, perito o intérprete falso, cuya declaración fuere prestada mediante cohecho, se agravará con una multa igual al duplo de la

cantidad ofrecida o recibida. El sobornante sufrirá la pena del simple testigo falso."

El Código Penal nombra específicamente al perito, la responsabilidad del mismo ante la ley es clara y contundente. En este sentido es interesante destacar que la amplitud de los términos empleados: "*afirmare una falsedad o negare o callare la verdad, en todo o en parte, en su deposición, informe, traducción o interpretación"*, es taxativa respecto de la acción pericial. El perito debe expresar todo lo que sabe respecto de los hechos investigados, es un testigo más. Sin embargo en materia civil, se produce una contradicción difícil de eludir. Estamos legalmente obligados a decir toda la verdad, ya que declaramos ante una autoridad competente, pero debemos limitarnos a responder los puntos de pericia, so pena de ser tildados de conniventes con alguna de las partes. La situación es sumamente delicada, nadie cree en la buena voluntad y el espíritu de investigación del perito, la ley lo obliga a decir la verdad, pero si se extralimita en la respuesta a los puntos periciales, de inmediato cae bajo la sospecha de parcialidad.

En este sentido, el problema deviene en un conflicto ético, la ley dice …*o callare la verdad, en todo o en parte*…, para nosotros como peritos, las conclusiones alcanzadas de manera imparcial y objetiva, fundamentadas científica, criminalística, metodológica, sistemática y técnicamente, son nuestra verdad. Tal vez no sea "*la verdad",* inclusive ésta es muy probable que ni siquiera exista. La problemática del testigo, que ya tratamos en otra parte de este libro, es clara, *"el testigo nunca expone lo que vio, sino lo que cree haber visto"*, si nos atuviéramos estrictamente a la ley, dos testigos que difieren a sus dichos respecto de un hecho determinado, implicarían el procesamiento de uno de ellos por falso testimonio. Siempre subyace el principio *No hay más verdad que la realidad*, pero como la realidad es parte del ser y *el ser es ser percibido*, entonces existe una realidad para cada individuo, quizá con pocas diferencias respecto de la realidad de su prójimo, pero nunca idéntica. *Toda realidad es realidad interpretada.*

No es posible legislar por analogía en Derecho Penal, pero al menos podemos analizar esta problemática de manera más profunda si la tratamos analógicamente. El matar a otra persona constituye un homicidio, nadie lo duda, pero sin embargo, la mayoría estaríamos de acuerdo en diferenciar el homicidio como consecuencia de un acto imprevisible (dos hombres discuten, uno golpea al otro, éste cae, impacta contra el piso y muere), del homicidio intencional (dos hombres discuten, uno de ellos toma un cuchillo y apuñala al otro), del homicidio que nos repugna (un violador estrangula a una nena, para que no pueda denunciarlo). La ley también ha entendido esto y por lo tanto tenemos en el Código Penal tres artículos referidos al homicidio simple (art. 79), al homicidio agravado (art. 80) y al homicidio atenuado (art. 81). El Código no nos habla de distintos homicidios, sino que determina ciertas circunstancias que agravan o

atenúan el acto. En todos los casos el homicidio es intencional, el delincuente, tiene la intención de matar, o por lo menos de herir y lo hace. Se trata de actos dolosos. Pero qué ocurre cuando no existe la intención de lastimar, como en los accidentes de tránsito o en los casos de iatrogenia médica. La muerte se produce y es irreversible, pero la intención del autor nunca fue matar, ni herir, simplemente, no supo o no pudo evitar la consecuencia de sus actos. También en estos casos el Código Penal acude en nuestra ayuda y tipifica el homicidio culposo (art. 84).

No podemos ser tan ingenuos como para pensar que todo perito, por el simple hecho de serlo, se ha convertido en un individuo honesto, incapaz de transgredir la ley y confiable como testigo. Este hecho es conocido por todo el aparato judicial y es una realidad intrínseca de la naturaleza humana. Todo hombre tiene su precio, sea éste económico o no, implica que todo hombre puede ser comprado o extorsionado, para que actúe de determinada manera, en este sentido los sistemas de control de identidad sólo aseguran la filiación de la persona, nunca su libertad para actuar. Llevado hasta las últimas consecuencias, debemos admitir que el hombre no tiene ninguna libertad, ya que no puede *"elegir: no elegir"*, es decir está condenado a elegir, si a esto sumamos que sólo puede elegir entre opciones posibles *"al menos por el momento, no puede: elegir no morir"*, entonces la libertad humana queda restringida a la obligación constante a tomar decisiones basadas en un conjunto limitado de opciones. *El hombre está obligado a optar durante toda su vida.*

Por lo tanto el perito puede faltar a la verdad, al menos de dos maneras posibles, pero fundamentalmente diferentes:

Falsedad Dolosa: El perito para satisfacer deseos propios o ajenos, falsifica los hechos. Evidentemente en este caso el falso testimonio es pleno y no es mucho lo que podamos aportar, la solución de este tema queda restringida a la prueba disponible y al proceso judicial correspondiente:

Falsedad Culposa: El perito convencido de los resultados alcanzados en sus investigaciones y análisis afirma una falsedad, que luego queda demostrada. En este sentido no existe o no debería existir sanción penal para el perito. Actuó de buena fe, su falencia es totalmente culposa. El delito de falso testimonio, no puede, ni debe ser interpretado como un delito culposo, esto implicaría el procesamiento de más del cincuenta por ciento de los testigos y de la totalidad de los testigos contradictorios.

No obstante esta última afirmación no pretende hacerse extensiva a la impunidad absoluta del perito que demuestre reiteradamente errores de apreciación atribuibles a: *"imprudencia, negligencia, impericia en su arte o profesión o inobservancia de los reglamentos o de los deberes de su cargo"*, pero la evaluación de estas circunstancias

debería ser parte de la labor de los colegios respectivos.

La matriculación de los peritos en un colegio determinado, debería constituir un requisito imprescindible para actuar como tal, al menos en aquellas especialidades claramente definidas dentro de la Criminalística. Si tenemos médicos ineptos, muchas personas pueden sufrir innecesariamente, la sociedad y los organismos de control tratan de evitarlo, pero si tenemos peritos ineptos, muchas personas pueden ser privadas injustamente de su libertad o liberadas sin merecerlo, la supervisión de estas profesiones aún se encuentra en pañales en nuestro país, pero la necesidad de reglamentarlas ya no es una cuestión de necesidad, sino de voluntad política. El colegio de pares constituye el organismo natural de selección, evaluación y certificación de profesionales, la simple certificación universitaria a partir de un título o un certificado no es suficiente, la idoneidad sólo se prueba por el examen ante los pares. Éste es un tema álgido y muy discutible, pero profundamente actual y controvertido.

En el primer caso señalado en el párrafo anterior la ley está de nuestro lado. Estamos protegidos y soportados por la validez legal que la requisitoria pericial aporta al acto en sí mismo. En este caso es suficiente con ajustarse a las normas formales impuestas por la ley para la aceptación del cargo pericial, cumplimentar los términos y ante cualquier duda consultar con el Juzgado interventor.

Legislación de forma

Este tema fue parcialmente tratado en el punto anterior debido a la necesidad de realizar una explicación integradora entre los conceptos de inspección judicial y su tratamiento desde los Códigos de Procedimientos. Insistimos en la necesidad de adecuar sus conocimientos a las particularidades de su área de trabajo. Esto se torna especialmente crítico cuando debido a su desarrollo profesional comience a interactuar en diferentes jurisdicciones y fueros judiciales. Es completamente natural que un perito en Informática Forense realice sus tareas en el ámbito de la Ciudad Autónoma de Buenos Aires y en distintas sedes judiciales de la provincia de Buenos Aires, con sus diferentes características y particularidades desde los códigos de fondo y las legislaciones particulares, hasta los actores dentro de la investigación penal (por ejemplo, el principal instigador de la acción penal en la Ciudad Autónoma de Buenos Aires es el juez de instrucción, mientras que en la provincia este trabajo prácticamente ha sido delegado al fiscal).

Legislación complementaria, leyes y proyectos

El problema del delito informático impropio que permite la transgresión de

prácticamente todos los artículos del Código Penal, de manera directa o indirecta, ha sido legislado por la ley

26.388. En cuanto a los delitos informáticos propios (la afectación es directa al bien jurídico protegido o a proteger denominado *información*), es un tema poco analizado y que requiere de mayor profundización legislativa, al menos al momento de redacción de este texto. Se torna evidente la necesidad de:

Nueva legislación de forma, para dar soporte legal a los métodos de investigación, sin afectar la confidencialidad asegurada a cada ciudadano sobre sus actos privados. (Dirección Nacional de Protección de Datos Personales).

Nuevas formas de auditoría informática para la detección de intrusiones a los sistemas de información en uso.

Nuevos métodos informáticos de análisis y recuperación de la información.

Nuevas reglas gerenciales de protección de la información, para asegurar la privacidad de las empresas y evitar los daños resultantes del espionaje industrial y/o comercial.

Nuevas técnicas criminalísticas que aseguren la recuperación, preservación y análisis de la prueba indiciaria resultante de los delitos informáticos (entre ella la prueba documental informático y sus protocolos de gestión).

Nuevas carreras universitarias que permitan la formación de peritos en informática forense (terciarias o tecnicaturas), o carreras de grado a igual tenor (licenciaturas) o especializaciones de postgrado para los profesionales ya formados (especialidad o maestría).

La suma de estas acciones se traducirá con seguridad en un futuro inmediato en nuevas leyes y reglamentaciones que permitan lidiar con el delito informático.

Jurisprudencia

El derecho en nuestro país no es absolutamente jurisprudencial. Es decir no es sujeto estricto de opinión. Sin embargo la jurisprudencia es una fuente del derecho y una fuente a considerar dada su importancia relativa para un determinado lugar y momento histórico. La capacidad del juez para interpretar la ley es una característica de los sistemas legislativos democráticos. No siempre ha sido así, pero el no considerarla implica un índice de mutabilidad muy alto en los contenidos legales de los códigos. La aplicación estricta y sin interpretación de la ley es imposible, ya que

todo hombre está inhibido de conocer la naturaleza real de su entorno y se limita a relacionarse con el mismo por medio de los sentidos y su propia concepción psicológica de los elementos percibidos. Al respecto Cesare Beccaria en su obra *De la naturaleza de las penas*, nos dice textualmente: *"Ni siquiera la autoridad de interpretar las leyes penales puede residir en los jueces criminales por la misma razón de que no son legisladores" "[…] En cada delito se debe hacer del juez un silogismo perfecto: la mayor debe ser la ley general y la menor la acción conforme o no a la ley; la consecuencia, la libertad o la pena." "No existe nada más peligroso que este axioma común según el cual es necesario consultar el espíritu de la ley." "Cada hombre tiene su punto de vista, cada hombre en tiempos diferentes tiene un punto de vista diferente" "…vemos los mismos delitos castigados de manera diferente por el mismo tribunal en tiempos diferentes, por haber consultado no a la voz constante y fija de la ley, sino a la errante inestabilidad de las interpretaciones."* Aunque la voz de Beccaria nos resulta sumamente atrayente, la realidad es que la jurisprudencia existe y actúa sobre la interpretación de la ley, analizaremos como ejemplo algunos elementos al respecto:

Es prueba facultativa (la inspección judicial) que el juez puede conceder o negar (Cám. Crim. y Correc., "L.L.", 10-653; 16-1233, y "J.A.", 62-214; 69-209, respectivamente).

El artículo 111 (actual 119) sólo tiene por objeto fijar reglas para la instrucción del sumario (S.C., 10-VII-103), a fin de obtener la mejor forma para la comprobación del hecho delictuoso, pero no tiende a hacer indispensable ese medio de comprobación, ni excluye a otros aceptados en el procedimiento penal para probar los hechos (S.C., 8-VI-278; 14-V-304), ni se infringe la disposición al dar valor de plena prueba al croquis no firmado si en acta anterior se lo menciona expresamente y ha sido firmado por el sumariante y testigos (S.C., "J.A.", 21-1085).

"C. F., D. A. s/extorsión", la sala de Feria B de la Cámara del Crimen (integrada por Luis María Bunge Campos y María Laura Garrigós de Rébori), confirmó el procesamiento de tres personas por "secuestros virtuales", pero modificó la calificación legal del hecho considerado como extorsión por el juez de primera instancia, considerando que se trata de una modalidad de estafa. Desde el Complejo Penitenciario de la Ciudad Autónoma de Buenos Aires, algunos detenidos realizaban "secuestros virtuales", efectuaban llamadas telefónicas y simulaban tener secuestrados a familiares de las víctimas, exigiendo dinero a los interlocutores. Aunque el juez de primera instancia sostuvo que la calificación legal era la de extorsión, los camaristas explicaron que *"si bien en este estadio procesal la tipificación legal escogida es provisoria, lo cierto es que en el presente caso se advierte que* ésta *puede afectar otros institutos, motivo por el cual señalaremos nuestra discrepancia con el encuadre*

legal asignado por el juez a quo”. “Entendemos que no nos hallamos frente a sucesos de extorsión, sino que la conducta desplegada encuadra en el delito de estafa”. “En la extorsión la acción típica consiste en obligar a otro mediante intimidación, a entregar, enviar, depositar o poner a su disposición o a la de un tercero, aquello que constituye objeto del delito pero siempre por medio de amenazas y éstas *no son más que el anuncio de un daño que se producirá en el caso de no cumplir con lo exigido, extremo que nunca podría haber ocurrido, toda vez que los dichos amenazantes proferidos por el imputado no se hubieran podido concretar al tratarse de un ‘secuestro virtual’”.* De esta forma confirmaron el procesamiento de los imputados, modificando la calificación legal por la del delito de estafa reiterado en doce oportunidades, en concurso real con el de estafa en grado de tentativa.

El análisis de casos, la revisión de nuestros trabajos anteriores, el estudio de la actividad de otros peritos, deben constituir nuestra fuente de consulta permanente. Debemos generar una auténtica “jurisprudencia” pericial, que nos aporte normas generales estrictas de comportamiento y trabajo profesional, sólo así lograremos regular de hecho (y con suerte de derecho) nuestra profesión. La reglamentación profesional de la informática forense debe ser un anhelo permanente de todo profesional que se precie de tal. La actual situación de anarquía e indefinición sólo contribuye a deteriorar la imagen de una actividad en pleno desarrollo y que recién comienza a desplegar sus alas. No es necesario esperar a que la criatura se termine de desarrollar para establecerle normas que la limiten, le brinden soporte, la ayuden a crecer y en definitiva contribuyan a su crecimiento y credibilidad.

CAPÍTULO 8
ACTIVIDADES PERICIALES COMPLEMENTARIAS

La aceptación del cargo

Cuando la requisitoria pericial proviene de un tribunal es necesario considerar tres situaciones respecto del perito:

El perito es llamado como perito oficial, es decir forma parte de una estructura que lo designa en este sentido y que normalmente está relacionada con Fuerzas de Seguridad, Policías Judiciales u organismos forenses dependientes del Poder Judicial. La aceptación del cargo es un requisito prácticamente integrado en la designación. El perito oficial no podrá excusarse de realizar la pericia (salvo en casos muy especiales, relacionados normalmente con problemas de salud, licencias especiales u otros actividades profesionales específicas que se lo impidan el momento) y su relación estará regida por las normas administrativas de la FFAA, FFSS u organismo del cual depende.

El perito es llamado como perito de oficio. Forma parte de una lista que obra en poder de determinados Juzgados, se ha inscripto como perito en el área judicial correspondiente, en el período establecido y ha fijado un domicilio legal dentro de la jurisdicción considerada. En estos casos, será notificado mediante cédula, que deberá contestar de inmediato (los plazos son establecidos específicamente en la cédula de notificación), concurriendo al Juzgado para aceptar el cargo de perito. Esta formalidad es obligatoria y en caso de existir elementos formales o de fondo que impidan al perito aceptar el cargo (por razones legales, particulares o éticas) deberá manifestarlo ante el tribunal, para no incurrir en falta.

El perito es llamado como perito de partes. Esta propuesta a pedido de las partes puede provenir de la misma lista que en punto anterior, por una recomendación profesional o por cualquier otra razón que induzca al abogado de una de las partes a proponer dicha designación. Se rige por los mismos cánones que el perito de oficio, en lo que se refiere a la notificación y la aceptación del cargo.

El perito actuará a solicitud de un cliente, por ejemplo, en la figura del consultor técnico.

En este caso en muchas jurisdicciones no existe la aceptación formal del cargo, pero

no olvidemos que este hecho no nos dispensa de las posibles transgresiones legales, normativas o éticas a que nos sujeta nuestra profesión. Es preferible actuar en todos los casos, siguiendo los mismos principios establecidos para los tres primeros puntos considerados. Si es posible documentar por escrito la solicitud pericial, el alcance de la misma y los objetivos pretendidos, este documento no nos eximirá de responsabilidad, pero permitirá establecer con claridad las razones de nuestro accionar y sus consecuencias.

Notificación por cédula:

La recepción de dicha cédula implica:

La concurrencia inmediata al tribunal que nos cita.

La revisión de la requisitoria pericial, para establecer su pertinencia y nuestra idoneidad profesional para realizarla, tener en cuenta:

Que puede encontrarse en el expediente principal, en el cuaderno de prueba de la actora o en el cuaderno de prueba de la demanda (si es que estos dos últimos han sido formados, acorde a lo establecido en el artículo 380 del Código Procesal Civil y Comercial de la Nación).

En caso de tratarse del expediente principal, la requisitoria podrá encontrarse normalmente en:

La demanda.

Contestación de demanda.

Reconvención.

Contestación de la reconvención.

Menos usualmente en otras partes del principal.

Si los cuadernos existen, siempre debemos revisarlos, aunque la requisitoria provenga del principal o del otro cuaderno. Por aplicación del artículo 458 del Código Procesal Civil y Comercial de la Nación, suele desinsacularse perito único de oficio, a solicitud de una de las partes. Esto no obsta que la otra parte pueda presentar puntos de pericia complementarios a la primera solicitud, acorde a lo establecido en el artículo 459 de la obra citada. De ahí la importancia de revisar la totalidad del expediente principal y sus cuadernos de prueba desprendidos.

Que esté referida a nuestra especialidad informática forense. Muchas veces por error se trata de una pericia contable o de otro tipo.

Controlar la pertinencia de los puntos de pericia, en igual sentido que el apartado anterior.

Aceptar el cargo, acompañando, en el mismo momento, un escrito en el que solicitamos:

El anticipo para gastos autorizado en el artículo 463 del antes citado cuerpo legal.

La suspensión de los plazos procesales, hasta la resolución por las partes del punto anterior.

La inclusión de alguna otra persona, para que pueda acceder al expediente.

Los hechos anteriores harán que el expediente pase a despacho para resolver la aceptación de cargo y las solicitudes presentadas. Por razones de economía procesal, la diligencia resolviendo estos temas, debería ser completa y resolver los tres pedidos. En la práctica, por razones espurias, no suele ser así y cuando volvemos a ver el expediente, nos encontramos con una diligencia simple (llamada generalmente proveído), muchas veces manuscrita, pocas veces legible, que suele referir más o menos lo siguiente: *"de la solicitud de fs…., traslado a las partes por cinco días"* o *"de la solicitud de fs…, notifíquese a las partes, por cinco días"*.

Este proveído no implica la realización de acción positiva alguna por parte del perito:

En el caso del traslado señala que las partes se considerarán como notificadas por el Ministerio de la Ley, a partir del siguiente día de notas (martes y viernes). Es decir que el plazo (de cinco días en nuestro ejemplo) comienza a correr desde el próximo de los días referidos, a partir de la puesta en letra del expediente. Antes del vencimiento del plazo, las partes deberán aceptar el pago del anticipo para gastos y realizar el depósito del cheque correspondiente ante el Juzgado. A veces deciden llamar al perito y abonarlo en persona, este hecho, si bien no está específicamente prohibido procesalmente y agiliza el procedimiento, no es demasiado conveniente, porque todo contacto innecesario con las partes generará situaciones por lo menos incómodas para la imparcialidad del dictamen y pondrán a prueba la ética del experto, de manera innecesaria.

En el caso de la notificación, la misma debe ser realizada por cédula, sin embargo, las notificaciones deben ser efectuadas por el tribunal o por las partes y el perito no es

parte del proceso (en realidad sólo es un testigo experto). A veces el perito confecciona las cédulas, pero esto no hace más que complicar las cosas, ya que lo sumirán en un largo y tedioso concurrir al Juzgado, revisar decenas, cuando no centenares de cédulas, para ver si la misma estaba bien confeccionada o fue observada. Esta tarea no compete al perito y es mejor no actuar como comedido, ya que no nos traerá beneficio alguno y por el contrario nos puede provocar una buena pérdida de tiempo.

A pesar de lo establecido en el artículo 463 en concordancia con el artículo 478 del Código Procesal Civil y Comercial de la Nación, el tribunal suele negar la solicitud de anticipo para gastos por "considerarla excesiva". En este momento el perito debe decidir si desea proseguir con la tarea pericial, soportando los gastos inherentes, desde su propio pecunio (traslados, insumos, horas-hombre, riesgos profesionales) con la esperanza (casi siempre infundada) de que alguna vez sus gastos sean compensados, al momento de regular los honorarios.

El informe pericial informático forense impreso y virtual

El informe pericial informático forense, no difiere de los informes periciales clásicos, utilizados históricamente por las disciplinas criminalísticas. Se compone de:

Un párrafo de presentación.

Cuatro secciones específicas denominadas sucesivamente:

Objeto de la pericia,

Elementos ofrecidos,

Operaciones realizadas,

Conclusiones.

Un párrafo de cierre, elevación y recibo en devolución.

Esta división formal del informe no es una formalidad antojadiza, sino que forma parte de la estructura lógica de interpretación de resultados, a partir de los estudios efectuados sobre la prueba recolectada y tiene por objeto facilitar la interpretación de dichos resultados.

Son raras las normas que establecen estas formalidades en la mayoría de las codificaciones procesales, sin embargo la sencillez de la estructura y la facilidad de interpretación, en particular para el lego, hacen que desde todo punto de vista sea conveniente respetarlas.

Es posible observar un curioso proceder por parte de los expertos, cuanto menor sea el grado de objetividad científica y metodológica de la disciplina pericial involucrada, tanto mayor es la confusión expositiva del informe. Parecería que los peritos provenientes de las disciplinas humanísticas tienen una mayor tendencia al desorden y la dispersión expositiva. Esto complica la lectura de los informes y permite realizar múltiples interpretaciones, con lo que se pierde el sentido final del informe pericial: informar e instruir al juez, acerca de un área del conocimiento en la cual es lego. Entre la oscuridad de Heráclito y la sencillez expositiva de Platón, media toda una gama de posibilidades, que cuanto más cerca de la estructura formal propuesta se encuentre, más fácil hará la aceptación por parte del tribunal interventor, de los resultados obtenidos en la pericia. De ahí que tenga suma importancia para la tarea, la revisión conjunta del informe final, por parte de los operadores del derecho involucrados, intentando lograr la máxima desambiguación y claridad de la exposición pretendida.

El párrafo de presentación

Este párrafo constituye la presentación en sociedad del informe, debe contener:

Destinatario: Tribunal interventor, organismo, estudio de abogados, etc., destacado y completo, para facilitar su identificación y pertinencia, en el momento de la entrega en barandilla.

Datos del perito que se presenta ante el tribunal:

Nombre y apellido,

Tipo y Número de Documento,

Número de CUIT/CUIL,

Número de Matrícula Profesional, referido a la institución que la otorgó,

Nacionalidad,

Estado Civil,

Profesión,

Domicilios particular y procesal,

Teléfonos (fijo/celular/fax),

Correo electrónico.

Carácter de la designación invocada: *"designado perito oficial (de oficio, de parte, consultor técnico)"*. En este punto es muy importante destacar que una cosa es la designación en la causa (a la que estamos haciendo referencia y otra la profesión de quien ha sido llamado a realizar la pericia. Pueden o no coincidir las mismas, por ejemplo un licenciado en Criminalística puede ser invocado para realizar una pericia balística, en cuyo caso y en esa causa específica se lo habrá designado como perito en balística, hecho que nada tiene que ver con el título específico de "Perito en Balística", otorgado por un centro de altos estudios de cualquier nivel.[1]

Denominación específica y detallada de los autos en que fue designado:

Tribunal interventor (Juzgado y Secretaría),

Número del expediente,

Denominación de la causa,

Partes involucradas.

Marco normativo procesal en que se desarrolló el informe.[2] Este elemento es primordial, porque circunscribe las acciones y plazos procesales involucrados a la jurisdicción en que se desarrolla el litigio en que se presenta el informe.

Sentido y fin de la presentación ante S. Sa.[3]

El objeto de la pericia y los puntos de pericia (tarea transdisciplinaria)

Ésta es una parte coyuntural del informe pericial, constituye la razón de ser del mismo y por lo tanto requiere de una ejecución metodológica estricta.

Todo informe pericial tiene por objeto brindar información sobre un área determinada, a partir de exámenes científico-técnicos, realizados por un profesional de dicha área del conocimiento. Pero dicha información no es una información genérica, sino estrictamente relacionado con el fin que dará quien solicita el informe a los resultados obtenidos.

Si consideramos que el caso más estricto de empleo de resultados periciales es el que involucra una prueba, a presentar ante el Juzgado Interventor para inducir al magistrado a que acepte la pretensión de una de las partes, canalizar el razonamiento judicial en el sentido pretendido y justificar la inclusión de la prueba solicitada en el marco judiciable específico de la causa, entonces dicha prueba debe ajustarse a los hechos pertinentes y conducentes que brinden soporte a la decisión de S. Sa.

Resulta por lo tanto una tarea transdisciplinaria, un tema difícil y que en general obra más en las palabras que en los hechos. El efecto transdisciplinario implica interacción, colaboración, discusión, integración, búsqueda del resultado común consensuado y "posible". Generalmente se aprecian trabajos interdisciplinarios en compartimentos estancos. El abogado planifica su estrategia ofensivo-defensiva, incluyendo la petición pretendida, la justificación racional y legal de la misma y la prueba involucrada. Realiza esta acción casi rutinariamente, utilizando en general modelos de consabida eficacia, eficiencia y efectividad que guarda entre su arsenal de formularios digitales. Entre dicha prueba propuesta obra la pericial, en el caso que nos interesa la prueba pericial informático forense. Deja para su oportunidad la designación por parte del tribunal de un perito para que realice el trabajo probatorio requerido.

Esta forma de actuar es absolutamente nociva a los efectos periciales informáticos ya que la prueba documental informática posee características propias que la hacen altamente vulnerable al paso del tiempo. Por otra parte no todo lo concebible e imaginable, como respuesta pericial informática, es posible. En el actual estado de avance de la disciplina, la leyenda urbana, la fantasía popular, la creencia infundada y el desorden metodológico, se conjugan con las acciones posibles y probables a esperar por parte de un sistema informático. No todo lo posible es probable y mucho menos factible.

Los pasos a seguir, antes de presentar la demanda, ante la necesidad inminente de utilizar prueba documental informática y eventualmente someterla a un informe pericial, deberían ser:

Seleccionar y contactar un experto en Informática Forense. Es necesario tener en cuenta la pertinencia entre la tarea a realizar y la profesión demostrada en autos por

quien realiza la pericia. Éste es un punto a considerar en el momento de planificar la prueba y antes de preparar los puntos de pericia.[4] La decisión no debe fundarse en la supuesta idoneidad o fama entre los legos de quien debe realizarlos, sino en la posesión efectiva y real de un título acorde con la materia a decidir, en nuestro caso el título debe ser de grado como mínimo y corresponder al área informática, de sistemas o de computación (cuyas incumbencias aún no están claramente definidas, de ahí la necesidad de una ley que lo establezca), de ninguna manera son aceptables las carreras de electrónica, contabilidad o administración de empresas.

Explicarle con claridad la línea argumental pretendida y el sustento probatorio planificado.

En este momento el experto debe dejar de lado su natural arrogancia y escuchar atentamente la exposición, para aportar aquellos elementos que realmente sean útiles a la estrategia decidida por el operador del derecho que lo consulta, descartar aquellos que son de utilización imposible y prevenir los que puedan provocar resultados adversos a la línea argumentativa proyectada.[5]

El experto debe sugerir al consultante, todos y cada uno de los aportes que desde su área puede realizar a la línea argumentativa establecida. Esta lista de acciones periciales debe ser exhaustiva, completa y estricta, no debe contener elementos superfluos, confusos, indeterminables o imposibles de alcanzar con los medios técnicos disponibles.[6]

A partir de esta interacción el consultante escribirá los puntos de pericia pretendidos. Éstos deben consistir en preguntas claras[7], cuya respuesta sea lógicamente determinable, argumentalmente coherente y pericialmente factible. Si las preguntas están bien hechas, las conclusiones del perito debería ser: SÍ o NO, sin otros agregados aclaratorios, esto no es siempre posible, pero es siempre deseable. En general *“el que trata de aclarar, oscurece”*.

Ambos (abogado y perito) revisarán los puntos para darles coherencia argumental, orden cronológico y especialmente para evitar superposiciones. Deben limitar la cantidad de puntos de pericia a los estrictamente necesarios para sustentar la argumentación planificada. Es frecuente observar en una solicitud de informe pericial, la aparición de cincuenta o más puntos de pericia, si analizamos cualquier estructura demostrativa racional a partir de argumentos lógicos, veremos que tal sobreabundancia de preguntas seguramente resultará excesiva, confusa y ambigua. Ninguna persona (esto incluye a todos los operadores del derecho) tiene capacidad intelectual, como para relacionar cincuenta variables dentro de un discurso coherente.

Lo bueno si breve, dos veces bueno.

Determinados los puntos de pericia, es necesario establecer los elementos ofrecidos, sobre los cuales se realizarán dichos puntos de pericia. Es decir planificar la detección, identificación, localización, certificación, resguardo, traslado, cadena de custodia y entrega al tribunal de la prueba documental informática disponible.

Para realizarlo es imprescindible determinar la ubicación física de dicha prueba, la que puede ser:

Información digital en poder de la parte que nos consulta.

Información digital pública de libre disponibilidad.

Información digital pública de disponibilidad restringida (reservada, confidencial, secreta).

Información digital privada de un tercero, no involucrado en la causa.

Información en poder de la contraparte.[8]

En los dos primeros apartados anteriores, la recolección de la prueba documental informática sólo depende de la decisión del consultante y basta con aplicar la metodología expuesta en otra parte de este libro para realizar la tarea.

En los restantes casos, es necesario contar con la correspondiente autorización judicial para realizar la tarea. No obstante la realización de los pasos imprescindibles para lograrlo, debe ser planificada en este momento. La fragilidad de la prueba documental informática ante ataques activos y pasivos, por medios locales y remotos, la constituye en un elemento sumamente delicado de manipular y asegurar.

En la mayoría de los casos la prueba documental informática debe ser gestionada, mediante una medida previa o preliminar *in audita altera pars*, su justificación ante el tribunal interventor, es una tarea ardua, compleja e inevitable, para reducir los riesgos de pérdida de información por manipulación de la contraparte u otros interesados. Esto implica que el artículo 388 del CPCCN, no puede ser aplicado so pena de destrucción de la prueba ofrecida por parte del afectado por la misma y aunque constituya presunción en su contra, esta presunción no sustituye a la prueba irremediablemente perdida.

Analizada y consolidada la propuesta de recolección de prueba documental informática y los pasos a seguir para obtenerla, es necesario a partir de la misma,

revisar los puntos de pericia ya consensuados. Aunque ya habíamos determinado que los mismos eran pertinentes y conducentes para la línea argumentativa pretendida, ahora debemos considerar si pueden alcanzarse a partir de la documental informática a recolectar, en especial si ésta se encuentra en poder de terceros o de la contraparte.

Las tareas anteriores finalizan con la confección de los puntos de pericia solicitados. Estos puntos de pericia obrarán en el expediente principal o en alguno de los cuadernos de prueba (en el caso en que existan). Deben ser copiados en esta parte del informe, de manera textual, no interpretada, ni resumida, ni sintetizada en forma alguna y con referencia específica al o los folios donde obran los mismos. Si han sido elaborados siguiendo la propuesta anterior, deben resultar claros, precisos, específicos y factibles, por lo que no requieren su modificación por parte del experto que realiza el informe, hecho que además le está específicamente prohibido, ya que debe limitarse estrictamente a responder los puntos de pericia solicitados.

Es sumamente importante que el perito tenga en cuenta los lugares, dentro del expediente judicial, donde frecuentemente aparecen puntos de pericia, lugares que muchas veces no están claramente referidos en las cédulas de notificación que pudiere recibir:

En la demanda, contestación de la demanda, reconvención y contestación de la reconvención.

En los cuadernos de prueba de la actora y de la demandada.

En todos o algunos de los documentos referidos en los puntos anteriores. Es posible por ejemplo, que nos convoque la parte actora y encontremos puntos de pericia en el cuaderno de la actora, pero que al ser designados peritos únicos de oficio, debamos también resolver los puntos propuestos por la demandada.

Si los puntos de pericia no son lo suficientemente claros, o no se corresponden con nuestra profesión o de alguna manera se denotan oscuros y difíciles de interpretar, es necesario informarlo al tribunal, pidiendo la suspensión de los plazos legales para presentar el informe. Se trata de una especie de aclaratoria, que el tribunal resolverá dando intervención a la parte solicitante. Nunca se deben resolver puntos de pericia confusos, apelando a una propia y particular interpretación, ya que este acto puede ser atacado de parcialidad, involucrando al experto en una situación incómoda y comprometida, en la que resulta fácil entrar y sumamente difícil salir airoso.

Los elementos ofrecidos (equipos, programas, indicios y rastros)

En este apartado es necesario detallar todos los elementos involucrados en las tareas periciales realizadas. Debe incluir:

Descripción clara y precisa de lugares y oportunidades de recolección de la prueba documental informática.

De ser necesaria descripción, con documentación fotográfica y planimétrica de los locales inspeccionados y la ubicación física de los lugares de acceso a la prueba documental informática recolectada. Esto incluye los accesos remotos legítimos y/o legalmente autorizados.

Descripción exhaustiva de los equipos informáticos involucrados en la tarea (computadoras, redes, equipos de conexión y distribución de datos, reservorios de información locales y remotos, distinción entre tecnologías y arquitecturas detectadas, soportes magnéticos, ópticos, biológicos, cuánticos, etc.). Esta descripción en lo posible debe acompañarse con las especificaciones técnicas de dichos equipos.

Descripción exhaustiva de los programas utilizados para realizar la tarea, consignando los tipos y números de licencia de cada uno de ellos en caso de corresponder. Debemos tener en cuenta que no contar con licencia en alguno de los programas de fondo o aplicaciones utilizadas, constituye un delito y que si utilizamos herramientas sin licencia, estamos anulando los resultados. El tribunal no admitirá resultados ciertos o inciertos obtenidos por medios fraudulentos. Esta característica debería ser revisada por el operador del derecho que cuestiona un informe pericial, ya que es equivalente a la obtención de una prueba confesional utilizando mecanismos de convicción o interrogación ilegales. En cuanto a los expertos, sería recomendable que utilizaran programas de libre distribución (Licencias GNU), para evitar estos contratiempos, por supuesto estos conocimientos específicos se obtienen mediante estudio, esfuerzo y dedicación, precio que no todos están dispuestos a pagar. *“Programa pirata, licencia inexistente, deberían implicar la inmediata desestimación de la prueba pericial obtenida por estos medios.”*

Explicación detallada, de las relaciones detectadas entre los componentes descriptos. Por ejemplo, qué programa estaba instalado en determinado equipo y sus relaciones de integración con los demás.

Elementos entregados al experto por parte del tribunal para realizar la pericia. Puede incluir equipos completos o elementos de almacenamiento secundario (discos ópticos o magnéticos). Por ejemplo la prueba documental informática, recolectada como medida previa o preliminar, resguardada en un dispositivo de almacenamiento óptico (DVD), con su correspondiente *hash* y cadena de custodia estricta.

Si estos elementos son entregados sin la correspondiente cadena de custodia, dicha circunstancia se debe destacar de manera explícita, para deslindar responsabilidades por parte del experto al asumir la responsabilidad sobre el material entregado. Ningún operador del derecho destruiría o interrumpiría una cadena de custodia en una muestra de ADN, la fragilidad de la muestra documental informática, es similar en todo sentido, respetar la cadena de custodia debería ser una tarea primordial e ineludible por parte de todos los actores involucrados en su confección, no hacerlo implica una grave irresponsabilidad, en el mejor de los casos a partir de una supina ignorancia de los mecanismos de gestión de la precitada documental informática.[9]

Como principio general el experto debe considerar que en el momento de describir las operaciones realizadas no podrá hacer referencia a elemento edilicio, físico o lógico alguno que no haya sido declarado en este párrafo. Es el equivalente programático de la declaración de variables. Por eso debe ser revisado concienzudamente, al finalizar la redacción del informe, para corregir las omisiones incurridas. Éste es otro punto a considerar en el momento de analizar un informe pericial, por parte de los operadores del derecho, sólo podemos analizar aquellas cosas declaradas, ninguna puede aparecer mágicamente en las operaciones realizadas, ya que esto implicaría intenciones desconocidas por parte del experto. El informe pericial como documento constituye un todo íntimamente relacionado y conceptualmente inescindible, de ahí que su coherencia metodológica debe ser estricta y comprobable.

Las operaciones realizadas

Éste es el momento de la verdad para el experto. A partir de los puntos de pericia y los elementos ofrecidos, el perito ha realizado una determinada planificación cronológica y metodológica que le permitirá dilucidar los interrogantes planteados en los puntos de pericia y arribar a conclusiones científicamente sustentadas, metodológicamente justificadas y técnicamente implementadas.

Las operaciones realizadas se describen a partir de un orden cronológico y lógico estricto. Este orden conforma una estructura demostrativa propia, cuya implementación requiere los siguientes pasos metodológicos:

Se determinan las variables involucradas (proposiciones lógicas).

Se simplifican las variables multidimensionales, transformándolas en otras variables binarias puras equivalentes (que admitan valor de verdad mensurable y representación mediante tablas de verdad).

Se establece el valor de verdad de las variables detectadas. Es decir se transforman

las variables en premisas. Éste es el punto candente de la cuestión, ya que implica establecer si una variable propuesta, para este caso, es verdadera o falsa. Este proceso debe ser amplia y minuciosamente detallado, ya que constituye el nudo a partir del cual se justificarán las conclusiones obtenidas.

Se relacionan las premisas mediante silogismos válidos.

Se construye el mecanismo argumental, relacionando los silogismos obtenidos.

A esta estructura demostrativa de fondo, que por supuesto desde el punto de vista de la redacción ha quedado excesivamente técnica, conspicua y desagradable, el experto deberá agregarle su propia capacidad narrativa. No se trata de construir poesía, pero sí de despertar interés y curiosidad en el lector interesado. *"Los silogismos constituyen el back borne, de nuestra redacción, su solidez aportará el tejido de sostén que permitirá rebatir o desestimar las agresiones retóricas comunes."*

A partir de una o varias operaciones realizadas, deben obtenerse respuestas a los interrogantes periciales. Respuestas concisas y claras a las preguntas efectuadas. Preferiblemente en términos afirmativos o negativos.

Las conclusiones

Si la planificación y desarrollo de las operaciones realizadas, a partir de los elementos ofrecidos, con el objeto de dar respuesta a los interrogantes periciales han sido implementadas de manera eficiente, efectiva y eficaz, entonces las conclusiones son prácticamente automáticas y dependientes directamente de las partes previas del informe pericial.

Aunque parezca escueto y ceñido, las conclusiones deberían ser del tipo:

Conclusión 1: *"Al punto pericial 1: SÍ",*

Conclusión 2: "*Al punto pericial 2: NO",*

Conclusión 3: "*Al punto pericial 3: No ha sido posible determinarlo"* (siempre cabe la posibilidad que aparezcan elementos no evaluados al momento de planificar los puntos de pericia que invaliden la pertinencia o factibilidad de los mismos).

Si en las conclusiones es necesario aclarar cosas, es simplemente porque no fueron aclaradas en el momento adecuado (normalmente durante las operaciones realizadas).

Las conclusiones no deberían contener ninguna otra apreciación objetiva o

subjetiva, más allá de la resolución de los interrogantes periciales. El perito debe limitar a responder dichos interrogantes. El perito no es juez, no es detective privado, no es parte de la causa y no debería intentar serlo, ya que existen razones de legitimidad y legalidad que se lo prohíben.

El párrafo de cierre (elevación, recibo en devolución y propuesta de nuevas pericias y/o pedidos de informes).

Este párrafo es de radical importancia, es preciso destacar que:

No forma parte de las conclusiones y por eso debe estar claramente separado de las mismas (es un párrafo aparte).

Puede incluir recomendaciones: Una vez finalizada la demostración argumentativa estricta, puede suceder que aparezcan situaciones particulares que impliquen nuevas estructuras o pruebas que puedan ayudar a la causa, pero que no han sido incluidas en la requisitoria pericial. En este punto surge una clara dualidad, el perito no puede expedirse más allá de la requisitoria pericial (so pena de ser considerado tendencioso o parcial), pero no puede dejar de decir lo que vio, porque el falso testimonio establecido en el artículo 275 del CPN, no sólo consiste en afirmar una falsedad, sino también en ocultar una verdad conocida.

Por lo tanto, no corresponde incluir estas apreciaciones en las conclusiones, que únicamente deben referirse a la requisitoria pericial, sin embargo nada impide incluirlas en este momento, explicitándolas y sugiriendo a S. Sa., que en caso de considerarlo necesario ordene la ejecución de una ampliación de pericia posterior. De esta manera se salvan ambas situaciones y se eluden responsabilidades innecesarias. Es conveniente "sugerir" asimismo los términos estrictos de dicha requisitoria, para evitar nuevas idas y vueltas por falta de claridad o definición en las mismas.

Ejemplo: *Luego de examinados los archivos detectados, ha sido posible determinar que los obrantes en el disco rígido correspondiente al servidor principal de la red (identificado como Servidor A, en el apartado II del presente informe) de la empresa R, son idénticos a los que obran en la terminal J (identificada…) de la Sucursal T. No obstante esta característica es se*ñalad*a a título informativo a S. Sa y en concordancia con el artículo 275 del CPN. Si S. Sa, estima conveniente analizar esta circunstancia es posible hacerlo mediante una ampliación del presente informe pericial orientada a: "establecer si los archivos obrantes en el Servidor Principal de la red de la empresa R, son los mismos que obran en la terminal J de la Sucursal".*[10]

Debe incluir la descripción del informe elevado: "*Se adjunta en devolución*[11] *al*

presente informe pericial compuesto de cinco (5) fojas útile*s, (en 173 renglones) y, de 8 Anexos (en un total de treinta y dos fojas* útile*s), el material descrito en el apartado II".* El numerar los renglones escritos (función automática de los procesadores de texto modernos), permite evitar la inclusión de texto espurio, *a posteriori*, de la confección del informe, previniendo múltiples circunstancia indeseadas para el autor del informe (inserciones, adulteraciones, raspados, lavados, etc.)

Debe integrar un párrafo solicitando el pago de los honorarios profesionales correspondientes a la tarea realizada[12] *"Con el objeto de informar a S. Sa., sobre las tareas realizadas y el tiempo demandado por las mismas, hago saber la siguiente distribución horaria:*

Nº	Tarea	Actividad	Horas	Obs.
01	Gestión de expediente	Administrativa	5	Sede Judicial
02	Inspección Judicial	Técnica/Pericial	8	Local Empresa
03	Reconocimiento Judicial	Técnica/Pericial	8	Gerencia
04	Análisis de Laboratorio	Técnica/Pericial	13	Local pericial
05	Confección del Informe Pericial	Administrativa	5	Local pericial
Total			39	

"Se hace constar que la hora técnico pericial vigente en el mercado para un profesional universitario con título de grado, se estima en ciento cincuenta pesos ($150),[13] *respecto de las horas de gestión administrativas, se estiman en un cuarto del costo anterior ($50), lo que en el presente caso prevé un valor total estimado de $6.300. El suscripto ruega a S. Sa. tener en cuenta estos valores, al momento de determinar los honorarios profesionales que le pudieran corresponder, considerando la complejidad del trabajo realizado y la capacitación profesional que el mismo requiere por parte de quien realiza la misma."* De esta forma estaremos asesorando a S. Sa.

Debe contener las palabras de elevación del informe al tribunal interventor: *"Sirva la presente de formal y atenta nota de cierre y elevación del informe pericial,*

constituyendo formal recibo de entrega y recepción de conformidad de los elementos detallados a continuación, a sus efectos legales." Esta aclaración de entrega y recepción, debe utilizarse para eludir responsabilidades posteriores ante la pérdida de alguno de los elementos devueltos.[14]

1 Esta confusión genera innumerables controversias a la hora de resolver disidencias en las conclusiones periciales entre peritos de igual designación. Complicando la cosa muchos profesionales anteponen a su nombre y apellido, títulos que no condicen con su formación académica certificada. El más común es el uso de la sigla Dr. (Doctor) por parte de abogados, médicos, contadores y otros profesionales que nunca han realizado un doctorado. Llegan hasta el agregado de dicha sigla en sus tarjetas de presentación personales y en la firma de sus escritos. Ésta es una acción típica, antijurídica y culpable de violación al artículo 247, segunda parte del Código Penal y quien la comete es simplemente un delincuente. La designación como perito en una causa judicial no es un título académico, sino un cargo a desempeñar en dicha causa. Su origen es asimilable al testimonio y en realidad el perito no es otra cosa más que un testigo experto, llamado para un fin y objetivos propios y que no trasciende el ámbito de la causa en que ha sido designado. Por otra parte, si bien no es un hecho frecuente, es un punto débil a atacar por el abogado de la contraparte, si advierte dicha circunstancia *(¿por qué se hace usted llamar doctor, si no posee doctorado alguno?... Su Señoría,* ¿como *puede el Tribunal confiar en una persona que abierta y públicamente transgrede una norma penal?)*

2 Por ejemplo: *"acorde a lo determinado en el artículos 457 y subsiguientes del Código Procesal Civil y Comercial de la Nación. Reconociendo el conocimiento, alcance y penas establecidas en los artículos 275 y 276 del Código Penal de la Nación, en concordancia con el artículo 449 y las salvedades del artículo 444 del Código Procesal Civil y Comercial de la Nación".*

3 Por ejemplo: *"...se constituye ante S. Sa, a efectos de informarle los resultados periciales alcanzados luego de las operaciones técnicas, realizadas sobre los elementos peritados (examinados, sometidos a estudio o examen, sub peritia)."*

4 "DESIGNACIÓN. PUNTOS DE PERICIA. Art. 459. Al ofrecer la prueba pericial se indicará la especialización que ha de tener el perito y se propondrán los puntos de pericia; si la parte ejerciera la facultad de designar consultor técnico, deberá indicar, en el mismo escrito, su nombre, profesión y domicilio."

5 Por ejemplo: Si bien es posible y hasta probable que utilizando las herramientas y métodos adecuados podamos establecer el origen de un mensaje de correo electrónico, determinando una dirección IP. Que también puede ocurrir que esa dirección IP sea específica de un equipo informático, situado en una determinada casa, propiedad de una persona. Sin embargo, esto no permite asignar autoría en la redacción del mensaje a dicha persona. La máquina pudo ser utilizada por otro miembro de la familia, un amigo, un extraño, un intruso o cualquier otro. Este hecho, el experto se lo debe aclarar al consultante, para evitar generar falsas expectativas. Históricamente la misma circunstancia se daba entre un escrito mecanografiado, la máquina de escribir con la que fue confeccionado y el autor del mismo. La máquina era muchas veces identificada categóricamente, por el contrario la autoría del documento era muy difícil de probar, al menos por medio de una prueba pericial documentológica. Por otra parte esta particularidad puede servir al consultante para poner en duda la pericia de la contraparte,

cuando afirma una posible autoría sobre el mensaje de marras. Un experto que se precie de tal, nunca debería sacar conclusiones que no sean directa y específicamente derivadas de la observación técnica de los elementos ofrecidos.

6 Uno de los elementos que constituyen este conjunto es el capital disponible para realizar la tarea. Por ejemplo, es posible recuperar información a partir de un disco rígido dañado físicamente, pero los costos involucrados en la operación, que incluyen trabajos realizados por laboratorios específicos, situados en general fuera del país, son tales, que su inclusión dependerá estrictamente del alcance de la pretensión especificada en la demanda y de los gastos que la parte está dispuesta a realizar. La falta de informe sobre estas circunstancias o su informe parcial por parte del experto consultado, puede llevar al operador del derecho a solicitar una tarea pericial, que luego no pueda solventar económicamente, perdiendo una prueba cuya utilidad no siempre es primordial y desacreditando profundamente el sentido común del experto que lo asesoró (recordemos que siempre los triunfos se logran por méritos propios y los fracasos son provocados por errores de nuestros asesores).

7 Aunque difiere en diversos aspectos, del interrogante pericial, la primera parte del artículo 443 del CPCCN, puede ser de utilidad en el momento de formular los puntos de pericia “FORMA DE LAS PREGUNTAS. Art. 443. Las preguntas no contendrán más de UN (1) hecho; serán claras y concretas; …”

8 Al respecto recordemos que la prueba documental informática es sólo una especie del género prueba documental (clásica: bibliográfica, foliográfica o pictográfica) y como ejemplo de la normativa obrante en esta materia, considero conveniente referirme al Código de Procedimientos Civil y Comercial de la Nación en especial: “SECCIÓN 2° PRUEBA DOCUMENTAL EXHIBICIÓN DE DOCUMENTOS. Art. 387. Las partes y los terceros en cuyo poder se encuentren documentos esenciales para la solución del litigio, estarán obligados a exhibirlos o a designar el protocolo o archivo en que se hallan los originales. El juez ordenará la exhibición de los documentos, sin sustanciación alguna, dentro del plazo que señale. DOCUMENTO EN PODER DE UNA DE LAS PARTES. Art. 388. Si el documento se encontrare en poder de UNA (1) de las partes, se le intimará su presentación en el plazo que el juez determine. Cuando por otros elementos de juicio resultare manifiestamente verosímil su existencia y contenido, la negativa a presentarlo, constituirá una presunción en su contra. DOCUMENTOS EN PODER DE TERCERO. Art.

9 Al respecto es de destacar que cuando el perito comete errores que pueden beneficiar a una de las partes, en general dichos errores son vistos con suspicacia por todos los actores (la parte considera que lo hizo a propósito para anular la prueba, la contraparte piensa que en realidad intentó provocarle un daño y el tribunal se enfrenta a la duda sobre el dolo o la culpa que llevaron a este error), el mismo mecanismo debería aplicarse al empleado de barandilla, que con absoluto desparpajo rompe un sobre, lacrado y sellado ante escribano público, dejando al descubierto su contenido, sin aceptar ni firmar la cadena de custodia que lo acompaña y limitándose a arrojarlo junto con otros elementos similares en la caja fuerte del tribunal, so pretexto de que su cargo le proporciona una inmarcesible confiabilidad procesal. *“La caridad bien entendida, debería comenzar por casa.”*

10 CPCCN, “TRASLADO. EXPLICACIONES. NUEVA PERICIA. Art. 473. […]Cuando el juez lo estimare necesario podrá disponer que se practique otra pericia, o se perfeccione o amplíe la anterior, por el mismo perito u otro de su elección.”

11 Siempre es conveniente que el informe pericial se presente en papel oficio (de tipo tribunales) escrito por ambos lados y conste de un número par de páginas. De esta manera el sello de recepción

queda en la misma hoja que la diligencia de cierre y convalida el recibo, deslindando al perito de responsabilidades, sobre la integridad o destino *a posteriori* de la prueba analizada.

12 CPCCN, “IMPUGNACIÓN. DESINTERÉS. CARGO DE LOS GASTOS Y HONORARIOS. Art. 478. Los jueces deberán regular los honorarios de los de peritos y demás auxiliares de la justicia, conforme a los respectivos aranceles, debiendo adecuarlos, por debajo de sus topes mínimos inclusive, a las regulaciones que se practicaren en favor de los restantes profesionales intervinientes, ponderando la naturaleza, complejidad, calidad y extensión en el tiempo de los respectivos trabajos.” *(Párrafo incorporado por art. 10 de la Ley N° 24.432 B.O. 10/1/1995).*Muchas veces a la hora de convenir, consensuar, acordar, concordar o desistir de un litigio, las partes y los operadores del derecho suelen “olvidar” el pago de honorarios de los peritos. Cuando el perito lo detecta, luego de muchos meses de no tener noticias del expediente, para poder reclamar necesita el patrocinio letrado y el círculo se reinicia. La solución más adecuada a este problema consiste en mantener una constante vigilancia sobre los expedientes en trámite, hacer “procuración” permanente y actuar en el momento oportuno (aunque a veces la mejor estrategia reside en dar por perdidos los honorarios).

13 Como equivalente podemos decir que lo normal sería pagar U$S 50 la hora profesional.

14 Generalmente, la mayoría de los empleados que recepcionan la documentación en la mesa de entrada de los Juzgados, se niega a firmar recibos por el material que oportunamente le fue entregado al perito para realizar su tarea. Este simple hecho, hace que si luego algún elemento de los devueltos “se pierde”, no hay forma de comprobar que el perito lo haya devuelto efectivamente. Los empleados se limitan a colocar la hora de recepción del informe, mediante el dispositivo fechador del juzgado y hacer una rúbrica. Pero tampoco pierden un instante en leer el informe que reciben. Si el perito aclara la entrega y recepción del material en el mismo informe, produce al menos una constancia de recepción (ya dijimos que el formulario de cadena de custodia no es un documento demasiado respetado por los empleados judiciales). Quien firma la recepción, firma la aceptación de lo entregado y recibido, si lo entregado contiene un recibo, entonces ese recibo es válido. No evita las “pérdidas” pero salvaguarda al perito.

CAPÍTULO 9
LA IMPUGNACIÓN

Éste es el trabajo de “abogado del diablo”, una auténtica auditoría informático forense, donde el profesional podrá demostrar sus conocimientos en la revisión de la tarea de otros colegas en paridad de condiciones.

El abogado que pretende impugnar un informe pericial deberá seguir los mismos procedimientos ya descriptos respecto de la solicitud de puntos de pericia. La interacción con el perito le permitirá detectar los errores conceptuales, falencias procedimentales, generalizaciones improcedentes, en fin, todos los puntos débiles en el informe cuestionado.

Sistematizando el procedimiento podemos decir, que el informe pericial debe ser analizado desde diversos puntos de vista, entre ellos:

Revisión legal.[15]

Revisión científica, tecnológica y técnica.

Revisión lógica.

Revisión formal.

Revisión legal

La pericia constituye una forma de prueba regulada específicamente en el derecho procesal, en todos los fueros. Su naturaleza, la asemeja a la prueba de testigos y difiere de ésta en que el testigo se expresa respecto de hechos que ha podido acceder a través de los sentidos, mientras que el perito expone sobre los resultados alcanzados por su labor técnica, respecto de un área del conocimiento en la que se lo supone experto. Sin embargo, todo ser es percibido y al ser percibido es por supuesto interpretado. De ahí que no existan dos seres humanos que compartan idéntica concepción respecto de un objeto material o ideal cualquiera. Hasta la más pura operación aritmética es susceptible de revisión y factible de error 7+1=8, es una forma de ver las cosas, pero también lo son 7+1=10 y ambas perfectamente defendibles y pertinentes.

Es por esa razón que la primera revisión del informe pericial debe ser el control de

legalidad del mismo. Esto incluye todas y cada una de las formas en que se evalúa la declaración de un testigo en sus aspectos legales. El perito no es parte de la causa, por lo tanto no puede ni debe realizar tareas procesales *motu proprio*. No está autorizado a realizar ni diligencias cédulas de notificación, no se le permite dejar nota, ni citar personas o fijar fechas de reconocimiento, revisión o instrumentación de tareas periciales. Todas y cada una de estas tareas deben ser solicitadas al tribunal interventor y éste establecerá su pertinencia. Por supuesto que el perito puede sugerir fechas tentativas, pero una vez autorizadas, la comunicación de las mismas a las partes no es tarea del perito, sino de la parte interesada en la pericia.

La relación del perito con las partes y con los abogados de las mismas

Éstas dependen claramente del rol que ocupa el perito:

El perito oficial: Debe regirse por las órdenes que recibe desde la institución a la que pertenece, es un empleado de la misma que realiza una tarea para dicha institución, aunque el resultado de ésta sea utilizado en una causa judicial, de ahí que la forma de relacionarse con las partes estará con seguridad determinada por las reglamentaciones de la institución madre o por las órdenes particulares que reciba desde la misma. Al respecto es importante tener en cuenta que está actuando como funcionario público. De ahí que deba cumplir con la totalidad de la legislación que regula dicha condición. (Entre ellas la ley 25.188: de Ética Pública; ley 24.156: de administración financiera y de los sistemas de control del sector público nacional; Decreto 41/1999: Código de Ética de la Función Pública,2 Resoluciones 8, 14, 15, 20 y 38/1999, de la Oficina Nacional de Ética Pública, Resolución 3/2000 de la Oficina Anticorrupción; Resolución 577/2006 de la Administración Nacional de la Seguridad Social.)

Es necesario tener en cuenta que las diferentes codificaciones procesales exigen al perito la posesión de título habilitante en la materia de la cual es experto y esta condición sólo puede ser dispensada por S. Sa., en casos excepcionales. La norma es que el perito tenga título habilitante, la excepción es que esto no sea así (por falta de profesionales en el área, o por falta de título específico, entre otras). Esta norma es perfectamente aplicable a las instituciones oficiales que realizan tareas periciales y es una de las principales falencias de las mismas. Por supuesto que la Morgue Judicial realiza necropsias firmadas por un profesional con título específico (médico legista), sin embargo las Fuerzas de Seguridad y algunos organismos judiciales realizan tareas periciales a partir de “idóneos”, cuya idoneidad en general sólo depende de la opinión

de dicha fuerza y de su necesidad de completar organigramas y roles preestablecidos. Hace falta un perito en informática forense, bueno, que lo cubra un oficial del cuerpo de pericias. Sin embargo ese oficial no requiere de ningún título universitario habilitante. Es así como muchas veces los profesionales de la Informática deban aceptar como contraparte pericial a una persona cuyas únicas credenciales de idoneidad, consistan en la pertenencia a la institución que lo designa.

Es indudable la experiencia de las Fuerzas Policiales en materias como papiloscopía, scopometría, balística o fotografía pericial, sin embargo su idoneidad en informática forense es absolutamente incierta. La informática forense surge en el decenio final del siglo pasado y en nuestro país comienza a tener importancia en los primeros años del actual. De ahí que no podamos hablar de preponderancia histórica o temporal. Las carreras básicas de las que se nutre la Informática Forense (así como la medicina legal se nutre de la Medicina) son las de Informática, Sistemas y Computación; no es concebible un profesional que actúe en el tema sin poseer título en una de estas especialidades. De la misma forma no es concebible un médico legista que no tenga título de médico (de hecho es prácticamente imposible). Tampoco alcanza con tener un título afín (por ejemplo Electrónica, Contabilidad, Administración de Empresas, entre otros), de la misma manera en que los veterinarios no son aceptados para cursar la carrera de médico legista. A esta situación ya de por sí compleja (de leyes hablan los abogados, de medicina los médicos, de informática todos los que pueden hablar), se agrega la multiplicidad de carreras y denominaciones de las mismas (Ingenierías y Licenciaturas en Informática, Sistemas de Información, Computación, Técnicos Superiores en Análisis de Sistemas, Analistas de Sistemas, Analistas Programadores…). Se hace evidente la necesidad de una ley que normalice la profesión, por supuesto esta ley es muy resistida por todos los interesados (que no poseen título, que no quieren o no pueden obtenerlo, que sacan beneficio a partir de la ignorancia general, lo que incluye a la mayoría de los operadores del derecho, ya que en el momento de seleccionar un profesional para realizar una pericia, optan simplemente por el más barato) en que la cosa siga como está.

Esta falta de título habilitante debe ser destacada por el abogado de la parte que pretende impugnar, aunque en general no sea tenida en cuenta por la mayoría de los tribunales (los mismos tribunales que aceptaría de inmediato la impugnación de una pericia médico forense, realizada por un profesional sin título de médico, cualquiera sea la institución a la que pertenezca).[16]

El juez puede asignar mayor o menor credibilidad a la opinión de un perito, sin embargo, tiene ciertas restricciones establecidas en el artículo 477 del CPCCN, a las que no debe o no debería sustraerse, debe constatar la competencia del perito y para eso nada mejor que el título de grado que lo certifica.[17] Considerar con igual peso la

opinión de un profesional de la Informática respecto de un funcionario, cuya única competencia consiste en la pertenencia a una institución, es un verdadero despropósito.

El perito oficial debe notificar a las partes la oportunidad y lugar donde se realizarán las experiencias tendientes a solucionar la requisitoria pericial. Este acto debe ser formal, constar en el expediente y reunir los requisitos procesales establecidos para cualquier notificación similar.

El perito oficial no tiene atribuciones para citar a las partes sin autorización del Juzgado. Los usos y costumbres hacen que debido a la gran cantidad de pericias en trámite los organismos establezcan sus propias fechas y actúen directamente sobre los involucrados, no obstante el único autorizado para ordenar este tipo de audiencias extra foro es el tribunal interventor y la falta de notificación debería constituir un elemento primordial a la hora de impugnar un informe pericial.

El perito de oficio: El perito no debe contactar a las partes y sólo se reunirá con ellas el tiempo estrictamente necesario para realizar la tarea pericial frente a las mismas (si éstas deciden concurrir al acto). También los usos y costumbres hacen que algunas diligencias se "simplifiquen". Cuando el perito solicita adelanto para gastos, muchas veces el abogado de la parte interesada en la pericia, suele llamar al perito y ofrecerle el pago de los mismos en el estudio del abogado.

Este accionar es totalmente ilegítimo, el perito de oficio no es un abogado que puede interactuar libremente con sus colegas, cobrar extrajudicialmente y luego hacer su trabajo. Aunque no está específicamente establecido, la notificación respecto de las medidas solicitadas por el experto antes o en el momento de aceptar el cargo deberían ser notificadas por Ministerio de la ley a quien solicita la pericia y éste debería encargarse de notificar por cédula a la contraparte. [18] No hay razón alguna para que el perito deba confeccionar cédulas de notificación e interactuar con los representantes o patrocinantes de las partes en litigio. Toda interacción con una de las partes es indiscutiblemente condicionante. En la firme convicción de que toda realidad es una "realidad interpretada" y por lo tanto subjetiva, la interacción con los abogados condiciona la visión que el perito tiene respecto de la tarea a realizar (no es lo mismo ver cómo es atropellado un desconocido que ver cómo es atropellada una persona que conocemos, aunque sólo haya sido una vez en la cola de un banco). Si se pretende que la prueba pericial sea realmente objetiva, la interacción perito partes debe estar absolutamente prohibida, con excepción de aquellas diligencias que inevitablemente lo requieran y que deberían estar expresamente autorizadas y ordenadas por el tribunal interventor (como, por ejemplo: ejecución de cuerpos de escritura, extracción de muestras biológicas, recolección de prueba documental informática, inspecciones o

reconocimientos judiciales). Si se detectan estas interacciones “extraordinarias”, las mismas deben ser destacadas en el momento de la impugnación.

El perito de parte o asesor técnico: En este caso la interacción con el abogado que lo requiere es de rigor y mientras el profesional mantenga la seriedad, protagonismo, imparcialidad y ecuanimidad que su condición requiere, la tarea debería discurrir dentro de los cauces normales. De todas formas este rol constituye un reaseguro para la parte respecto de la corrección de los informes periciales presentados o la planificación de la estrategia probatoria pericial que brinda sustento a la argumentación establecida para alcanzar un resultado positivo respecto de la pretensión en curso.

En lo que respecta a los requisitos procesales, la falta de un requisito primordial en el perito designado, como ser el título habilitante (aunque la profesión no esté reglamentada, eso no significa, que cualquier persona tenga o no título alguno, pueda realizar una pericia informático forense), debe ser motivo de recusación.[19] Esta recusación es sumamente pertinente al revisar los informes periciales procedentes de instituciones oficiales, donde la tarea pericial la realiza un empleado sin título relacionado con la materia en cuestión. Aunque dicha recusación sea denegada por el *a quo*, es importante realizarla porque luego es motivo de revisión por la alzada al resolver lo principal[20].

Las operaciones pueden ser presenciadas por las partes, respecto de la recolección de la prueba documental informática y su revisión pericial *a posteriori*, es imprescindible que las parte presencie todas y cada una de las tareas, siempre que esto sea posible. En efecto, en este caso vuelven a enfrentarse dos derechos inalienables, el derecho de una parte de preservar la prueba que lo favorece, evitando que la contraparte, la dañe, elimine o modifique y el derecho de la contraparte a presenciar las tareas de recolección de la prueba que lo involucra. En este caso, se mantiene la recomendación de recolectar la prueba como medida previa o anticipada, generalmente *in audita altera pars*, pero una vez reunida la misma y presentada, debe ser susceptible de revisión por la contraparte. No nos estamos refiriendo a la revisión de los resultados periciales, sino a la revisión de las operaciones técnicas realizadas para recolectar la prueba y su control de legalidad. En cuanto a los frecuentes reconocimientos judiciales y tareas periciales de laboratorio (por ejemplo, la obtención de copias de resguardo, con fines de análisis pericial), es sumamente conveniente designar un consultor técnico que supervise las operaciones.[21]

Es importante tener en cuenta que para poder sustentar con solvencia una determinada impugnación, siempre es conveniente haber realizado tareas previas que sirvan de antecedentes, de ahí la importancia del dictamen por parte del consultor

técnico designado. El destacar las divergencias en los criterios y resultados obtenidos, es un precedente de suma utilidad a la hora de impugnar.[22]

Un viejo refrán indica *"el que pega primero pega dos veces"*, muchos operadores del derecho tienen tendencia a dejar todo para "las dos primeras", esta costumbre es sumamente perjudicial para la parte involucrada, en lo que se refiere a la pericia informático forense y a la gestión de la prueba documental informática, sin embargo en el primer caso, esta falencia puede ser subsanada oportunamente por el letrado patrocinante o representante[23], aunque esta forma de actuar implique pagar innecesariamente un alto costo de oportunidad, muchas veces insustituible e irrecuperable.

La concurrencia a los actos periciales (especialmente de recolección de prueba documental informática, constatación de sitios[24], reconocimientos judiciales, entre otras), es sumamente importante, en ésta debe encontrarse siempre presente el consultor técnico, para realizar las observaciones *in situ* y dejar constancia en el acta respectiva de las mismas[25].

Un mecanismo de suma utilidad es la demostración de los errores conceptuales y procedimentales detectados en el informe a impugnar, consiste en el uso de herramientas informáticas para sustentarlo. La reconstrucción del hecho empleando aplicaciones informáticas no debe restringirse únicamente a los hechos controvertidos resultantes de las pretensiones en litigio, sino también a la simulación de los errores cometidos durante las tareas periciales revisadas. La generación de un lugar del hecho virtual para describir la acción del perito cuestionado puede constituirse en una herramienta de discusión lógica, de fácil interpretación por parte del juez, en temas difíciles de representar por medios escritos u orales.[26]

Control, revisión y exigencia de legalidad en las herramientas utilizadas

No es aceptable una prueba obtenida por medios ilícitos, de ahí que las herramientas informáticas utilizadas por el perito que realiza el informe deben contar con las correspondientes licencias uso, obtenidas en legal y legítima forma. En este sentido las licencias deben incluir:

Licencia de uso del sistema operativo instalado en todos y cada uno de los equipos involucrados en la obtención de la documental informática, en las tareas de reconocimiento judicial y en las prácticas periciales declaradas y constatadas, incluyendo los equipos auxiliares que brinden soporte al equipamiento principal

(instalados en reservorios de información, elementos de conectividad, etc.).

Licencia de uso de las aplicaciones específicas de investigación genérica o específica informática forense.

Licencia de uso de las aplicaciones de oficina con que se generó el informe pericial.

Es de destacar que pese a la minuciosidad que suele observarse en otros detalles periciales, los recién referidos en general son poco frecuentes. Quien utiliza una aplicación informática de cualquier tipo sin licencias está cometiendo un delito, que no debe o no debería ser tolerado por la jurisdicción involucrada. Si admitimos prueba soportada, investigada o confeccionada mediante instrumentos ilegalmente obtenidos, estamos confirmando la legitimidad de estas partes. Muchas instituciones oficiales, realizan pericias con profesionales sin título, empleando en el mejor de los casos una aplicación de Informática Forense paga (por ejemplo, el reconocido Encase), sin embargo a la hora de presentar el informe o resguardar la información utilizan máquinas sin licencia para el sistema operativo instalado y mucho menos para el paquete de oficina con que realizan el informe. Como regla general el abogado debe pedir la licencia de todos los elementos lógicos involucrados en la tarea. En cuanto al perito que no posea los recursos económicos necesarios para pagar dichas licencias, la mejor sugerencia es que utilice aplicaciones de *software* libre, es cierto que requieren mayor esfuerzo, dedicación y sobre todo estudio, bueno, es el precio a pagar por la profesión elegida.

Revisión científica, tecnológica y técnica

Esta tarea debe por supuesto ser realizada en conjunto entre el abogado y el consultor técnico. Debe primar lo procedimental, es decir:

La revisión científica, debe ser efectuada utilizando los mecanismos establecidos en el Método Científico clásico, adaptado a la disciplina de la cual se trate. En el caso de la Informática Forense, dicha revisión se basa en los principios de la disciplina (véase capítulo correspondiente), los que deben ser analizados y exigidos de manera exhaustiva. Ninguna aseveración presente en el informe debe contravenir las leyes de las ciencias naturales y formales. El análisis profundo de los algoritmos establecidos como fundamento de las conclusiones alcanzadas es la primera tarea a realizar por el experto y a explicar al abogado que lo contrató. Esto incluye, el diseño, la implementación, la programación y el empleo específico de cada herramienta utilizada. Para el perito significa una profunda y clara formación en Sistemas

Operativos, su desarrollo e instrumentación. Muchos principios considerados inamovibles en las disciplinas criminalísticas dejan de ser válidos en la informática forense, como ejemplo el principio de identidad, ya que dos bits no son iguales sino idénticos. El orden de revisión implica que dentro de las ciencias teóricoexperimentales, se encuentra la Criminalística como disciplina autónoma y en el marco de la Criminalística, se inserta la Informática Forense. Sin olvidar que dos de los sustentos principales y razones de ser de la Informática Forense, lo constituyen la Informática y el Derecho (en particular el Derecho Procesal). Un profesional de la Informática Forense que no esté versado en Derecho Procesal, seguramente terminará arruinando la prueba pretendida, por desconocimiento de las formas que la abarcan y constituyen.

En lo referido a lo tecnológico, dependerá directamente del estado de avance de la especialidad en el momento considerado. La Informática, uno de los pilares de la Informática Forense, avanza a cada segundo, los instrumentos no llegan a venderse, cuando ya son superados por otros mejores, más eficientes, efectivos y eficaces. La única constante de la Informática es su cambio permanente. La Informática se encuentra instaurada en la mayoría de los elementos tecnológicos que nos rodean, forma el entramado lógico que brinda soporte a las comunicaciones, a la difusión del conocimiento y al contacto interpersonal indiferente a las distancias que separan a los interlocutores. Por lo tanto es imposible establecer una posición tecnológica sostenible, por un plazo superior a una semana, en el mejor de los casos. La respuesta a este requerimiento es la investigación permanente sobre los nuevos desarrollos y sus modos de empleo. El perito debe permanecer actualizado, estar siempre en formación, si cree que no necesita actualizar sus conocimientos es un ignorante. En Informática los que hablan con más seguridad, son generalmente los que menos conocen, más suponen y por lo tanto deberían ser menos confiables.

En lo referido a la tecnología disponible, es preciso establecer la pertinencia en el empleo de los instrumentos utilizados. Existen herramientas específicas para la gestión de la prueba documental informática y su revisión por medios periciales informático forense. Es decir no cualquier instrumento de almacenamiento permite resguardar la información y preservarla para futuros exámenes sin que sea modificada en un solo bit. El desarrollo de estos instrumentos (*hardware*), permite la realización de la tarea en condiciones de seguridad que son ineludibles en la labor pericial. Es por ello que el empleo de terminales forenses es el objetivo de máxima que debería pretender el perito, es cierto que sus costos son elevados y que pueden ser sustituidos por elementos similares utilizados de manera apropiada.

La terminal autónoma informática forense cumple una función equivalente al laboratorio químico portátil, para quienes deben buscar, detectar y secuestrar drogas.

El técnico que utiliza una reacción orientativa de cocaína, actúa en el lugar del hecho y brinda importante información decisoria al organismo judicial interventor, mucho antes de la confirmación por medios periciales en el laboratorio químico especializado. Algo similar ocurre con la informática forense. Sus herramientas se componen de instrumentos (*hardware)* y aplicaciones (*software)*, que aseguran los elementos mínimos de preservación de la prueba exigidos en cualquier otro análisis pericial criminalístico. Si no se puede asegurar la integridad y disponibilidad de los datos recolectados o procesados, el procedimiento debería ser declarado nulo, ya que no puede ser comprobado *a posteriori,* por otros expertos, afectando el derecho constitucional al debido proceso de quien resulte perjudicado por los resultados de dicha tarea.

Las mismas consideraciones deben aplicarse a las aplicaciones utilizadas en los instrumentos específicos o generales empleados en la tarea. Existen aplicaciones comerciales específicas y otras similares desde el ámbito del *software libre*, es decir que están a disposición de los expertos, ya sea que tengan o no suficiente poder adquisitivo para adquirirlas. Reiteramos, el precio a pagar es el esfuerzo, la dedicación y el estudio, monedas con las que deberíamos contar en todo momento.

En lo técnico, aunque supeditado al punto anterior, es necesario establecer que el cambio tecnológico y la sustitución científica de ciertos principios generales (como el referido principio de identidad impropio), no implican la ausencia de técnicas de investigación, análisis y obtención de conclusiones específicas, claras e ineludibles. Las técnicas a utilizar (con las particularidades referidas), son las clásicas técnicas Criminalísticas. Casi todas las referencias establecidas para la búsqueda, detección y preservación de prueba, ya consolidadas por la Criminalística, son pertinentes en nuestro caso. Está claro que no es lo mismo una inspección judicial para comprobar un homicidio, detectar huellas dactilares, analizar activos contables, reconocer el lugar de un accidente de tránsito, que para recolectar prueba documental informática, pero todas estas tareas difieren en lo específico y concuerdan en lo general. La formación criminalística del perito en informática forense no es una característica deseable, sino una condición ineludible.

Reconocidos los principios científicos involucrados, utilizando la mejor tecnología disponible o accesible (siempre están presentes los recursos económicos), mediante una actitud proactiva de aprendizaje y capacitación permanentes y aplicando las técnicas criminalísticas generales y los protocolos particulares de la informática forense, el navegante de la Informática Forense tiene muchas posibilidades de arribar a buen puerto en su tarea pericial.

Revisión lógica

Esta etapa suele ser tenida en menos por muchos profesionales, ya sea por subestimar la potencia de la lógica como herramienta de análisis del discurso o por haber tenido malas experiencias educativas a su respecto. Existe toda una corriente de pensadores de todas las disciplinas que han optado por mantenerla alejada de su acervo de investigación. Eso ha configurado una extraña situación por parte de la ciencia en general; aparecen las ciencias duras (que parecen incluir a las ciencias naturales), las ciencias blandas (que mantienen los más alejado posible al fenómeno numérico) y todo un espectro de grises que las relacionan. En realidad, es poco concebible un hombre que actúe sin ningún tipo de lógica, utilizando este concepto en su mínima expresión, como orden y sucesión de conductas. Hasta los dementes tienen sus propias y personales razones para actuar. Claro esto está muy lejos de la lógica simbólica y sus significados. Pero aquel profesional que la utilice tendrá una clara ventaja sobre quien no lo hace.

El análisis lógico debe incluir:

Revisión de los conceptos involucrados en la fundamentación de los resultados periciales.

Construcción de proposiciones lógicas a partir de dichos conceptos (variables binarias puras).

Resolución de las proposiciones conseguidas, mediante métodos adecuados (transformación de proposiciones en premisas, mediante la determinación de su valor de verdad real, para el caso considerado).

Integración de las premisas en silogismos.

Revisión de los silogismos que dan lugar a la construcción argumental demostrativa.

La tarea pretendida no es simple, la mayoría de los profesionales ignora esta forma de construir el pensamiento y su consecuencia la expresión oral y escrita. Se piensa de forma desordenada, se escribe de igual manera y se discute sin ninguna estructura lógica de fondo. Es un tema de sumo interés pero que trasciende los alcances de esta obra; como sugerencia general para todos los actores involucrados en una pericia infomático-forense se recomienda la lectura profunda de al menos las obras más pertinentes al respecto, puesto que éstas deberían formar parte de la formación académica de todos los profesionales.[27]

Revisión formal

Este punto también es de suma importancia y no debe ser descuidado por quien realiza una revisión de un informe pericial. El informe pericial debe contener determinados elementos, sin los cuales pierde su razón de ser. En lo que hace al perito se sugiere seguir estrictamente los pasos establecidos en el capítulo anterior, respecto de la presentación formal del mismo (Introducción, Objeto, Elementos, Operaciones, etc.), de esta manera se logran varios resultados positivos para la tarea pericial, entre ellos presentar la información de manera ordenada y fácilmente asequible por el lego, demostrar idoneidad de fondo y forma al expresarnos de manera escrita, implementar una estructura de informe ampliamente probada por la Criminalística y sobre todo cumplir sobradamente con los requisitos procesales exigidos.[28]

Está claro que no es posible exigirle una estructura estricta, como la propuesta en esta obra, a muchos de los profesionales que pueden actuar como peritos ante el órgano judicial. Un perito puede ser simplemente el mecánico de la cuadra que se refiere a la rotura de un vidrio o a los daños de un vehículo (algo sumamente frecuente en especial al litigar con o contra las empresas de seguros automotores) y muchos otros casos similares. Sin embargo, el perito en informática forense no está (o no debería estar) incluido entre dichas excepciones, debe ser un profesional formado, con título de grado y expresión oral y escrita acordes, con su pretensión pericial.

Podemos aceptar un programador cuasi autista por decisión propia (abstraído de la realidad y con muy poca interacción social), un diseñador de redes con tendencias ermitañas, un generador de aplicaciones disociado de la realidad (de hecho a diario nos topamos con ellos), pero no podemos admitirlo en un perito o experto en Informática Forense. Si el profesional de la Informática Forense no es capaz de expresarse correctamente, en forma oral y escrita, siguiendo una estructura discursiva de amplia aplicación en criminalística y de excelentes resultados como soporte probatorio, dichas falencias deben ser suplidas por el operador del derecho que lo contrata (revisando el informe antes de su entrega al tribunal) o lo mejor de todo debe prescindir de él.

En cuanto a las listas de peritos de oficio, cuyo único requisito es la presentación de un título académico, las mismas adolecen de estas falencias que la mayoría de los Colegios de Abogados; alcanza con tener el título, para ser considerado idóneo en la materia (por eso se pierden tantos juicios, con personas que pierden su patrimonio o su libertad, se dilapidan tantas vidas en los quirófanos y mueren tantas personas en accidentes de tránsito). El título de grado debería ser requisito necesario para el perito informático forense, pero no condición suficiente. A los Consejos Profesionales les incumbe encargarse de evaluar la idoneidad de sus matriculados (aun en perjuicio de sus ganancias por matriculación, que parece ser el único objetivo que pretenden). Tal vez sea utópico, pero los Consejos Profesionales, herederos de los viejos gremios

medievales, deberían ser centros de capacitación y estímulo profesional, en vez de simples oficinas de recaudación y generación de empleo administrativo. De más está decir que la inscripción en la lista de peritos debería incluir un examen propedéutico inicial y un examen de actualización quinquenal (tiempo por otra parte excesivamente extenso en lo referido a la disciplina informático forense y sus cambios tecnológicos asociados). Es tanto o más peligroso aceptar la idoneidad de un perito por la simple presentación de un currículum y un título, que entregar un carné de conducir, mediante la presentación de testimonios a elección del solicitante.

Como complemento de lo expresado, es posible sugerir el control de los siguientes componentes periciales:

Comprobar la pertinencia científica, tecnológica y técnica de los conceptos vertidos.

Ídem sobre las operaciones realizadas.

Analizar la coherencia lógica argumental en el desarrollo expositivo.

Revisar la inserción procesal del informe, adecuado a la jurisdicción y competencia de la causa en trámite.

Determinar el cumplimiento de los requisitos legales, respecto de la propiedad intelectual de los instrumentos utilizados en el análisis.

Solicitar al perito propio que reúna los puntos periciales de la contraparte para ver si son redundantes, inconducentes o impertinentes.

Comprobar el uso de instrumental específico (*hardware*).

Ídem, de programas específicos (*software*).

Ídem, de licencias de uso de los programas de base y aplicaciones utilizados (copia ilegal).

Detectar errores metodológicos (faja de clausura y disco conectado).

Establecer la idoneidad real del personal asignado a la tarea: título de grado necesario (no es de aplicación la excepción del art. 464, CPCCN, ya que la obtención del título de grado correspondiente es posible en todo el territorio nacional) y especialización informático forense deseable.

Mostrar las fallas formales en el informe técnico: carencia de separaciones temáticas, incumplimiento estricto de los puntos de pericia (por falta o por exceso).

15 CPCCN. “IMPUGNACIÓN. DESINTERÉS. CARGO DE LOS GASTOS Y HONORARIOS. Art. 478. Los jueces deberán regular los honorarios de los de peritos y demás auxiliares de la justicia, conforme a los respectivos aranceles, debiendo adecuarlos, por debajo de sus topes mínimos inclusive, a las regulaciones que se practicaren en favor de los restantes profesionales intervinientes, ponderando la naturaleza, complejidad, calidad y extensión en el tiempo de los respectivos trabajos. *(Párrafo incorporado por art. 10 de la Ley N° 24.432 B.O. 10/1/1995)* Al contestar el traslado a que se refiere el segundo párrafo del artículo 459, la parte contraria a la que ha ofrecido la prueba pericial podrá: 1) Impugnar su procedencia por no corresponder conforme a lo dispuesto en el artículo 457; si no obstante haber sido declarada procedente, de la sentencia resultare que no ha constituído UNO (1) de los elementos de convicción coadyuvante para la decisión, los gastos y honorarios del perito y consultores técnicos serán a cargo de la parte que propuso la pericia. 2) Manifestar que no tiene interés en la pericia, y que se abstendrá, por tal razón, de participar en ella; en este caso, los gastos y honorarios del perito y consultor técnico serán siempre a cargo de quien la solicitó, excepto cuando para resolver a su favor se hiciere mérito de aquélla.”

16 CPCCN. “IDONEIDAD. Art. 464. Si la profesión estuviese reglamentada, el perito deberá tener título habilitante en la ciencia, arte, industria o actividad técnica especializada a que pertenezcan las cuestiones acerca de las cuales deba expedirse. En caso contrario, o cuando no hubiere en el lugar del proceso perito con título habilitante, podrá ser nombrada cualquier persona con conocimientos en la materia.”

17 CPCCN. “EFICACIA PROBATORIA DEL DICTAMEN. Art. 477. La fuerza probatoria del dictamen pericial será estimada por el juez teniendo en cuenta la competencia del perito, los principios científicos o técnicos en que se funda, la concordancia de su aplicación con las reglas de la sana crítica, las observaciones formuladas por los consultores técnicos o los letrados, conforme a los artículos 473 y 474 y los demás elementos de convicción que la causa ofrezca.”

18 CPCCN. “ANTICIPO DE GASTOS. Art. 463. Si el perito lo solicitare dentro de tercero día de haber aceptado el cargo, y si correspondiere por la índole de la pericia, la o las partes que han ofrecido la prueba deberán depositar la suma que el juzgado fije para gastos de las diligencias. Dicho importe deberá ser depositado dentro del quinto día, plazo que comenzará a correr a partir de la notificación personal o por cédula de la providencia que lo ordena; se entregará al perito, sin perjuicio de lo que en definitiva se resuelva respecto de las costas y del pago de honorarios. La resolución sólo será susceptible de recurso de reposición. La falta de depósito dentro del plazo importará el desistimiento de la prueba.”

19 CPCCN. “RECUSACIÓN. Art. 465. El perito podrá ser recusado por justa causa, dentro del quinto día de la audiencia preliminar. *(Artículo sustituido por art. 2° de la Ley N° 25.488 B.O. 22/11/2001)* CAUSALES. Art. 466. Son causas de recusación del perito las previstas respecto de los jueces; también, la falta de título o incompetencia en la materia de que se trate, en el supuesto del artículo 464, párrafo segundo. REEMPLAZO. Art. 468. En caso de ser admitida la recusación, el juez, de oficio,

reemplazará al perito recusado, sin otra sustanciación.”

20 CPCCN. “TRÁMITE. RESOLUCIÓN. Art. 467. Deducida la recusación se hará saber al perito para que en el acto de la notificación o dentro de tercero día manifieste si es o no cierta la causal. Reconocido el hecho o guardado silencio, será reemplazado; si se lo negare, el incidente tramitará por separado, sin interrumpir el curso del proceso. De la resolución no habrá recurso pero esta circunstancia podrá ser considerada por la alzada al resolver sobre lo principal.”

21 CPCCN. “PERITO. CONSULTORES TÉCNICOS. Art. 458. La prueba pericial estará a cargo de UN (1) perito único designado de oficio por el juez, salvo cuando una ley especial establezca un régimen distinto… Cada parte tiene la facultad de designar una consultor técnico”.

22 CPCCN. “PRESENTACIÓN DEL DICTAMEN. Art. 472. El perito presentará su dictamen por escrito, con copias para las partes. Contendrá la explicación detallada de las operaciones técnicas realizadas y de los principios científicos en que se funde. Los consultores técnicos de las partes dentro del plazo fijado al perito podrán presentar por separado sus respectivos informes, cumpliendo los mismos requisitos”.

23 CPCCN. “TRASLADO. EXPLICACIONES. NUEVA PERICIA. Art. 473. Del dictamen del perito se dará traslado a las partes, que se notificará por cédula. De oficio o a instancia de cualquiera de ellas, el juez podrá ordenar que el perito dé las explicaciones que se consideren convenientes, en audiencia o por escrito, atendiendo a las circunstancias del caso… Si las explicaciones debieran presentarse por escrito, las observaciones a las dadas por el perito podrán ser formuladas por los consultores técnicos o, en su defecto, por las partes dentro del quinto día de notificadas por ministerio de la ley. La falta de impugnaciones o pedidos de explicaciones u observaciones a las explicaciones que diere el perito, no es óbice para que la eficacia probatoria del dictamen pueda ser cuestionada por los letrados hasta la oportunidad de alegar con arreglo a lo dispuesto por el artículo 477”.

24 CPCCN. “DICTAMEN INMEDIATO. Art. 474. Cuando el objeto de la diligencia pericial fuese de tal naturaleza que permita al perito dictaminar inmediatamente, podrá dar su informe por escrito o en audiencia; en el mismo acto los consultores técnicos podrán formular las observaciones pertinentes”.

25 “SECCIÓN 7° RECONOCIMIENTO JUDICIAL MEDIDAS ADMISIBLES Art. 479. El juez o tribunal podrá ordenar, de oficio o a pedido de parte: 1) El reconocimiento judicial de lugares o de cosas. 2) La concurrencia de peritos y testigos a dicho acto. 3) Las medidas previstas en el artículo 475. Al decretar el examen se individualizará lo quedeba constituir su objeto y se determinará el lugar, fecha y hora en que se realizará. Si hubiere urgencia, la notificación se hará de oficio y con UN (1) día de anticipación. FORMA DE LA DILIGENCIA. Art. 480. A la diligencia asistirá el juez o los miembros del tribunal que éste determine. Las partes podrán concurrir con sus representantes y letrados y formular las observaciones pertinentes, de las que se dejará constancia en acta”.

26 CPCCN. “PLANOS, EX ÁMENES CIENTÍFICOS Y RECONSTRUCCIÓN DE LOS HECHOS Art. 475. De oficio o a ped ido de pa r te, el juez podrá ordenar: 1) Ejecución de planos, relevamientos, reproducciones fotográficas, cinematográficas, o de ot ra especie, de objetos, documentos o lugares, con empleo de medios o instrumentos técnicos. 2) Exámenes científicos necesarios para el mejor esclarecimiento de los hechos controvertidos. 3) Reconstrucción de hechos, para comprobar si se han producido o pudieron realizarse de una manera determinada. A estos efectos podrá disponer que comparezcan el perito y los testigos y hacer saber a las partes que podrán designar consultores técnicos o hacer comparecer a los ya designados para que participen en las tareas, en los términos de los

artículos 471 y, en su caso, 473”.

27 Bibliografía básica, mínima, indispensable, sugerida:Echave, Delia Teresa; Urquijo, María Eugenia y Guibourg, Ricardo, *Lógica, proposición y norma.* Editorial Astrea. Buenos Aires, 2008.Guarinoni, Ricardo, *Derecho Lenguaje y Lógica*, Editorial Lexis Nexis. Buenos Aires, 2006.Alchourrón, Carlos; Bulygin, Eugenio, *Introducción a la metodología de las ciencias jurídicas y sociales*, Editorial Astrea, Buenos Aires, 2006.

28 CPCCN. “PRESENTACIÓN DEL DICTAMEN. Art. 472. El perito presentará su dictamen por escrito, con copias para las partes. Contendrá la explicación detallada de las operaciones técnicas realizadas y de los principios científicos en que se funde. Los consultores técnicos de las partes dentro del plazo fijado al perito podrán presentar por separado sus respectivos informes, cumpliendo los mismos requisitos”.

CAPÍTULO 10
VALOR PROBATORIO
DE LA PRUEBA INDICIARIA
INFORMÁTICO FORENSE

Prueba documental informática (recaudos procesales)

Estamos absolutamente convencidos de la pertinencia del trabajo transdisciplinario en la gestión de la prueba informático forense, la cual se muestra compleja para todos los operadores del Derecho, de la Criminalística y de la Informática, ya que es atinente a las tres disciplinas, pero independiente e integradora en su composición.

Independiente, porque trasgrede principios de las tres disciplinas e integradora, porque se refiere específicamente a la información y desde la Teoría de la Información nos dicen que *"Información: no es otra cosa que la magnitud en la reducción de la incertidumbre"*. La prueba documental informática (una especie de la prueba indiciaria informática), tiene todas las características de la documental bibliográfica o foliográfica, que desde antaño manipulan los operadores del Derecho, adquiere principios que la asemejan a la prueba pericial documentológica (Criminalística) y requiere de conocimientos propios de la Informática. Sin embargo, en todos los casos, muestra notorias diferencias con los puntos referidos.

Se hace entonces imprescindible una visión transdisciplinaria e integradora, que facilite la interacción, el debate y la reformulación conceptual, procedimental y actitudinal, en los equipos de tareas que brinden soporte a la decisión de S. Sa. A tal efecto intentaremos realizar una aproximación desde las tres visiones, que permita establecer un lenguaje dialogal útil, para la discusión argumental y probatorio de rigor y en particular al uso de la prueba pericial informático forense.

Las siguientes consideraciones nos serán de utilidad para aproximarnos al tema analizado:

"La prueba documental informática es a la Pericia Informática-Forense, lo que la prueba documental es a la Pericia Documentológica."

"La Informática Forense es a la Informática, lo que la Medicina Legal a la Medicina."

“El lugar del hecho virtual es al lugar del hecho, lo que la realidad virtual, es a la realidad”.

“Informática Forense es el conjunto multidisciplinario de teorías, técnicas y métodos de análisis, que brindan soporte conceptual y procedimental, a la investigación de la prueba indiciaria informática.”

Inserción de la prueba documental informática

La prueba documental informática obra como parte de la prueba documental tradicional (foliográfica y/o bibliográfica). En efecto, este aserto parte de diversos supuestos a destacar:

La prueba documental, que es regulada en los distintos Códigos de Procedimientos y aceptada en forma homogénea, es tratada como una prueba única, sin embargo, técnicamente es posible subdividirla en dos grupos principales:

La prueba documental bibliográfica: integrada por todo tipo de documentos, cuya principal característica es que se trata de documentos escritos (de texto) en diversos soportes, siendo el más frecuente el papel.[29]

La prueba documental foliográfica: en forma autónoma, o complementaria de la bibliográfica, integrada, por todos aquellos documentos en diversos soportes (el más frecuente nuevamente es el papel) que contienen datos representados en forma gráfica (pictográfica o no, entre otros: gráficos, planos, mapas, esquemas, tablas, etc.).

La prueba documental informática sólo difiere de la prueba documental referida en el apartado anterior en un aspecto: “el soporte”. Por esta razón, no debería ser tratada por el Derecho Procesal en una forma notoriamente diferente de lo acostumbrado:

Se trata de archivos (en papel o digitales, pero conteniendo texto y/o gráficos).

Se pueden reproducir sin restricciones.

Son adulterables mediante maniobras de modificación remotas.

Pueden ser firmadas y certificadas.

Constituyen elementos probatorios de similar valor decisivo.

Difieren en dos puntos principales:

Mientras los documentos en papel, adhieren al principio de identidad criminalístico, los digitales no lo hacen.[30] Por otra parte, esta característica nos asegura que al realizar operaciones sobre la copia, los resultados no son similares, sino idénticos a los obtenidos trabajando sobre el original.

Los documentos digitales son fácilmente modificables por medios remotos, lo que no ocurre con los documentos bibliográficos o foliográficos.

La prueba documental informática puede ser utilizada en igual forma que la bibliográfica o la foliográfica, ya que:

Es susceptible de certificación por medio de un escribano digital (autoridad certificante y firma digital).

También por medio de un escribano tradicional (escribano, acta notarial, rutina de *hash* certificada en el acta notarial).

Acorde con su nivel de certificación y clasificación de seguridad (pública, pública interna, reservada, confidencial, secreta, estrictamente confidencial y secreta) su solidez probatoria es equivalente a la documental foliográfica o bibliográfica, es decir depende de la validez que le asignen los códigos de forma o fondo de la Nación. Puede conformar un documento público o privado indistintamente y ser susceptible de revisión pericial similar a la documental clásica.

Pertinencia de la prueba documental informática

Establecidas las similitudes entre la prueba documental bibliográfica, su homónima foliográfica y la documental informática, podemos afirmar que ambas son igualmente pertinentes, ya que sólo difieren en el soporte que las contiene. Respecto de su validez probatoria es idéntica y en lo referente a su comprobación pericial, respetando lo afirmado respecto del principio de identidad impropia y la posibilidad de modificación a distancia son perfectamente equivalentes, por lo que no requieren ninguna modificación en los textos procesales. La asimilación del correo electrónico con la correspondencia epistolar es un ejemplo de uso de la herramienta informática en sentido similar a su equivalente tradicional, que fija un antecedente válido para la afirmación realizada. *"El correo electrónico es al correo epistolar lo que la prueba documental informática es a la prueba documental tradicional (foliográfica o bibliográfica) y a la pericia informático forense a la pericia documentológica."*

No obstante es necesario aclarar que la pertinencia de la prueba dependerá de la

correcta interpretación de sus características particulares al solicitarla, implementarla y especialmente al evaluarla. En un fallo reciente, de la Cámara Nacional de Apelaciones en lo Comercial, Sala "D",[31] se acepta el valor probatorio de un mensaje de correo electrónico, que no ha sido firmado digitalmente. Entre los fundamentos para adoptar tal decisión, me parece conveniente destacar:

> *"En el valor probatorio del correo electrónico ocupan un lugar preeminente a partir de la vigencia de la ley 25.506 los documentos con firma digital, en tanto su valor probatorio es equiparable al de los instrumentos privados, y se presume la autoría e integridad del mensaje, correspondiendo a la otra parte destruir tales presunciones (v. Hocsman, H.* Negocios en Internet*, cap. II, Nº 63.b. pp. 162/164, ed. 2005)."*

Esta afirmación, ya está arraigada en la doctrina y jurisprudencia vigentes que asimilan la firma digital a la firma hológrafa, pero constituye la base de la argumentación posterior.

> *"Aun cuando en este caso se trata de documentos que carecen de firma digital a los que no puede otorgarse un valor de convicción preeminente por no cumplir con los requisitos de los arts. 2 y 5 de la ley 25.506 sobre* firma digital *puesto que el elemento de autenticación o certificación es un requisito esencial de autenticidad (Conf., esta sala, 16.02.2007 Henry Hirschen y Cía. S.A. c/ Easy Argentina S.R.L. [Fallo en extenso: el Dial AA3CEE]), no existe impedimento a mi juicio para que se los ofrezca como medio de prueba (C.P.C. 378:2), considerándoselos principios de prueba por escrito como había aceptado la doctrina de los autores antes de la sanción de la citada ley Nº 25.506. Tal valor probatorio se sustenta en las normas del C.C. 1190, 1191, 1192, pues aunque por no estar firmados no alcancen la categoría de documento privado es admisible su presentación en juicio para probar un contrato siempre que emanen del adversario, hagan verosímil el hecho litigioso y que las restantes pruebas examinadas a la luz de la sana crítica corroboren su autenticidad. Por lo tanto, es decisiva la prueba complementaria que se produzca merituada conforme con los criterios de la sana crítica y conjuntamente con las restantes pruebas del proceso (vid. esta Sala, 26/9/2006, 'Gómez Fabián c/ Banco de la Ciudad de Buenos Aires'; Kielmanovich, J. 'Teoría de la prueba y medios probatorios' /cap. XI', nros. 2. c y 3, pp. 393/ 398, ed. 2004; Somer, M. 'Documento Electrónico', J.A. 2004-I pp. 1034/1035; Gaibrois, L.,'Un aporte para el estudio del valor probatorio del documento electrónico', J.A. 1993, II, ap. IX, p. 963)."*

La fundamentación anterior se sustenta en diversas afirmaciones que me parece interesante evaluar:

Afirma que se trata de documentos sin firma digital, es decir si el soporte fuera papel serían documentos sin firma hológrafa.

Les reconoce no obstante el valor de *"principio de prueba por escrito"*, sustentado en los artículos 1190, 1191 y 1192 del Código Civil.[32] Es interesante destacar que se trata de artículos referidos exclusivamente a la prueba de los contratos, lo que no impide su uso por analogía en otros casos no penales.

Deben ser corroborados por otros elementos de prueba y no resultar contrarios o contradictorios con los mismos.

Este último punto es primordial para analizar las consecuencias de esta argumentación. En ella se hace referencia a un caso particular, en que el mensaje de correo electrónico coincide y es soportado por otros elementos probatorios, los que se complementan entre sí, coinciden y no difieren. Nada dice respecto del supuesto en que el "único" elemento probatorio existente sea un mensaje de correo electrónico, algo muy frecuente en los contratos internacionales de bajo monto, que obran a diario en el marco del Derecho Internacional Privado[33] Es decir, no deberíamos inferir *a contrario sensu* que el mensaje de correo electrónico no firmado digitalmente como elemento probatorio único es válido (ni tampoco inválido), ya que sería el equivalente a un documento no firmado (cuyo valor indiciario es susceptible de evaluación, pero difícilmente alcance la categoría de prueba plena sobre el hecho pretendido).

> *"Es un hecho público y notorio (v. Couture, E. 'Fundamentos del Derecho Procesal Civil', Nº 150, p. 233, ed. 1993) en este sentido que una dirección de correo electrónico es individual y que no pueden registrarse dos iguales, por lo que puede presumirse sin ninguna duda razonable que la sigla IBM pertenece a la demandada (v. Leguisamón, H. 'Las presunciones judiciales y los indicios', cap. IX, Nº A.2, p. 92, ed. 1991)."*

Ésta es una realidad técnica y administrativa comprobable, no obstante, se refiere a la individualidad de los registros de cuentas, que impide su duplicidad en el entorno de un determinado proveedor de Servicios de Correo Electrónico.[34] Sin embargo, para analizar estrictamente la pertinencia técnica de este aserto, es imprescindible considerar:

Cuando se crea un nombre de dominio (por ejemplo, www.lacartuja.com.ar) este dominio es único y no puede ser asignado a otro requirente.7 Dicha univocidad está siendo certificada por un organismo oficial argentino (www.nic.ar Network Information Center Argentina), o por sus equivalentes internacionales. En cambio en el caso de la creación de una cuenta de correo electrónico la certificación la realiza el

Proveedor de Servicio de Correo Electrónico, en la mayoría de los casos un ente privado con fines de lucro (que las cuentas sean gratis para los usuarios, no implica que no reporten beneficios económicos a quienes las administran y asignan), o una empresa, o una institución oficial o privada cualquiera.

La diferencia establecida en el punto anterior determina que los requisitos necesarios para crear una cuenta ante el NICAR difieran notoriamente de los exigidos para crear una cuenta en ar.yahoo.com. En el segundo caso prácticamente no existen y salvo que usted coloque una fecha de nacimiento que establezca su edad, en menos de 18 años, prácticamente no existe restricción alguna, para su creación y operación posterior. Si está libre la dirección ford-argentina@yahoo.com.ar, nada impide que usted cree la cuenta, aunque se llame López, viva en Tanzania y se dedique a operar una empresa de turismo. Este hecho es frecuente entre la juventud informatizada, que crean de manera rutinaria cuentas de correo con nombres y datos falsos, para utilizarlas como una especie de "correo anónimo", especialmente en sus relaciones con otros adolescentes.[35]

Del apartado anterior podemos inferir que una cosa es el nombre de la cuenta de correo y otra muy distinta la identidad de su propietario. Ambos pueden coincidir o no, pero esta circunstancia, debe ser determinada por otros medios probatorios (pruebas de informes al Proveedor de Servicios, Datos Personales de la Cuenta, Dirección IP desde la cual fue creada la cuenta, empleo de la misma en operaciones típicas de la empresa, etc.)

Considero que el argumento no especifica con claridad la diferencia entre el nombre de la casilla de correo electrónico, que no puede ser duplicado en el mismo entorno restringido (Proveedor de Servicio de Correo Electrónico) y la identidad y datos filiatorios de quien la creó y utiliza. Para establecer estos últimos datos, es necesario contar con otro tipo de prueba (Informes del ISP o del proveedor de Servicio de Correo Electrónico, comprobación de datos de la cuenta, pericia informático forense, entre otros). De lo contrario se corre el riesgo de asignar autoría de un hecho a una persona, a partir de una cuenta fraudulenta (algo así como responsabilizar a una persona, por los dichos contenidos en una carta anónima, realizada por un tercero).

"Todos estos elementos permiten inferir con el valor del C.P.C. 165 la verdad y existencia del hecho constitutivo de la pretensión, esto es: que tuvo lugar una brusca ruptura de las tratativas después de haber sido confirmada la fabricación de los gabinetes por medio de los correos electrónicos (conf. Palacio, L. y Alvarado Velloso, A., Código Procesal Civil y Comercial de la Nación, explicado y anotado jurisprudencial y bibliográficamente*; t. 4, art. 163, Nº 172.1.1.7.5.1., p. 416, ed. 1989) configurándose de esa forma, un supuesto de responsabilidad precontractual en razón*

de haber operado una ruptura intempestiva e injustificada de las tratativas preliminares que es generador de responsabilidad en tanto presuponen un deber general de no causar un daño y el eventual deber de repararlo en caso contrario (v. Etcheverry, R. A. Derecho comercial y económico Obligaciones y contratos comercialesParte general, *Nº 68.c., p. 212, ed. 1994; Waisman, A 'Responsabilidad precontractual en función del precontrato', en www.laleyonline.com.ar).''*

Este colofón es un resultado inferido en razón de los apartados anteriores, es concluyente y establece una responsabilidad real que puede devenir en afectaciones patrimoniales de los destinatarios de la misma (en otros casos podría llegar a la imposición a un acusado de una pena restrictiva de la libertad ambulatoria).[36] No pretendo discutir la conclusión alcanzada, que supongo ha sido obtenida a partir de otros medios probatorios concluyentes, siendo el mensaje de correo electrónico un simple complemento de los mismos, pero considero que el empleo de los mensajes de correo electrónico, no firmados digitalmente, deberían ser motivo de un amplio debate transdisciplinario, en aras de establecer específicamente su naturaleza y pertinencia probatorias.

El acceso y resguardo de la documental informática

Es necesario al respecto establecer las condiciones de legitimidad y legalidad al acceder, detectar, resguardar y certificar la documental informática, para evitar la vulneración de derechos personalísimos (como, por ejemplo, la privacidad y la propiedad de la información afectada).

En ese sentido es preciso dividir a la información disponible, acorde con su alojamiento, al ser accedida:

Información pública: Es de libre disponibilidad, se encuentra publicada en cualquier medio irrestricto de almacenamiento de información (publicidad, propaganda, páginas Web, grupos abiertos, almacenamiento sin restricciones, etc.), esta información puede ser libremente accedida, resguardada en un soporte adecuado (generalmente CD o DVD, por sus condiciones de seguridad en prevención de falsificaciones y/o adulteraciones) y certificada por los medios que trataremos más adelante.

Información privada disponible en equipos del actor: Tiene las mismas características que la información pública, sólo difiere en que se encuentra alojada en la máquina del actor. Es imprescindible destacar que puede ser información generada o recolectada por el actor (por medios legales y lícitos) o información que le fuera

enviada por un tercero. En este sentido, los mensajes de correo electrónico recibidos por el actor y guardados en su máquina son propiedad del actor, de la misma forma en que la correspondencia epistolar enviada por un tercero le pertenece a partir del momento de su recepción. Se aplican las mismas consideraciones del apartado anterior.

Información privada disponible en equipos de terceros: En este caso es necesario distinguir la calidad de dicho equipo respecto de su propietario:

Los equipos de un Ciber Café son propiedad del dueño del establecimiento, sin embargo, por ser equipos de libre disponibilidad, la información almacenada en los mismos no goza de protección alguna, de la misma forma en que un cartel de propaganda colgado de una pared o pendiente de un pizarrón de anuncios es absolutamente público (pensemos en la analogía con sistemas como Veraz, que además tiene fines de lucro). Se le aplican las consideraciones de los apartados anteriores.

Sin embargo, si de trata de máquinas particulares y de uso exclusivo de una persona, entonces y sólo entonces gozan de la absoluta privacidad que le otorga la ley, desde el Derecho Constitucional, hasta la Ley de Fondo y sus Reglamentación, Normas y Disposiciones. Esta información sólo puede ser accedida con orden judicial previa y no pueden admitirse excepciones. El acceso por medios ilegítimos e ilegales (normalmente llamado *hacking, cracking* y sus similares) invalida la prueba, en el Derecho Penal, por aplicación de la Doctrina del Fruto del Árbol Envenenado (Venenoso), y en los restantes fueros por la ilegalidad del método de acceso utilizado, sin el correspondiente aval judicial (Acta de Allanamiento u Orden de Acceso Forzado), con las condiciones, prevenciones y resguardos establecidos para cada procedimiento.

La certificación de la documental informática

Me referiré ahora a la certificación de la prueba documental informática en las siguientes condiciones:

Sólo en los casos señalados en el parágrafo anterior, identificados como 1. 2. y 3. a.

Siempre con fines de:

Resguardar elementos probatorios disponibles en el equipo del actor o en equipos públicos.

Proveer al cumplimiento de medidas previas, preliminares, diligencias *in audita altera pars* y pruebas anticipadas, preservando los requisitos procesales asociados.

Asegurando el cumplimiento de los requisitos establecidos para la protección de los activos informáticos en general y de la documental informática en particular respecto de su confiabilidad como elemento probatorio, la que descansa en los siguientes componentes:

Integridad que implica:

Autenticidad,

Seguridad ante ataques pasivos y activos (tema demasiado amplio para ser tratado en este punto).

Autenticidad,

Confidencialidad,

Privacidad,

Disponibilidad que implica:

Evitar la denegación de servicios,

Asegurar el no repudio.

Asegurando al solicitarla o resguardarla *per se*, los mismos componentes que cualquier cautelar:

Verosimilitud del derecho invocado o a invocar.

Peligro en la demora.

Contracautela lógica: Cumplimiento estricto del punto 3, del presente parágrafo (ley

25.326 y art. 90, CPPCABA). No sustituye la contracautela requerida por el tribunal interventor, sino que deviene en una medida complementaria que asegure la privacidad de los datos accedidos.

Participación de los actores necesarios para el resguardo de la prueba:

Interesado (futuro o actual actor)

Funcionario convalidante (oficial de Justicia u otra autoridad pública en los casos descriptos en el punto 3. b. del parágrafo anterior.

Funcionario certificante (escribano público en los casos de resguardar la prueba, antes de iniciar las acciones judiciales).

Personal informático calificado (debería corresponder de manera estricta al perito/experto en Informática Forense,[37] no obstante dado lo escaso de estos expertos, eventualmente pueden ser reemplazados por licenciados/ingenieros en Computación, Sistemas de Información o Informática, en lo posible especializados y/o certificados en Seguridad Informática)

Acta notarial de resguardo y certificación (conforme con los rigores formales establecidos por la ley).

Testigos.

Componentes informáticos físicos y lógicos (rutinas de *hash*, firma digital, clausura de dispositivos de almacenamiento).

Recolección estratégica de la documental informática

Si bien es imposible unificar los criterios de los operadores del derecho, en su forma de planificar, preparar y presentar sus estrategias técnicas probatorias, acorde con el rol que les toque cumplir ante un caso determinado, partiré de un presupuesto posible: "al contactarse con su cliente, el abogado analiza el caso, determina su pertinencia jurídica y luego establece su estrategia personal, para atender a la pretensión de su cliente. A partir de esta estrategia planifica su estructura argumental discursiva (lógica y jurídicamente sustentable), buscará doctrina, jurisprudencia y por supuesto planificará los elementos probatorios conducentes y pertinentes a su línea argumental, para sostener sus asertos. Es en ese momento donde reúne la documental relacionada con su tarea profesional (documentos públicos y privados), la que será presentada junto con la demanda o como soporte de los actos jurídicos relacionados con la querella, la actividad fiscal o la defensa. Éste es precisamente el momento de agregar la documental informática, ya que sólo difiere a la documental tradicional en el soporte que la contiene. Si bien la documental tradicional e informática pueden ser elementos suficientes para comprobar una pretensión específica (demandar, contestar demanda, reconvenir, solicitar procesamiento o sobreseimiento, etc.), no es éste el caso más común.[38] Es mucho más común el empleo de otras pruebas que

complementen y brinden sustento a la estrategia argumental planificada. Por ello tradicionalmente se complementa la documental con pruebas de informes, de testigos, de peritos, incluyendo inspecciones y reconocimientos judiciales. Al respecto, en términos generales la documental informática se comporta de manera similar a la documental tradicional, pero deseamos destacar algunas características peculiares de la primera:

En el momento de planificar su empleo es conveniente complementarla con una prueba de informes en relación directa con la misma.[39]

Determinar la existencia de testigos virtuales de los hechos manifestados.[40]

Ante la posible negativa de la contraparte, solicitar la prueba pericial informático forense pertinente.[41] Los puntos de pericia deben ser consensuados con un experto (no todo punto pericial es posible de comprobar y muchos de los que pueden ser comprobados son desconocidos por el lego en la materia), ya que un error en la formulación de los mismos, puede provocar la desestimación, la impugnación y/o la absoluta ineptitud de ésta, para actuar como soporte de la argumentación planeada.

Prueba pericial

En este sentido, debe ser empleada en condiciones similares a la prueba pericial documentológica. Sólo difiere de ésta en el soporte (papel en la mayoría de los casos para la primera y bits representados en forma magnética u óptica en la segunda). Ya hemos tratado en forma extensiva la forma de generar los puntos de pericia. En cuanto a su validez pericial, tiene el mismo respaldo científico tecnológico y técnico que la prueba documental clásica, sólo hace falta que se la acepte y se imponga ante los tribunales. Su necesidad depende únicamente del avance tecnológico que no muestra la misma lentitud que la evolución normativa.

En el delito informático propio e impropio

En el delito informático impropio la documental informática tiene preponderantemente funciones documentales. Se basa en la descripción de lo ocurrido, buscando la reconstrucción del hecho, mediante, representaciones digitales, las cuales incluyen simulaciones e interacción a distancia. Generado el modelo se puede realizar una sesión por teleconferencia, donde una víctima interactúe con los sospechados en una rueda de personas, cambiando su ropa, entorno y accesorios, desde una terminal en su casa y en presencia (virtual) del Juez y los profesionales que sean necesarios. La enorme ventaja que presenta la simulación, empleando medios de

realidad virtual, es que evita el desplazamiento de las personas, se puede grabar lo que las desentiende del tiempo y se puede repetir y revisar las veces que sea necesario (algo que en la reconstrucción del hecho real es sumamente dificultoso y a veces imposible).

En el delito informático propio constituye la manera ideal de mostrar al juez los distintos eventos ocurridos y su correlato temporal. Por ejemplo, se puede simular con realidad virtual el trayecto seguido por los mensajes y las interacciones resultantes para lograr una transferencia de Montevideo a Chile, luego de robar una clave bancaria, hallándose el delincuente en España y atacando con servidores localizados en Pakistán. La simple descripción de estas acciones, torna confuso su desarrollo escrito y tediosa su lectura, mediante la realidad virtual se transforma en una película interactiva, donde el final depende de las variables introducidas por los involucrados y expuestas al Juez.

29 Por supuesto si bien el soporte de papel es el más común, no es el único, ya que puede incluir papiros, pergaminos, transparencias, etcétera.

30 El principio de identidad en Criminalística establece que los objetos *sub peritia*, son sólo idénticos a sí mismos, de esta forma podemos discernir entre un documento en soporte de papel original y su copia (carbónica, por transparencia, facsímil, electrostática, etc.). Sin embargo dos archivos (no importa si contienen programas ejecutables, gráficos, fotografías, texto, archivos de música o lo que fuere), son dos conjuntos numéricos binarios. Por lo tanto es imposible determinar entre dos archivos iguales bit a bit, ¿cuál es el original y cuál la copia?, como se trata de archivos digitales, ambos son idénticos e indistinguibles. Esto puede parecerle extraño al lego, sin embargo no está relacionado con objetos cualesquiera, sino con números y un número es idéntico a otro número e indistinguible (4=4).

31 29.958/2004 “Bunker Diseños S.A. c/ IBM Argentina S.A. S/ Ordinario” – CNCom – Sala D – 02/03/2010.

32 “CAPÍTULO V. De la prueba de los contratos. Artículo 1190: Los contratos se prueban por el modo que dispongan los códigos de procedimientos de las Provincias Federadas: Por instrumentos públicos. Por instrumentos particulares firmados o no firmados. Por confesión de partes, judicial o extrajudicial. Por juramento judicial. Por presunciones legales o judiciales. Por testigos. ”Artículo 1191: Los contratos que tengan una forma determinada por las leyes, no se juzgarán probados, si no estuvieren en la forma prescrita, a no ser que hubiese habido imposibilidad de obtener la prueba designada por la ley, o que hubiese habido un principio de prueba por escrito en los contratos que pueden hacerse por instrumentos privados, o que la cuestión versare sobre los vicios de error, dolo, violencia, fraude, simulación, o falsedad de los instrumentos de donde constare, o cuando una de las partes hubiese recibido alguna prestación y se negase a cumplir el contrato. En estos casos son admisibles los medios de prueba designados.”Artículo 1192: Se juzgará que hay imposibilidad de obtener o de presentar prueba escrita del contrato, en los casos de depósito necesario o cuando la obligación hubiese sido

contraída por incidentes imprevistos en que hubiese sido imposible formarla por escrito. Se considerará principio de prueba por escrito, cualquier documento público o privado que emane del adversario, de su causante o de parte interesada en el asunto, o que tendría interés si viviera y que haga verosímil el hecho litigioso."

33 Contratos generados por el intercambio de bienes y servicios de poco costo, como ser jugo de arándanos, miel, jalea real, dulces regionales, trabajadores golondrina, talleres móviles, traslado de vehículos averiados, etc., que ante el incumplimiento contractual sólo pueden esgrimir mensajes de correo electrónico intercambiados, pero sin firma digital alguna. No existen en este momento autoridades certificantes internacionales que avalen las firmas digitales, ni siquiera en el marco limitado del Mercosur.

34 No pueden coexistir dos cuentas de correo con el mismo nombre y el mismo proveedor. Ejemplo: sandrita@hotmail.com, al ser registrada ante www.hotmail.com, impide que se vuelva a genear un homónimo en ese entorno, nada impide la existencia de otra cuenta, con igual nombre, en otro proveedor de servicios de correo electrónico: sandrita@yahoo.com.

35 O en casos mucho más aberrantes, cuando los pedófilos se hacen pasar por niños, para interactuar con sus blancos de perversión (incluyendo las cuentas digitales en sitios de chat infantiles). En otro sentido, también delictivo, se sustituye la identidad de personas de existencia f ìsica o ideal, para estafar o defraudar a los incautos.
Por ejemplo, puedo recibir un mensaje desde la dirección bancomercosudaca@gmail.com, con el siguiente texto: *"El Banco del Mercosur ha establecido que existe una cuenta a su nombre con 200.000 Bolivianos de Oro, que están disponibles, por favor responda urgente este mensaje, ya que en cinco días se cumplen los 20 años de depósito y el dinero pasará a la CARICOM"*. Más allá de lo absurdo de las afirmaciones (recordemos que no todas las personas tienen los conocimientos legales o la cultura general necesarios para detectar las falacias insertas en el mensaje), el método suele rendir beneficios, de ahí que siga en operación (al igual que las cadenas de mensajes que prometen milagro o muerte súbita, ya sea que lo reenviemos a nuestros amigos o no).
Si razonamos analógicamente respecto de la prueba pericial mecanográfica, podíamos arribar a conclusiones del tipo *"este escrito ha sido realizado con la máquina de escribir marca Olivetti, Lexicon 80, Serie A345876, secuestrada en el comercio referido"*, ésta puede ser una conclusión categórica científica, tecnológica, técnica y lógicamente comprobada, sin embargo nada nos dice respecto de la identidad del dactilógrafo que confeccionó el escrito.
Lo mismo ocurre con la relación entre un proyectil o una vaina servida y el arma de fuego que se utilizó para efectuar el disparo, esta relación nada aporta respecto de la identidad del tirador, que deberá ser determinada por otros medios probatorios.En el caso que nos ocupa, una cosa es el nombre de la cuenta de correo y otra la identidad y los datos filiatorios de su propietario en sentido lato (me refiero al creador y usuario de la ésta).

36 Digo pena "restrictiva de la libertad ambulatoria", ya que la denominación "pena privativa de la libertad", es fácticamente imposible. Tal vez la única forma de privar de la libertad a una persona sea la muerte o la inducción de un coma profundo. Inclusive hasta el prisionero sujeto al potro, puede contraer algunos músculos y seguir pensando. El lenguaje técnico no requiere necesariamente transgredir los usos, costumbres y reglas de derivación, del lenguaje natural.(www.rae.es) Privar: (Del lat. *priv re*). 1. tr. Despojar a alguien de algo que poseía. 2. tr. Destituir a alguien de un empleo, ministerio, dignidad, etc. 3. tr. Prohibir o vedar. 4. tr. Quitar o perder el sentido, como sucede con un golpe violento u olor sumamente vivo...

37 Salvo que no quede otra solución (por inexistencia del actor adecuado), un tribunal nunca admitiría una autopsia realizada por un médico generalista, sin especialización en Medicina Legal/Forense, ya que la misma requiere técnicas y conocimientos que no son exclusivos de la medicina sino transdisciplinarios (Médicos, Criminalísticos, Legales y Criminológicos). De ahí que resulte incomprensible que las pericias informático forenses sean realizadas por cualquier profesional, con el simple requisito de tener un título terciario en Informática, Sistemas o Computación. Ninguna de estas capacitaciones aporta asignaturas o conocimientos que aseguren la idoneidad de sus egresados como peritos en un área tan específica y particular como la informática forense. Es cierto que se trata de una disciplina en sus albores, estamos en una especie de "protomedicato" informático, pero esta situación no debe proseguir indefinidamente. La tarea de profesionalizar esta área pericial criminalística es responsabilidad de todos, pero en particular de los operadores del derecho que deben forzar la división de aguas, si pretenden obtener resultados periciales materialmente comprobables, lógicamente demostrables y en particular jurídicamente pertinentes y conducentes, en relación con la investigación judicial en desarrollo, o la pretensión del actor o de su contraparte.

38 Un ejemplo típico para esclarecer esta afirmación: En el supuesto de una inserción errónea de una persona en una base de datos utilizados para brindar referencias financieras o bancarias (del tipo Veraz), bastaría con demostrar esa inserción, mediante un informe obtenido por el legitimado activo de la acción autosatisfactiva (el afectado por el error). Satisfecha la eliminación por parte de la empresa, finaliza el proceso, sin otros requerimientos probatorios.

39 Ejemplo: Al resguardar la prueba obrante en la máquina del futuro actor, se encuentran una serie de mensajes de correo electrónico, que prueban una determinada relación jurídica (por ejemplo, un contrato comercial). Resguardada la misma, se obtienen la dirección IP de origen y destino del mensaje (que, en este caso, se corresponden con las direcciones de las dos partes contractuales), su contenido y la hora GMT de emisión del mensaje. El abogado que planifica la prueba, a presentar la demanda, debería solicitar un informe al ISP (Internet Service Provider), que certifique dicha circunstancia (fecha, hora, origen y destino del mensaje referido y su contenido si es que ha sido resguardado). Este informe complementa y completa la prueba pretendida (comprobar la relación contractual, a partir del mensaje). Este informe aumenta la credibilidad y pertinencia de la documental informática recolectada, ya que procede de un tercero independiente y sin interés alguno en el resultado del proceso controversial en desarrollo.

40 Ejemplo: Prosiguiendo con el ejemplo anterior, podría tratarse de otros detentadores de cuentas de correo electrónico, que hayan recibido el mensaje resguardado.

41 La planificación de los puntos de pericia siempre debe ser una labor transdisciplinaria entre el abogado y el perito informático forense, a efectos de adecuar los mismos a la pretensión del proceso y a brindar soporte a la argumentación planificada. El rol del asesor técnico en la causa civil y del perito de partes se vuelve crítico en las causas penales, ante la posibilidad de exponer los resultados periciales frente al tribunal, en el marco de una audiencia oral, de ahí la necesidad de contar con profesionales adecuadamente formados en la faz técnica, criminalística y jurídica. La justificación de una pericia caligráfica o balística, generalmente requiere de un esfuerzo para ajustar el informe técnico a la característica de legos de quienes deben evaluarla, no obstante el referido carácter de "lego", es relativo, cualquier abogado con experiencia puede leer e interpretar adecuadamente dichos informes, sin embargo, el informe pericial informático forense es demasiado novedoso como para ser reconocido en plenitud por los mismos operadores (actualmente existen profesionales que no pueden establecer con claridad las incumbencias y facilidades que ofrece la pericial informático forense), de ahí el especial

cuidado que debe tener el experto en el momento de presentar y justificar sus conclusiones. De más está decir que sin la permanente e intensiva interacción abogado-perito, el trabajo pericial puede terminar en fracaso o lo que es peor, no ser comprendido por sus destinatarios.

CAPÍTULO 11
UN EJEMPLO DE DELITO INFORMÁTICO PROPIO (EL PHISHING)

La recolección ilegítima de datos de todo tipo es una costumbre instaurada en nuestra sociedad y con la cual debemos convivir a diario. Se manifiesta por medio de encuestas "cuasi voluntarias"; ya que quien las realiza prácticamente nos obliga a responder sus preguntas, apelando a una insistencia y argumentación tal, que muchas veces nos hace responder con tal de que no siga hablando. Lo mismo ocurre con las ofertas de productos, los "premios" con condiciones, las ofertas automáticas (que suelen llenar nuestros contestadores, hecho que detectamos al regresar de nuestro trabajo, impidiendo que recibamos otros mensajes realmente de nuestro interés, cuando no han agotado de forma automática el papel de nuestro fax, o llenan nuestras casillas de correo electrónico en forma de SPAM). Estos suplicios con cierto sadismo medieval, forman parte de nuestra rutina y ya casi no nos sorprende una llamada telefónica a las tres de la madrugada, para escuchar una voz que nos dice: *"por favor necesitamos cinco minutos de su atención para que responda una breve encuesta sobre la programación televisiva…"*.

En este entorno es donde se produce la recolección de datos. Al responder un llamado telefónico, aunque sólo digamos *"hola"*, ya estamos brindando información sobre nuestra conducta. De hecho con perseverancia y tenacidad asnales, algunos delincuentes utilizan este método para conocer efectivamente los momentos en que los hogares están sin ocupantes, establecer de esta manera las rutinas hogareñas y visitarlos cuando están desocupados. Sin pretender llevar al lector a un estado de paranoia alienante y oscurantista, lo cierto es que estamos en el siglo de la información y ésta tiene su precio, ya sea que se utilice con fines lícitos (como la llamada nocturna antes descripta) o con otras intenciones (obtener una clave de acceso para una cuenta bancaria personal, una dirección de correo electrónico, etc.).

Aunque tenemos nuestras propias palabras para representar este accionar (recolección ilegítima de información personal), como debemos sostener el *"snobismo"* social y la tendencia a mantener incólumes los vocablos provenientes del techo de nuestro planeta, lo llamamos *"Phishing"*[42] y lo integramos a los peligros habituales que la vida conlleva (algo así como: *"el nivel de riesgo esperado, que debemos soportar para vivir en sociedad y que sin el cual sería imposible la convivencia y las relaciones hum…"*), reflejado en la respuesta habitual, ante el típico ¿cómo *estás?*: *"mal pero acostumbrado"*.

Si hacemos caso a la definición que nos aporta la nota al pie anterior, veremos que es definido como un *"delito encuadrado dentro de las estafas cibernéticas"*. Aunque el término cibernético es de todo menos unívoco, si prescindimos de este detalle, sin embargo nos resta un problema sumamente complejo de determinar. En nuestro país y según la doctrina penalista mayoritaria, un delito es *"una acción típica, antijurídica y culpable"*. Pero siguiendo este orden, ¿cómo establecer la tipicidad? Para eso debemos recurrir al Código Penal y sus leyes complementarias, si algo está tipificado en dicho cuerpo legal, entonces seguramente es un delito, quien lo comete es un delincuente, puede ser penalmente perseguido y eventualmente condenado.

Respecto de esta figura nuestra legislación de fondo (el Código Penal) ha sido modificada por la ley 26.388, denominada Ley de Delitos Informáticos. Cuando revisamos su contenido podemos comprobar que: modifica algunos artículos del Código Penal y sustituye otros, en lo que nos interesa tipifica algunas acciones para su sanción penal, pero el *Phishing*, no es un acceso indebido a una comunicación (art. 153), no constituye un acceso indebido a un sistema o dato informático de acceso restringido (art. 153 bis), no consiste en la posesión de una comunicación electrónica no destinada a la publicidad (art. 155), no se trata de revelar datos secretos (art. 157), no consiste en acceder a un banco de datos personales, este hecho por sí solo no conforma una defraudación,[43] ya que no tiene resultados propios, sino que los mismos dependerán de futuras acciones delictivas (las que pueden ser posibles y hasta probables, pero en esta etapa indeterminables y por lo tanto imposibles de tipificar), si es que se producen (art. 173, inc. 16), no está alterando, destruyendo, o inutilizando datos, documentos, programas o sistemas informáticos, tampoco está vendiendo, distribuyendo, haciendo circular o introduciendo en un sistema informático un programa destinado a causar daños (art. 183), no modifica sistemas informáticos públicos, ni de prestación de servicios(art. 184), no interrumpe medios de comunicación (art. 197), no daña elementos probatorios (art. 255), por lo tanto no es una acción típica y no constituye un delito.[44]

El falsario sólo está utilizando información apócrifa para obtener datos, a partir de una acción positiva por parte de la víctima (una especie de instigación a difundir sus datos por medios virtuales). Se podría argumentar que está recolectando información para realizar un ilícito, pero esto requeriría de un poder de adivinación, que en general no poseemos. Tal vez el que recolecta la información lo hace sin ninguna otra intención posterior, recolecta datos únicamente para coleccionarlos.

Podríamos suponer que lo hace con una intención altamente probable de delinquir y solicitar una medida preventiva, pero esta medida sería una especie de sanción preventiva, *a priori*, que se parece mucho a las medidas que adoptan los regímenes totalitarios. Por otra parte el delito siempre es una acción o una omisión, nunca una

intención (o las cárceles estarían llenas de mal intencionados y por supuesto de bien intencionados también).

Argumentaremos que lo hace utilizando mediante información falsa. Pero entonces, ¿qué hacemos con los señores y señoras que falsean su edad en Facebook? o mandan fotos de otros, o "mejoran" las propias con programas de edición fotográfica, o se autodenominan doctores sin tener un doctorado (aunque esto esté tipificado en el artículo 247 segundo párrafo, del Código Penal), o dicen ser amables, tolerantes y afectuosos (como un osito de peluche), o más hermosas que las ninfas. Evidentemente podemos suponer que se utilizarán con fines lícitos, aunque no sean muy ortodoxos y tampoco podamos asegurar su destino. ¿Los castigamos con una cautelar *a priori*, por las dudas? Imaginemos la medida: *"elimínese la información ficticia, puesta por su titular en una página de contactos, por decir que tiene 20 años, cuando en realidad tiene 33 o 40 o 75, con vaya a saber qué intenciones funestas para su destinatario"*. Es decir una especie de medida precautoria (seguramente soportada por la Ley de Hábeas Data), para protegerlo de sí mismo (acusado y víctima integrados en una persona física determinada). En aras de elucubrar, cualquier cosa es posible, pero la realidad jurídica la determina la ley. No es, tal vez, como nos gustaría que fuera, sino como obra normado. Si no nos gusta hay que cambiar la ley, por mecanismos legales y legítimos.

Pero, supongamos que luego de transcurridos los tiempos judiciales que conocemos y reconocemos, al final logramos una cautelar para que suspendan el sitio, o lo eliminen. A esa altura el falsario ya se cambió de sitio, estafó a todos los que quiso y sigue operando en otro lado (inclusive empleando los servicios del mismo ISP,[45] *más vale malo conocido que bueno por conocer*).

Ante este estado de cosas voy a referirme a un ejemplo que tal vez nos permita clarificar la situación imperante en nuestra legislación y el estado de indefección en que nos encontramos respecto de este tipo de actividades, que aun siendo claramente ilegítimas, no por eso devienen en ilegales y mucho menos en delictivas.

Entre los múltiples servicios disponibles en la red, existen algunos auténticos guardianes de la privacidad informática, éste es el caso de un grupo de expertos en Informática Forense, que se dedican a detectar y desenmascarar los distintos métodos de engaño, que se remiten a diario a los usuarios de Internet para obtener sus datos personales y sacar provecho de los mismos. Entre ellos figuran algunas tarjetas de felicitación o de salutación, que se envían automáticamente a nuestros amigos y que nos piden algunos datos personales para realizar la tarea, datos que luego serán empleados para acceder a nuestra cuenta personal de correo electrónico y obtener más información útil para futuras estafas o para conformar bancos de datos que luego son

vendidos con fines legítimos o ilegítimos, de algún lado salen los datos que permiten a ciertas instituciones enviarnos tarjetas de crédito preaprobadas, desde instituciones con las cuales nunca hemos tenido contacto alguno, o las propagandas especialmente orientadas a nuestros intereses particulares, profesión, hábitos sociales y deportivos, preferencias culinarias o afectivas, entre otros.

Detectada una fuente de emisión de estas tarjetas, el grupo referido comprobó que lo realizaba desde una página Web, alojada en un sitio de alquiler de espacio para este tipo de proyecto informático. El sitio de origen es por lo tanto un espacio de almacenamiento alquilado por un particular al correspondiente proveedor de servicios de Internet (ISP). Notificado el locador, sobre la actividad que realizaba su locatario, la respuesta del mismo fue (sic): *"Desafortunadamente no podemos dar de baja un servicio ya que el cliente pago por un servicio con nosotros, pero te recomiendo que vayas con las autoridades correspondientes y ya si ellos nos hacen la petición de baja del dominio lo haremos, es la* única *manera de que podamos darlo de baja. Por tu notificación,* ¡g*racias!"*

Pero… ¿esto qué significa? Que el ISP no puede hacer nada, que no quiere hacer nada, que la ley le prohíbe hacer algo sin la correspondiente orden judicial, que la responsabilidad por la denuncia se ha trasladado al grupo de adolescentes, que el ISP no quiere perder dinero ni clientes, que *las brujas no existen pero…*

Revisemos un poco el problema: El primer elemento a determinar es si la conducta evidenciada por el sitio es "típica", es decir si contraviene alguna norma jurídica vigente (en general deben ser normas penales, aunque también pueden ser normas administrativas).

Pero... para establecer si una acción es típica (el derecho penal nos exige que sea típica, antijurídica y culpable), es necesario someterla a proceso judicial. Recién cuando exista la firme convicción de que se trata de una trasgresión (por ejemplo, ante el pedido de medidas por parte del fiscal o por la aceptación por parte del Juez de medidas solicitadas por el querellante), entonces estaremos ante un hecho que *prima facie* (nadie es culpable, hasta la sentencia definitiva) constituye una trasgresión normativa. Entonces podemos pedir una cautelar del tipo de innovar: *"que se elimine preventivamente el sitio"*. Como decía antes, a esta altura de los acontecimientos el falsario ya ha recolectado la información, realizado una serie de estafas y seguramente se ha mudado a otro sitio. Bueno, al parecer estamos ante el problema del huevo y la gallina.

Supongamos que decidimos apoyar nuestra solicitud en la jurisprudencia que, con anterioridad, ha establecido que esta conducta constituye una violación normativa

(cierta o ¿en potencia?...). Entonces el Juez debería pensar en la forma de realizar y tipificar dicha trasgresión. Una vez logrado (a la sazón por algún medio poco conocido) determina la cadena causal que llevó a la concreción del ilícito. El que trasgrede no puede hacerlo sin tener un lugar desde el cual actuar (una especie de "aguantadero virtual"). Lugar que le otorga el proveedor de servicios. Por lo tanto... ¿El proveedor de servicios es entonces un partícipe primario? Evidentemente sin su colaboración (o al menos tolerancia) el trasgresor no habría alcanzado su cometido. ¿Debería procesar a ambos, en prevención de algo que posible o probablemente ocurra?

Se parece a la situación del locatario que alquila una propiedad a un tercero y éste la utiliza para alojar víctimas de secuestros extorsivos. Claro que para asemejarlo a este caso debemos considerar que al propietario le avisan que en el lugar tienen personas secuestradas y se niega a cancelar el alquiler. Pero a él: ¿le consta o no le consta que a partir de su "aguantadero virtual", se están realizando acciones ilegales o son sólo ilegítimas? ¿Sí?, ¿No?, ¿Ni? Para aumentar la complejidad debemos decir que la simple recolección de datos por medios truculentos (ya que no llegan a constituir por sí mismos la acción típica de defraudación o estafa), no es un delito, ya que no ha sido tipificado por el Código Penal y/o su legislación complementaria.

Por otra parte y desde el derecho civil, analizando la referencia al pago efectuado por el cliente: no todo contrato es válido, para que un contrato sea válido no puede tener como objeto una acción ilegal. Pero el proveedor de servicios no lo alquila específicamente para una acción ilegal (en caso contrario sería un cómplice). Analicemos la situación de cada actor *a priori,* en el momento de alquilar el sitio:

EL LOCADOR:

Desde la óptica Civil y Comercial pretende realizar un contrato de locación de servicios y aunque cabe la posibilidad de que desde la misma se realicen actos ilícitos o ilegítimos, éste no puede ser un supuesto generalizado. La buena fe, por el contrario, es un presupuesto de la relación contractual. En todo hecho ilícito deben darse los siguientes elementos:

Debe haber violación normativa (art. 1066 del Código Civil), consistente en una acción o en una omisión (art. 1073 del Código Civil). Por lo ya expresado y reiterado esta conducta no está tipificada.

Debe producir daño a terceros. Si un hecho no ocasiona daño, no es un hecho ilícito (art. 1067 del Código Civil). No estamos ante el resultado de acciones posteriores, sino ante el hecho, hasta el momento impensable de utilizar el sitio para estimular mediante mentiras a las personas a brindar información. Pensemos en el caso descrito

de las páginas de contactos personales con datos falseados. ¿Debería el locador de servicios controlar la veracidad de los datos de edad, del perfil del contactante? ¿Debería controlar que la foto que agrega a su página sea reciente y no de hace veinte años? ¿Es responsable de la información que su locador coloca, intentando mejorar su imagen y aspirar a mejores contactos personales? Hasta el momento no se ha producido daño alguno.

Debe haber dolo o culpa: Evidentemente hay dolo, quien sube información fraudulenta a un sitio sabe lo que hace, pero también sabe lo que hace cuando la oculta. Si pudiéramos comprobar los datos vertidos en los currículums personales o en las solicitudes de empleo, tal vez nos llevaríamos algunas sorpresas similares a la implementación de una prueba de paternidad obligatoria, mediante la técnica de ADN, a toda la población del territorio. Pero ¿dolo respecto de qué? ¿De una acción no típica y hasta el momento sin intención dañina alguna? La culpa por negligencia, impericia o imprudencia, en este supuesto (art. 1109 del Código Civil) es casi inimaginable.

Debe haber relación causal, entre el hecho ilícito y el daño. ¿Qué hecho ilícito? ¿Qué daño *a priori?*

En cuanto a las consecuencias (art. 901 y concordantes del Código Civil):

Si piensa en las consecuencias inmediatas (art. 901 del Código Civil), no tiene razones para no alquilar, ya que si como resultado del curso natural y ordinario de las cosas se producen daños, el responsable será el locatario y no obstan a la realización del contrato.

En cuanto a las consecuencias mediatas, casuales o remotas, son imprevisibles y tampoco debe tenerlas en cuenta.

Creo que no tiene razón alguna para negarse a celebrar el contrato de alquiler. Aunque no estaría de más establecer cláusulas que prohíban específicamente el *Phising*, algo fácil de decir y difícil de implementar: ¿La cláusula debe establecer la prohibición de mentir o sólo la prohibición de mentir con malas intenciones? ¿Es lícito mentir si no se afecta la moral y las buenas costumbres? (una especie de "mentira piadosa", como las que a veces se nos escapan en nuestras relaciones diarias, del tipo "¿Cómo *estás?* "aunque no nos importe mucho y que se responde *"Bien"*, aunque nada tenga que ver con nuestra situación personal real). ¿Quién debe actuar como *censor* de la información que se ingresa al sitio? La cosa cada vez tiene más visos dictatoriales.

EL LOCATARIO:

De buena fe: Indiscutiblemente es apto para realizar el contrato y no hay razón para cuestionar la validez del mismo.

De mala fe: Difícilmente lo exprese de viva voz al locador. Inclusive no es inconcebible que alquile el sitio sin tener muy claro su destino y empleo finales (sean éstos lícitos o ilícitos, legales o ilegales). No podemos presumir su mala fe, de lo contrario todos los contratos quedarían inconclusos (hasta entre las peores sociedades mafiosas se presupone la buena fe de las transacciones y se confía en que serán pagadas en tiempo y forma, acorde con la remuneración prometida, aunque claramente estemos en presencia de una asociación ilícita y si se produce un incumplimiento no se litigue ante el Poder Judicial respectivo).

EL DAMNIFICADO:

Por el momento no tiene respaldo legal alguno. Se encuentra ante hechos desarrollados en distintas etapas.

Primera etapa: la recolección de datos, utilizando información falsa, tiene todo el aspecto de ser ilegítima, pero no es ilegal. En realidad la mayoría sospechamos de los contactos virtuales demasiado hermosos, ricos y jóvenes, ya que no entendemos muy bien ¿qué hacen en este sitio? Y ¿por qué se identifican precisamente con nosotros?[46] Por el momento el riesgo de daño es sólo potencial. (Observamos la foto, de la hermosa veinteañera, rubia, de un metro setenta y cinco, medidas de concurso, con tres títulos universitarios, hija única de un latifundista neocelandés, que busca un sudamericano pobre e inculto, de la tercera edad, con un perfil idéntico al nuestro, pero aún no hemos concertado la cita.)

Segunda etapa: el uso de los datos con fines ilegítimos y/o ilegales. Aquí recién aparece la conducta reprochable. Pero esta etapa no tiene por qué suceder indefectiblemente a la anterior. De hecho esta etapa puede no producirse. (Es decir la cita con la veinteañera se ha concertado, está en nosotros concurrir o no.) Tampoco puede ser deducida estrictamente de los actos previos, que ni siquiera configuran una violación normativa en grado de tentativa.

Toda esta situación nos hace pensar que estamos analizando las cosas con cierta ingenuidad intelectual, con un sincero candor jurídico, una especie de infantilidad deóntica. La interacción judicial nos indica que la realidad jurídica: siempre depende de los intereses del intérprete. Y normalmente el intérprete está profundamente influenciado por sus tendencias filosóficoconfesionales, que hasta hace poco tiempo eran del tipo monoteísta (US$) y actualmente se ha escindido en una nueva secta que prefiere el Nuevo Testamento generado por el euro.

Esto no debería afectarnos en manera alguna, ya que desde el surgimiento de las religiones, primera oportunidad en que se creó una deidad a partir del desconocimiento y la necesidad de trascendencia física humana, luego de varios intentos (múltiples deidades, deidades auxiliares, buenas, malas, tontas y complacientes) se logró unificar a todas las deidades en una sola y se la llamó dinero y se convirtió en nuestro primer ídolo de silicio (al estilo Michael Shallis).[47] La política y su aliado el dinero forman parte de las opiniones, de hecho hasta logran revertirlas con una eficiencia muy superior a cualquier argumentación conocida. Al parecer en derecho todo es relativo (sin necesidad de entender demasiado a Einstein). Los caminos de allá son incomprensibles y los de acá… mucho más.

Sin embargo esta evidente laguna del derecho debería estimularnos para analizar, planificar y determinar acciones positivas a seguir. De manera transdisciplinaria y contemplando la evolución probable de los hechos que se evidencian a diario. Al menos sería posible legislar al respecto de manera positiva, aunque los resultados resultaren escasos e insuficientes. En especial, porque involucran actores no siempre situados en el mismo país, con lo que el problema de la jurisdicción y la competencia adquiere dimensiones colosales.[48]

Para complicar un poco más las cosas, el valor probatorio de la prueba documental informática aún es un tema por resolver. La detección, recolección, reunión, certificación, traslado, presentación y análisis de esta prueba, mediante protocolos estrictos e irrefutables, que sean reconocidos por la totalidad de los fueros involucrados, es por el momento un proceso en vías de desarrollo.

Suponiendo obtenida la prueba, aceptada por el tribunal y ofrecida en autos, queda el problema de la asignación de responsabilidades, eterna espada de Damocles que se cierne permanentemente sobre quien debe juzgar, ya que no es lo mismo determinar el origen de una comunicación (oral, escrita, visual) y establecer su autoría. La historia nos ha mostrado que una cosa es establecer con precisión meridiana la máquina de escribir con la que se realizó un documento y otra muy distinta afirmar quién fue su autor.[49]

El futuro se nos viene encima, las garras de la virtualidad se cierran sobre nuestros cuellos, es necesario estar a la altura de las circunstancias, el algoritmo del avestruz no podrá salvarnos esta vez.

Herramienta de análisis del lugar del hecho real

Respecto del lugar del hecho real, sustituye con soltura a todos los demás elementos

utilizados con anterioridad (fotografía, planimetría, reconstrucciones, etc.) brindando además la posibilidad de interactuar y modificar las condiciones imperantes en el momento pretendido, las veces que se quiera, ante todos los invitados y sin que estén juntos físicamente. Es el equivalente de la intervención quirúrgica remota con soporte robótico.

Por otra parte, siempre es posible consultar al mejor experto de todos, ya que éste no está supeditado a viajar e interactúa desde su lugar de residencia habitual, un auténtico teletrabajo pericial. Sólo es necesario pagar la hora profesional involucrada, sin gastos de traslado, hotelería y viáticos, con los mismos resultados y sin el cansancio posterior. Además, permite al experto interactuar en las antípodas del mundo, el mismo día y sin moverse de su casa.

Herramienta de análisis del lugar del hecho virtual

En este caso la relación es directa, la mejor manera de describir un lugar del hecho virtual, casi con seguridad, relacionado con un delito informático propio, es utilizar herramientas virtuales: realidad virtual, simulación, redes neuronales, inteligencia artificial. Una auténtica policía judicial virtual, en apoyo de la Investigación Criminal. La Criminalística en el Ciber espacio. El futuro que ya nos rodea y nos deja atrás.

42 *Phishing* es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de alguna forma de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas. Dado el creciente número de denuncias de incidentes relacionados con el *phishing*, se requieren métodos adicionales de protección. Se han realizado intentos con leyes que castigan la práctica y campañas para prevenir a los usuarios con la aplicación de medidas técnicas a los programas. Fuente: http://es.wikipedia.org/wiki/Phishing.

Phishing (2): Engañar a las personas para que revelen información personal a través de medios falaces basados en computadoras.

Fuente. Glossary of key information Security Terms http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf Guide to Malware Incident Prevention and Handling Special Publication 800-83 Sponsored by the Department of

Homeland Security http://csrc.nist.gov/publications/nistpubs/800-83/SP80083.pdf

43 Aunque este acto no resulta voluntario, ya que la voluntad de quien lo realiza se encuentra viciada por un error de hecho excusable, de nada sirve a los efectos legales, ya que no produce consecuencias jurídicas por sí mismo (el solicitar la información por medios fraudulentos no constituye un fin en sí mismo (salvo para los chismosos), pero sí conforma un acto preparatorio, sin el cual no podrían realizarse las maniobras delictivas posteriores, que son soportadas por dicha información. De todas maneras analizando *a priori* este hecho, no hay forma de determinar si será utilizado con fines delictivos o no y prevenir no quiere decir castigar por anticipado o "por las dudas".

44 Razonando por analogía, existen algunas situaciones similares, pero de ninguna manera idénticas, que han sido recientemente solucionadas por vía jurisprudencial, una de ellas está constituida por los llamados "secuestros virtuales", muchos de los cuales consisten sólo en algunas llamadas telefónicas desde la cárcel, informando a la víctima sobre el secuestro de un familiar, por el cual se pide rescate y uno o varios cómplices en el exterior que cobran el rescate. Curiosamente aún no se les ha ocurrido pedir directamente una transferencia electrónica de fondos, sobre alguna cuenta disponible (obtenida por medios legales o ilegales). En la causa "C. F., D. A. s/extorsión", la sala de Feria B de la Cámara del Crimen, integrada (Luis María Bunge Campos y María Laura Garrigós de Rébori), confirmó el procesamiento de tres personas por "secuestros virtuales", pero modificó la calificación legal del hecho considerado como extorsión por el juez de primera instancia, considerando que se trata de una modalidad de estafa. Desde el Complejo Penitenciario de la Ciudad Autónoma de Buenos Aires, algunos detenidosrealizaban "secuestros virtuales", efectuaban llamadas telefónicas y simulaban tener secuestrados a familiares de las víctimas, exigiendo dinero a los interlocutores. Aunque el juez de primera instancia sostuvo que la calificación legal era la de extorsión, los camaristas explicaron que *"si bien en este estadio procesal la tipificación legal escogida es provisoria, lo cierto es que en el presente caso se advierte que* ésta *puede afectar otros institutos, motivo por el cual señalaremos nuestra discrepancia con el encuadre legal asignado por el juez a quo". "Entendemos que no nos hallamos frente a sucesos de extorsión, sino que la conducta desplegada encuadra en el delito de estafa". "En la extorsión la acción típica consiste en obligar a otro mediante intimidación, a entregar, enviar, depositar o poner a su disposición o a la de un tercero, aquello que constituye objeto del delito pero siempre por medio de amenazas y* éstas *no son más que el anuncio de un daño que se producirá en el caso de no cumplir con lo exigido, extremo que nunca podría haber ocurrido, toda vez que los dichos amenazantes proferidos por el imputado no se hubieran podido concretar al tratarse de un 'secuestro virtual'."* De esta forma confirmaron el procesamiento de los imputados, modificando la calificación legal por la del delito de estafa reiterado en doce oportunidades, en concurso real con el de estafa en grado de tentativa.

45 ISP: Internet Service Provider. Proveedor de Servicios de Internet.

46 En este sentido los mecanismos de ingeniería social e ingeniería social inversa han desarrollado una serie de pautas que se apoyan en el ego potenciado que solemos evidenciar los habitantes de este planeta. "*Me niego a ser miembro de un club, que me acepte entre sus miembros",* decía Groucho Marx.

47 *Que pues doblón o sencillo. Hace todo cuanto quiero, …Y pues quien le trae al lado, es hermoso aunque sea fiero...Mas pues que su fuerza humilla, al cobarde y al guerrero… Más valen en cualquier tierra, (Mirad si es harto sagaz) Sus escudos en la paz, Que rodelas en la guerra. Pues al natural destierra, Y hace propio al forastero. Poderoso caballero es don Dinero."* Francisco de Quevedo y

Villegas.

48 “No es imposible, ni tampoco improbable, la situación en la que un locador que ofrece servidores en EE.UU., brinda facilidades de alojamiento a un cliente de Nigeria, que manda cartas a una serie de argentinos, donde les dice: *que es un filántropo, que los ha detectado por casualidad y quiere dejarles todas sus propiedades (consistentes en varias minas de oro y algunas de diamantes en Sudáfrica), pero que necesita sus datos personales para poder transferirles las propiedades.* Si un cliente nos consulta ante este hecho y nos dice que sospecha una estafa y que sería bueno requerir al locador que deje de brindar servicios al locatario, que por otra parte ya abonó la locación por anticipado. ¿Qué podemos responder? (la respuesta trivial no es válida) ¿Dónde litigar? ¿Con qué normativa?

49 España: El Juzgado de lo Penal número 3 de Valladolid ha dictado sentencia absolutoria en el caso de la joven vallisoletana Rebeca G. L. que fue acusada de colgar en marzo de 2007 en Internet varias fotografías de la novia de su ex pareja ofreciendo sexo ocasional. Frente al año y ocho meses de prisión y al pago de una multa de 4.500 euros que solicitaba el fiscal y los dos años de privación de libertad que pedía el acusador particular, junto con una indemnización de 12.000 euros interesada por los dos acusadores, por un delito de descubrimiento y revelación de secretos y una falta de vejaciones —esta última la había incluido la segunda acusación—, el juez estimó la pretensión absolutoria de la defensa basado en el principio *in dubio pro reo*, según informaron a Europa Press fuentes jurídicas. Y es que, en su sentencia, contra la que cabe recurso de apelación ante la Audiencia Provincial, el magistrado recuerda que el ordenador investigado no sólo era utilizado por la acusada sino por otros miembros de su entorno familiar, de ahí la imposibilidad de establecer sin ningún género de duda que la persona que colgó las fotos en Internet fuera Rebeca G. L. *“Aunque pueda hipotéticamente concebirse un mayor grado de probabilidad en el caso de la acusada, en atención a la naturaleza de su relación con J.S.I, no pueden descartarse otras posibilidades en cuanto a la autoría de los hechos”,* especialmente teniendo en cuenta la *“laguna existente en la investigación”* puesto que ningún miembro de su entorno familiar fue citado a declarar al objeto de aclarar la autoría.

CAPÍTULO 12
GUÍA PARA EJECUTAR LA RECOLECCIÓN DE LA DOCUMENTAL INFORMÁTICA

A continuación intentaremos presentar una serie de operaciones destinadas a detectar, resguardar, preservar, certificar y ofrecer la documental informática.

Al entrevistar a su cliente, averigüe la ubicación de la documental informática que resulte de interés a efectos de alcanzar la pretensión detectada y brindar soporte a la justificación argumental de la misma.

Clasifique dichas ubicaciones:

Información de libre accesibilidad: en poder de su cliente, en poder de un tercero no controvertido, en poder de una institución pública o privada.

Información de accesibilidad restringida: en poder de la contraparte o de terceros en oposición a su pretensión.

Planifique la recolección de la documental informática, considerando:

Realizar la totalidad de la recolección en un solo acto, para evitar redundancia y aumento excesivo de los costos asociados.

Coordinar una fecha y hora para la actividad, en la que deberán estar presentes su cliente, un escribano público, un perito/experto en Informática Forense (en su defecto un profesional de la Informática idóneo en el tema), los testigos que estime corresponder y usted.

Realice la recolección:

En razón de la complejidad de las tareas a efectuar, confeccione el acta notarial del escribano en paralelo con las tareas técnicas en desarrollo, para simplificar la determinación y especificación de éstas. Es mucho más fácil para usted, su cliente y el escribano, realizar preguntas al experto, a medida que surgen y no intentar reconstruir todo *a posteriori* (esta descripción, minuciosa exhaustiva y profundamente detallada de las tareas efectuadas, será el primer punto a analizar por su contraparte en el momento de pretender impugnar la pertinencia de la documental informática presentada).

El acta notarial debe contener los datos de rigor (incluyendo los títulos académicos del experto que realiza la tarea) y como condiciones *sine qua non:*

La autorización expresa del titular de la propiedad de la información a ser accedida para realizar las tareas de recolección, que le serán claramente explicadas por el abogado y el experto.

En el caso de acceder a equipos informáticos de empleados o dependientes del futuro actor (o rol que le pueda corresponder) es necesario respetar la privacidad de éstos obteniendo la correspondiente autorización de acceso, aun ante la eventualidad de que los equipos sean propiedad de la empresa o del futuro actor. Esta autorización debe constar en el acta notarial con la firma de los autorizantes.

El experto determinará la ubicación específica de la información a ser accedida y solicitará, en cada caso que sea necesario, al titular de la misma que facilite su acceso. Esto implica que el titular ingresará a las distintas cuentas personales, aplicativos, zonas de almacenamiento públicas y privadas, cuentas de correo electrónico, utilizando sus propias claves de seguridad, las que no serán reveladas al experto, para preservar la privacidad de las cuentas accedidas.

En el caso de resguardar mensajes de correo electrónico, éstos deberán contener la totalidad de los datos de sus encabezados, para posteriores tareas de certificación (esta medida debe ser solicitada por el abogado, pero es de responsabilidad exclusiva del experto que realiza la tarea, so pena de impugnación del mensaje resguardado). En todos los casos el resguardo contendrá las direcciones IP de origen y destino del mensaje, los datos identificatorios de las cuentas de correo electrónicas relacionadas con el mismo, la hora GMT de transmisión y los datos del ISP.

En lo que respecta a la información pública o privada, accedida la misma se resguardará en archivos de texto, generados mediante procesadores de texto que cuenten con su licencia pertinente o de programas de libres disponibilidad (*software* libre del tipo Linux,Open Office, etc.).[50]

Organizar la información en carpetas (directorios) acorde con su origen y pertinencia probatoria.

Capturar y resguardar las pantallas en los distintos accesos a la información, insertarlas en un archivo de texto detallado y grabarlo en una carpeta claramente identificada.

Generar un digesto o síntesis digital (rutina de *hash* o *hashing*)[51] a partir de cada

uno de los archivos generados, guardar dichos datos en un archivo de texto, junto con los anteriores. Copiar el resultado, agregarlo al acta notarial, con especificación del mecanismo de *hashing* utilizado, a efectos de que pueda ser repetido *a posteriori* por otros interesados en comprobar la integridad y autenticidad de la información presentada como documental informática. Ésta es otra condición *sine qua non* para asegurar la integridad de los datos preservados y su posterior confiabilidad probatoria.

Guardar la información en un dispositivo de almacenamiento secundario (en general se recomienda el CD o DVD, no regrabables y no utilizar el modo multisesión, de esta forma al finalizar el grabado de éste ya no puede ser modificado por maniobras posteriores), de esta tarea se debe dejar especial constancia en el acta notarial.

Se deben generar tantas copias del CD o DVD como sean necesarias, al menos una para cada parte, a efectos de adjuntarla a la notificación de demanda, una para reservar en la secretaría del tribunal, una para el escribano y una para cada uno de los dueños de los datos que han sido accedidos (el futuro actor y los terceros que accedieron a entregar información).

Cada copia debe ser individualizada por el escribano en el acta notarial, debidamente etiquetada (la etiqueta debe contener el resultado del *hash* realizado, claramente visible). Luego cada copia será cerrada y lacrada por el escribano. La apertura de cada una de las copias debe ser realizada ante el tribunal interventor y con las formalidades de rigor (acta de apertura, testigos, etc.), si estas formalidades no son respetadas se corren los riesgos de nulidad asociados.

Se dejará constancia expresa de la entrega de cada copia al respectivo interesado, iniciando el correspondiente formulario de cadena de custodia, a efectos de deslindar responsabilidades en caso de producirse una apertura irregular, ilegal o ilegítima de los sobres certificados formalmente.[52]

Como en toda acta notarial, se procederá a su cierre, lectura y firma, con las formalidades pertinentes.

Al presentar la demanda (o contestarla, o reconvenir, o acusar, o querellar, o defender) o cuando estime corresponder, presente ante el tribunal la documental informática resguardada, junto con el acta notarial y la cadena de custodia que la acompaña.

Utilice la documental informática en condiciones y con fines similares a la documental tradicional.

50 Recordemos que la recolección de la documental informática por medio de herramientas informáticas ilegales (sin licencia) es en realidad una actividad delictiva que vulnera derechos de autor y por lo tanto invalida la prueba). Ésta es un arma de doble filo, ya que debe ser la primera consideración a realizar por el abogado, respecto de la documental informática presentada por la contraparte. Esto incluye a los informes periciales, no es necesario realizar una larga y ardua refutación técnica si podemos demostrar que las herramientas empleadas para recolectar, clasificar, resguardar, certificar y finalmente presentar la documental, son ilegales por carecer de licencia. Abreviando, antes de discutir el fondo de la documental o la pericial, siempre debe comprobar la legalidad de la misma, mediante la presentación de las licencias asociadas o la constancia de utilizar programas de libre disponibilidad. Lo más simple suele ser lo más efectivo (especialmente si se realiza en el marco de una audiencia oral, o en el entorno de una audiencia de las establecidas por el artículo 360 del CPCCN, o en otros momentos similares). *El fin no justifica los medios.*

51 El *hash* o *cheksum* criptográfico, es una función matemática unidireccional e irreversible que convierte cualquier tamaño de datos (cualquier archivo o conjunto de ellos, sean de texto, ejecutables, de audio, imágenes, videos, etc.) en una número de longitud fija. Si se modifica el archivo original, cambiando aunque sólo sea un bit y se repite la operación, el nuevo *hash* generado difiere notoriamente del anterior, lo que permite asegurar la integridad de los datos preservados ante maniobras posteriores de modificación y/o adulteración (ejemplo: MD5).

52 La costumbre inveterada de abrir los sobres conteniendo elementos probatorios, en la barandilla de los tribunales, por personal inexperto en el manejo de esta prueba y sin respetar los cuidados particulares que requiere dicha tarea, ni cumplir con las formalidades necesarias (acta de apertura, prosecución estricta de la cadena de custodia), constituye una clara violación a las normas técnicas de preservación y prevención de contaminación o adulteración de la prueba ofrecida. Aunque no constituya una infracción procesal, debería ser erradicada en beneficio de la preservación de la prueba y consecuentemente, del derecho de defensa, constitucionalmente reconocido a las partes.

CAPÍTULO 13
MARCO TECNOLÓGICO PERICIAL
(LA PERICIA INFORMÁTICO FORENSE EN LA PRÁCTICA)

El perito informático forense debe reunir y tener preparado, previamente a la realización de una pericia, un conjunto de elementos que conformarán el maletín del perito informático forense que llevará consigo al lugar del hecho y que se corresponderá con lo solicitado en la requisitoria pericial o en la solicitud de asesoramiento técnico. Estos elementos incluyen una serie de componentes propios del profesional del área criminalística y específicos de *hardware* y de *software* de la Informática Forense que le permitirán realizar las tareas relacionadas con el Marco Tecnológico Pericial que, posteriormente, se verán reflejadas en la redacción del informe pericial. A lo largo de todas las etapas del Marco Tecnológico Pericial el perito informático forense deberá evitar que se produzcan acciones judiciales en su contra por desconocimiento de la ley.

Las herramientas de *software* de Informática Forense se caracterizan por ser comerciales, con versiones de prueba del tipo demostraciones o "trial", que en algunos casos sólo muestran las funcionalidades básicas y para acceder al producto completo es necesario adquirirlo o, también, pueden ser del tipo de código abierto, de distribución gratuita y con la posibilidad de modificación del código fuente del programa. Respecto de la funcionalidad de las herramientas, pueden ser específicas para cada tarea o reunir una serie de capacidades para resolver más de una. Con relación a la presentación de las herramientas de *software*, éstas pueden ofrecerse como una herramienta única y aislada o en paquetes junto con otras herramientas, brindando una solución integral a la mayoría de las tareas que debe realizar el perito informático forense.

En el lugar en donde el perito informático forense realice sus tareas de elaboración del informe pericial, ya sea el laboratorio, estudio o consultora efectuará la verificación previa del equipo y del conjunto de herramientas de *software* y/o *hardware* de uso específico. Con el fin de evitar la omisión de los elementos requeridos para la realización de la pericia, el perito informático forense realizará el control por medio de un formulario de control del equipo pericial. A continuación se muestra una lista de ejemplo que puede ser tomada como referencia y agregar o quitar elementos según corresponda:

Listas de Control del Equipo del perito informático forense

Elementos	OBSERVACIONES
Generales	
1. Guantes	
2. Cinta para delimitación del lugar del hecho	
3. Cámara fotográfica y / o filmadora	
4. Telémetro portátil	
5. Teléfono móvil, GPS	
6. Cuaderno de notas	
7. Marcadores, lapiceras	
Formularios y Listas de Control para:	
Claves de bios o setup	
Inspección judicial	
Recolección de evidencia	
Análisis de evidencia	
Acta de secuestro de elementos	
Cadena de custodia	
Informe pericial	
9. Rótulos para las evidencias, autoadhesivos	

10. Bolsas plásticas antiestáticas

11. Sobres de papel

12. Cajas para el transporte seguro de la evidencia

13. Rollo de cinta adhesiva

Hardware

1. Computadora portátil, con lecto-grabadora de CD o DVD, placa de red, módem, dispositivo para conexiones inalámbricas, interfaces pcmcia, firewire, usb

2. Dispositivos específicos de *hardware* para la copia de dispositivos de almacenamiento (tipo Image MASSter Solo Forensic)

a. Disco rígido sin datos de xGB (acorde al caso)

b. Convertidor IDE de 3.5” para notebook

3. Impresora

4. Cables

a. Plano IDE de 40 pines

b. Plano IDE de 80 pines

c. De alimentación IDE

d. Centronics a 68 pines SCSI

Elementos	**OBSERVACIONES**
e. 68 pines a 68 pines SCSI	

f. 68 pines a 50 pines SCSI

g. De red, UTP directo y cruzado. Coaxial

h. De consola (roll-over)

i. De interconexión entre computadoras (de puerto serial y paralelo)

5. De alimentación eléctrica

6. Conector eléctrico múltiple

7. Dispositivo de alimentación eléctrica ininterrumpible. Baterías

8. Concentrador o Hub Ethernet, con conector coaxial

9. Transceptores y convertidores

10. Módem externo

11. Unidad de Zip o Jazz externa

12. Disco rígido externo

13. Pen Drive

14. Diskettes en blanco

15. CD-RW o DVD en blanco

16. Zip en blanco

17. Conjunto de herramientas (destornilladores, medidor de tensión, medidor de cables de red)

Software

a. De diferentes marcas de discos rígidos

b. De Linux, con el comando dd

c. De DOS, con fdisk, format

d. De Windows 95, 98 NT, 2000, XP, con fdisk

e. De herramientas forenses integradas del tipo comercial o de código abierto

2. Diskette o CD-ROM o DVD con la utilidad para duplicación y autenticación

3. Diskette o CD-ROM o DVD con la utilidad de reconocimiento de particiones. Ej: Partinfo

4. Diskette o CD-ROM/DVD con herramientas forenses para Linux y Windows

Elementos	**OBSERVACIONES**
5. De diferentes placas madre.	
6. Disco rígido con Linux y *software* integral de Informática Forense, comercial o de código abierto. Ej., Encase, Helix o SleuthKit y Autopsy	
7. Disco rígido con Windows 98 y *software* y *software* integral de Informática Forense, comercial o de código abierto. Ej., Encase o SleuthKit y Autopsy	
Uso personal	
1. De aseo	
2. Bebidas	

2. Bebidas

3. Alimentos

4. Vestimenta extra

La solicitud de la pericia informático forense puede comprender una amplia variedad de temas relacionados con la Informática y puede ser originada por:

Una orden judicial.

Algún particular, ya sea una persona específica, consultoras, empresas u otros profesionales. En este caso la recolección de la evidencia deberá realizarse ante escribano público, para que la evidencia sea certificada.

Acorde a estas circunstancias el perito informático forense desempeñará acciones específicas y acudirá al lugar del hecho acompañado por diferente tipo de personal y/o autoridades legales.

En las distintas etapas de la pericia Informático Forense el perito deberá utilizar un conjunto de herramientas acorde a cada situación en particular.

Las herramientas de *software* de informática forense mencionadas en este capítulo pueden pertenecer a productos comerciales o a productos de licencias públicas de *software* libre (GNU Public License). Se recomienda el acceso al sitio http://www2.opensourceforensics.org/,53 donde se listan un conjunto variado de herramientas de código abierto.

El perito informático forense deberá efectuar prácticas previas en el laboratorio de las herramientas de *software*, con el fin de adquirir la habilidad necesaria en su manejo y comprender las capacidades que las herramientas brindan y determinar posteriormente su uso adecuado y pertinente. Lo mismo ocurre con los distintos procedimientos a seguir según las operaciones que se deban realizar en la pericia, es decir, que es importante efectuar prácticas previas y simulaciones de las secuencias de tareas a realizar en el lugar del hecho evitando errores por impericia, negligencia o desconocimiento.

Es importante aclarar que la selección, comprobación, análisis y aplicación de las herramientas de *software* de informática forense requieren que el perito informático forense posea profundos conocimientos en:

Software de base, es decir, sobre los sistemas operativos comerciales o de código

escrito, las características particulares de los gestores de procesos, de archivos y directorios o carpetas, dememoria, de entrada y salida, de comunicación y sincronización de procesos, de seguridad y protección.[54]

Redes de computadoras, topologías física y lógica, protocolos de comunicación, gestión de equipos de interconectividad.

Estos conocimientos se pueden adquirir por medio de la formación académica pertinente. Es muy difícil poder reunir el saber de todos los aspectos relacionados con la Informática Forense, pero para evitar acciones perjudiciales por conductas negligentes debidas a la ausencia de la formación académica adecuada, se recomienda que si no se posee tal formación se consulte o se busque en las fuentes de información de asesoramiento confiable y responsable.

Herramientas de hardware y software del perito informático forense

Las herramientas de *software* y *hardware* que utilice el perito informático forense deberán ser comprobadas previamente en el laboratorio. La verificación de la integridad y confiabilidad, tanto de las herramientas de *software*, como de los datos de la evidencia, ya sea previa recolección de la misma o posterior a su análisis, se efectúa por medio de una verificación matemática o firma. Esta certificación consiste en la aplicación de un algoritmo matemático o *checksum* criptográfico, denominado *hash* o digesto o síntesis o resumen de los datos. El *hash* es una función matemática unidireccional e irreversible, que convierte cualquier tamaño de los datos en un número de longitud fija.

El maletín del perito informático forense está compuesto por una serie de elementos de *hardware* y *software* que fueron previamente seleccionados acorde a la requisitoria pericial. A continuación se describirán los elementos de *hardware* que pueden conformar el equipo fijo o de laboratorio o el equipo móvil para el traslado al lugar del hecho.

Elementos de hardware del laboratorio del perito informático forense

El perito informático forense necesita de una serie de elementos de *hardware* para efectuar su actividad pericial. El equipamiento a utilizar puede ser fijo, en el laboratorio pericial o móvil para efectuar las actividades periciales en el lugar del hecho. Existen en el mercado diversas empresas que han desarrollado equipamientos

hecho. Existen en el mercado diversas empresas que han desarrollado equipamientos específicos de computadoras fijas o móviles que incluyen *software* para la Informática Forense y aplicables en diferentes sistemas operativos. El sitio de Internet, http://www.forensic-computers.com,[55] ofrece diversos equipos de estaciones informáticas forenses. No obstante, el perito puede armar su equipo de laboratorio contemplando ciertas características técnicas del *hardware* que faciliten la actividad pericial.

A continuación y a modo de guía se describe el *hardware* que podría ser utilizado tanto en el laboratorio como en el lugar del hecho, integrado en un solo equipo o elementos separados para diversas funciones.

Equipo fijo de Laboratorio Estación de trabajo



http://www.forensic-computers.com/ft4dx.php#specs

Especificaciones técnicas:

Gabinete: Torre de acero sólido con 10 bahías externas; tres ventiladores

Alimentación eléctrica: Fuente de 1000 Modular

Placa madre: Intel® IOH-36D y ICH10R

Procesadores: dos-Intel® E5620 Quad-Core 2.4GHz, 1333MHz FSB, LGA1366, 12MB Cache

Memoria: 24GB DDR3 Registrada ECC DDR3 PC3-10600

de 10/100/1000Mbps

Placa de video: 1GB (Dual DVI Head)

Placa de sonido: RealTek® Audio Codec de alta definición

Configuración de la bahía externa:

Bahía 1: Dispositivo de múltiples conectores T34585is para controladoras SATA/SCSI/ IDE/USB

Bahía 2: Lecto grabadora triple (BluRay, DVD, CD)

Bahía 3: Un Puerto de datos CRU V Plus SATA para almacenamiento removible en caliente –hot swappmodular

Bahía 4: Panel de entrada y salida con USB 2.0 x2, FireWire 400 x 2, and eSATA x 2

Bahía 5: Dispositivo de RAID de discos del tipo SuperMicro 4con bahía de 2.5" para 4 discos x 300GB con dispositivo Velociraptor, dos dispositivos en RAID 0 para la base de datos de Oracle de Forensic Tool Kit y dos RAID 0 para archivos temporales

Bahía 6: Un disco rígido Western Digital VelociRapter de 300 GB SATA instalado en un ensamblado sin bandeja para el sistema operativo del tipo WiebeTech RTX100H-INT Trayless SATA

Bahía 7: Ensamblado SATA sin bandeja del tipo WiebeTech RTX100H-INT con disco rígido de 2TB (DATA 1)

Bahía 8: Ensamblado SATA sin bandeja del tipo WiebeTech RTX100H-INT con disco rígido de 2TB (DATA 2)

Bahía 9: Ensamblado SATA sin bandeja del tipo WiebeTech RTX100H-INT con disco rígido de 2TB (DATA 3)

Bahía 10: Ensamblado SATA sin bandeja del tipo WiebeTech RTX100H-INT con disco rígido de 2TB (DATA 4)

Placa de RAID de discos: Controladora con cablesAdaptec 5805

Monitor: Dos 22" Pantalla ancha LCD con parlantes

Monitor: Dos 22” Pantalla ancha LCD con parlantes

Software: QuickView Plus Version 11 (para la visualización de diferentes tipos de archivos) y Norton Anti-Virus (OEM)

Sistema Operativo: Microsoft Windows 7 final 64-bit (OEM w/CD y COA)

Costo aproximado en dólares: 12.149.

Cada equipo posee un conjunto de elementos accesorios y opciones que se pueden consultar en las siguientes direcciones de Internet, respectivamente:

Accesorios: http://www.forensic-computers.com/ft4dx.php#acc, Opciones: http://www.forensic-computers.com/ft4dx.php#options.

Equipo móvil de Laboratorio





http://www.forensic-computers.com/fmw2.php http://www.forensic-computers.com/fmw1-ts.php



http://www.forensic-computers.com/fal5mk3.php#specs

Especificaciones técnicas del modelo que se encuentra en la siguiente dirección de

http://www.forensic-computers.com/fal5mk3.php#specs

Gab**i**nete: Micro-ATX de aluminio, superficie cubierta con protección durable, bisagra única para el módulo ensamblado de la controladora de disco IDE y grabadora de DVD, Caja para el ventilador de 80 mm instalada en la parte posterior del chasis. Caja del ventilador de 40 mm en la fuente de alimentación. Caja del ventilador de 40 mm instalada en la parte posterior. Sistema de caja de transporte del tipo Pelican 1520.

Panel LCD: 14.1" con máxima resolución de 1024 x 768. 16.7M. Control de colores: Brillo, Contraste, Foco, Reloj, Posición Horizontal y Vertical, Idioma, Color Temperatura (C1, C2), Reinicio, Salida, RGB

Placa Madre: Intel® G41/ICH7 chipset

Procesador: Intel® Quad Core Q9650 2.5GHz, 12MB Cache, EM64T, 1333 MHz FSB

Fuente de alimentación: 1U 400W 90V a 132V o 180 a 264V-Selección automática 47 Hz a 63 Hz, Cable de alimentacióndel tipo estadounidense.

Memoria: 4GB PC2-5300 667

Adaptador para conexiones de múltiples conectores: SATA/IDE, con un Puerto SATA y uno IDE

Dispositivo para el sistema operativo: Un disco de 500GB SATA 7200RPM HD instalado en un Puerto de datos del tipo *CRU DataPort 25 en bandeja adicional*

Dispositivo de datos: Un disco de 500GB SATA 7200RPM HD instalado en un Puerto de datos del tipo *CRU DataPort 25 en bandeja adicional*

Controladora de video integrada: Intel® Graphics GMA4500

Grabadora de DVD: DVD -R/-RW/+R/+RW

Placa de red integrada: NIC soporta 10/100/1000 Mbps

Placa de sonido: Realtek® ALC887 audio codec de alta definición –auriculares en estéreo con control de volumen.

Placa FireWire IEEE-1394: Una placa FireWire IEEE-1394 y una placa combo USB 2.0

Placa FireWire IEEE-1394: Una placa FireWire IEEE-1394 y una placa combo USB 2.0

Puertos: Un Puerto serial 16550, Un Puerto paralelo ECP/EPP, cuatro puertos USB 2.0, un Puerto PS/2 para teclado y un puerto PS/2 para mouse

Disco rígido externo: Bahía Antec MX-1 con un disco 1TB SATA, eSATA e interfaces USB 2.0

Disketera: USB 1.44

Software**:** QuickView Plus Version 11 (para la visualización de diferentes tipos de archivos) y Norton Anti-Virus (OEM)

Sistema Operativo: Microsoft Windows XP Professional (OEM w/CD y COA)

Dimensiones y peso: La computadora está en una caja Pelican 1550. Peso: 5,44 kg.

Las situaciones en las que el perito informático forense deberá aplicar las diferentes herramientas de *software* o *hardware*, dependerán si la recolección, análisis y redacción del informe pericial se debe efectuar en el lugar del hecho, en la computadora *sub peritia* activa o en el laboratorio con la evidencia resguardada.

Las direcciones de Internet, en donde se referencia la ubicación de las herramientas, pueden haberse modificado en el momento de la lectura de este material. En algunos casos las empresas de *software* y *hardware* modifican sus nombres o son compradas por otras empresas, o simplemente desaparecen como producto, y por consiguiente no se podrán ubicar en las direcciones especificadas.

Componentes de hardware **de uso específico:**

Acorde a la tarea pericial el perito puede conformar su equipo móvil o fijo con un conjunto de componentes de *hardware* que cumplen funciones específicas tales como:

Bloqueadores de escritura www.icsforensics.com

Dispositivos de borrado seguro –degausserwww.datadev.com, http://www.degausser.us/, http://www.ontrackdatarecovery.co.uk/data-management/secure-data-deletion/degausser/

Dispositivo de registro de eventos por teclado –keylogger-http://www.keelog.com/

Fabricantes de discos rígidos

En EE.UU., ONTRACK, www.ontrack.com

En Reino Unido, http://www.ontrackdatarecovery.co.uk/

En Noruega existe el laboratorio Ibas, www.ibas.net

Equipo para la autenticación y duplicación de evidencia del disco rígido:

Conjunto de discos removibles y bahías metálicas, www.exabyte.com

Image Masster, Equipo de duplicación, desinfección y certificación, http://www.ics-iq. com/, capacidades:

En el modo Forensics efectúa la imagen de resguardo, está diseñado para hacer una copia bit a bit, en forma rápida y fácil e incluye adaptadores para computadoras portátiles. Se conecta el dispositivo de la imagen en la unidad y el disco *sub peritia* a la manguera o cable externo y a la alimentación eléctrica y se enciende la unidad Image MASSter Solo y se selecciona resguardo Forensic y se oprime aceptar.

Posee placa SCSI.

Contiene un dispositivo de cinta de gran capacidad de tipo SCSI. Cualquier *software* de imagen que se utilice incluye una opción para crear imágenes en cintas. Si se elige hacer la imagen de una cinta, el uso de una interfaz SCSI reduce el tiempo de que se utiliza para efectuar el resguardo de una computadora o esperar su restauración. Las cintas que no son SCSI, por ejemplo las del puerto paralelo, son extremadamente lentas, pero es una alternativa viable ya que la mayoría de las computadoras poseen un puerto paralelo. Con SCSI se pueden resguardar 10 a 12 Gb en 45 minutos contra 1 Gb por hora de los dispositivos por puerto paralelo.

Este sitio ofrece un conjunto muy variado de accesorios de *hardware* para informática forense

Dispositivo de discos rígidos para la captura de datos con verificación MD5, www.logicube.com, logicubeforensic.com.

Herramientas de software para Informática Forense

El perito informático forense puede utilizar herramientas de *software* de carácter comercial o de *software* libre, a continuación se detallan algunos sitios de Internet4 en donde se pueden encontrar herramientas para uso específico o conjunto de herramientas que componen un paquete integrado para realizar diversas tareas y en distintos sistemas operativos:

Conjunto de herramientas integradas en un solo paquete de software de arranque en modo "en vivo" (live) disponibles para CD, DVD, Pendrive – Programas de Software Libre Centrux (ex Condor Linux), basado en Debian, herramientas para Informática Forense y Respuesta a Incidentes, desarrollado por Marcos Pablo Russo (egresado del curso de Informática Forense de la Universidad Tecnológica Nacional – Regional AvellanedaAño 2004)

Caine, Computer Aided Investigative Environment, distribución Linux conteniendo un amplio conjunto de herramientas para Informática Forense, de inicio en vivo. http://www. caine-live.net/page11/page11.html The Penguin Sleuth Kit, www.linux-forensics.com, (sleuth: detective), de Ernest Baca, basado en la distribución de Linux Knoppix (de Klauss Knopper, http://www.knopper.net/ knoppix/) es un producto con licencia pública GNU.www.knopper.net/knoppix/ Smart Linux**,** basado en Slackware de Linux, diseñado para análisis informático forense, www.asrdata2.com Snarl, basado en Unix FreeBSD, www.securitydistro.com/security-distros/SNARL, es una imagen ISO de inicio automático.

Open Computer Forensics Architecture (OCFA) de la Agencia Nacional Policial Alemana,de inicio en vivo. http://ocfa.sourceforge.net/

The Penguin Sleuth Kit, **www.linux-forensics.com** (sleuth: detective), de Ernest Baca, basado en la distribución de Linux Knoppix (de Klauss Knopper, http://www.knopper.net/ knoppix/) es un producto con licencia pública GNU. Se puede descargar del sitio y generar un CD-ROM de arranque. Presenta una interfaz gráfica, se pueden ejecutar las herramientas desde la línea de comando y siempre como root. Este *software* se actualiza frecuentemente, agregando, quitando o modificando diferentes características y utilidades. En la versión que se analizó en el momento de la escritura de este material, aparecen algunas consideraciones importantes como, por ejemplo, en las particiones del tipo EXT3 y Reiserfs montadas en modo solo lectura mostraban cambios en el MD5, no ocurriendo lo mismo con particiones FAT32, NTFS y EXT2, acorde a lo expresado por Arthur Bowker en la página inicial del CD-ROM. Como toda herramienta se debe verificar previamente en

laboratorio. A continuación se muestra una lista de herramientas para Informática Forense y seguridad que contiene Penguin Sleuth, obtenida de la página inicial del CD-ROM del sistema operativo:

Sleuth Kit – Herramientas de informática forense por línea de comandowww.sleuthkit.

org *autopsy* – Herramienta de interfaz gráfica del conjunto de Penguin Sleuth, permite examinar archivos asignados, rchivos borrados previamente, directorios, unidades de datos y metadatos de imágenes de dispositivos en un entorno de modo solo lectura.

foremost – Herramienta de línea de comando, diseñada por Jess Kornblum y Kris Kendall, graduados del MIT. El archivo se configura en /foremost directory. Para funcionar correctamente requiere almacenamiento externo. Permite recuperar archivos eliminados en los sistemas operativos de Linux, Unix y Windows – foremost.sourceforge.net

glimpse Herramienta de línea de comando de indexación y búsqueda. Para funcionar correctamente requiere almacenamiento externo www.webglimpse.net *wipe* Herramienta de línea de comando para el borrado seguro de dispositivos de almacenamiento no volátil y de archivos wipe.sourceforge.net

dcfldd – Herramienta mejorada de DD con generación de *hashing*. Semejante al comando dd. Para ampliar información se puede leer el ayuda (man dcfldd).

etherape – Monitor de red gráfico etherape.sourceforge.net/

fenris – Herramienta de trazado de ruta multipropósito razor.bindview.com/tools/fenris/

honeyd – Programa Honeypot de línea de commando www.citi.umich.edu/u/provos/honeyd/

snort (Reglas predeterminadas) Herramienta de línea de comando para la detección de intrusiones www.snort.org

dsniff Herramienta de línea de comando para la auditoría de red y tests de penetración www.monkey.org/~dugsong/dsniff/

John The Ripper Herramienta de línea de comando para crack www.openwall.com/john/

Nikto – Herramienta para la inspección de servidores web www.cirt.net/code/nikto.shtml

nbtscan Herramienta de línea de comando que examina servidores de nombres con el puerto de NETBIOS abierto www.unixwiz.net/tools/nbtscan.html

xprobe Herramienta de línea de comando de huellas digitales de los sistemas operativos remotos www.sys-security.com

Ngrep Herramienta de línea de comando para el comando grep en red www.packetfactory.net/projects/ngrep/

Nemesis Herramienta de línea de comando para la introducción de paquetes en la red www.packetfactory.net/Projects/nemesis/

fragroute Herramienta de línea de comando para la detección y prueba de intrusiones en la red monkey.org/~dugsong/fragroute/

fping Herramienta de línea de comando para ping de múltiples hosts www.fping.com

TCPtraceroute Herramienta de línea de comando, semejante al comando traceroute, pero para paquetes TCP michael.toren.net/code/tcptraceroute/

tcpreplay – Herramienta de línea de comando que reproduce la descarga de tcp tcpreplay.sourceforge.net

Nessus – Herramienta gráfica de exploración de seguridad www.nessus.org

Ethereal – Herramienta gráfica de análisis de tráfico de la red www.ethereal.com

Netcat – Herramienta de línea de comando para leer y escribir en la red www.atstake.

com/research/tools/network_utilities/

tcpdump – Herramienta de línea de comando que descarga el tráfico de la red www.

tcpdump.org/

hping2 – Herramienta de línea de comando para ensamblar y analizar paquetes www.

hping.org

ettercap Herramienta de línea de comando para rastrear, interceptar y registrar redes

Ethernet ettercap.sourceforge.net

openssh – Herramienta de conexión remota segura www.openssh.com

Kismet – Herramienta gráfica para rastrear redes inalámbricas www.kismetwireless.net

airsnort – Herramienta gráfica para la detección de intrusión en redes inalámbricas -

airsnort.shmoo.com

GPG – Herramienta para encripción www.gnupg.org/

OpenSSL – Herramienta para la conexión remota segura www.openssl.org/

lsof Herramienta de línea de comando para listar todos los archivos abiertos Para mayor información consultar el archivo de ayuda (man lsof).

hunt Herramienta de línea de comando de exploración de vulnerabilidades de TCP /

IP (exploit) lin.fsid.cvut.cz/~kra/index.html

stunnel – Paquete de conexión SSL (Secure Socket Layer) stunnel.mirt.net

arpwatch Herramienta de línea de comando para el monitoreo de EthernetPara mayor información consultar el archivo de ayuda (man arpwatch)

dig Herramienta de línea de comando para consultas de servidores de nombre de dominio Para mayor información consultar el archivo de ayuda (man dig)

chkrootkit – Busca indicios de herramientas de rootkit www.chkrootkit.org

ForensiX, creado por Dr.Fred Cohen, experto en código malicioso, www.all.net Es un conjunto de herramientas para la recolección y análisis de datos basadas en el sistema operativo Linux. Reconoce una gran variedad de *hardware*. Genera la imagen a partir de cualquier dispositivo de almacenamiento, realiza la verificación de la integridad de los datos con MD5 y crea un registro en la base de datos del caso. Esta herramienta al estar basada en Linux reconoce diferentes tipos de sistemas de archivos, montando la imagen o dispositivo en distintos sistemas de archivos en modo

solo lectura para prevenir cualquier tipo de modificación de la evidencia. Permite efectuar búsqueda de cadenas de caracteres o aplicar operaciones booleanas para búsquedas acotadas y una herramienta para la búsqueda de imágenes y mostrar bitmaps. La mayoría de las aplicaciones son accedidas por medio de una interfaz gráfica.

Forensic Toolkit, http://www.mcafee.com/us/downloads/free-tools/forensic-toolkit.aspx, producto formado por un conjunto de comandos para la reconstrucción de actividades de accesos en el sistema de archivo Windows NTFS Incluye:

AFind, proporciona una lista de archivos por sus últimos tiempos de acceso y no modifica los tiempos de acceso de los directorios

HFind, examina un disco para detectar los archivos que tienen configurado el atributo de oculto o utilizan el directorio de Windows NT y los atributos de sistema para ocultar archivos *SFind,* efectúa la búsqueda de flujo de caracteres (stream) ocultos en algún archivo

FileStat, genera un informe de todos los atributos de un solo archivo

NTLast, esta herramienta muy poderosa puede estar o no incluida en el paquete, y permite obtener los tiempos de inicio y cierre de sesión y si se realizó en forma remota o interactiva

Helix, http://www.e-fense.com/products.php, conjunto de herramienta integradas para inicio en vivo para los sistemas operativos Linux/Unix, Mac y Windows

LNX 4N6, basado en Debian, sitio belga de informática forense, http://www.lnx4n6.be/

GRML, http://grml.org/, sistema de inicio en vivo. Basado en Debian, herramientas para administración de sistemas, detección de *hardware*, rescate, análisis de sistemas de archivos.

Conjunto de herramientas integradas en un solo paquete de software Productos Comerciales:

EnCase, de Guidance Software. www.encase.com

Es una herramienta basada en Windows. El entorno gráfico facilita la actividad de investigación. Las funciones que realiza esta herramienta son las siguientes: Duplicación de dispositivos de escritura bit a bit y certificación matemática –*hash*–.

Vista previa de un volumen, Búsquedas con expresiones para filtrado (números, fechas de nacimiento, números de teléfonos y de identificación personal) y búsqueda de texto, las que se pueden efectuar en segundo plano, Visualización de los discos y volúmenes, Apertura de un caso, Generación de un archivo de evidencia, Resguardo del caso. Generación de informes de todas las tareas realizadas y sus resultados. Utiliza una metodología de casos para el análisis de cualquiera de los dispositivos o discos que se relacionan con la misma investigación, trabaja con la imagen generada con el programa EnCase DOS como el archivo de la evidencia. Es posible agregar todos los archivos de evidencias y efectuar búsquedas simultáneas en todos ellos. Esto es muy útil cuando se deben efectuar búsquedas en múltiples computadoras y en pilas de disquetes. Al crear un nuevo caso el programa solicita información relevante acerca de éste para ser incluida posteriormente en el informe pericial. Durante el análisis se pueden marcar elementos de interés y efectuar comentarios en el área de texto y volver a estas marcas en otro instante de la investigación. Estas indicaciones y comentarios sirven para ser agregadas al informe y facilitar la tarea del perito informático forense señalando los aspectos relevantes de la investigación a medida que se está realizando el análisis. Al finalizar el análisis se puede exportar el archivo a un formato del tipo ".RTF"(rich text file, archivo de texto enriquecido), esto permite la edición del archivo en cualquier procesador de texto. Para la visualización de imágenes ofrece un visor que permite ordenar los gráficos y visualizar solamente los requeridos. A través de la opción de Identificación de la firma del archivo y Análisis, se pueden detectar archivos anómalos con extensiones que no condicen con el contenido actual del archivo, esta herramienta efectúa la búsqueda de archivos sospechosos que puedan contener datos ocultos. Este programa intenta ofrecer un conjunto de herramientas totalmente integradas.

Forensic Toolkit, *http://www.digitalintelligence.com/software/accessdata/forensictoolkit3/*

New Technologies Incorporated (NTI), http://www.forensics-intl.com/tools.html, producto comercial. El *software* está basado en aplicaciones de línea de comando. Algunas de estas aplicaciones pueden ser:

CRCMD5, un programa para validar el contenido de uno o más archivos.

DiskScrub, permite eliminar datos del disco rígido.

DiskSig, un programa para validar la precisión de los resguardos de las imágenes espejadas.

FileList, crea una lista de los archivos del sistema ordenados por la última fecha de acceso.

Filter_we, un filtro de lógica difusa para utilizarlo con los datos de entorno.

GetFree, recolecta información de los espacios no asignados.

GetSlack, recolecta información de los espacios desperdiciados.

GetSwap, recolecta información de la memoria virtual.

GetTime, Obtiene la hora del sistema del CMOS y la fecha.

NetTreat Analyzer, identifica el abuso de cuentas en Internet.

NTI-Doc, registra fechas y atributos de los archivos.

PTable, analiza y documenta las particiones del disco rígido.

Seized, permite cerrar y asegurar la evidencia.

ShowFl. Analiza la salida de una lista.

TextSearch Plus, ubica cadenas de texto y archivos gráficos.

WinHex, editor de hexadecimal y herramientas de análisis forense, http://www.x-ways.net/

forensics/index-m.html**,** es un entorno de trabajo avanzado para los investigadores en Informática Forense. Se ejecuta bajo Windows 2000/XP/2003/Vista * / 2008 * / 7 *, 32 Bit/64 bits. Se basa en el programa hexadecimal WinHex y editor de discos, todas las características generales y específicas conocidas de WinHex, tales como:

La duplicación de discos y de imágenes

Capacidad para leer las estructuras de separación y en el interior del sistema de archivos en modo hexadecimal y binario (. dd) archivos de imagen, imágenes ISO y VHD

Acceso completo a los discos, RAID, y las imágenes de más de 2 TB de tamaño (más de 232 sectores) con tamaños de sector hasta 8 KB

Interpretación de JBOD, RAID 0 y RAID 5 y los sistemas de discos dinámicos

Soporte nativo para FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, ext2, ext3,

ext4, Next3,

CDFS/ISO9660/Joliet, UDF

Visualización y descarga de RAM física y de la memoria virtual de los procesos en ejecución

Diversas técnicas de recuperación de datos

Base de datos de firma de los encabezados de archivos basados en GREP

Limpieza del disco duro para producir los medios forenses estériles

Búsqueda espacio desperdiciado, espacio libre, el espacio entre particiones, y el texto genérico de los discos y las imágenes

Catálogo de creación de archivos y directorios para todos los dispositivos

Fácil de detección y el acceso a los datos de flujos de caracteres NTFS alternativos (ADS)

Cálculo masivo de *hash* del tipo (CRC32, MD4, ed2k, MD5, SHA-1, SHA-256, RIPEMD)

Poderosas capacidades de búsqueda física y lógica de palabras claves realizando varias al mismo tiempo

Vista recursiva de todos los archivos existentes y eliminados en todos los subdirectorios

Duplicación automática para la estructura de registro de archivo en NTFS

Opciones para generar casos, incorporar marcadores / anotaciones y generar informes

parciales de cada tarea o generales

Forensic-Computer, http://www.forensic-computers.com/software.php, listado de productos comerciales de diferentes fabricantes.

FResponse, http://www.forensic-computers.com/fresponse.php, Provee acceso de solo lectura a los discos de cualquier computadora en red y a la memoria RAM de la mayoría de los sistemas operativos de Microsoft Windows. Permite realizar tareas de

Informática Forense a través de redes ip utilizando la opción de herramientas del investigador.

Herramientas individuales e integradas en paquetes de función específica http://www2.opensourceforensics.org/, herramientas variadas para Informática Forense,

respuesta a incidentes, se aplican a la mayoría de las tareas requeridas en la recolección y análisis de datos, así como también presenta una serie de procedimientos para la verificación de la funcionalidad de las herramientas con el fin de que el perito determine si la herramienta reúne las capacidades esperadas para su labor pericial. Además de las herramientas y procedimientos se encuentran artículos relacionados con la Informática Forense y un conjunto de archivos de imágenes de discos para efectuar las pruebas de las aplicaciones. El conjunto de herramientas que ofrece este sitio aparece en las siguientes categorías, tanto para los sistemas operativos Linux como para Windows:

Ambientes de inicio o arranque automático: para iniciar el sistema dubitado en modo seguro o confiable

Obtención o adquisición de datos: para la recolección de información a partir de un equipo apagado o encendido

Particiones del sistema: para examinar la estructura de organización de los datos en los dispositivos de almacenamiento secundario, tal como tablas de particiones y etiquetas de los discos

Sistema de archivos: para examinar sistemas de archivos o imágenes de discos y mostrar el contenido de los archivos y cualquier otra meta data o información de la estructura del mismo

Aplicaciones: para analizar los contenidos de un archivo a nivel de la capa de aplicación

Red: para analizar paquetes y tráfico de red. No incluye los registros de eventos de los dispositivos de red

Memoria:. Para analizar la información de la memoria volátil

Entornos de programación: para construir herramientas de Informática Forense personalizadas

www.cromwell-intl.com/security/security-forensics.html, listado variado de herramientas para computadoras y cámaras digitales

www.evestigate.com/computer%20forensic%20resources.htm, listado de herramientas y procedimientos para diferentes dispositivos, como por ejemplo PDA

FAU, *Forensic Adquisition Utlilites,* George M. Garner Jr. conjunto de herramientas y librerías para Microsoft Windows, se pueden colocar en un diskette de inicio o dispositivo óptico. **www.gmgsystemsinc.com/fau/.** Listado de herramientas:

Dd.exe: basado en el dd de Linux

Volume_dump.exe: para descargar la información del dispositivo de almacenamiento volátil

FMData.exe: obtiene información de los descriptores de archivos, verificación matemática

Wipe.exe: limpia y desinfecta los dispositivos previa duplicación

Nc.exe: Aplicación para windows de netcat inspirada en la version original de Hobbit.

Librerías para la salida de la información generada por FAU: Zlib.dll, Bzip2.dll, Boost_regex-vc80-mt-1_34_1.dll, Fauerror_xxx.dll

The Coroner's Toolkit (TCT), de Dan Farmer y Wietse Venema, *http://www.porcupine.org/*

forensics/tct.html, conjunto de herramientas variadas de análisis forense para Unix, incorporadas en la mayoría de los paquetes integrados de *software* de arranque en vivo. Recolecta información específica que requiere de conocimientos avanzados del sistema operativo por parte del perito y además debe ser ejecutada en la computadora vulnerada, esta acción podría considerarse que altera la evidencia. La característica relevante es que permite capturar el estado actual de la información que resultaría casi imposible realizarlo de forma manual. La información que se almacena en los dispositivos de memoria volátil contiene datos relevantes para la obtención de la evidencia y detección de actividades no permitidas. Incluye herramientas para recuperar archivos borrados en Unix, para reconstruir datos coherentes a partir de un flujo de bits. A continuación se citan algunos de los comandos de este conjunto de herramientas:

grave-robber, recolecta información de los procesos activos, conexiones de red y contenidos de los dispositivos de almacenamiento no volátil. La herramienta comienza a relevar datos por orden de volatilidad. La recolección de datos puede ser muy lenta y tardar varias horas. La forma óptima de ejecutar grave-robber, es recolectar los datos volátiles en un sistema activo, apagar la computadora, crear una imagen del disco y luego utilizar la opción –f grave-robber en la copia del sistema de archivo.

mac, esta herramienta puede funcionar junto con grave-rober o en forma aislada. Permite recolectar una lista ordenada cronológicamente de las modificaciones, accesos y

53 Fecha de consulta: 25 de febrero de 2011.

54 Carretero Pérez, "Sistemas Operativos Una Visión Aplicada", http://www.arcos.inf.uc3m.es/~ssoo-va/, Fecha de consulta 25 de febrero de 2011.

55 Fecha de consulta: 25 de febrero de 2011.

ambios de hora de cada inodo, junto con su nombre de archivo. Esto facilita la correlación de datos en el análisis de las actividades efectuadas en el sistema de archivos. Se puede utilizar en cualquier sistema de archivo.

Unrm, permite generar un solo objeto conteniendo todo lo que se encuentra en los espacios no asignados en un sistema de archivo, lo cual puede ser de un tamaño considerable. No se debe efectuar la recolección de estos datos en el disco que se está analizando, porque sobrescribirá los propios datos de la investigación. Cuanto mayor sea el espacio libre, mayor será la cantidad de información. El comando *df,* de Linux o Unix muestra el sistema de archivo y el tamaño utilizado y disponible. Luego de crear el archivo, la herramienta *Lazarus,* analiza los datos determinando si los datos son de tipo texto o binario.

The Sleuth Kit, herramientas de línea de comandos de Unix para el análisis forense de diferentes sistemas de archivos, de Brian Carrier[1] http://www.sleuthkit.org/sleuthkit/desc. php, esta herramienta se encuentra incorporada en la mayoría de los paquetes de *software* de arranque en vivo o automático. Permite analizar diferentes volúmenes y sistemas de archivos.

Las herramientas Sleuth Kit están divididas en 4 categorías.

La primera muestra información de sistemas de archivos completos y sólo contiene el comando “fsstat”.

El segundo grupo comienza por “d” y nos permite acceder a los datos almacenados en archivos como: “dcalc”, “dcat”, “dls”, y “dstat”.

Sleuth Kit proporciona las siguientes herramientas para información del tipo metadatos almacenada en ínodos: “icat”, “ifind”, “ils”, e “istat”.

Los comandos en el 4º grupo comienzan con “f” y están diseñados para tareas de nivel de archivos como la creación de listas y búsqueda de archivos.

El comando “mactime” muestra los eventos cronológicamente en un sistema.

Los comandos “file” y “sorter” clasifican los archivos en la imagen del disco duro por tipo.

The Autopsy Forensic Browser, para analizar discos y sistemas de archivos de Windows y UNIX, Linux, de Brian Carrier.

La herramienta de gestión de pericias de informática forense Autopsy, desarrollada por Brian Carrier y accesible desde el sitio http://www.sleuthkit.org/autopsy/, es un programa con licencia GNU General Public License. (Apéndice 5 – Manual de Autopsy).

La ejecución de Autopsy requiere de la instalación previa del conjunto de herramientas Sleuth Kit. Autopsy se puede ejecutar en sistemas operativos Linux, Unix y en entornos Microsoft Windows. En el caso de que se desee ejecutar en sistemas operativos del tipo Microsoft Windows se deberá instalar previamente un emulador "Cygwin" del sistema operativo Linux o Unix. El navegador del tipo web de Autopsy es una interfaz gráfica para la ejecución de los comandos de las herramientas forenses y estándar de las utilidades de Unix. Permite realizar el análisis de volúmenes y sistemas de archivos sobre los sistemas operativos Unix y Windows. Los datos se almacenan en un directorio dentro del *"Evidence Locker"* (Casillero de Evidencia), el cual se especifica en el momento de la instalación o al ejecutar el programa. En el modo normal, Autopsy importa un archivo de una imagen de un disco o partición. En el modo "en vivo", Autopsy puede analizar un sistema en ejecución y no almacena ningún dato en el disco rígido local. Autopsy puede generar informes o reportes de cada una de los análisis que se efectúen, brindando información con diferentes niveles de detalle. Esta herramienta aparece también en la mayoría de los paquetes de *software* de código abierto y con *software* de base Linux que se ejecutan en el modo de arranque en vivo o automático.

Digital Corpora, sitio para la investigación y enseñanza de la informática forense. Contiene imágenes discos, memoria y captura de paquetes de tráfico de redes de uso libre, http:// digitalcorpora.org/

Sysinternals Suite, de Mark Russinovich. technet.microsoft.com/en-us/sysinternals/bb842062.aspx

Herramientas de funciones específicas:

Hash – **Verificación o comprobación matemática Md5summer,** http://www.md5summer.org/, herramienta de código abierto con interfaz gráfica para Microsoft Windows 9x, NT, ME, 2000 y XP. Fsum Frontend, es una herramienta de código abierto para efectuar el cálculo del *hash* o digesto, efectuar *checksums* y HMAC (*Hash-based Message Authentication Code*-Código de autenticación de mensaje basado con clave) para archivos de texto y cadena de caracteres. Permite arrastrar muchos archivos de una sola vez.

Soporta 96 algoritmos: alder8, adler16, adler32, ap *hash*, bdkr, cksum, cksum

mpeg2, crc8, crc16, crc16 ccitt, crc16 ibm, crc16 x25, crc16 xmodem, crc16 zmodem, crc24, crc32, crc32 bzip2, crc32 jamcrc, crc32 mpeg2, crc64, crc64 ecma, djb *hash*, dha256, edonley/emule, elf32, fletcher8, fletcher16, fletcher32, fnv0-32, fnv0-64, fnv1-32, fnv1-64, fnv1a-32, fnv1a-64, fork256, g*hash*3, g*hash*5, gost, has160, haval (128, 160, 192, 224, 256 bits) (3, 4, 5 pasadas), j*hash*, js *hash*, md2, md4, md5, panama, pjw32, ripemd128, ripemd160, ripemd256, ripemd320, rs *hash*, sdbm, sha0, sha1, sha224, sha256, sha384, sha512, size64, snefru2 (128, 256 bits) (4, 8 pasadas), sum8, sum16, sum24, sum32, sum64, sumbsd, sumsyv, tiger128, tiger160, tiger192, tiger2, tiger tree, tiger tree 2, whirlpool0, whirlpool1, whirlpool2, xor8, xum32. También SFV, MD5, SHA1/SHA2 para la creación y verificación de archivos. Fsum también está disponible como línea de comando. http://fsumfe.sourceforge.net/

DiskSig y CRCMD5, *software* comercial de New Technologies International, NTI http:// www.forensics-intl.com/disksig.html, se incluyen en el conjunto de herramientas de Informática Forense pero pueden también ser adquiridas individualmente. CRCMD5, muestra si el valor de *hash* se mantuvo igual o si en el caso que sea diferente, muestra los archivos que fueron modificados.

Md5sum es un algoritmo creado por Ron Rivest, del MIT (Instituto Tecnológico de Massachussetts) y publicada en 1992 como el RFC 1321. Es un algoritmo de verificación de 128 bits. Existen aplicaciones tanto para Unix, Linux como para Windows.

md5sum & sha1sum & sha2sum, http://www2.opensourceforensics.org/node/73

NIST NSRL: National Software Reference Library [Biblioteca de Referencia Nacional de Software] http://www.nsrl.nist.gov/ contiene las firmas o *hashes* de *software* de base y de aplicaciones. El programa Autopsy utiliza la base de datos de NSRL para ignorar los archivos de firmas conocidas y registradas en la biblioteca de referencia, reduciendo el tiempo de búsqueda para la verificación de firma de los programas.

Borrado seguro, limpieza y desinfección:

Comando dd, del sistema operativo Unix/Linux y versiones dd.exe para Windows

Active@ KillDisk, www.killdisk.com, producto comercial. Responde a los requisitos de Departamento de Defensa[2] de EE.UU. de Norteamérica e incluye el método de destrucción de Peter Gutmann, de 35 pasadas.

DiskScrub, http://www.forensics-intl.com/diskscrb.html producto comercial,

responde al estándar del Departamento de Defensa de EE.UU. de Norteamérica.

Steganos Privacy Suite, http://www.steganos.com/us/products/data-security/privacysuite/features, contiene la herramienta Shredder, producto comercial, disponible para prueba por 30 días la versión demo. Responde al estándar del DoD 5220.22-M/NISPOM 8-306 y permite seleccionar la opción de la tecnología de borrado de Peter Gutmann de 35 pasadas y la del borrado profundo, es decir el borrado de los datos que pudieron almacenarse en operaciones de eliminación y escritura anterior en los espacios libres, destruyendo todos los espacios libres de la unidad.

Duplicación de discos

FTKImager, **Forensic Toolkit Imager**, crea y certifica imágenes de diferentes dispositivos de almacenamientos y en formatos del tipo E01 –formato de Encase para CD y DVD–, AFF, formato forense avanzado, es un formato abierto, que permite al investigador no depender de un formato propietario y almacenar cualquier tipo de formato, como coordenadas de GPS, etc. Presenta opciones para montar distintos tipos de imágenes y exportarlas. http:// accessdata.com/support/adownloads#FTKImager

Safeback, www.forensics-intl.com, producto comercial, efectúa la duplicación bit a bit y genera un *hash* del tipo SHA 256.

SnapBack DatArrest, www.snapback.com, de Columbia Data Products (CDP), producto comercial que responde al estándar del NIST.

Ghost, www.symantec.com, producto comercial. Acorde a lo expresado en el libro *Computer Forensics, Incident Response Essentials* de W.G. Kruse II y J. G. Heiser, la línea de comando a utilizar con el programa Ghost,

Comando dd, responde al estándard del NIST, comando de los sistemas operativos Unix y Linux, dd copia un sistema de archivo completo, una partición o un dispositivo de almacenamiento con un tamaño de bloque que puede seleccionar el usuario, en forma predeterminada utiliza 512 bytes, realizando al mismo tiempo ciertas conversiones sobre él. Al finalizar informa cuántos bloques fueron procesados y puede generar un archivo de error para comprobar si la imagen se ha realizado satisfactoriamente. El comando dd permite también efectuar la duplicación y generación del *hash* del tipo md5sum o *sha1*. http:// www2.opensourceforensics.org/taxonomy/term/4

odd (open data duplicator), es una herramienta de *software* libre, sourceforge.net, sigue el modelo cliente/servidor y permite efectuar duplicaciones en forma simultánea en un número de computadoras en una red de área local.

dc3dd, http://dc3dd.sourceforge.net/

AIR Automated Image and Restore, es una la interfaz gráfica del comando dd/dc3dd, di-

señada para la creación fácil de imágenes en informática forense por Steve Gibson y Nanni Bassetti. http://sourceforge.net/

Características:

Detección automática de dispositivos IDE y SCSI, CD-ROM, cintas y cintas SCSI

Opciones para utilizar dd o dc3dd

Verificación matemática de la imagen origen y copia con MD5 o SHA1/256/384/512

Compresión de la imagen a través de gzip/bzip2

Crea imágenes en redes TCP/IP a través de las herramientas netcat/cryptcat

Limpieza , desinfección o sobreescritura de los dispositivos de almacenamiento o particiones con ceros

División de las imágenes en múltiples segmentos

Registro de eventos detallado con fecha y hora

Guymager http://guymager.sourceforge.net/

Duplicación en forma remota

Netcat http://www.securityfocus.com/tools/137

RDA http://md5sa.com/downloads/rda/index.htm

Manejo de Particiones

Partition Magic, Partinfo, esta utilidad pertenecía a Powerquest, la empresa fue adquirida

por Symantec. La aplicación genera un informe del contenido de la tabla de particiones y permite examinar las particiones de un disco en modo solo lectura, no cambia ninguna partición sólo muestra la información, lo cual es más confiable ya que no da lugar a posibles errores en el procedimiento del perito informático forense. El modificador /EPC permite a Partinfo verificar los dispositivos lógicos en las particiones extendidas. Con estas herramientas se puede generar un informe que muestre los contenidos de la tabla de particiones del disco rígido.

Gparted, Gome Partition Editor, es un editor gráfico de código abierto para el manejo de las particiones del dispositivo de almacenamiento. http://gparted.sourceforge.net/

RED

Network Miner, Netetwork Forensic Analysis Tool (NFAT) para Windows http://networkminer.sourceforge.net/

Xplico para Unix http://www.xplico.org

TCPFLOW, http://www.circlemud.org/~jelson/software/tcpflow/ ,

Wireshark, análisis de protocolos. http://www.wireshark.org

Recuperación de archivos eliminados

En Windows y Linux, Sleuth Kit (su nombre anterior era TASK), es *software* libre, para analizar los sistemas de archivos de Windows y Linux. Recupera archivos de particiones FAT, FAT12, FAT16, FAT32, FreeBSD, EXT2, EXT3, OpenBSD y UFS. Autopsy, es una interfaz gráfica para las utilidades de TASK, ambas se pueden obtener encontrar en www.sleuthkit.org.

Foremost – Herramienta de línea de comando, diseñada por Jess Kornblum y Kris Kendall,

graduados del MIT. El archivo se configura en /foremost directory. Para funcionar correctamente requiere almacenamiento externo. permite recuperar archivos perdidos en los sistemas operativos de Linux, Unix y Windows – foremost.sourceforge.net

Fatback, desarrollado por Nick Harbour del Departamento de Defensa de Estados Unidos

de Norteamérica http://sourceforge.net/projects/fatback/. Permite recuperar archivos en sistemas de archivos FAT12, FAT16 y FAT32. Se utiliza en sistemas operativos Linux o Unix.

En Windows

Norton Utilities Diskedit y Unerase, este conjunto de programas permite acceder a siste-

mas operativos del tipo DOS y Windows 3.x para recuperar archivos eliminados. Con la aparición de Windows 9x y versiones posteriores, esta herramienta resulta poco práctica para buscar en cada sector de los discos de gran capacidad de almacenamiento y de diferentes tipos de sistemas de archivos.

Active@Undelete – Data Recovery Tool, www.active-undelete.com, producto comercial, se puede descargar una versión demo. Permite recuperar archivos borrados de particiones NTFS (New Technology File System), NTFS + EFS (Encrypted File System), de datos borrados de particiones eliminadas o dañadas, de sistemas de archivos EFS, ofrece funciones para RAID de discos y red, permite restaurar archivos borrados de Windows 2000, Windows XP, Windows 98, Windows ME, Windows NT, Vista, Windows 2003. Imagen disponible para crear CD o DVD de arranque o inicio.

DNA (Distributted Network Attack) de AccessData, www.accessdata.com permite acceder a los programas de oficina que se encuentran distribuidos en múltiples computadoras, distribuyendo la recuperación de clave entre las mismas y consumiendo escasos recursos de procesador, utilizando el tiempo ocioso, se basa en un ataque de fuerza bruta. Se debe configurar una computadora como DNA Maestro y es la única que puede abrir el archivo una vez que se recuperó la clave. Asimismo

posee una opción para la configuración remota.

Recuperación de archivos con claves

La empresa Elcomsoft http://www.elcomsoft.com/ofrece una amplia lista de productos para obtener las claves de documentos creados por distintas aplicaciones:

ElcomSoft Distributed Password Recovery, recupera las claves de una gran variedad de

aplicaciones de oficina de Microsoft, de OpenOffice, PGP, Adobe pdf, Claves del sistema, resguardos de Iphone, Ipad, Ipod, Blackberry. También presenta productos para aplicaciones específicas en paquetes individuales:

Advanced Office XP password recovery, es específica para recuperar los archivos guardados con clave y generados para esta versión.

Advanced ZIP Password Recovery, se utiliza para la recuperación de claves de diversas aplicaciones de Windows y de archivos zip. Para los archivos comprimidos con zip y protegidos con claves se puede utilizar la herramienta ZipPassword. http://www.elcomsoft.com/archpr.html

Advanced PDF Password Recovery, archivos del tipo pdf

Advanced SQL Password Recovery, archivos de SQL

Recuperación de archivos de la papelera de reciclaje:

Papelera de Reciclaje, utilidad del sistema operativo Windows 9x, Windows NT, Windows 200x, Windows XP. Acorde a la configuración de este objeto los datos eliminados se pueden recuperar o restaurar a su lugar de origen. Si la opción para eliminar los archivos es de no enviar o mover a la papelera de reciclaje, no se podrán restaurar a partir de esta aplicación.

Rifiuti (basura en italiano), permite obtener toda la información del archivo INFO2 en forma automática, ejecutando: ./rifiuti INFO2 > INFO2.txt

Con la opción –t se puede modificar el delimitador de campos, la salida estándar del comando se envía a la consola en forma predeterminada. El archivo INFO2 se puede importar en una planilla de cálculo para efectuar búsquedas u ordenar la información

y dar formato a los datos para presentar en el informe pericial. http://www.mcafee.com/es/downloads/freetools/rifiuti.aspx

En Linux / Unix

Debugfs, es una poderosa herramienta para la recuperación de archivos eliminados. Por ejemplo utilizarla para acceder en modo solo lectura al dispositivo hda2.

#debugfs /dev/hda2

Telefonía, Celulares, PDA, GPS

E-evidence Info, *www.e-evidence.info/cellular.html*, listado de herramientas comerciales y libres

Bitpin, visualiza y administra información de teléfonos LG, Samsung, etc (Licencia GPL)

www.bitpim.org

Chip IT, home.scarlet.be/chipit/Chipit.html

SIMfill, Subscriber Identity Modules (SIMs), NIST National Insitute of Standards and Technology, herramienta para la validación experimental de celulares, http://www.sciencedaily. com/releases/2009/12/091202091032.htm

Oxygen Forensic Suite 2010 (comercial), www.oxygen-forensic.com/en/

UFED Cellebrite (comercial), extracción de datos, análisis físico y lógico, www.cellebrite.com

Device Seizure 4.0, celulares, PDA , GPS, (comercial) www.paraben.com/

Neutrino (comercial), de Guidance Software. www.guidancesoftware.com

Herramientas para la elaboración del informe pericial

En la redacción del informe pericial se pueden utilizar una serie de herramientas de *software* para:

La descripción y documentación de la ubicación geográfica accediendo al siguiente *soft-*

ware disponible de manera gratuita en Internet:

Google Earth, Google maps, para obtener la ubicación y luego con herramientas como los graficadores incorporarles información de texto o de referencia como flechas, etc.

Sistemas de información geográfica –GIS– de código abierto, en este sitio se encuentra

un amplio listado de diferentes desarrollos de herramientas GIS. http://opensourcegis.org/

El croquis o esquicio o representación del lugar del hecho específico se pueden utilizar he-

rramientas de diseño de planos como:

Microsoft Visio http://visiotoolbox.com/2010/ o SmartDraw, http://www.smartdraw.com/, ambos productos comerciales con versiones de prueba.

CAD de código abierto, http://www.osalt.com/autocad, http://www.freebyte.com/cad/cad.htm#architecturalsystems.

La redacción del informe se puede utilizar un procesador de texto de código abierto como

Writer de OpenOffice.

La digitalización de las fotografías o películas: generalmente forman parte del equipo en el

momento de su compra.

Clasificación e identificación de las pericias informático forenses

En Criminalística las pericias se clasifican según el tipo de especialidad, por

ejemplo, Balística (BAL), Papiloscopía (PAL), Dactiloscopía (DAL). En el caso de las pericias informático forenses, podría colocarse una nomenclatura común, no sería necesario determinar la especialidad ya que todas pertenecen al mismo conjunto. Sin embargo, si se desea efectuar una clasificación detallada, podría utilizarse una identificación acorde al tipo de incidente o delito dentro de la temática informática forense. Cualquiera sea la forma de identificar las pericias, debe aplicarse a todos los elementos que conformen la pericia, es decir, a la información recolectada, analizada, a la documentación, al dispositivo de herramientas de recolección. Al asignar nombres a los archivos generados en las diversas etapas, para identificarlos y asociarlos con la pericia y con la tarea realizada, es importante que se considere el número adecuado de caracteres, de modo que permita especificar con claridad la pericia y que, a su vez, no sea excesivamente largo.

Nomenclatura

PIF (Pericia Informático Forense), en el caso de que se desee identificar la especialidad criminalística a la que pertenece la pericia.

NRO, número de la pericia, para la organización y clasificación de las pericias realizadas por el perito informático forense.

RI (Respuesta Incidente), en el caso de que la pericia sea una respuesta a un incidente.

Dirección IP de la computadora, 192.168.1.6.

EMPRESA, nombre abreviado o completo del particular que solicitó la pericia.

CNRO, CAUSA NRO, número de la causa que originó la pericia.

Tipo de delito, identificación abreviada del delito informático. Defraudación, estafa, robo, hurto.

Fecha, el formato puede ser dos dígitos para el día, el mes con 3 letras abreviado, dos dígitos para el año: 07Nov04.

Nombre del archivo, fecha.txt, dir.txt, ram.txt, procesos.txt.

Ejemplos

PIF001-RI-AZR-07Nov04

PIF001-RI-AZR-07Nov04-procesos.txt

PIF001-RI-AZR-07Nov04-192.168.1.6-procesos.txt

Nro de pericia, Nro de Causa, Tipo de delito, Fecha:

001-C13631-Robo-07Nov04

001-C13631-Robo-07Nov04-temp.txt

Etapas del Marco Tecnológico Pericial

Se debe considerar una etapa previa a las del Marco Tecnológico Pericial que está relacionada con la Preparación de las herramientas de software y *hardware* a utilizar en diferentes casos o situaciones.

Procedimientos a efectuar en el laboratorio para la preparación de las herramientas de

software y *hardware*

Importante

En el laboratorio y antes de concurrir al lugar del hecho, el perito informático forense deberá asegurarse de que conoce el manejo de las herramientas de *software* y que ha efectuado su comprobación matemática –*hash*– y que los dispositivos de *hardware* que utilice para la duplicación de la evidencia se encuentren limpios, desinfectados y sin ningún dato que puedan generar confusiones en el momento del análisis de la prueba. En esta operación es recomendable desconectar todos los dispositivos de disco de la estación forense para evitar borrar otras evidencias y conectar solamente la unidad que se desea borrar en modo seguro.

Tarea a realizar en el Laboratorio

Procedimiento para la comprobación matemática de las herramientas

Para comprobar la integridad y confiabilidad de la herramienta, previamente en el laboratorio, deberá efectuar las siguientes acciones:

Generar el *hash* en un disco del laboratorio que contenga datos a examinar.

Guardar el resultado del *hash*.

Utilizar la herramienta deseada para analizar los datos del disco, una vez finalizado el análisis:

Generar nuevamente el *hash* del disco.

Verificar si el *hash* se ha modificado, o se mantiene igual que el obtenido previamente a la realización del análisis de la información. Si los valores de *hash* son distintos, significa que la herramienta utilizada contaminará los datos que se están analizando. Por lo tanto es necesario determinar qué datos fueron los modificados.

Para preparar una herramienta o conjunto de herramientas que se utilizarán en la recolección de datos, en cada uno de los casos, efectuar la siguiente secuencia:

Rotular el dispositivo físico que contendrá las herramientas de recolección de datos, ya sean diskettes, CD-ROM, Zip, Pen Drive:

Número o identificación específica del caso

Fecha y hora

Nombre o responsable que generó el conjunto de herramientas

Nombre del perito informático forense que utilizará las herramientas en un determinado caso

Verificar las dependencias de las librerías o archivos que utiliza cada herramienta, los archivos que accede o modifica.

Certificación matemática de cada herramienta, se pueden almacenar en un archivo de texto dentro del dispositivo que contiene las herramientas y del dispositivo completo (diskette, CD-ROM, Zip, Pen Drive).

Protección contra escritura de los diskettes: si el conjunto de herramientas se encuentra en un diskette, se debe proteger contra escritura luego de finalizar la preparación de la herramienta de recolección de evidencia.

Ejemplo con md5sum:

Línea de comando de md5sum En Linux o Unix:

#md5sum /etc/passwd b256ffa6286ef598bf204d9bdf3fb8e4 /etc/passwd En Windows

c:\>md5sum.exe md5sum.exe d41d8cd98f00b204e9800998ecf8427e md5sum.exe

Sitio de obtención de la herramienta md5sum.exe: http://www.etree.org/md5com.html

Procedimiento para la limpieza y desinfección de los dispositivos de escritura

En el laboratorio el perito informático forense podrá efectuar la limpieza o desinfección de los dispositivos de almacenamiento utilizando algunas de las siguientes herramientas que pueden ser de código abierto o comercial:

1. Comando dd[3]

dd, comando de los sistemas operativos Unix y Linux, permite asegurar la inexistencia de datos que pueda dañar la evidencia a través de un borrado seguro de los datos:

Línea de comando:

#dd if=/dev/zero of =/dev/fd0 2>/home/pericia/imagen/discolimpio

La herramienta mejorada de *dd* es *dcfldd* y funciona en forma semejante a la de *dd*. Posteriormente se debe verificar con una herramienta de edición de disco para confirmar que los datos consisten en una cadena de ceros.

Sitio de obtención de la herramienta *dd*: http://www2.opensourceforensics.org/tools/data-acquisition

El perito informático forense en el reconocimiento judicial y en la inspección judicial.

El reconocimiento judicial y la inspección judicial incluyen a un determinado conjunto de pasos a seguir acorde al Marco Tecnológico Pericial. Las etapas son las siguientes:

Acceso a los recursos informáticos dubitados, es decir el acceso físico al lugar del hecho, en donde se realizará la recolección de evidencia.

Identificación y registro de cada uno de los elementos de la escena del peritaje, desde el ingreso al área hasta el arribo al elemento específico dubitado.

Autenticación, duplicación y resguardo de la prueba, incluye:

La certificación matemática de la evidencia para su autenticación. Esta comprobación se efectúa a través de herramientas de *software* o *hardware* que calculan el valor *hash* o huella digital de los datos.

La duplicación permite generar una copia idéntica del dispositivo de almacenamiento secundario dubitado. El número de copias a realizar dependerá del tipo de requisitoria pericial. En algunos casos se deberán realizar dos copias. Una copia se deja en el lugar del hecho para permitir la continuidad de las actividades, otra copia se utiliza para el análisis en el laboratorio del perito informático forense y el original se deja en depósito judicial o si la pericia ha sido solicitada por un particular, certificarlo ante escribano público y guardarlo según sea indicado por el solicitante de la pericia y el escribano público.

El resguardo de la prueba, especifica la forma de rotular y proteger la evidencia, ya sea para su traslado al laboratorio, para el depósito de la misma y/o para su futura reapertura.

En esta etapa participan un conjunto de recursos humanos, tales como las víctimas del delito, los posibles causantes del delito, las fuerzas de seguridad, escribanos públicos, peritos de otras especialidades criminalísticas, autoridades judiciales.

Detección, recolección, registro de indicios probatorios y cadena de custodia: en esta etapa el perito informático forense accede a la evidencia específicamente y efectúa todas las tareas relacionadas con la detección de los ilícitos, la recolección de los elementos probatorios y la documentación en los formularios pertinentes de la evidencia obtenida. En esta situación el perito informático forense determinará acorde a la requisitoria de la pericia o del caso particular, si el abordaje a la evidencia digital

se efectuará con el equipo encendido, en tiempo real o con el equipo apagado, en el lugar del hecho o en el laboratorio.

En este punto el reconocimiento judicial y la inspección judicial propiamente dicha culminan y se continúa con la etapa de:

Análisis e interpretación de los indicios probatorios: acorde a las circunstancias, estas actividades se realizarán en el lugar del hecho o en el laboratorio. Se utilizarán todas aquellas herramientas que permitan el análisis de la evidencia recolectada y su posterior interpretación. La reconstrucción y/o simulación del incidente se efectuará preferentemente en el laboratorio. Los datos obtenidos se documentarán en formularios específicos.

Cotejo, correlación de datos y conclusiones: según la requisitoria pericial, se podrá realizar en el lugar del hecho o en el laboratorio. Se efectuarán las tareas necesarias para obtener las conclusiones que comprueben o no la concurrencia del delito, ilícito o incidente, a través de comparaciones, correlaciones y verificaciones de la integridad de los datos obtenidos. En esta etapa el perito informático forense deberá utilizar el criterio, el sentido común y los conocimientos académicos para generar conclusiones coherentes y contundentes.

Resguardo de herramientas de *hardware* y *software* utilizadas en la elaboración de la pericia, en esta etapa se deberá documentar todos los elementos utilizados en la pericia informático forense, resguardando el material en sitios de acceso restringido y adecuadamente protegidos. Deberá existir un recipiente específico para guardar los elementos de cada pericia realizada para acciones futuras.

Generación del informe pericial, en esta etapa el perito informático forense, concluye la pericia, efectuando las acciones de revisión del escrito y comprobación de posibles errores. Evitando de esta forma la omisión de datos relevantes o la inclusión de datos superfluos o equívocos.

Según la naturaleza de la requisitoria pericial el perito informático forense podrá elaborar un conjunto de medidas de respuesta a incidentes.

Los modos de acceso al lugar del hecho dependerán particularmente de la situación específica y del elemento dubitado. Generalmente se recomienda que se efectúe un recorrido visual en forma de espiral de la periferia al centro –en donde se encuentran el o los elementos dubitados–, utilizando equipamiento como cámaras fotográficas, filmadoras, equipos de planimetría.

A continuación se analizarán las etapas referidas en el Marco Tecnológico Pericial,

los procedimientos a realizar y las posibles herramientas a implementar en cada una de ellas. En algunas de las etapas se efectuarán aclaraciones preliminares y se describirán contenidos conceptuales relacionados con las funciones específicas de la etapa en cuestión.

– Etapa: Acceso a los recursos dubitados

En el acceso al lugar del hecho, pueden ocurrir diversas circunstancias acorde al origen de la solicitud de la pericia.

Por orden judicial: El acceso será compulsivo, el perito informático forense concurrirá acompañado de otros peritos o con personal policial o con fuerzas de seguridad. El lugar podrá encontrarse, clausurado y custodiado por personal policial, quienes le indicarán al perito informático forense el lugar en donde se encuentran los recursos dubitados.

Por un particular: El acceso al sitio de recolección de la evidencia se efectuará con la guía de la persona o personas pertenecientes al lugar del hecho, o por quienes solicitaron la pericia, con testigos y con escribano público.

– Etapa: Identificación y registro

La inspección judicial para el perito informático forense incluye los requisitos generales de la inspección judicial en Criminalística. En la mayoría de los casos se debe identificar todos los elementos posibles **–Anexo – Lista de Control de** Hardware **en la Inspección y Reconocimiento Judicial–,** tanto si se trata de una única computadora como de una red de computadoras. Al arribar al lugar del hecho se deben seguir una serie de pasos acorde al siguiente procedimiento y documentar o registrar la información obtenida:

Colocarse guantes.

Fotografiar el lugar del hecho o filmar todos los elementos que se encuentran en el área de inspección, desde la periferia hacia el área dubitada.

Fotografiar los elementos informáticos, determinando en cuál de ellos efectuar macrofotografía:

Pantallas del monitor de la computadora.

Computadora, vistas frontal, lateral y posterior

Números de series de los elementos informáticos, etiquetas de garantías.

Periféricos (teclados, mouse, monitor, impresoras, agendas PDA, videocámaras, video grabadora, Pen Drive, dispositivos de almacenamiento en red, Unidades de Zip o Jazz, celulares, entre otros)

Material impreso en la bandeja de la impresora o circundante

Cableados

Dispositivos de conectividad, alámbricos e inalámbricos

Diagramas de la red y topologías

Inventariar todos los elementos utilizando una planilla de registro del *hardware*, identificando: Tipo, Marca, Número de serie, Registro de garantía, Estado (normal, dañado), Observaciones Particulares. consultar Anexo – Lista de control del *hardware* de la Inspección Judicial y Reconocimiento Judicial – Anexo – Formulario de Registro de evidencia de la computadora

Efectuar un croquis del lugar del hecho, especificando el acceso al lugar, la ubicación del o los equipos informáticos y de cualquier otro elemento, mobiliario, racks, cableado, existentes en el área a inspeccionar, para luego representarlo con cualquier herramienta de diseño. Este paso está relacionado con la Planimetría, descripta en el **Anexo – Lista de control del** hardware **de la Inspección Judicial y Reconocimiento Judicial.**

En los casos que sean factibles, entrevistar a los responsables del área y solicitar copias, si hubiere, de la documentación relacionada con el organigrama del área, políticas, procedimientos y planes de contingencia, listado de recursos humanos responsables actuales de la administración y operación del o los equipos dubitados, listado del personal que se desempeñó en la administración de los equipos en años anteriores, ya sea de personal despedido por la empresa o que hayan renunciado por propia voluntad, listado de los horarios de trabajo y funciones específicas del personal actual y de años anteriores.

– Etapa: Autenticación, duplicación y resguardo de la prueba

En esta etapa el perito informático forense deberá secuestrar la evidencia procediendo acorde al origen del requerimiento de la pericia informático forense, a

saber:

Procedimiento

Por orden judicial, cuyo texto indica:

Secuestrar la evidencia para su posterior análisis en el laboratorio, el perito informático forense procederá a:

Certificar matemáticamente la evidencia

Identificar y registrar la evidencia

Elaborar un acta ante testigos

Iniciar la cadena de custodia

Transportar la evidencia al laboratorio

Efectuar la copia de la evidencia para su posterior análisis en el laboratorio, el perito informático forense procederá a:

Certificar matemáticamente la evidencia

Duplicar la evidencia

Identificar y registrar la evidencia y la copia

Elaborar un acta ante testigos

Transportar la copia o duplicación de la evidencia al laboratorio

Por solicitud particular de una persona específica, de una consultora, empresa, institución, organismo o por otros profesionales, el perito informático forense procederá a:

Concurrir al lugar del hecho con un escribano público

Certificar matemáticamente la evidencia ante el escribano público

Duplicar la evidencia ante escribano público

Solicitar al escribano que deje constancia en el acta de los motivos del secuestro, de

los datos de la o las personas que solicitaron la pericia, las razones argumentadas y los fines pretendidos.

Solicitar una copia del acta realizada por el escribano.

Transportar la copia de la evidencia para su posterior análisis en el laboratorio

Duplicación y autenticación de la prueba

A continuación se enuncian los pasos para efectuar la autenticación y duplicación de la prueba, el perito informático forense llevará en su maletín los dispositivos de almacenamiento limpios y desinfectados y el dispositivo de arranque (disco rígido externo, CD-Rom, DVD, diskette) o inicio en vivo protegido contra escritura, que contiene el *software* de base seleccionado para la tarea y el *software* de autenticación y duplicación.

Las imágenes de los discos se deben realizar bit a bit para capturar la totalidad del disco rígido los espacios libres, no asignados y los archivos de intercambio, archivos eliminados y ocultos. Acorde a lo expresado por el NIST[4] (National Institute of Standard and Technlogy), la herramienta utilizada para la generación de la imagen debe reunir ciertas especificaciones, a saber:

La herramienta deberá efectuar una imagen bit a bit de un disco original o de una partición en un dispositivo fijo o removible.

La herramienta debe asegurar que no alterará el disco original.

La herramienta podrá acceder tanto a discos SCSI como IDE.

La herramienta deberá verificar la integridad de la imagen de disco generada.

La herramienta deberá registrar errores tanto de entrada como de salida e informar si el dispositivo de origen es más grande que el de destino.

La documentación de la herramienta deberá ser consistente para cada uno de los procedimientos. Esta imagen del disco se utilizará en la computadora del laboratorio para efectuar el análisis correspondiente.

Apagar el equipo desconectando el cable de alimentación eléctrica

Retirar diskettes, Pen Drive, Zip.

Descargar la propia electricidad estática, tocando alguna parte metálica y abrir el gabinete.

Desconectar la interfaz o manguera de datos, puede ser IDE o SCSI.

Desconectar la alimentación eléctrica del dispositivo de disco rígido.

Ingresar al CMOS (Complementary Metal Oxide Semiconductor) o Configuración del BIOS (Sistema de entrada y salida de la computadora):

Encender la computadora.

Oprimir el conjunto de teclas que se muestra en el monitor cuando se inicia la computadora para acceder al CMOS.

Verificar la fecha y hora del CMOS y registrarla en el formulario de recolección de evidencia y documentar todo tipo de dato que el perito informático forense considere relevante.

Modificar la unidad de inicio o arranque del sistema operativo, es decir seleccionar la unidad de diskete, CD-ROM / DVD o zip.

Guardar los cambios al salir

Verificar la existencia de discos CD-ROM o DVD:

h. Abrir la lectora o grabadora de CD-ROM o de DVD y quitar el disco pertinente

Colocar la unidad de arranque, diskette, CD-ROM/DVD o zip en el dispositivo de *hardware*

pertinente.

Verificar el inicio desde la unidad seleccionada.

Apagar el equipo.

Asegurar el dispositivo de almacenamiento secundario original, generalmente está configurado en el CMOS como Master –maestro o primario– con protección de sólo lectura, a través de la configuración de los *jumpers* que indique el fabricante del disco o a través de *hardware* bloqueador de lectura.

Conectar el cable plano al disco rígido, puede ser IDE o SCSI.

Conectar la alimentación eléctrica del dispositivo de disco rígido master –maestro o primario.

Conectar el dispositivo que se utilice como destino para hacer la duplicación del disco rígido dubitado como slave –esclavo o secundario–, ya sea una controladora SCSI, un disco IDE esclavo o una unidad de cinta, o cualquier otro *hardware* utilizado para la duplicación de tamaño superior al disco original o dubitado. Si el almacenamiento secundario original es demasiado grande o es un arreglo de discos, efectuar la copia en cintas.

Verificar que en el dispositivo de arranque seleccionado se encuentren los controladores del *hardware* para la duplicación, en caso de que sean requeridos.

Encender la computadora iniciando desde la unidad de arranque configurada en el CMOS.

Efectuar la certificación matemática del dispositivo dubitado.

Guardar el resultado en un dispositivo de almacenamiento

Registrar el resultado en el formulario verificación de la evidencia

Duplicar el dispositivo de los datos con la herramienta de *software* y *hardware* seleccionada.

Efectuar, acorde al requerimiento de la pericia una o dos copias de la evidencia. En el caso de realizar dos copias, una se deja en el lugar del hecho, para permitir la continuidad de las actividades, otra copia se utiliza para el análisis en el laboratorio del perito informático forense y el original se deja en depósito judicial o si la pericia ha sido solicitada por un particular, registrarlo ante escribano público y guardarlo, según lo indicado por el solicitante de la pericia y el escribano público.

Efectuar la certificación matemática de la o las copias del dispositivo dubitado.

Guardar el resultado generado por las copias duplicadas en un dispositivo de almacenamiento.

Registrar el resultado generado por las copias duplicadas en el formulario de recolección de la evidencia.

Apagar el equipo.

Retirar los tornillos de sujeción del dispositivo de disco rígido.

Retirar el disco rígido con cuidado de no dañar el circuito electrónico.

Ejemplo de duplicación con el comando dd, que se encuentra en el disco de arranque o inicio en vivo con las herramientas informático forense, a través de la línea de comando:

dd if=/dev/sda of=/dev/sdb bs=1M

dd = es el comando para realizar la duplicación

if = indica el origen, es decir, desde el dispositivo (/dev/sda) que puede ser del tipo SATA, configurado como master, maestro o primario.

of = indica el dispositivo destino en donde se duplicará bit a bit (/dev/sda) que puede ser del tipo SATA, configurado como slave, esclavo o secundario.

bs =1M; indica que la duplicación se realizará en tamaños de bloques de 1 Mb

Procedimiento para el resguardo de la prueba y preparación para su traslado Procedimiento

Disponer, según sea el caso, las pruebas obtenidas en una zona despejada, para su posterior rotulado y registro.

Registrar en el formulario de registro de la evidencia cada uno de los elementos dubitados, acorde a lo especificado en dicho formulario y agregando cualquier otra información que considere pertinente el perito informático forense.

Proteger en bolsas antiestáticas los elementos de almacenamiento secundario, registrando: Fecha y hora del secuestro, Tipo, Número de serie del elemento si se puede obtener, Capacidad de almacenamiento, Apellido, Nombre y DNI del perito informático forense, Firma del perito informático forense. **Anexo – Rótulos de Evidencia.**

Proteger con plástico y/o con bolsas estériles cualquier otro elemento que considere relevante el perito informático forense y rotularlos con los datos pertinentes al elemento, Apellido, Nombre y DNI del perito informático forense, Firma del perito informático forense.

Elaborar el acta de secuestro acorde al formulario del **Anexo – Recibo de Efectos.**

Colocar los elementos identificados y registrados en una caja o recipiente de traslado que asegure la suficiente rigidez, aislamiento térmico, electromagnético y protección para evitar daños accidentales en el traslado de los elementos probatorios.

Trasladar, en lo posible, los elementos secuestrados reunidos en un único recipiente, evitando la confusión, separación o pérdida durante su almacenamiento posterior. **Anexo – Formulario Cadena de Custodia.**

Elementos para el traslado de evidencias

La evidencia puede ser colocada en bolsas antiestáticas o sobres de papel, rotulada y sellada. www.premiercrown.com, www.fitzcoinc.com

El traslado de la evidencia puede realizarse en cajas especialmente protegidas y antiestáticas. www.pelican.com

– Etapa: Detección, recolección y registro de indicios probatorios

Acorde al tipo de pericia, al estado en que se encuentren el o los recursos dubitados y al propio criterio y sentido común, el perito informático forense podrá optar por una de las dos alternativas para el abordaje de la recolección de la evidencia, en particular al tratarse de computadoras o redes de computadoras, es decir, acceder con el equipo encendido o con el equipo apagado.

El perito informático forense debe tener un conjunto de herramientas disponibles en uno o varios paquetes de datos que permitan y faciliten efectuar la tarea de recolección de evidencias y análisis de los datos en el lugar del hecho o en el laboratorio, ya sea de una computadora aislada o de una computadora en un entorno de red. Existen un conjunto de herramientas que automatizan estas tareas, algunas de ellas son productos comerciales y otras son productos de licencias de *software* libre. No obstante estos productos no realizan todo lo que el perito informático forense necesita, por consiguiente es necesario evaluar y verificar los resultados que se obtienen a partir del uso de estas herramientas y agregarlas como un elemento más del paquete de herramientas a utilizar.

Alternativa I, para el acceso con el equipo encendido

En el caso de que se deba acceder a un equipo encendido, se debe considerar la obtención de los datos en tiempo real y de los dispositivos de almacenamiento volátil. Los dispositivos de almacenamiento volátil de datos pierden la información luego de interrumpirse la alimentación eléctrica, es decir al apagar la computadora la información almacenada se pierde.

Los datos que se encuentran en el almacenamiento volátil muestran la actividad actual del sistema operativo y de las aplicaciones, como, por ejemplo: procesos en el estado de ejecución, en el estado de listo o bloqueado, actividad de la impresora (estado, cola de impresión), conexiones de red activas, puertos abiertos, (puerto es una estructura a la que los procesos pueden enviar mensajes o de la que pueden extraer mensajes, para comunicarse entre sí, siempre está asociado a un proceso o aplicación, por consiguiente sólo puede recibir de un puerto un proceso, **Listado Puertos Troyanos**, recursos compartidos, estado de los dispositivos como discos rígidos, disqueteras, cintas, unidades ópticas. Los datos volátiles están presentes en los registros de la unidad central de procesamiento del microprocesador, en la memoria caché, en la memoria RAM o en la memoria virtual.

En la siguiente tabla se muestra una clasificación de los dispositivos de almacenamiento volátil y el orden en que los datos deberían ser recolectados (Concepto introducido por Dan Farmer y Wietse Venema,[5] creadores de la herramienta de informática forense The Coroner's Toolkit), para un sistema operativo Unix o Linux (Fuente: *Computer Forensics, Incident Response Essentials* de Warren G. Kruse II y Jay G. Heiser):

Tiempo de duración	**Dispositivo**	**Tipo de datos almacenados**	**Importancia para el perito informático forense**
Ciclo de reloj	CPU	Registros	Difícil de capturar y de importancia mínima
		Cache	Difícil de capturar como una entidad discreta, pero debería capturarse como parte de la imagen de memoria del sistema
	Video	RAM	Se puede capturar la pantalla, aparte de fotografiarla, puede brindar importantes datos

Hasta que se apaga la computadora	Almacenamiento del sistema	RAM	Incluye información de todos los procesos activos y el estado del núcleo del sistema operativo. Es de fácil captura pero esta acción modifica los datos. Se requiere conocimientos avanzados para determinar estos cambios.
	Tablas del núcleo del sistema operativo	Estado de la red	Se puede determinar si un programa de puerta trasera ha sido instalado y si está activo. Se debe examinar si existe actividad de red.
		Procesos activos	Algunos procesos pueden evidenciar una actividad no autorizada. Todos los procesos se deben comparar con los archivos binarios respectivos para asegurar que no son programas troyanos.

Tiempo de duración	**Dispositivo**	**Tipo de datos almacenados**	**Importancia para el perito informático forense**
Hasta que es sobrescrito o eliminado en forma segura	Disco rígido	Espacio de intercambio	Cuando el sistema operativo demanda más memoria RAM, algunos de los datos del núcleo se intercambian con el disco rígido. Estos datos son tan relevantes como los datos de la RAM en el momento de analizar lo que está ocurriendo en una determinada unidad de tiempo.
		Directorios con datos pendientes	Incluye información de los procesos activos y de las operaciones incompletas. Pueden incluir correo saliente, trabajos en cola de impresión, los cuales no se encuentran en ninguna otra parte del sistema.
		Directorios temporales	Los directorios / tmp y en algunos casos el directorio /usr/tmp son utilizados por el sistema como sitio de almacenamiento temporal de datos. Algunos usuarios suelen periódicamente eliminar

			los datos en estos directorios, pero si no lo hacen pueden ofrecer información relevante.

Tiempo de duración	Dispositivo	Tipo de datos almacenados	Importancia para el perito informático forense
		Directorio de registros de eventos	Relevante para la reconstrucción de eventos. El mantenimiento de estos registros implica la sobreescritura eventual para evitar su crecimiento a grandes tamaños de almacenamiento.
		Directorios de Usuarios, Binarios, de Bibliotecas y de Configuración	Cada parte del sistema de archivo que no es considerada del tipo temporal, de registro o de directorios con datos pendientes, contienen información que puede permanecer por indefinidamente. No obstante alguien con acceso de escritura puede modificarlos o borrarlos en cualquier momento.
	Dispositivos removibles	Disquetes ZIP Jazz	De uso menos frecuente, pero pueden contener información relevante. Los dispositivos de alta capacidad de almacenamiento como el ZIP y Jazz, pueden ser utilizados como unidades de resguardo de datos.

Tiempo de duración	Dispositivo	Tipo de datos almacenados	Importancia para el perito informático forense
		Cintas	Ofrecen información histórica del contenido del sistema de archivos. Si existen resguardos previos al incidente pueden ser utilizadas como elemento para acotar la investigación y ocurrencia del incidente

Lectura/escritura	Estas unidades generan multisesiones, las cuales no pueden ser sobrescritas, cada sesión genera una nueva tabla de directorios. Se deben examinar todas las sesiones.
CD-ROM sólo escritura	La escritura de una sola vez almacena archivos de registros que no pueden ser alterados y se pueden realizar búsquedas electrónicas de datos.
Papel impreso	En cantidades grandes de información impresa se torna difícil la búsqueda de datos específicos, salvo por su destrucción física, serían una de las fuentes de almacenamiento que conserva la información por más tiempo

La captura completa del estado actual de la computadora es imposible. La acción de examinar los datos en un almacenamiento volátil produce alteración de los mismos. En una computadora portátil la opción Hibernar, almacena todo lo que posee en la memoria RAM en el disco rígido y luego apaga la computadora, al reiniciar y salir de la hibernación, vuelve al estado previo. En el sistema operativo Windows XP, esta opción aparece en el Panel de Control en el icono Opciones de Energía, en la ficha Hibernación. Por lo tanto se puede verificar si se encuentra habilitada o no y considerar esta opción como una forma de obtener los datos del estado anterior del sistema.

En un considerable número de situaciones, la recolección de los datos deberá efectuarse a partir de los datos volátiles, en estos casos, se debe tener la precaución de utilizar las herramientas adecuadas y previamente comprobadas para evitar dañar la información. Como primera medida para el abordaje de los datos volátiles sería la de ejecutar una secuencia de tareas que disminuyan el riesgo de alterar la información. (*Incident Response and Computer Forensics, Kevin Mandia, Chris Prosise y Matt Pepe*),10 a saber:

Procedimiento

Conjunto de tareas a realizar en el acceso a los dispositivos de almacenamiento volátil:

Ejecutar un intérprete de comandos confiable o verificado matemáticamente.

Registrar la fecha, hora del sistema, zona horaria.

Determinar quién o quiénes se encuentran con una sesión abierta, ya sea usuarios locales o remotos.

Registrar los tiempos de creación, modificación y acceso de todos los archivos.

Verificar y registrar todos los puertos de comunicación abiertos.

Registrar las aplicaciones relacionadas con los puertos abiertos.

Registrar todos los procesos activos.

Verificar y registrar las conexiones de redes actuales y recientes.

Registrar la fecha y hora del sistema.

Verificar la integridad de los datos.

Documentar todas las tareas y comandos efectuados durante la recolección.

Posteriormente, en lo posible, se debe realizar una recolección más detallada de los datos existentes en el almacenamiento volátil, efectuando las siguientes tareas:

Examinar y extraer los registros de eventos.

Examinar la base de datos o los módulos del núcleo del sistema operativo.

Verificar la legitimidad de los comandos del sistema operativo.

Examinar y extraer los archivos de claves del sistema operativo.

Obtener y examinar los archivos de configuración relevantes del sistema operativo.

Obtener y examinar la información contenida en la memoria RAM del sistema.

Procedimiento

En la computadora, con el equipo encendido, acceder al recurso acorde al orden de volatilidad de la información, con las herramientas forenses almacenadas en diskette o CD-ROM y de acceso de sólo lectura:

Prosise, Chris. Mandia, Kevin and Pepe, Matt. *Incident Response & Computer Forensic*. Second Edition. McGrawHill Osborne, California, 2003.

Ejecutar un intérprete de comandos legítimo.

Obtener y transferir el listado de comandos utilizados en la computadora, antes de la recolección de datos.

Registrar fecha y hora del sistema.

Recolectar, transferir a la estación forense o medio de recolección forense y documentar:

Fecha y hora del sistema

Memoria Principal

Usuarios conectados al sistema

Registro de modificación, creación y tiempos de acceso de todos los archivos

Listado de puertos abiertos y de aplicaciones escuchando en dichos puertos

Listado de las aplicaciones asociadas con los puertos abiertos

Tabla de procesos activos

Conexiones de red actuales o recientes

Recursos compartidos

Tablas de ruteo

Tabla de ARP

Registros de eventos de seguridad, del sistema, de las aplicaciones, servicios activos

Configuración de las políticas de auditoría del sistema operativo

Estadísticas del núcleo del sistema operativo

Archivos de usuarios y contraseñas del sistema operativo

Archivos de configuración relevantes del sistema operativo

Archivos temporales

Enlaces rotos

Archivos de correo electrónico

Archivos de navegación en Internet

Certificación matemática de la integridad de los datos

Listado de los comandos utilizados en la computadora, durante la recolección de datos.

Recolectar la topología de la red

Si es factible, apagar el equipo.

A continuación se describen algunas herramientas de software **para la recolección en vivo:**

En Sistemas operativos Linux/Unix Memoria RAM

Strings

nc (netcat). Este comando permite leer y escribir datos a través de conexiones de red por medio del protocolo tcp/ip. Para recolectar datos con este comando se necesita tener un sistema de archivo con espacio libre suficiente para almacenar la información capturada. Para el perito informático forense esta herramienta le permite transferir información relevante para luego confirmar o no la ocurrencia de un incidente, se puede ingresar y salir rápidamente del sistema dubitado y se puede realizar un análisis de la información recolectada en el laboratorio.

Memoria de video

xwd. La captura de una pantalla se puede realizar no sólo a través de una fotografía sino también, por medio de un comando que permite descargar la pantalla activa o completa de un entorno X Windows (X Windows System es estándar de ventanas del MIT, Instituto Tecnológico de Massachusetts, que permite mostrar las ventanas de los procesos que se ejecutan en un sistema de red en el sitio que sea más conveniente para el usuario.

Procesos activos

uptime. Muestra cuánto tiempo lleva activo el sistema operativo.

/proc. En el seudo sistema de archivos /proc, se encuentra un directorio para cada proceso activo, identificado por su PID o identificador de proceso.

ps. Este comando muestra los procesos actuales en el sistema, su estado y contexto asociado.

whereis. Muestra la ubicación del archivo ejecutable dentro del sistema de archivos del sistema operativo.

fuser

Identifica los procesos que utilizan determinados archivos o sockets

Strace. Traza las llamadas al sistema operativo que efectúan los procesos en ejecución o activos.

Ltrace. Muestra las librerías utilizadas por los procesos activos en el sistema.

Ldd. Muestra las dependencias de las librerías compartidas que utiliza un programa o librería compartida.

Lsof. Muestra todos los archivos actuales abiertos relacionados con los procesos activos y que generaron la apertura de los mismos.

#lsof –i. Muestra sólo los procesos que han abierto sockets en la red, o en Internet.

#lsof –D r. En un incidente en tiempo real, permite efectuar el menor número de modificaciones en el sistema, -D, utiliza el archivo de cache, con la función r, de lectura del archivo de cache.

Who. Muestra los usuarios conectados al sistema, con –a, presenta todas las opciones del comando.

W. Muestra quiénes están en el sistema y qué están ejecutando.

Verificación de las conexiones de red

netstat

Este comando muestra las conexiones de red, tablas de ruteo, estadísticas de las interfaces de red, conexiones enmascaradas y multidifusión. El estado de la red muestra información relevante acerca de las conexiones actuales y de los procesos o aplicaciones que se encuentran escuchando en el sistema. Un intruso puede dejar programas ejecutándose o conexiones abiertas que el perito informático forense debe verificar. Este comando brinda información detallada del protocolo, del estado de la conexión, de la dirección remota, de la dirección local, número de bytes no copiados, número de bytes sin acuse de recibo, información sobre los servicios de X Windows. Las conexiones del tipo HTTP tienen un corto período de duración. La opción –n, muestra la dirección ip, en vez del nombre de la conexión establecida y con la opción –r, se muestra la tabla de ruteo almacenadas en el núcleo. En el directorio /proc/net, se encuentran los archivos de tabla de ruteo, interfaces, paquetes, tcp, ip, unix, entre otros, que deben consultarse o descargar la información para un análisis posterior. La visualización de estos archivos se puede efectuar con los comandos cat, vi, more o reenviarla a un archivo de texto.

#netstat –p, la opción –p, indica el PID, identificador del proceso y nombre del programa al que cada socket (dirección ip + puerto) pertenece.

arp

Este comando muestra la asociación de la dirección física de la placa de red (MAC, Media Access Control, Control de Acceso al Medio), que puede ser modificada por el intruso.

#arp –v, en Linux.

#arp –a, en FreeBSD

netcat

En los casos en que se esté efectuando un ataque o una intrusión en el sistema, será necesario capturar la mayor cantidad de información en el menor tiempo posible, dado que se encuentra en un almacenamiento volátil, previendo que el intruso pueda borrar sus huellas o se pierda la información al apagar la computadora. Una forma rápida es utilizando el comando nc.

Primero se debe crear un puerto de escucha en la computadora donde se efectuará la recolección de los datos:

#nc –l –p 10003 > estadodelared.txt

y a continuación a través de una sola línea de comando colectar toda la información:

#(date; netstat –p; netstat –rn; arp –v) | nc 10.1.1.1 10003 –w3

Registros del sistema

lastlog, muestra el último archivo de registro de la última sesión iniciada en el sistema, el archivo se almacena en el directorio /var/log/lastlog.

Los registros del sistema responden al archivo de configuración de /etc/syslog.conf, que es conveniente examinar para determinar la ubicación de los registros.

Los registros de tipo ASCII pueden ser de Web, /var/log/httpd/access_log. Xferlog, de la aplicación FTP y de archivos del Historial.

El archivo de mensajes de /var/log/messages, se puede obtener ejecutando la siguiente línea desde la computadora de la víctima y enviando los datos en una transferencia encriptada:

dd if=/var/log/messages | des –e –c –k password | nc -w 3

10.1.1.1 3333

Y en la estación forense, ejecutar:

nc –l –p 3333 | des –d –c –k password | dd of=messages md5sum messages

Otros archivos a examinar son los ubicados en:

/etc/passwd, para buscar cuentas de usuarios no autorizados o nivel de acceso

/etc/shadow, para verificar que las cuentas requieren autenticación por contraseña

/etc/groups, verificar los privilegios de los grupos

/etc/hosts, examinar las entradas de nombres de dominio (DNS)

/etc/rc, para verificar los archivos de inicio crontab, para verificar los eventos planificados

/etc/inetd.con y /etc/xinetd.conf, para examinar los servicios iniciados

Los intérpretes de comandos o shell pueden tener configurado el archivo de historia

de comandos, para que el usuario repita los comandos utilizados en sesiones anteriores. Este archivo es eliminado cuando no se desea dejar rastro de una intrusión. Para el shell sh el historial de comandos es el .sh_history, para csh .history, para ksh .sh_history, para bash .bash_history, para tcsh.history.

En sistemas operativos Microsoft Windows

Para recolectar información volátil en el sistema operativo Windows desde la línea de comandos, se debe ejecutar el comando cmd.exe, previamente verificado y desde el conjunto de herramientas preparado por el perito informático forense, con el fin de evitar que la ejecución de cualquier comando en el sistema operativo de la computadora dubitada (\WINNT\System32\cmd.exe), posea comandos falsificados por el intruso o por el delincuente. Por ejemplo, si el comando ha sido modificado, en vez de abrir una consola de DOS, ejecuta el borrado de todo el disco (del *.*) o le da formato rápido al disco, no permitiendo el uso del comando unformat (echo s | format c: /q /u).

Certificación matemática de los archivos

MD5Sum, Efectuar la certificación matemática de todas las herramientas de recolección de la evidencia en el dispositivo forense y almacenar todas las certificaciones en un archivo de texto.

A:\>md5sum md5sum.exe > certificaciones.txt A:\>md5sum cmd.exe >> certificaciones.txt A:\>md5sum nc.exe >> certificaciones.txt A:\>type certificaciones.txt

f6f875a036f500370e485b1ea965377f A:\temp\win32forensic\md5deep.exe
f9a0eef6e9b67d91284032df81a68c1c A:\temp\win32forensic\cmd.exe
e0fb946c00b140693e3cf5de258c22a1 A:\temp\win32forensic\nc.exe

Envío de la evidencia a través de una conexión remota

En las situaciones que se deban enviar los archivos de recolección de la evidencia a una conexión remota, se pueden utilizar los siguientes comandos:

cryptcat, para encriptar canales de comunicación. **cryptcat.sourceforge.net nc (netcat .exe)**

Por ejemplo para activar netcat en la estación forense y redireccionar los datos a un archivo, se debe ejecutar:

a:\>nc –l –p 3333 > pslist a:\>pslist | nc 10.1.1.1 3333

Ejecución de un intérprete de comandos legítimo

cmd.exe, línea de comando del sistema operativo

Registro de la fecha y hora

Los comandos "date" y "time", forman parte del comando "cmd.exe". Con la opción "/t", la salida del comando muestra solamente la fecha y hora actual, y no muestra la opción para ingresar nueva fecha u hora. Por lo tanto para registrar la fecha y hora del sistema y enviar el resultado a un archivo de texto, se debe ejecutar:

A:\>cmd.exe

A:\>date > fecha.txt, presionar enter, para no modificar la fecha.

A:\>time >> fecha.txt, presionar enter para no modificar la hora, se concatena la salida del comando time al archivo fecha.txt, agregando la hora a continuación de la fecha.

Para visualizar los resultados, ejecutar el comando type: A:\>type fecha.txt

La fecha actual es: 07/11/2004

Ingresar la nueva fecha: (dd-mm-yy) La hora actual es: 12:03:41,39 Ingresar la nueva hora:

A:\>

Descarga de la memoria RAM

En este sistema operativo es un tanto difícil obtener el contenido de la memoria RAM. Existen dos tipos de memoria que el perito informático forense puede obtener:

Memoria del modo usuario (aplicación) con la herramienta:

userdump.exe, que forma parte del paquete de herramientas de soporte de Microsoft OEM, http://download.microsoft.com/download/win2000srv/Utility/3.0/NT45/EN-US/ Oem3sr2.zip .

Memoria completa del sistema, con la herramienta de George Garner, que es una modificación de la versión de la utilidad GNU, dd.

Dd.exe, www.gmgsystemsinc.com/fau/.

Verificación de los usuarios conectados al sistema y de los usuarios con acceso remoto

Las aplicaciones de terceros que se ejecutan en el sistema operativo Windows suelen utilizar servicios de acceso remoto que pueden ser un punto de acceso para los intrusos. Algunos de estos servicios son:

Servidor de Terminal.

SQL/Oracle.

Servicios de telnet de terceros para Windows NT.

Servidor de Telnet de Windows 2000.

Servicios FTP de terceros.

Servidores de Web (Apache o IIS, Internet Information Server).

VNC (Virtual Network Computing, Computación de Redes Virtuales, Puerto TCP 5800) y PC Anywhere (Puerto TCP 563).

Acceso de servicios remoto (PPP y PPTP).

Servidores X.

Se deben identificar los puntos de accesos al sistema operativo para determinar la

forma en que se obtuvo el mismo. Los comandos netsat y fport utilizan llamadas del tipo API (Application Program Interface,[Interfaz de Programación de la Aplicación], para leer el contenido del núcleo y las tablas de conexión de TCP y UDP. Los servicios de discado para el acceso a Windows más comunes son PC Anywhere, RAS (Remote Access Server [Servidor de Acceso Remoto]) y otras herramientas de acceso telefónico a redes. Las aplicaciones que permiten control remoto, como PC Anywhere o AT & T VNC, toman control total en el sistema al que se accedió en forma remota, a través de un solo usuario, manejando el teclado, el mouse y la pantalla, por medio de netstat, Fport y PsList se pueden determinar los puertos abiertos para estas aplicaciones (563, 5800). Las aplicaciones como el Servidor de Acceso Remoto de Windows (RAS) permite el acceso remoto de múltiples usuarios (256) en forma simultánea a través del acceso telefónico.

Usrmgr, herramienta del sistema operativo. En el Administrador de Usuarios se deben buscar las cuentas de usuarios no autorizadas.

Usrstat, herramienta del Kit de Recursos de Windows x, permite ver las cuentas del controlador de dominio, buscando entradas sospechosas.

Eventvwr, herramienta del sistema operativo Windows para visualizar los sucesos ocurridos en el sistema. Visualizar el registro de seguridad, filtrando los eventos ID 624 (Agregar cuentas de usuarios), ID 626 (Habilitar la cuenta de un usuario), ID 636 (Cambiar una cuenta de grupo), ID 642 (la cuenta de un usuario cambió).

Se debe verificar el directorio \%SystemRoot%\Perfiles\ para comprobar la existencia de la cuenta del usuario, si no aparece el usuario, significa que la cuenta de ese usuario no ha sido utilizada todavía para iniciar sesión. Si la cuenta existe en el directorio de \%SystemRoot%\ Perfiles\, pero la cuenta no aparece en el Administrador de Usuario o en la clave del Registro

\HKEY_LOCAL_MACHINE\SAM\Domains\Account\Users\Names, significa que el usuario existió en algún momento en el sistema, pero que actualmente ya no existe.

Cuando una cuenta de usuario es eliminada, la entrada de directorio del perfil del usuario correspondiente no es eliminada y el respectivo SID (Identificador de Seguridad) permanecerá en la base de datos del Registro (HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\ProfileList). Esto permite verificar y rastrear las cuentas de usuario eliminadas.

Psloggedon, muestra los usuarios conectados al sistema, ya sean locales o remotos.

Si el sistema operativo ofrece conexión remota a través de la línea telefónica, se debe determinar cuáles son los usuarios con este tipo de acceso permitido, si no existe ningún usuario con este privilegio, se puede determinar que el módem es para conexiones salientes, y aparentemente no se utiliza para el servicio de acceso remoto. Si existen usuarios con privilegio de acceso remoto, se debe evaluar si se desconecta la línea telefónica o no, en el caso de que se esté respondiendo a un incidente.

Tokenmon: Herramienta de monitoreo que muestra los inicios y cierre de sesión, los privilegios utilizados y apócrifos. **technet.microsoft.com/en-us/sysinternals/bb842062.aspx.**

Rasusers.exe*:* Herramienta del Kit de Recursos de Windows NT que lista todas las cuentas de los usuarios en un dominio o servidor que tiene permisos de acceso telefónico a redes por medio del Servidor de Acceso Remoto.

Verificación de las fechas y hora de acceso, creación o modificación de todos los archivos

Esta tarea es una de las más importantes y críticas cuando se responde a un incidente. Si se puede determinar el momento aproximado de la ocurrencia del incidente, la fecha y hora comprobarían los archivos que fueron modificados por el intruso, instalados, descargados y ejecutados. Para identificar a los usuarios que han instalado programas no autorizados en una computadora se puede utilizar un rastreador de la red y verificar los accesos a la computadora o auditar los accesos a los archivos a través de los registros de eventos del sistema operativo. Si el sistema de archivos es NTFS, se puede configurar la auditoría de Seguridad Local y monitorear los accesos exitosos a los archivos y carpetas y habilitar la auditoría de Inicio y Cierre de Sesión. El registro de evento muestra el nombre del archivo agregado y la cuenta del usuario responsable. Los identificadores de eventos que muestran el acceso exitoso o fallido a los Archivo Objetos son los siguientes:

Identificador del Evento	Descripción
560	Apertura del objeto
561	Asignación del objeto
562	Cierre del objeto

563	Apertura del objeto para borrado
564	Elimación del objeto
565	Apertura del objeto, en Windows 2000
566	Operación del objeto, en Windows 2000

En los registros de los eventos generados por la categoría Aplicación se pueden encontrar datos relacionados con ataques efectuados a los servicios que se ejecutan en el sistema y que por ser vulnerables se utilizan para introducir código malicioso.

dir, muestra el listado de todos los archivos y directorios. Con determinados modificadores es posible obtener la fecha y hora de: acceso (a), la modificación (w) y la creación (c).

A:\>dir /t:a/a/s/o:d c:\ > A:\PIF001-AZR-07Nov04-dir.txt, lista en forma recursiva las fechas de acceso de todos los archivos en el disco rígido C.

A:\>dir /t:w/a/s/o:d c:\ > A:\PIF001-AZR-07Nov04-dir.txt, lista en forma recursiva las fechas de modificación de todos los archivos en el disco rígido C.

A:\>dir /t:c/a/s/o:d c:\ > A:\PIF001-AZR-07Nov04-dir.txt, lista en forma recursiva las fechas de creación de todos los archivos en el disco rígido C.

Afind, **http://www.mcafee.com/us/downloads/free-tools/forensic-toolkit.aspx,** busca en el sistema de archivos los archivos accedidos en determinado horario.

Filemon: Herramienta de monitoreo que muestra toda la actividad del sistema de archivo en tiempo real.

Handle: Herramienta que muestra qué archivos han sido abiertos por los procesos.

Verificación de los puertos abiertos

net start, comando del sistema operativo (net) con la opción start sin argumentos para verificar todos los servicios en ejecución.

netstat, comando del sistema operativo, que enumera los puertos que están escuchando y los puertos actualmente conectados. Este comando puede mostrar

conexiones entre aplicaciones en la máquina local, localhost 127.0.0.1. Estas conexiones no son relevantes para el perito informático forense, se deben observar las direcciones IP remotas y los puertos en estado de escucha (Listening).

A:\> netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:7	0.0.0.0:0	LISTENING
TCP	0.0.0.0:9	0.0.0.0:0	LISTENING

TCP	0.0.0.0:13	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1025	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1025	127.0.0.1:1026	ESTABLISHED
TCP	127.0.0.1:3003	0.0.0.0:0	LISTENING
TCP	127.0.0.1:3007	0.0.0.0:0	LISTENING
..TCP	192.168.1.1:139	0.0.0.0:0	LISTENING
..TCP	192.168.1.1:139	192.168.1.13:1054	LISTENING
UDP	0.0.0.0:7	*:*	
UDP	0.0.0.0:9	*:*	

Verificación de las aplicaciones asociadas con los puertos abiertos

Netstat:

Los puertos están asociados a determinados procesos o aplicaciones, algunos de

estos procesos pueden estar ejecutando código malicioso (**Véase Listado – Puertos Troyanos**).

FPort. Herramienta de Foundstone, **http://www.mcafee.com/us/downloads/free-tools/ fport.aspx,** que muestra la asociación de las aplicaciones con sus respectivos puertos en donde escuchan, en los sistemas operativos Windows NT y 2000.

A:\fport

FPort v1.33 TCP/IP Process to Port Mapper Copyright 2000 by Foundstone, Inc. http://www.foundstone.com

Pid Process Port Proto Path

628 tcpsvcs -> 7 TCP C:\WINNT\System32\tcpsvcs.exe

628 tcpsvcs -> 19 TCP C:\WINNT\System32\tcpsvcs.exe

1308 inetinfo -> 21 TCP C:\WINNT\System32\inetsrv\inetinfo.exe

1308 inetinfo -> 25 TCP C:\WINNT\System32\inetsrv\inetinfo.exe

1244 wins -> 42 TCP C:\WINNT\System32\wins.exe

1292 dns -> 53 TCP C:\WINNT\System32\dns.exe

1308 inetinfo -> 80 TCP C:\WINNT\System32\inetsrv\inetinfo.exe

444 svchost -> 135 TCP C:\WINNT\system32\svchost.exe

8 System -> 139 TCP

1308 inetinfo -> 443 TCP C:\WINNT\System32\inetsrv\inetinfo.exe

8 System -> 445 TCP

1480 nsum -> 6666 TCP C:\WINNT\System32\WINDOW~1\Server\nsum.exe

840 nscm -> 7007 TCP C:\WINNT\System32\WINDOW~1\Server\nscm.exe

788 nspmon -> 7778 TCP C:\WINNT\System32\WINDOW~1\Server\nspmon.exe

1308 inetinfo -> 9365 TCP C:\WINNT\System32\inetsrv\inetinfo.exe

628 tcpsvcs -> 7 UDP C:\WINNT\System32\tcpsvcs.exe

628 tcpsvcs -> 9 UDP C:\WINNT\System32\tcpsvcs.exe

628 tcpsvcs -> 13 UDP C:\WINNT\System32\tcpsvcs.exe

Si el comando **"fport",** muestra un proceso sospechoso en estado "escuchando" y por otro lado el comando **"netstat"** muestra una conexión activa con este proceso, sería prudente terminar el proceso o matar el proceso con el fin de proteger el sistema de un potencial código malicioso y del acceso de intrusos. El comando **"kill.exe"** permite terminar un proceso. Por ejemplo, una aplicación como \WINNT\winpop.exe, puede estar escuchando en los puertos 6000 o 12346, que son los utilizados por el código malicioso, troyano, Netbus. Se puede copiar el archivo sospechoso al disco de respuesta al incidente, para analizar el programa en el laboratorio y determinar si es un código malicioso de acceso remoto, y en la máquina afectada ejecutar un programa Antivirus. **Véase Listado –Puertos Troyanos.**

PestPatrol, www.pestpatrol.com, identifica aplicaciones de código malicioso (troyanos, backdoors, keystoke loggers).

Verificación de los procesos activos

El sistema operativo Windows, dependiendo de la versión y de la configuración específica que se haya realizado, posee una serie de procesos predeterminados y de servicios los cuales se pueden verificar y comparar con los procesos y servicios que se encuentran activos o en ejecución en la computadora dubitada. Cuando se ejecuta un proceso en Windows, se crea un objeto del núcleo y un espacio de direcciones que contiene el código del proceso. El objeto del kernel es utilizado por el sistema operativo para administrar el proceso y mantener información estadística del mismo. La herramienta gráfica Administrador de Tareas (taskmgr.exe), del sistema operativo Windows, muestra los procesos activos y se pueden seleccionar una serie de columnas que brindan información detallada de cada proceso en ejecución:

Pslist, de Mark Russinovich, muestra la lista de procesos del sistema, **technet.microsoft. com/en-us/sysinternals/bb842062.aspx**

A:\>pslist

Name	Pid	Pri	Thd	Hnd	Mem	User Time	Kernel Time	Elapsed Time
Idle	0	0	1	0	20	0:00:00.000	15:19:15.579	0:00:00.000
System	4	8	60	438	216	0:00:00.000	0:01:23.860	0:00:00.000
smss	848	11	3	21	344	0:00:00.010	0:00:00.020	17:43:35.612
csrss	896	13	12	604	2556	0:00:04.766	0:00:35.901	17:43:31.616
winlogon	920	13	17	440	1080	0:00:02.563	0:00:02.934	17:43:28.662
services	964	9	16	370	3512	0:00:05.778	0:00:05.187	17:43:25.838
lsass	976	9	20	318	860	0:00:23.603	0:00:28.851	17:43:25.778
svchost	1148	8	8	357	3128	0:00:00.901	0:00:01.261	17:43:21.492
svchost	1476	8	92	1422	21860	0:00:22.942	0:00:28.350	17:43:20.740

En la lista de procesos actuales se debe verificar la presencia de los procesos y servicios nor-

males y distinguir aquellos que sean sospechosos o que no deban estar ejecutándose, como, por ejemplo, el Visor de Eventos, EVENTVWR.EXE, algún intruso podría estar revisando los registros de eventos o sucesos del sistema, o el USRMGR.EXE, donde alguien podría estar modificando las claves de las cuentas de usuarios, creando o eliminando cuentas de usuario, modificando la configuración de las políticas de auditoría.

Psinfo: Muestra la fecha de inicio del sistema, versión del kernel, procesador, memoria física, entre otros. **technet.microsoft.com/en-us/sysinternals/bb842062.aspx.**

Psinfo: Herramienta de **http://www.mcafee.com/us/downloads/free-tools/index.aspx,** que recolecta información del sistema local.

Pstat.exe, pview: Herramientas del Kit de Recursos de Windows NT que muestran los procesos actuales del sistema a nivel de detalle.

top.exe: Herramienta del Kit de Recursos de Windows NT que muestra los procesos actuales del sistema en tiempo real, refrescando la información periódicamente.

Process Explorer: Herramienta que muestra los archivos abiertos, los procesos objeto, las claves del registro las librerías dinámicas y los propietarios de los procesos.

PsService: Herramienta de **http://www.mcafee.com/us/downloads/free-tools/index.aspx,**

para mostrar información de los procesos actuales y sus procesos hijos.

At: comando del sistema operativo que permite planificar la ejecución de procesos en un determinado horario. Al ejecutarlo sin ningún otro parámetro muestra la existencia o no de trabajos o procesos planificados. Por medio de este comando los intrusos pueden planificar trabajos o procesos de código malicioso.

Kill.exe: Herramienta de Windows 2000 de soporte, para finalizar un tarea o proceso determinado.

Verificación de las conexiones actuales y recientes

nbtstat: Comando del sistema operativo, que accede al caché de nombre NetBios remoto, lista las conexiones de NetBios recientes de los últimos 10 minutos.

arp: Comando del sistema operativo que accede a la tabla ARP (Address Resolution Protocol [Protocolo de Resolución de Direcciones]) que asocia la dirección lógica IP a la dirección física MAC (Media Access Control, Control de Acceso al Medio) de la o las computadoras conectadas a la máquina local y que han establecido comunicación con ella en el último minuto.

TCPView: Una herramienta que muestra el punto final de la comunicación de todas las conexiones TCP y UDP.

Ipconfig: Comando del sistema operativo que muestra la configuración de la interfaz de la placa de red.

route print: Comando del sistema operativo que muestra las tablas de enrutamiento determinando el recorrido de los paquetes, las redes de destino, las máscaras de subred, las puertas de enlace, la dirección ip de la interfaz de la placa de red y la métrica o saltos por los que debe pasar el paquete para llegar a la red de destino.

Srvcheck.exe: Herramienta del Kit de Recursos de Windows NT que muestra los recursos compartidos locales y remotos. En Windows existe un conjunto de recursos ocultos compartidos para la administración (*administrative shares*), los cuales están disponibles automáticamente cada vez que se reinicia el sistema para su uso por parte

de usuarios remotos. Se utiliza el signo a continuación del recurso $ (IPC$, C$) para identificarlos como recursos compartidos ocultos. El IPC (Inter Process Communication) utiliza el puerto 139, por medio del cual se puede intentar conectarse a un recurso administrativo compartido como el disco rígido C$. Si el sistema de archivos es NTFS (necesario para la auditoría de acceso a determinados archivos, NTFS genera ACL o Listas de Control de Acceso para archivos y carpetas) y tiene seleccionada la opción de auditoría de eventos de Archivo y Acceso a Objetos para un determinado recurso compartido se podrán registrar los accesos de usuarios remotos, de lo contrario el sistema operativo no registrará ninguno de estos accesos. Los accesos de usuarios a través de conexiones anónimas a los recursos compartidos, generan un evento o suceso, si en el sistema se auditan los Inicio y Cierres de sesión. El identificador de evento 528, muestra los inicio de sesión con éxito. Si el inicio de sesión fue anónimo, en el detalle del evento no se observará el nombre de la estación de trabajo por la cual se conecta, esto indicaría que el intruso intentará utilizar una herramienta (DumpSec, **www.somarsoft. com**, que inspecciona las ACL o Listas de Control de Acceso de los archivos y carpetas y genera un listado de los recursos, grupos y nivel de acceso) que le permita obtener todas las cuentas de usuarios válidas, para un posterior ataque.

Revisión de los registros de eventos o sucesos del sistema operativo

Los registros de sucesos pueden brindar importante información, especialmente si ha sido activada la configuración de auditoria.

Psloglist: Herramienta de **http://www.mcafee.com/us/downloads/free-tools/index.aspx** , para descargar el contenido del registro de eventos.

auditpol: Herramienta del Kit de Recursos de Windows NT, para mostrar las configuraciones actuales de seguridad y auditoría. Si la categoría de Cambio de Política, fue activada, se visualizará el evento con el ID 612, indicando la auditoria del Cambio de Política y qué usuario la cambió:

Event Type: Success Audit Event Source: Security

Event Category: Policy Change Event ID: 612

Date: 07/11/2004

Time: 06:50:21 a.m.

User: NT AUTHORITY\SYSTEM

Computer: SERVER1 Description:

Audit Policy Change: New Policy:

Success Failure

+ + Logon/Logoff

- Object Access

- Privilege Use

+ + Account Management

+ + Policy Change

+ + System

- Detailed Tracking

- Directory Service Access

+ + Account Logon Changed By:

User Name: SERVER1$ Domain Name: CENTRO Logon ID: (0x0,0x3E7)

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/ events.asp

NTLast: De J. D. Glaser, **http://www.mcafee.com/us/downloads/free-tools/ntlast.aspx,** esta herramienta permite obtener los tiempos de inicio y cierre de sesión, si se realizó con éxito o no o en forma remota o interactiva. Si la política de Inicio y Cierre de sesión esta activada, se puede verificar el acceso de cuentas de usuarios sospechosas.

El comando se puede ejecutar con las siguientes opciones:

ntlast –f, muestra los inicio de sesión fallidos

ntlast –r, muestra los inicio de sesión exitosos realizados en forma remota ntlast –f –r, muestra los inicio de sesión fallidos realizados en forma remota **A:\>ntlast -f**

Maria SERVER1 SERVER1 Mon Oct 11 06:40:59pm 2004 Maria SERVER1

SERVER1 Sun Oct 10 04:23:43pm 2004 Maria SERVER1 SERVER1 Sun Oct 10 04:23:43pm 2004 samba SERVER1 SERVER1 Sun Sep 12 04:08:07pm 2004

End Of File -

Dumpel.exe: Herramienta del Kit de Recursos de Windows NT que descarga y genera una copia en ASCII de los registros del visor de eventos de un determinado tipo (Aplicación, Sistema, Seguridad), para su posterior análisis. Si los registros se deben descargar en forma remota, será necesario utilizar la herramienta netcat, para leer y escribir desde la red. Al ejecutar el comando dumpel.exe, se debe especificar el tipo de evento a descargar con la opción –l y el separador de campo, por ejemplo, tabulación, con la opción –t y enviarlo a un archivo de recolección de la evidencia:

A:\>dumpel –l security -t > A:\PIF001-AZR-07Nov04-eventos_seg.txt
A:\>dumpel –l application -t > A:\PIF001-AZR-07Nov04-evnetos_apl.txt
A:\>dumpel –l system -t > A:\PIF001-AZR-07Nov04-eventos_sis.txt

Si se tiene un nivel de acceso del tipo administrador, se pueden examinar y guardar en un archivo los eventos de seguridad de una computadora remota (pcremota), a través de una conexión NetBios hacia el recurso compartido (IPC$, inter process communication) ejecutando la siguiente línea de comando:

D:\>net use \\pcremota\ipc$ */user:usuarioadministrador

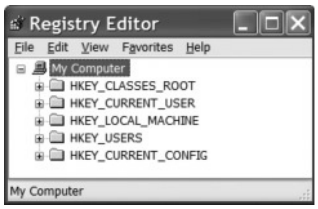
En los registros de eventos se pueden detectar accesos de intrusos o la ejecución o intento de ejecución de un código malicioso.

Verificación de la base de datos del Registro del sistema operativo

Esta base de datos brinda información relevante sobre el estado actual del sistema. El sistema operativo utiliza la base del Registro para almacenar información acerca del *hardware*, *software* instalado, perfiles de usuario y configuraciones de las propiedades de las carpetas e íconos, puertos abiertos y otros componentes del sistema operativo. Para el perito informático forense es una fuente importante de información para verificar los programas instalados, las configuraciones de seguridad, librerías de enlaces de datos del tipo código malicioso, programas que se ejecutan al arrancar la computadora, programas no autorizados como herramientas de esteganografía, desencriptadores de claves (archivos de extensión .lc, de la aplicación L0phtcrack), rastreadores de la red o programas eliminados manualmente por el usuario. El Registro no elimina los programas que fueron borrados manualmente, generalmente la

opción de desinstalación de las aplicaciones no limpia la subclave UNINSTALL del Registro.

El Registro está organizado como un árbol jerárquico de carpetas denominadas claves, que contienen subclaves, las cuales están divididas en secciones del registro (hives o colmena, por su semejanza con la estructura celular de un panal de abejas) que aparecen como archivos en el disco rígido y de valores asignados a cada elemento de la sección. Los archivos a los cuales hacen referencia, son los principales archivos del sistema operativo: SAM (Security Accounts Manager), SECURITY, SOFTWARE y SYSTEM,. la ubicación predeterminada de estos archivos en Windows NT, WINDOWS 2000, es en el directorio \WINNT\System32\Config. En Windows XP, \WINDOWS\System32\Config y al archivo PROFILES, que se encuentra en \WINNT\Profiles\All Users y contiene el perfil del usuario de cada usuario de la computadora. Estos archivos se pueden mover de una computadora a otra, pero se pueden editarse con el editor del Registro, ejecutando el comando REGEDIT.EXE. En el Registro las cinco claves se denominan:



En el modelo de seguridad de Windows se encuentran:

Los descriptores de seguridad (SD, security descriptor).

Las listas de control de acceso (ACL,Access Control Lists).

Los objetos asegurables como unidades de almacenamiento, archivos, procesos, procesos hilos, impresoras, papelera de reciclaje, entre otros, poseen un descriptor de seguridad. Este descriptor está compuesto por:

El descriptor de seguridad del objeto propietario.

El descriptor de seguridad del grupo propietario principal.

La lista de control de acceso discrecional (DACL, discretionary access list control).

La lista de control de acceso del sistema (SACL, system access control list).

El identificador de seguridad es un número de longitud variable que utiliza Windows para representar cada cuenta de usuario, grupos de usuarios, computadoras y dominios. El SID o identificador de seguridad contiene los siguientes campos:

Nivel de revisión del SID, 8 bits.

Una cuenta del número de subautoridades presentes, 8 bits.

Autoridad del identificador, hasta 3 SID de autoridad del indentificador, 48 bits.

Cualquier número de SID de subautoridad e idenrificadores relativos (RID, relative identifier) En el registro en la clave HKEY_USERS\S-1-5-21-610489928-3332149871-147929544-1008,

se encuentra la representación de un despcriptor de seguridad, donde el prefijo S y los guiones

que separan los campos aparecen para facilitar su comprensión, el sistema operativo los identifica como una secuencia numérica, el formato del SID describe la siguiente estructura:

S, se antepone al número para que sea comprensible e identifica la serie de dígitos como un SID.

1 es el nivel de revisión actual en el sistema operativo.

5 (SECURITY_NT_AUTHORITY) y 21 (indica que no es un SID interno) son autoridades de identificador internas, es el valor del identificador de la autoridad, pueden ser varios (0, SECURITY_NULL_SID_AUTHORITY – 1, SECURITY_WORLD_SID_AUTHORITY – 2, SECURITY_LOCAL_SID_AUTHORITY – 3, SECURITY_CREATOR_SID_AUTHORITY).

610489928-3332149871-147929544, incluye los valores de identificación de la subautoridad, computadora local y dominio.

1008 es el identificador relativo. Durante la instalación el sistema operativo Windows crea un SID aleatorio, basado en el número de elementos e incluyendo la fecha y hora, asegurándose de que es un identificador único. El último campo del SID es una cifra denominada 1000, es el RID o identificador relativo, el cual está unido al final del SID de la computadora para crear SID del tipo únicos para los usuarios y grupos. El sistema operativo comienza a enumerar desde 1000, que sería la primera

cuenta creada en una computadora. En este caso 1008, sería la octava cuenta creada.

Cada sistema tiene su propio identificador y cada usuario o grupo tiene su propio identificador dentro del sistema. El SID puede ser la huella digital del usuario. La siguiente es una tabla de los SID bien conocidos, obtenida de la *Guía Avanzada de Seguridad en Windows 2000*, de Jeff Schmidt, Prentice Hall, 2000).

El resguardo del Registro es otro de los lugares donde se debe buscar evidencia, se encuentran en la carpeta \WINNT\Repair o Windows\Repair, que contiene en forma comprimida los archivos del Registro y se utilizan al crear un disco de Emergencia o ERD Emergency Repair Disk, por medio del comando **rdisk /s.** En Windows 2000 o XP se realiza a través de la herramienta de Backup (INICIO|Programas|Accesorios|Herramientas del Sistema|Backup. Los archivos del Registro se pueden descomprimir con la herramienta de Windows NT, **expand.exe.**

La base de datos del Registro (%Systemroot%\System32\Config), se puede copiar a la estación forense o al medio de recolección de la evidencia, para luego analizarla en el laboratorio, sin necesidad de iniciar desde el sistema operativo nativo, ejecutando el editor del Registro e importando estos archivos por medio de la opción del menú principal del editor del Registro: Archivo| Importar. La base de datos del Registro se puede exportar a un archivo .reg, desde la opción del menú principal del editor: Archivo|Exportar. El perito informático forense debe buscar archivos de extensión .reg.

Regback o regrest: Herramientas del Kit de Recursos de Windows NT, para restaurar los archivos de resguardo y visualizarlos luego con el editor del Registro.

Regmon: Herramienta de monitoreo que muestra toda la actividad del registro en tiempo real.

Regdump: Herramienta del Kit de Recursos de Windows NT, crea un enorme archivo de texto del registro.

regquery: Herramienta del Kit de Recursos de Windows NT, que permite efectuar consultas específicas a determinadas claves del registro:

A:\> reg query “HKLM\Software**Microsoft\Windows\CurrentVersion\policies”**

Se puede generar un archivo de procesamiento secuencial o Bat (registro.bat), efectuando consultas a determinadas claves del registro (*Incident Response and Computer Forensics*, Kevin Mandia, Chris Prosise y Matt Pepe), el perito informático

forense podrá agregar todas aquellas consultas que considere pertinentes según cada caso particular.

Examinar los archivos de configuración del sistema operativo

El sistema operativo Windows es actualizado con frecuencia para resolver problemas de seguridad o para optimizar determinados componentes y cubrir fallas en el diseño y programación del *software* de base. Los conjuntos de archivos que se utilizan para actualizar el sistema por parte de Microsoft se denominan paquetes de actualización o Service Pack. Determinando la versión del paquete de actualización que posee el sistema operativo, es posible diagnosticar las vulnerabilidades y eventual delito. En la clave del Registro:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\CSDVersion En CSD Version aparece el valor del paquete o Service Pack instalado.

ListDLLs: Herramienta que lista todas las DLLs que están cargadas actualmente incluyendo su origen y muestra la línea completa del comando y sus argumentos de cada proceso en ejecución. **technet.microsoft.com/en-us/sysinternals/bb842062.aspx.**

Loaded: Número de versión y ruta completa de los módulos **cargados**.

Verificación y obtención de las claves de los usuarios del sistema

En algunos casos será necesario obtener el archivo de claves del sistema operativo (SAM, Security Account Manager) para su posterior análisis en el laboratorio. El archivo se debe obtener reiniciando desde el modo DOS y se describen las herramientas a utilizar, en la Alternativa II, Recolección de datos a partir del equipo apagado. Una vez obtenido el archivo de las cuentas y claves de usuarios, será necesario desencriptar las claves, las herramientas que se pueden utilizar son las siguientes:

pwdump, descarga la base de datos SAM.

pwdump3e, es una actualización de pwdump, **www.pestpatrol.com/zks/pestinfo/p/pwdump.asp.**

L0phtcrack, **www.l0phtcrack.com/** y John the Ripper, www.openwall.com/john/**,** para desencriptar las claves de los usuarios.

Verificación de archivos relevantes

Se deben examinar los archivos temporales, archivos de cache, los archivos de uso recientes que aparecen en el Registro, la papelera de reciclaje y conocer las extensiones de los archivos en Windows (.tmp, .doc, .txt, .jpg, .exe, .com, .bat, log, .reg, .pst, gif, mpeg) y las aplcaciones que los generan.

Herramientas

File System Investigator http://www.rossi.com/fstools/intro.html.

analyzeMFT http://www.integriography.com/, analiza la tabla maestra de archivos.

Encase, www.encase.com, visualiza una gran variedad de tipos de archivos, pero no todos.

Quickview Plus, de JASC Software**, www.avantstar.com** muestra los archivos ignorando las extensiones, que en algunos casos podrían ser falsas y no corresponder a la aplicación que aparentemente lo genera.

Descarga de los archivos temporales

La mayoría de las aplicaciones como los navegadores de Internet, los clientes de correo u otros programas del usuario final, suelen generar archivos temporales para su adecuado funcionamiento.

En Windows, estos archivos suelen tener la extensión .tmp, estos archivos se eliminan o se quitan del sistema una vez que finalizó la aplicación. Al recibir correo con mensajes adjuntos grandes, es posible que la mayoría de estos archivos se almacenen en archivos temporales. Se efectuar búsquedas de los archivos con extensión .tmp y enviarlos a un archivo para su posterior análisis. La descarga de los archivos temporales se puede hacer en las dos Alternativas, es decir con el equipo encendido y con el equipo apagado.

A:\find “” c:\windows*.tmp

A:\>find “” c:\windows*.tmp > temporales.txt A:\>type temporales.txt

--------- C:\WINDOWS\SET3.TMP

--------- C:\WINDOWS\SETA.TMP

--------- C:\WINDOWS\~GLC0000.TMP

--------- C:\WINDOWS\~GLH0000.TMP

--------- C:\WINDOWS\~GLH0001.TMP

Verificación de los enlaces a archivos rotos

En la base de datos del Registro se puede determinar cuál ha sido el *software* instalado y encontrar algún rastro de aplicaciones que fueron quitadas o desinstaladas en forma no apropiada. La verificación de estos enlaces, permite saber qué programa ha sido instalado en el sistema. Los enlaces están asociados a un acceso directo del Escritorio o del menú de Inicio con una aplicación o documento existente en el sistema. Los usuarios pueden borrar las aplicaciones, pero los enlaces siguen presentes si no son también eliminados. En el Conjunto de Recursos de Windows NT, se encuentra la aplicación chklnks.exe, para ubicar enlaces rotos.

Estos enlaces son muy importantes cuando se consideran las conexiones de red y los accesos directos. La mayoría de los usuarios para ahorrar tiempo en ejecutar la aplicación deseada, crean accesos directos en el Escritorio, por ejemplo el acceso directo al proveedor del servicio de Internet. Para visualizar los archvos .lnk, verificar el directorio raíz, la carpeta perfiles y el nombre del usuario:

\%systemroot%\Perfiles\<usuario>

Verificación de los archivos de navegación por Internet

Las aplicaciones para navegar en Internet como Netscape o Internet Explorer, generan registros de la actividad de navegación efectuada por el usuario, tales como el Historial de los sitios navegados en las semanas anteriores o en fechas recientes (depende de la configuración que haya realizado el usuario para esta característica). Además existe un espacio de caché una determinada cantidad de archivos e imágenes de las páginas navegadas recientemente.

Archivos	Netscape	Internet Explorer
Historial	\Archivos de Programas\Netscape\ Usuarios<nombre del usuario>\ netscape.hst	\Documentos y configuracion\ <Usuario>\Configuracion Local\Historial

Archivos	Netscape	Internet Explorer
Cache	\Archivos de Programas\Netscape\ Usuarios<nombre del usuario>\Cache\ fat.db, este archivo contiene un historial de navegación mucho más largo que el de netscape.hst Los usuarios suelen eliminar el archivo netscape.hst, pero generalmente desconocen la existencia de fat.db, que contiene información de navegación de larga data.	En Windows NT los archivos recientes de navegación, se almacenan en \WINNT\Archivos Temporales de Internet En Windows 2000 en \Documentos y Configuración\<Usuario>\ Configuracion Local\Archivos Temporales de Internet\ El archivo index.dat que asocia las páginas navegadas a la fecha actual, hora actual y URLs (Universal Research Locator), se ubica en \Documentos y Configuración\<Usuario>\Datos de la Aplicacion\Microsoft\Internet Explorer\Datos del Usuario\
Archivos temporales		\Documentos y Configuración\ <Usuario>\Configuracion Local\Archivos Temporales de Internet\. El archivo index.dat contiene el visor del historial

Historial	El archivo binario index.dat contiene el historial

Los archivos fat.db, netscape.hst e index.dat son binarios y requieren un visor específico:

Visor de Internet Explorer: Permite ver la mayoría de los archivos binarios tanto del Internet Explorer como de Netscape.

Pasco: Es una herramienta de *software* libre, escrita por Keith Jones de Foundstone, http:// www.mcafee.com/us/downloads/free-tools/pasco.aspx, permite visualizar los archivos de cache del Internet Explorer.

Encase: Herramienta comercial, **www.encase.com**, automatiza la recolección de la actividad de navegación en Internet a través de diferentes secuencias de comandos.

La configuración del DUN (Dialup Networking, [discado de red]), posee la característica de discado a demanda que la mayoría de las aplicaciones intentan configurarla como predeterminada. El discado automático o discado a demanda permite que el sistema operativo Windows se conecte automáticamente cuando una aplicación requiere el uso de Internet. El sistema operativo mantiene una lista de direcciones que se conectaron a través de las características de autodiscado, para visualizar la base de datos del autodiscado, se puede utilizar el siguiente comando:

rasautou -s

Verificación y descarga de los archivos de correo electrónico

La visualización de los archivos de correo de las distintas aplicaciones (Microsoft Outlook o Outlook Express, Netscape Messenger), donde cada una poseen un formato diferente, debe efectuarse con un cliente de la misma aplicación que lo generó. Por lo tanto se deben copiar los archivos del cliente de correo, para analizarlos luego en el laboratorio con el mismo cliente de correo.

Cliente de correo Outlook Express

Ubicación de los archivos de Outlook Express

Las carpetas con la configuración predeterminada se encuentran en la siguiente ruta: C:\Documents and Settings**Cuenta de usuario**\Configuración Local\Application Data\

Identities\{A47FC4DA-5DAD-4DDF-BF25-76A8CABC0188}\Microsoft\Outlook Express



Cuenta de usuario, es el nombre del usuario al que pertenece la cuenta de correo. En la ruta anterior se encuentran los siguientes archivos a copiar:

Cuando los mensajes se guardan desde el cliente de correo con la opción de menú Archivo– Guardar como, la extensión predeterminada es .EML, por lo tanto también se deben buscar este tipo de archivos.

Cliente de correo Microsoft Outlook

Los archivos de mensajes de correo electrónico se almacenan en Windows 2000 en la carpeta:

\Documentos y Configuracion\<Cuenta de Usuario>\Configuracion Local\Datos de la Aplicacion\Microsoft\Outlook. Los archivos a copiar son los de extensión .pst (Archivos de la carpeta personal), que se almacenan localmente para cada cuenta de usuario y contienen todas las carpetas dentro del Outlook (Calendario, Elementos Eliminados, Borrador, Entrada, Enviados, Salida, Tareas), excepto la carpeta Contactos. El archivo .pst puede estar en cualquier carpeta del sistema de archivo. Para analizar el archivo .pst, se debe copiar en la ruta mencionada en la computadora forense y abrir el archivo con el cliente de correo respectivo.

Cliente de correo Netscape Messenger

Los archivos se mantienen en formato de texto plano. Se encuentran en la carpeta del perfil del usuario propietario, \Archivos de Programas\Netscape\Usuarios\<Cuenta del Usuario>\ Correo. Cada casilla de correo tiene dos archivos que la componen: un archivo index, con la extensión .snm, y un archivo de texto del mensaje, sin extensión. Cada carpeta en esta aplicación se almacena como un único archivo. La carpeta de Entrada de correos se almacena como un archivo con el nombre de la bandeja y los mensajes enviados se almacenan como Enviados o Sent. La visualización del contenido de estos archivos se puede hacer con el editor de texto WordPad del sistema operativo o con cualquier editor de texto.

Documentar los comandos utilizados durante la recolección de datos o en la respuesta al incidente

doskey /history: Este comando del sistema operativo muestra el listado de comandos ejecutados, se puede ejecutar previamente para determinar los comandos ejecutados en la consola del sistema dubitado y luego para documentar los comandos ejecutados durante la recolección de la evidencia.

Generación de un script o secuencia de comandos

Al recolectar la información de la computadora dubitada se puede efectuar un programa del tipo ejecutable .bat, para automatizar la obtención de la evidencia, enviando los resultados al dispositivo preparado para la recolección de la evidencia o, si es necesario, enviarla en forma encriptada por la red. La secuencia de comandos se puede crear en un archivo de texto y almacenarla como .bat.

Ejemplo, comandos.bat:

doskey /history

time /t

date /t

psloggedon

dir /t:a/a/s/o:d c:\ > A:\PIF001-AZR-07Nov04-dir.txt

dir /t:w/a/s/o:d c:\ > A:\PIF001-AZR-07Nov04-dir.txt

dir /t:c/a/s/o:d c:\ > A:\PIF001-AZR-07Nov04-dir.txt

netstat –an

fport

pslist

nbtstat –c

time /t

date /t

doskey /history

Para redireccionar la salida de la secuencia de comandos a un socket del comando netcat, se debe usar la siguiente línea de comando:

nc.exe –L –p 2222 >>comandos.txt, la opción –L, significa que el socket de netcat no se debe cerrar sin no interviene el usuario (CTRL-C).

Respuesta a incidentes

Detección de intrusos

El uso de las redes de información trae aparejado un conjunto de amenazas y riesgos relacionados con el accionar del ser humano y su inevitable tendencia a dañar lo ajeno. Las razones para este tipo de conducta pueden ser diversas, pero lo más importante para el dueño de la información y para el mantenimiento de su privacidad es protegerse. Por lo tanto existen diversos mecanismos para detectar el acceso de intrusos a la red, ya sean locales o externos. Las intrusiones generalmente aprovechan las vulnerabilidades propias de los sistemas operativos y aplicaciones provocando la explosión de esa vulnerabilidad y a partir de ella buscar, indagar, inferir y en la mayoría de los casos dañar la información existente. Para detectar el acceso de intrusos a la red de una determinada organización, se utilizan mecanismos basados en el monitoreo permanente de la información que ingresa a la red y en una política de

seguridad adecuada dentro de la empresa, **Anexo – Lista de Control de Respuesta a Incidentes**. Generalmente se puede monitorear actividades sospechosas que permitan analizar los datos y prevenir un incidente de seguridad y generar la correspondiente alerta, a saber:

Consumo de recursos de forma inusual y conducta anormal de los procesos del sistema

Pérdida de procesos.

Incremento de procesos.

Procesos que tienen asociado una identidad de usuario no común, por ejemplo el ID de usuario pertenece a un usuario que no pertenece a la organización.

Presencia de código malicioso, como virus, gusanos y aplicaciones del tipo caballo de Troya.

Presencia de programas del tipo espía, que transmite información a un tercero sin la debida autorización del usuario o víctima.

Los archivos de registros del sistema deberían ser verificados en búsqueda de conexiones remotas o de actividad inusual o no autorizada. Los sistemas operativos como Windows NT, 2000, XP, Linux, Unix, permiten registrar este tipo de actividad y analizar posteriormente los registros y generar alarmas en caso de que se hallan configurado. Los datos obtenidos del la recolección de información de los registros puede brindar la siguiente información:

Los nombres de los procesos y su hora de inicio.

El estado de los procesos, duración, recursos consumidos, identificador, usuario.

Cantidad de recursos consumidos por cada proceso como CPU, memoria, disco.

Procesos del usuario y del sistema y los servicios que se ejecutan en un determinado momento.

El método por el cual un proceso es iniciado normalmente, por ejemplo, lo inicia el administrador, un usuario autorizado, otros programas y qué privilegios han sido asignados a dicho proceso.

Los dispositivos de *hardware* utilizados por un proceso determinado.

Los archivos abiertos y en uso por un proceso determinado.

Al revisar el sistema operativo y los registros de la red, se deberá buscar la siguiente información:

Procesos que se encuentren consumiendo una excesiva cantidad de recursos: memoria, disco, microprocesador.

Procesos iniciados en horarios inusuales o inesperados.

Procesos inusuales que no son los que se ejecutan normalmente en el sistema operativo o en el sistema en general, como, por ejemplo: rastreo de la red o sniffing, ruptura de claves, etc.

Procesos que finalizan inesperada y abruptamente.

Cuentas de usuarios previamente inactivas y que se encuentran iniciando procesos y consumiendo recursos de la red.

Procesos inesperados o previamente deshabilitados y que pueden indicar que un intruso instaló su propia versión de un comando o servicio, como una herramienta del tipo rootkit.

Una estación de trabajo o computadora que comienza a presentar una conducta anormal de entrada y salida.

Múltiples procesos con nombres similares. Por ejemplo, cuando existe un virus ejecuta, Explorer.exe, utilizando la letra mayúscula para enmascarar el proceso actual del sistema operativo que lo denomina explorer.exe.

Un número elevado e inusual de procesos.

Alternativa II, con el equipo apagado

En el caso que el perito informático forense efectúe la recolección de la evidencia a partir del equipo apagado, deberá previamente asegurarse de que el dispositivo de inicio del equipo no se realice a través del disco rígido o dispositivo de almacenamiento secundario dubitado. Deberá utilizar dispositivos de arranque en el modo sólo lectura, con herramientas informáticas forenses para realizar la detección, recolección y registro de indicios probatorios. Las herramientas comprobadas en el

laboratorio podrán estar en un diskette, CD-ROM / DVD, zip o en cualquier otro dispositivo considerado confiable de inicio del sistema.

Procedimiento

Procedimiento en la computadora, con el equipo apagado:

Apagar el equipo desconectando el cable de alimentación eléctrica.

Retirar diskettes, Pen Drive, Zip.

Descargar la propia electricidad estática, tocando alguna parte metálica y abrir el gabinete.

Desconectar la interfaz o manguera de datos, puede ser IDE o SCSI.

Desconectar la alimentación eléctrica del dispositivo de disco rígido.

Ingresar al CMOS (Complementary Metal Oxide Semiconductor) o Configuración del BIOS (Sistema de entrada y salida de la computadora):

Encender la computadora.

Oprimir el conjunto de teclas que se muestra en el monitor cuando se inicia la computadora para acceder al CMOS.

Verificar la fecha y hora del CMOS y registrarla en el formulario de recolección de evidencia y documentar todo tipo de dato que el perito informático forense considere relevante y documentarlo con fotografía, filmadora o en la lista de control.

Modificar la unidad de inicio o arranque del sistema operativo, es decir seleccionar la unidad de diskette, CD-ROM/DVD o zip de sólo lectura con las herramientas informáticas forenses.

Guardar los cambios al salir.

Colocar la unidad de arranque, diskette, CD-ROM/DVD o zip en el dispositivo de *hardware*

pertinente.

Verificar el inicio desde la unidad seleccionada.

Apagar el equipo.

Acorde a la decisión del perito informático forense o a lo solicitado en la requisitoria pericial, se podrá realizar el Procedimiento de duplicación y autenticación de la prueba, explicado anteriormente o continuar con la lectura del dispositivo original, configurando el mismo con los jumpers que el fabricante indique como sólo lectura o colocando un dispositivo de *hardware* de bloqueo de escritura.

Conectar el cable plano al disco rígido, puede ser IDE o SCSI.

Conectar la alimentación eléctrica del dispositivo de disco rígido.

Encender la computadora iniciando desde la unidad de arranque configurada en el CMOS.

Colocar el dispositivo de almacenamiento forense.

Efectuar la certificación matemática del dispositivo dubitado.

Guardar el resultado en un dispositivo de almacenamiento forense.

Registrar el resultado en el formulario de recolección de la evidencia.

Por medio del conjunto de herramientas informático forense, obtener la siguiente información del disco dubitado, documentarla y almacenarla en dispositivos de almacenamiento forense, para su posterior análisis, ya sea en el lugar del hecho o en el laboratorio:

Tipo de sistema operativo.

Fecha, hora y zona horaria del sistema operativo.

Versión del sistema operativo.

Número de particiones.

Tipo de particiones.

) Esquema de la tabla de particiones.

Listado de todos los nombre de archivos, fecha y hora.

Registro del espacio descuidado o desperdiciado.

Incluido el MBR.

Incluida la tabla de particiones.

Incluida la partición de inicio del sistema y los archivos de comandos.

Registro del espacio no asignado.

Registro del espacio de intercambio.

Recuperación de archivos eliminados.

Búsqueda de archivos ocultos con las palabras claves en el:

espacio desperdiciado.

espacio no asignado.

espacio de intercambio.

MBR y tabla de particiones.

Listado de todas las aplicaciones existentes en el sistema.

Búsqueda de programas ejecutables sospechosos.

Identificación de extensiones de archivos sospechosas.

Listado de todos los archivos protegidos con claves.

Listado del contenido de los archivos de cada usuario en el directorio raíz y si existen, en los subdirectorios.

Verificación del comportamiento del sistema operativo:

Integridad de los comandos.

Integridad de los módulos.

Captura de pantallas.

Generar la autenticación matemática de los datos a través del algoritmo de *hash* al

finalizar la detección, recolección y registro.

Conservar las copias del *software* utilizado.

Apagar o dejar funcionando el equipo, esto dependerá de la requisitoria pericial.

Análisis e interpretación de los indicios probatorios. Reconstrucción y / o simulación del incidente

El análisis de los indicios probatorios, acorde a la requisitoria pericial, podrá efectuarse en el lugar del hecho o en el laboratorio sobre el dispositivo duplicado. En esta etapa el perito informático forense debe comprender una serie de contenidos conceptuales que le permitan efectuar un análisis de la información adecuado y pertinente para comprobar o no la concurrencia de un delito.

Procedimiento para el análisis e interpretación de los indicios probatorios Procedimiento

En el laboratorio o en el lugar del hecho, el perito informático forense efectuará el análisis de la evidencia recolectada, preferentemente en la copia del dispositivo dubitado y la interpretación de los datos obtenidos.

En el caso de que se haya recolectado información en tiempo real de los dispositivos de almacenamiento volátil, se deberá proceder al análisis de los mismos, ya sea a través de la información digitalizada en la computadora forense portátil o en dispositivos de almacenamiento secundario del perito.

Capturar todas las pantallas pertinentes.

Imprimir la información relevante de la recolección de los datos, para incluirla en el informe pericial.

Analizar la fecha y hora del sistema en el momento de la recolección.

Analizar la información obtenida de:

Registros y Caché.

Tablas de ruteo, determinar las direcciones lógicas o ip de las computadoras vecinas, las rutas por defecto, direcciones de difusión y multidifusión, las clases a las

que pertenecen las direcciones ip de la tabla, determinando si son públicas o privadas.

Tabla de ARP, determinar las direcciones físicas o MAC (Medium Control Access) de las placas de red de las computadoras que en el momento de la recolección estaban asociadas al equipo dubitado.

Tabla de procesos activos, determinar los programas activos en RAM y el consumo de recursos de memoria y microprocesador en el momento de la captura, así como también el nombre de los programas.

Estadísticas del núcleo del sistema operativo, verificar el nivel de uso de los recursos de memoria RAM, procesador, Memoria caché, fallos de página.

Memoria Principal, verificar el contenido, buscando información por medio de palabras claves.

Archivos temporales, determinar los archivos temporales existentes en el sistema. viii.Registros de eventos de seguridad, del sistema, de las aplicaciones y servicios acti-

vos. Verificar todos los eventos, clasificándolos acorde a su nivel de criticidad.

Recursos compartidos, determinar el tipo de recurso compartido y el nivel de acceso permitido o restringido.

Usuarios conectados al sistema, listar los usuarios conectados, verificando su nivel de acceso a los recursos compartidos.

Conexiones de red actuales, verificar los tipos de conexiones actuales y los usuarios asociados con el uso de la conexión y con el tipo de recurso accedido.

Listado de puertos abiertos y de aplicaciones escuchando en dichos puertos, inicio de la conexión, duración de la conexión.

Comparar los resultados de los comandos que indican las conexiones de red actuales con los comandos que listan los puertos abiertos, verificando si el número de puerto pertenece a los relacionados con código malicioso.

Registro de modificación, creación y tiempos de acceso de todos los archivos. Verificar estos datos en las aplicaciones en ejecución o procesos activos en el momento de la recolección.

Comprobar la certificación matemática de la integridad de los datos luego del

análisis de la información.

Recolectar la topología de la red, graficar la distribución de los equipos y los accesos desde la red interna, DMZ o externa.

En la copia de la evidencia, realizar las siguientes acciones:

Efectuar autenticación matemática en cada uno de los datos analizados a través del algoritmo de *hash*.

Efectuar capturas de pantalla, según se requiera, de cada una de las evidencias halladas y documentarlas para luego incluirlas en el informe pericial.

Generar un listado de palabras claves para la búsqueda de datos sospechosos en los distintos sectores o clusters del dispositivo de almacenamiento.

Verificar el sistema operativo y determinar posibles deficiencias.

Verificar la versión del sistema operativo.

Verificar el tipo de sistemas de archivos.

Documentar, o capturar la pantalla del esquema de particiones.

Analizar el listado de todos los archivos encontrados en el sistema.

Registrar las diferencias.

Capturar pantallas.

Imprimir los datos obtenidos para la posterior fundamentación en el informe pericial.

Examinar el sector del Master Boot Record en busca de archivos ocultos o perdidos, utilizar palabras claves y en caso de aparecer datos ocultos, verificar la fecha y hora de su creación. Efectuar búsquedas con palabras claves. Esta tarea efectuarla también para:

La tabla de particiones, el espacio sin asignar, el espacio desperdiciado o slack, el espacio de intercambio.

La partición de inicio y archivos de comandos de arranque.

Examinar los archivos de intercambio o swap, analizar el contenido visualizando la información con herramientas específicas y efectuar búsquedas con palabras claves.

Restaurar todos los archivos eliminados. En lo posible anteponerles un caracter único para su identificación. Capturar la pantalla del listado de los archivos eliminados, para agregarla al informe pericial.

Analizar las aplicaciones existentes.

Examinar las extensiones de los archivos y verificar que exista coherencia con las aplicaciones que los ejecutan o generan, para determinar o no la presencia de código malicioso.

Examinar archivos en busca de datos ocultos (esteganografía) ya sean de tipo gráficos, imágenes, de texto, comprimidos o de cualquier otro tipo de extensión, para determinar ocultamiento de información comprometedora o código malicioso.

Examinar los archivos protegidos con claves, descifrando la clave previamente.

Examinar el contenido de los archivos de cada usuario en el directorio raíz y en los subdirectorios.

Examinar los programas ejecutables que sean sospechosos (relacionados con técnicas de escucha telefónica, captura de teclas por medio de *hardware* o intercepción radial, captura de imágenes en forma remota, de escucha de celulares o pagers, de identificación oraciones o frases en binario de idiomas extranjeros, falsificación de tarjetas magnéticas archivos con extensión .vba, escritos en Visual Basic).

Verificar la funcionalidad del sistema operativo y de las aplicaciones, determinando la posible emulación de comandos propios del sistema operativo realizado a través de la ejecución de código maliciosa, se deberá comprobar la

Integridad de los comandos, comparando con el comando original y a través del *hash*.

Integridad de los módulos del núcleo, comparando con los módulos originales y a través del *hash*.

Efectuar la certificación matemática de la integridad de los datos del dispositivo.

Documentar todas las aplicaciones y comandos utilizados en el análisis de la

evidencia.

Verificar las tareas realizadas con la lista de control de análisis de disco.

A continuación se expondrán diversas situaciones, aspectos conceptuales y descripción y uso de herramientas de *software* que el perito informático forense deberá considerar en el momento de efectuar el análisis e interpretación de la información recolectada en la etapa anterior:

Elementos a examinar en el disco duro: (Anexo Lista de control de Análisis de discos)

Número y tipo de particiones.

Tamaño de las particiones, verificando que la suma total de las particiones está relacionada con el tamaño del disco. Algunos fabricantes redondean los valores en potencias de 10 (4000 Kb) en vez de hacerlo en potencia de 2 (4096 Kb), por lo tanto queda un espacio de 96 Kb con información a verificar y que podría no ser utilizado en una partición. La tabla de particiones no es una gran porción de datos, aun si comparte una pista con algún código de inicio, no llega a ocupar toda una pista. Este espacio podría ser utilizado para ocultar información, en donde ni el sistema operativo ni los programas pueden acceder. La herramienta *fdisk* tampoco puede ver la pista utilizada por la tabla de partición, sin embargo un editor de disco podría hacerlo. El programa de análisis informático forense como Autopsy, Winhex, Encase, pueden identificar los datos en el área de partición como desperdicio de la partición.

Contenido de los espacios no asignados: estos espacios pueden contener cualquier dato que se haya escrito en el disco.

Archivos temporales, la mayoría de las aplicaciones como los navegadores de Internet, los clientes de correo u otros programas del usuario final, suelen generar archivos temporales para su adecuado funcionamiento. En Windows, estos archivos suelen tener la extensión

.tmp, estos archivos se eliminan o se quitan del sistema una vez que finalizó la aplicación. Al recibir correo con mensajes adjuntos grandes, es posible que la mayoría de estos archivos se almacenen en archivos temporales. Se deben revisar los archivos con extensión .tmp.

Memoria virtual, en este espacio se escriben datos cuando el tamaño de la memoria

RAM no es suficiente, efectuando un intercambio de datos según se requiera durante la ejecución de los procesos, generalmente es el doble del tamaño de la memoria RAM.

Acorde a lo expresado en el libro de *Sistemas Operativos Una visión Aplicada*, de Carretero Pérez, F. García, P. de Miguel, F. Pérez,[6] el mecanismo de memoria virtual sería el siguiente:

El procesador utiliza y genera direcciones virtuales.

Parte del mapa de memoria (virtual) está en disco (swap) y parte en memoria principal.

La MMU (memory management unit) traduce las direcciones virtuales en físicas.

La MMU produce un fallo de página (trap) cuando la dirección no está en memoria principal.

El SO trata el fallo de página, haciendo un transvase entre la memoria principal y el swap (disco).

Este archivo de intercambio en algunos sistemas operativos como Unix o Windows, puede crecer o decrecer según sean los requerimientos. Por lo tanto el contenido almacenado en este espacio de intercambio podría ser crítico, como, por ejemplo, contener contraseñas o claves, correos electrónicos almacenados en el servidor y abiertos para leer el mensaje o eliminados. El espacio de intercambio es un archivo en Windows, un archivo o particiones en Unix o Linux, y puede ser almacenado en forma remota.

Datos ocultos, código malicioso. El contenido real de ciertos archivos puede ser diferente del tipo de archivo o extensión que se observa en una primera instancia o pueden almacenar porciones de código que se distribuyen en forma silenciosa, sin que el usuario perciba su existencia, con el fin de obtener información personal del usuario o generar un daño específico.

Cuando se efectúa el análisis de los discos duros, se necesita obtener la mayor cantidad de información posible acerca del mismo. Una opción es empezar con el programa *fdisk*, tanto en sistemas operativos Linux como en Windows. Este comando muestra la información del tipo de partición, el número de particiones, los cilindros, el inicio y fin de cada uno. El perito informático forense debe tener especial cuidado al ejecutar este comando para evitar borrar particiones accidentalmente.

Discos rígidos de computadoras portátiles

En estas computadoras se utilizan los mismos estándares lógicos que en las computadoras de escritorio, pero tienen conectores físicos más pequeños para las controladoras. Un aspecto muy práctico para el perito informático forense es tener un adaptador o convertidor que permita conectar el disco de la computadora portátil con la computadora personal.

Uno de estos convertidores puede ser del tipo IDE, que consta, por un lado, de un conector y alimentación eléctrica, para la conexión con la computadora personal, la cual tiene un conector para el cable plano y otro para la alimentación y, por otro lado, un solo conector, para la interfaz IDE y para la alimentación del disco de la computadora portátil.

Si se desconoce las características de la computadora portátil se puede acudir al sitio web del fabricante y verificar las especificaciones técnicas, diagramas e instrucciones particulares sobre los discos, conexión o remoción de éstos. Normalmente los discos rígidos en las computadoras portátiles tienen un acceso fácil y se encuentran en una caja metálica que se debe quitar para remover el conector del fabricante que permite ver los pins a los cuales se conectará el adaptador para la computadora personal. Se debe verificar la ubicación del pin 1 en el disco rígido de la computadora portátil, que es siempre el lado del disco rígido con la línea roja del cable plano.

En el caso de las computadoras personales la ubicación del cable plano es más fácil debido a que la interfaz IDE o SCSI se deben conectar de una sola forma. Pero en una computadora portátil si no se conecta de manera correcta se puede dañar el disco rígido. El pin 1, el lado rojo del cable plano es contrario al conector de alimentación. Una vez identificado el conector se conecta el disco de la computadora portátil como esclavo en la computadora personal, se debe verificar si tiene el jumper en master, si es así se debe colocar en esclavo, a partir de aquí se puede generar la imagen del disco.

El conector de Forensic-Computers es un tipo de conector robusto muy útil cuando se está trabajando en el lugar del hecho, **www.forensic-computers.com**. Este conector no expone los pines como en otros adaptadores, por esa razón es preferible, ya que no permiten que se curven o doblen los pines por el uso, **www.ics-iq.com**.

Aspectos a considerar de los sistemas de archivos de los sistemas operativos

El sistema operativo y los programas controladores de los dispositivos de *hardware* permiten hacer transparente a las aplicaciones de usuario el *hardware* que utilizan, es decir que la aplicación de planilla de cálculo no necesita saber si está escribiendo en un disco rígido tipo IDE o SCSI, esta función del sistema operativo como gestor de recursos se efectúa a través de una capa de abstracción del *software* de base denominada Interfaz de Programación de Aplicación (Aplication Programming Interface, API). Los sistemas operativos tienen un gestor de entrada y salida, en el caso de los dispositivos de almacenamiento este gestor maneja las operaciones de lectura y escritura, pero en ciertos sistemas operativos como Linux o Unix, se trata a todos los elementos de *hardware* como archivos. Por ejemplo, un dispositivo como el disco rígido se puede tratar como un único archivo. Esto puede ser de gran utilidad cuando se crea una imagen del disco, además cada partición también es tratada como un archivo, de esta forma no importa el sistema operativo o la aplicación utilizada para crear y almacenar los datos en ese dispositivo. En este caso el sistema operativo trata al disco y a las particiones como un flujo de bytes.

En el sistema operativo de la línea de Windows, asigna letras para identificar a todos los dispositivos que pueden almacenar un sistema de archivos, tal como sucede con todos los discos, algunas de esas letras pueden representar no sólo a un disco rígido, sino también sus particiones, creando la confusión acerca del número real de discos rígidos existentes en una computadora. Por ejemplo, en forma predeterminada el disco rígido conectado a la primera controladora es denominado con la letra C, y es la partición de inicio de la computadora, pero esto también puede variar. Si el disco C tiene otra partición, el sistema operativo le asignará la letra D, aparentando ser otro disco duro. Se debe tener especial cuidado al analizar el disco rígido y sus unidades lógicas en el sistema operativo Windows, para evitar correlaciones incoherentes.

La **Master File Table** o **MFT – Tabla Maestra de Archivos es el lugar donde se encuentra la información de cada archivo y directorio en un volumen NTFS. La MFT es en esencia una tabla de una base de datos relacional. Los directorios son índices, más que datos. http://technet. microsoft.com/es-es/sysinternals/default.aspx**. La descripción es la siguiente:

Cada archivo en un volumen NTFS está representado por un registro en un archivo especial denominado Tabla Maestra de Archivo (MFT).

NTFS reserva los primeros 16 registros de la tabla para información especial.

El primer registro de la tabla describe a la propia tabla MFT, seguido por un registro espejado de la MFT.

Si el primer registro MFT está corrupto, NTFS lee el segundo registro para

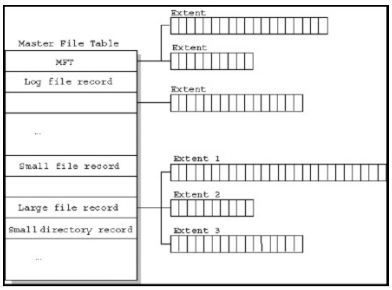
encontrar el archivo espejado de la tabla MFT, cuyo primer registro es idéntico al primer registro de la tabla MFT.

La ubicación de los segmentos de datos para ambas tablas MFT y MFT espejada se registran en el sector de inicio. Un duplicado del sector de inicio se almacena en el centro lógico del disco.

El tercer registro de la tabla MFT es un archivo de registro (log), utilizado para la recuperación del archivo.

El registro 17 y los siguientes de la tabla MFT son para cada archivo y directorio (también visto como un archivo para NTFS) del volumen.

ESTRUCTURA NTFS Master File Table (MFT) www.ntfs.com



La Tabla Maestra de Archivos (MFT) asigna una cierta cantidad de espacio para cada registro.

Los atributos de un archivo se escriben en el espacio asignado en la tabla MFT.

Los archivos o los directorios pequeños (típicamente de 1500 bytes o menos), pueden estar contenidos completamente dentro del registro de la tabla MFT.

Este diseño favorece el acceso rápido a los archivos.

En el caso del sistema de archivo FAT, utiliza una tabla de asignación de archivo para listar los nombres y direcciones de cada archivo.

Las entradas a los directorios FAT contienen un índice dentro de la tabla de asignación.

Cuando se quiere ver un archivo, la tabla FAT lee primero la tabla de asignación de archivo y se asegura de que el archivo existe.

Luego la tabla FAT devuelve el archivo buscando la cadena de asignaciones de las unidades asignadas al archivo.

En NTFS en el mismo momento que se mira un archivo se accede inmediatamente.

Los registros de los directorios se encuentran dentro de la tabla maestra de archivo de la misma forma que los registros de archivos.

En vez de datos, los directorios contienen información indexada.

Los registros de pequeños directorios residen enteramente dentro de la estructura de la tabla MFT.

Los directorios más grandes está organizados en árboles B (binarios), teniendo registros con punteros a clusters externos que contienen entradas de directorios que podrían no estar contenidos dentro de la estructura MFT.

El inodo o nodo índice es un sistema de archivos que pertenece a los sistemas operativos Unix y Linux. Se caracteriza por tener dos tablas. La tabla índice o inodo contiene punteros a los bloques de discos que constituyen el archivo actual, en el caso de que el archivo sea más grande, existirán una serie de punteros a punteros de bloques. Los nombres de los archivos se encuentran en otra tabla, que es un archivo especial denominado el directorio.

Estructura del inodo

El estándar POSIX establece un modelo de sistema de archivos que se ajusta al empleado en los UNIX tradicionales. Un archivo ordinario tendrá las propiedades siguientes:

El *identificador de dispositivo* del dispositivo que alberga al sistema de archivos.

El *número de inodo* que identifica al archivo dentro del sistema de archivos.

La *longitud* del archivo en bytes.

El *identificador de usuario* del creador o un propietario del archivo con derechos diferenciados.

El *identificador de grupo* de un grupo de usuarios con derechos diferenciados.

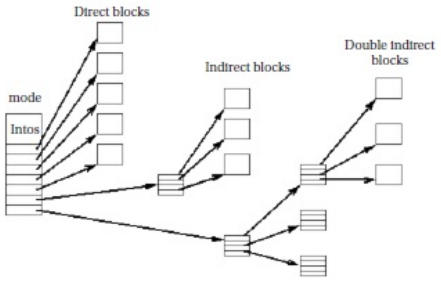
El *modo* de acceso: capacidad de leer, escribir, y ejecutar el archivo por parte del propietario, del grupo y de otros usuarios.

Las *marcas de tiempo* con las fechas de última modificación (*mtime*), acceso (atime) y de alteración del propio inodo (ctime).

El *número de enlaces*, esto es, el número de nombres (entradas de directorio) asociados con este inodo.

El número de enlaces se emplea por el sistema operativo para eliminar el archivo del sistema de ficheros, tanto el inodo como el contenido, cuando se han borrado todos los enlaces y el contador queda a cero.

Ejemplo de inodo:



Se denomina montaje de un sistema de archivo al proceso de hacer que el entorno de la computadora reconozca y detecte un sistema de archivo. El sistema operativo identifica el sistema de archivo de una determinada partición, asocia esta partición con un nombre específico o ruta y copia la tabla de archivo en la memoria RAM, de esta forma puede ser referenciada y administrada. En el caso de Unix o Linux, los sistemas de archivos se montan en forma predeterminada o están configurados para ser montados en el momento del arranque del sistema operativo, pero también pueden montarse según los requerimientos del usuario y en forma no predeterminada y desmontarse de igual forma. Por ejemplo en Unix o Linux, además de poder configurar la opción de montaje automático, el usuario podría tener no montada la disquetera y para la lectura de un disquete requiere el montaje de éste, a través de la interfaz CLI, o línea de comandos, o de la interfaz gráfica. Si es por línea de comando se ejecutaría lo siguiente:

Montar el sistema de archivo del disquete

#mount /mnt/floppy o mount /mnt/fd0, dos formas de referenciar a la disquetera.

Desmontar el sistema de archivo del disquete

#umount /mnt/floppy o umount /mnt/fd0,

También se pueden montar en forma automática o a través de la línea de comando otros sistemas de archivos, como FAT, VFAT, NTFS.

Para que cada partición pueda reconocer un determinado sistema de archivo se debe dar formato a esa partición utilizando, por ejemplo, el comando format en Windows y DOS y el comando *mkfs* en Unix o Linux. Este comando efectúa una reorganización de la partición, y si existía información, el comando *format* deja gran parte de ella en la partición. Reconstruye las tablas utilizadas para referenciar los archivos y crea una nueva lista vacía, esta lista es el índice de los bloques no asignados, pero no toca ningún contenido de un sistema de archivo. Al menos que se utilice una herramienta para borrado seguro, la eliminación de un archivo no implica que realmente se haya eliminado o borrado. Los clusters o bloques que forman el archivo están en un área donde no son visibles por los comandos de visualización de archivos del sistema operativo. En vez de estar referenciados por una entrada en el directorio o inodo, los bloques o clusters son referenciados por la lista de bloques no asignados o libres.

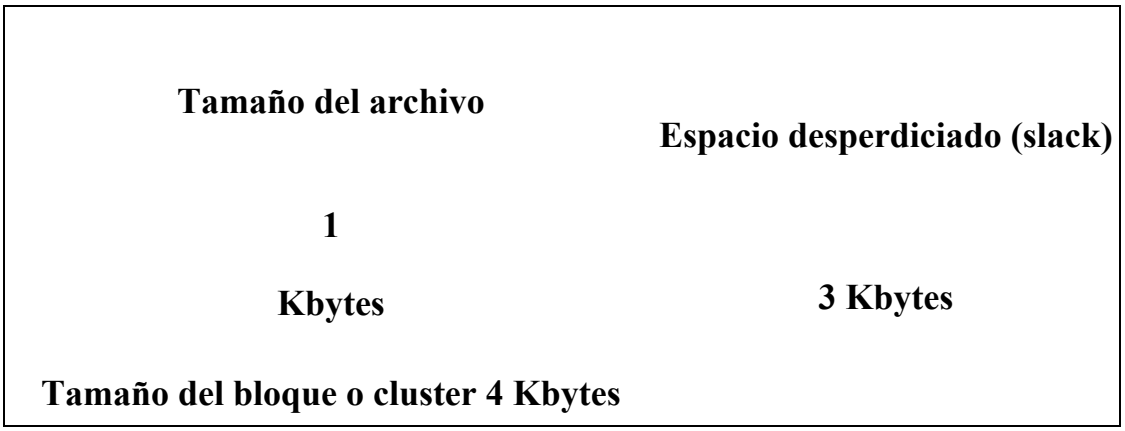
El sistema de archivo maneja los datos en unidades de medidas específicas. En Unix se denominan bloques y en Windows clusters. Estas porciones o trozos de información son las unidades mínimas de almacenamiento de información donde el sistema operativo puede ubicar información. Cada archivo está constituido por un conjunto de bloques o clusters. Los bloques o clusters no utilizados quedan a la espera de ser utilizados. Cuanto más grande sea la medida de estos bloques o clusters más, rápido se podrá mover información desde y hacia el disco. No obstante si estos bloques o clusters no se completan con datos en su totalidad, y esto ocurre frecuentemente con el último bloque o cluster de almacenamiento de un archivo, queda un espacio desperdiciado. Este espacio sobrante y no utilizado del cluster o bloque se denomina espacio desperdiciado o *slack space*. Es el espacio que se deja entre el final del dato y el final del último cluster o bloque. Cada archivo que no es par múltiplo del cluster o bloque tienen algún espacio desperdiciado asociado con el mismo.

La cantidad de espacio desperdiciado por archivo es, en promedio, un medio del tamaño del bloque, por lo tanto cuanto más grande sea el cluster, más grande es el espacio desperdiciado al final del último bloque (FAT 32 utiliza bloques de 4 Kb, 4096 bytes).

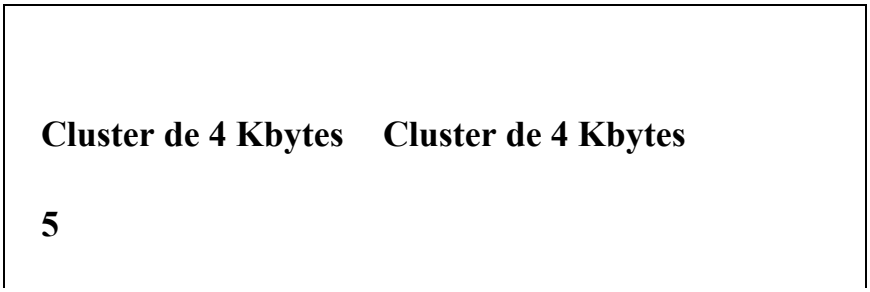
Cuando se lee un archivo a través de una aplicación del sistema operativo, no se puede acceder al espacio desperdiciado porque el sistema operativo no le deja leer el contenido que se encuentra al final del archivo. Si se lee el archivo en la memoria RAM el espacio desperdiciado no aparece junto con el archivo. Si el archivo se escribe en un dispositivo de almacenamiento removible con un tamaño de bloque diferente, el archivo resultante tendrá un espacio desperdiciado de tamaño diferente y puede contener cualquier dato que pudo estar previamente en el dispositivo. Si se envía por correo electrónico un archivo o por medio de FTP, no se incluirá el espacio desperdiciado. Una copia del disco no puede verificar estos espacios desperdiciados pero una imagen bit a bit del disco permite detectar estos espacios.

Los sistemas de archivos con bloques o clusters más pequeños tienen menor espacio sobrante o desperdiciado, pero su rendimiento es mucho menor. Los sistemas de archivos actuales tratan de compensar el rendimiento y la eficiencia dando más flexibilidad a los tamaños de bloques. A continuación se muestran dos posibles casos de espacio desperdiciado:

El tamaño del archivo es menor que el tamaño del cluster o bloque:



El tamaño del archivo es mayor que el tamaño del cluster o bloque:



Kbytes	**3 Kbytes**
	Espacio desperdiciado o slack
Total del almacenamiento: 8 Kbytes	

Niveles de almacenamiento en el sistema de archivos

Una visión del sistema de archivos para el perito informático forense, sería considerarlo como un modelo de capas, semejante al modelo de referencia OSI, Opens System Interconexion, de la ISO, International Standard Organization, para la comprensión y estudio de la comunicación en los sistemas abiertos. Acorde a lo expresado en el libro *Incident Response, Second Edition &, Computer Forensics*, de Kevin Mandia, Chris Posisse y Matt Pepe.12 Los niveles del sistema de archivos son los siguientes:

Físico.

Clasificación de datos.

Unidades de asignación.

Administración del espacio de almacenamiento.

Clasificación de la información.

Almacenamiento del nivel de aplicación.

Prosise, Chris; Mandia, Kevin y Pepe, Matt., *Incident Response & Computer Forensic*, 2° ed., McGraw-Hill Osborne, California, 2003.

Niveles de almacenamiento del sistema de archivos
Almacenamiento del nivel de aplicación
Clasificación de la información

Administración del espacio de almacenamiento

Unidades de asignación

Clasificación de la información

Físico

Estos niveles facilitan el hallazgo de evidencia y su posterior análisis, a continuación se describirá cada uno de estos niveles:

Nivel físico

Este nivel representa el dispositivo físico de almacenamiento común a cualquier sistema operativo. El dispositivo físico permitirá la lectura y escritura en bloques o sectores, los cuales se enumeran en forma secuencial, comenzando por 0 (cero) y continuando la numeración hasta finalizar el tamaño del disco. Generalmente, una o dos pistas están reservadas para el uso del propio dispositivo físico, por ejemplo, disco rígido, y es posible que se almacene una pequeña cantidad de datos en este espacio. La tecnología de *hardware* Intel ofrece una interfaz adicional que utiliza los valores de Cilindro, Cabeza y Sector (C/H/S). Para la recuperación de los datos es importante que el perito informático forense esté familiarizado con esta distribución física.

Nivel de clasificación de la información

En este nivel se encuentra el esquema de particiones configurado al instalar el sistema operativo. Las formas de distribución de las particiones dependerán de los niveles de seguridad y protección que se hayan seleccionado al instalar el *software* de base, por ejemplo, en una partición colocar solamente el sistema operativo y asignar otras particiones para los documentos, otra para los registros de eventos. Al aislar la partición del sistema operativo se favorece, por un lado, el desempeño del mismo y por otro, en el supuesto caso que se produzca un daño en la partición del sistema operativo, se pueden conservar el resto de las particiones y reinstalar el sistema operativo en su propia partición.

A cada partición, en el momento de su creación, se le asigna un identificador de partición. Es un código que le informará al sistema operativo qué tipo de sistema

operativo debe esperar para este identificador de partición, en el caso de que se realice el montaje de la partición. En algunos gestores de arranque, la táctica es marcar las particiones no deseadas con un código no válido. Por ejemplo, si el sistema operativo Windows detecta un identificador de partición no válido, ignorará completamente la partición, aun si es correctamente formateada y contiene datos válidos.

En algunos sistemas operativos del tipo Unix, como BSD, Berkeley Software Development, utilizan el término *slice* o rodaja para las particiones, son conceptos similares pero de implementación diferente. Para ser compatible con la tecnología Intel, el sistema opeartivo BSD, encapsula la tabla de particiones dentro de un esquema de partición estándar. El sistema de archivo completo para una nueva instalación del sistema operativo FreeBSD en un computadora del tipo Intel, residirá dentro de la primera partición del disco rígido. En el inicio de la partición primaria el sistema operativo BSD ubicará una tabla que subdividirá dicha partición en particiones del estilo BSD. Ejemplo:

Esquema de particiones en la tecnología Intel

Sector de Arranque	**Primera Partición FreeBSD**	**Segunda Partición 2000**	**Windows**

Tabla de Partición	**Rodaja 0**	**Rodaja 1**	**Rodaja 2**	**Rodaja 3**	**Rodaja 4**	**Rodaja 5**	**Rodaja 6**
FreeBSD	**/**	**swap**	**Disco Completo**	**/tmp**	**/usr**	**/var**	**/home**

Esquema de particiones de BSD

Cuando se efectúa el análisis forense desde un entorno Linux, se debe compilar el kernel o núcleo del sistema operativo para agregarle las opciones del esquema de partición de BSD.

Nivel de unidades de asignación

Este nivel se refiere al método de asignación de unidades o bloques utilizado por el sistema operativo. El tamaño de cada unidad de asignación depende del:

tipo de sistema de archivos

tamaño de la partición

conocimiento del administrador del sistema operativo

Cada sistema de archivo define su propio esquema de asignación en el medio de almacenamiento secundario. La mayoría utiliza un tamaño de bloque que es optimizado por el tamaño de la partición. Un esquema de asignación que utiliza de forma más eficiente el espacio y un número más pequeño de bloques grandes, equilibrando la cantidad entre bloques grandes y pequeños, optimiza las operaciones de búsqueda y transferencia.

Nivel de gestión del espacio de almacenamiento

En este nivel se administran las miles de unidades de asignación presentes en el sistema de archivo. La unidad de asignación es la porción más pequeña de datos direccionable que el sistema operativo puede manejar. El gestor de espacio de almacenamiento contiene información acerca del estado de las unidades de asignación, por ejemplo, si están libres, ocupadas, generando un mapa del dispositivo de almacenamiento físico. En los sistemas de archivos FAT, existen dos mapas y son sincronizados por el sistema operativo. En otros sistemas de archivos las particiones se dividen en secciones y mantienen un mapa individual por cada sección. Por ejemplo los sistemas de archivos FAT, utilizan una Tabla de Asignación de Archivos (FAT, File Allocation Table), para mantener un registro del estado de las unidades de asignación o cluster, verificando si está en uso, si existen unidades de asignación adicionales en la cadena, si es el fin de la cadena, o si contiene bloques defectuosos. La tabla de gestión del almacenamiento es una cadena a seguir para el sistema operativo cuando tiene que reconstruir un archivo. En FAT cada bloque puede tener uno de los siguientes tres valores:

Si existen bloques adicionales de datos en el archivo, el valor apunta a la dirección del próximo bloque en la cadena.

Si el bloque es el último de un archivo, el valor contiene una marca de Fin de Archivo (End of File).

Si el bloque está dañado o es defectuoso, el valor contiene una marca de sector dañado, o el número hexadecimal FFF7. Este bloque al ser marcado por como defectuoso por el sistema operativo, no será utilizado en asignaciones futuras de espacio de almacenamiento, lo que no significa que el sector defectuoso se encuentre libre de datos, en realidad es una de antigua técnica de ocultamiento de datos.

A continuación se muestra el ejemplo citado en el libro *Incident Response & Computer Forensics,* de Kevin Mandia, Chris Posisse y Matt Pepe,13 considerando la unidad de asignación de un tamaño de 2048 bytes y:

Crear un archivo de texto Carta1.txt (archivo A) fragmentado, que ocupa 4659 bytes o sea, tres unidades de asignación, a continuación.

Crear un nuevo archivo de texto Carta2.txt (archivo B), que ocupa 2503 bytes, o sea dos unidades de asignación, y luego

Agregar 8907 bytes al archivo Carta1.txt (archivo A), alcanzando un tamaño de 13.566 bytes o sea siete unidades de asignación.

Los bloques se van asignando a media que lo solicita el sistema operativo en la mayoría de los sistemas de archivos actuales, no obstante, existen métodos para reducir la cantidad de fragmentación que ocurre cuando se graban los archivos modificados.

Unidades de asignación (FAT Clusters)

2	3	4	5	6	7	8	9	10
Carta1	**Carta1**	**Carta1**	**Carta2**	**Carta2**	**Carta1**	**Carta1**	**Carta1**	**Ca**

Gestión del espacio de almacenamiento (Tabla FAT)

2						3	4	5	6	7	8	9	10	11	12

3 4 7 6 EOF 8 9 10 EOF 0 0

Prosise, Chris. Mandia, Kevin and Pepe, Matt. *Incident Response & Computer Forensic.* 2° Ed, McGraw-Hill Osborne, California, 2003.

Entradas de directorios

Nombre de Archivo	Tamaño	Fecha	Hora	Comienzo de la Unidad de Asignación
Carta1.txt	13566	21-10-04	13:13	2
Carta2.txt	2503	21-10-04	13:16	5

La tabla de gestión del almacenamiento contiene los valores de los clusters a los que apunta, o el valor de Fin de Archivo o el valor 0, de libre.

Por ejemplo, el cluster 2 donde comienza el archivo Carta1, contiene el número 3 del cluster donde continúa el archivo Carta1, el cluster 3 contiene el número 4 del cluster donde continúa el archivo Carta1, el cluster 5 contiene el número 6 del cluster donde comienza el nuevo archivo creado Carta2, el cluster 6 contiene el valor Fin de Archivo del archivo Carta2, el cluster siete contiene el número 8 del cluster donde se agregó información y modificó el archivo Carta1, el cluster número 9 contiene el número 10 del cluster donde se continúa el archivo modificado Carta2, el cluster 10 contiene el valor de Fin de Archivo. Por lo tanto el archivo Carta1 está fragmentado y ocupa los clusters 2,3,4,7,8,9 y 10.

La tabla de entrada de directorios indica el nombre de archivo, el tamaño, la fecha y hora de creación y /o modificación y el número de cluster donde comienza el archivo. Estos datos los utilizará el sistema operativo para reconstruir los archivos.

Nivel de clasificación y almacenamiento del nivel de aplicación

Estos niveles son los que contienen los archivos y directorios. Estas capas son definidas por el sistema operativo acorde al tipo de partición utilizada. Para el análisis forense existen varios tipos de archivos que se deben verificar:

Sistema operativo y archivos de utilidades

Archivos de configuración del sistema operativo

Archivos de soporte y de aplicaciones

Archivos de configuración de aplicaciones

Archivos de datos de los usuarios

Una de las formas de reducir el número de archivos a examinar es comparando los valores de *hash* con la lista de archivos confiables. Esta lista es obtenida de la instalación del sistema operativo original y de los archivos de aplicaciones. Otro método de reducir información espuria es eliminar datos basados en la fecha y hora de los archivos.

Análisis de particiones de los discos duros

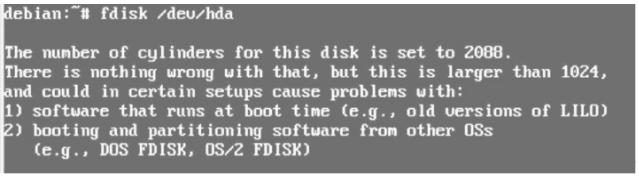
La visualización de las particiones de o los discos duros permite determinar la geometría de los discos, el número de particiones y los tipos de sistemas de archivos. El comando *fdisk* de las primeras versiones del sistema operativo DOS, puede resultar obsoleto para detectar ciertos sistemas de archivos. Si bien este comando está disponible en DOS, en algunas versiones de Windows, en Linux y Unix, puede ser peligrosa su ejecución porque ofrece la posibilidad de modificar las particiones y por lo tanto eliminarlas o modificarlas.

Herramientas

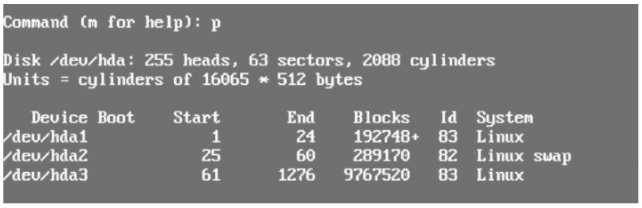
Comando del sistema operativo: *fdisk*

En Linux, distribución Debian:

#fdisk /dev/hda



Oprimir la letra *m* para el menú de ayuda y luego oprimir la opción *p* que muestra en pantalla los datos del disco rígido(/dev/hda, número de cabezas, sectores y cilindros), las particiones (/dev/hda1, /dev/hda2,/dev/hda3), inicio y fin de los cilindros, número de bloques de la partición, identificación del tipo de partición (Id) y del sistema de archivo (Linux, Linux swap):



Linux, distribución Red Hat, comando *fdisk –l*, el modificador l permite visualizar las particiones y salir del comando, si no se asigna un dispositivo específico, obtiene la información mencionada en del directorio /proc/partitions (es decir de la memoria RAM).

Rh9#fdisk l

Disco /dev/hdd: 853 MB, 853622784 bytes

32 cabezas, 63 sectores/pista, 827 cilindros Unidades = cilindros de 2016 * 512 = 1032192 bytes Disposit. Inicio Principio Fin Bloques Id Sistema

/dev/hdd1 * 1 826 832576+ 6 FAT16

Disco /dev/hda: 10.2 GB, 10262568960 bytes

255 cabezas, 63 sectores/pista, 1247 cilindros Unidades = cilindros de 16065 * 512 = 8225280 bytes Disposit. Inicio Principio Fin Bloques Id Sistema

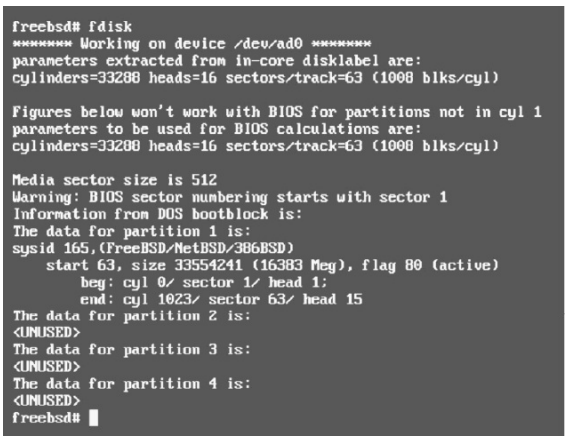
/dev/hda4	1216	1247	257040 f Win95 Ext'd (LBA)
/dev/hda5	1216	1247	257008+ 82 Linux swap

En este ejemplo aparecen dos discos, hdd con la geometría de 32 cabezas, 63 sectores por pista y 827 cilindros y hda con 255 cabezas, 63 sectores por pista y 1247 cilindros. a En Unix FreeBSD.

#fdisk

Muestra el dispositivo /dev/ad0, número de cilindros, cabezas y sectores por pista. Los datos son semejantes a los que ofrece el comando fdisk en Linux, el tamaño lo muestra también en megabytes.

En Windows XP



En la Referencia de Línea de Comandos, en el menú de Ayuda, se encuentra la herramienta **Fsutil**, que puede ser ejecutada con diferentes comandos (behavoir-dirty-file-fsinfo-hardlinkobjectid-quota-reparsepoint-sparse-usn-volume). Fsutil con la opción Fsinfo, lista todos los dispositivos, ofrece información sobre los volúmenes de los dispositivos, consulta en forma específica volúmenes NTFS y ofrece estadísticas del sistema de archivo:

Lista todos los dispositivos en una computadora

C:\>fsutil fsinfo drives Drives: A:\ C:\ D:\ C:\>fsutil fsinfo drivetype c: c: Fixed Drive

C:\>fsutil fsinfo drivetype a: a: Removable Drive C:\>fsutil fsinfo drivetype d: d: CD-ROM Drive

Lista la información de los volúmenes de tipo NTFS, tal como el número de sectores, total de clusters, clusters libres e inicio y fin de la zona MFT (master file table, es el primer archivo en un volumen NTFS que contiene información de cada archivo y carpeta de la partición).

C:\>fsutil fsinfo ntfsinfo c:

NTFS Volume Serial Number : 0x1194a36355002626 Version : 3.1

Number Sectors : 0x000000000950a5c0 Total Clusters : 0x00000000012a14b8 Free Clusters : 0x000000000095a9aa Total Reserved : 0x0000000000000180 Bytes Per Sector: 512

Bytes Per Cluster: 4096

Bytes Per FileRecord Segment: 1024 Clusters Per FileRecord Segment: 0

Mft Valid Data Length: 0x000000000c73d800 Mft Start Lcn: 0x0000000000000006

Mft2 Start Lcn: 0x000000000007af54 Mft Zone Start: 0x0000000000a5abe0 Mft Zone End: 0x0000000000a60020

Lista las estadísticas del volumen especificado, tal como los metadatos (datos sobre los archivos: título, autor, asunto y tamaño), archivos de registros y las lecturas y escrituras de la MTF

C:\>fsutil fsinfo statistics c: File System Type : NTFS UserFileReads : 50063

UserFileReadBytes : 621338624

UserDiskReads : 48706

UserFileWrites : 62494

UserFileWriteBytes : 1164166176

UserDiskWrites : 61843

MetaDataReads : 4315

MetaDataReadBytes : 19861504

MetaDataDiskReads : 5807

MetaDataWrites : 10847

MetaDataWriteBytes : 56250368

MetaDataDiskWrites : 14758

MftReads : 3290

MftReadBytes : 15663104

MftWrites : 9281

MftWriteBytes : 47595520

Mft2Writes : 0

Mft2WriteBytes : 0

RootIndexReads : 0

RootIndexReadBytes : 0

RootIndexWrites : 0

RootIndexWriteBytes : 0

BitmapReads : 602

BitmapReadBytes : 2465792

BitmapWrites : 967

BitmapWriteBytes : 5513216

MftBitmapReads : 11

MftBitmapReadBytes : 45056

MftBitmapWrites : 204

MftBitmapWriteBytes : 991232

UserIndexReads : 1720

UserIndexReadBytes : 7045120

UserIndexWrites : 3873

UserIndexWriteBytes : 18046976

LogFileReads : 6

LogFileReadBytes : 24576

LogFileWrites : 19460

LogFileWriteBytes : 181436416

Lista información sobre un volumen específico, tal como el tipo de sistema de archivo, soporte de flujo de caracteres, cuotas de disco, archivos sensibles a mayúsculas y minúsculas, entre otros. A continuación se lista la información obtenida de los dispositivo A:, C: y D:.

C:\>fsutil fsinfo volumeinfo c:

Volume Name :

Volume Serial Number : 0x55002626 Max Component Length : 255

File System Name : NTFS Supports Case-sensitive filenames Preserves Case of filenames Supports Unicode in filenames Preserves & Enforces ACL's Supports file-based Compression Supports Disk Quotas

Supports Sparse files Supports Reparse Points Supports Object Identifiers Supports Named Streams

C:\>fsutil fsinfo volumeinfo a:

Volume Name :

Volume Serial Number : 0x28127834 Max Component Length : 255

File System Name : FAT Preserves Case of filenames Supports Unicode in filenames **C:\>fsutil fsinfo volumeinfo d:** Volume Name : 040914_1200

Volume Serial Number : 0xe72b4791 Max Component Length : 110

File System Name : CDFS Supports Case-sensitive filenames Supports Unicode in filenames Análisis de la memoria virtual

En Unix / Linux

Herramientas

El archivo swaps del directorio /proc, indica en qué partición se encuentra el espacio de intercambio:

#cat /proc/swaps

Filename Type Size Used Priority

/dev/hda2 partition 289169 15980 -1 Esta información también se obtiene con el comando:

#fdisk -l

El contenido del archivo swap se puede obtener en forma similar a la de mem:

#strings /dev/hda2 > swap.txt

En Windows

El archivo swaps del directorio /proc, indica en qué partición se encuentra el espacio de intercambio:

#cat /proc/swaps

Filename Type Size Used Priority

/dev/hda2 partition 289169 15980 -1 Esta información también se obtiene con el comando:

#fdisk -l

El contenido del archivo swap se puede obtener en forma similar a la de mem:

#strings /dev/hda2 > swap.txt

En Windows

El archivo de intercambio de Windows es denominado pagefile.sys y está oculto. Se utiliza como expansión de la Memoria Ram y suele tener doble de tamaño de la misma. Para quitarle la opción de oculto, se puede ejecutar:

c:\>dir /ah, o utilizar el explorador de windows y cambiar la opción de visualización selec- cionando mostrar archivos ocultos.

La visualización del archivo de intercambio es un tanto difícil. Pero se puede examinar en forma diferida. Para esto se debe asegurar de no sobreescribir el archivo de memoria virtual. Esta información se puede obtener, si es que se efectuó la recolección de evidencia, a partir del equipo encendido, de la consulta realizada a la base de datos del Registro, efectuada en la Alternativa I, Recolección de datos con el equipo encendido, en el paso Verificación de la base de datos del Registro:

reg query
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown"

Si aparece con el valor 0, significa que el archivo no se sobreescribirá con 0000 (ceros) al apagar el sistema, esta configuración es la predeterminada.

En Windows 2000 un usuario puede habilitar una política local denominada Clear Virtual Memory Page File When Shuts Down, a través de las configuraciones de Seguridad Local, Políti- cas locales, Opciones de seguridad. Funciona de la misma forma que la configuración mencio- nada para el registro anterior. La descarga de la Memoria Virtual se puede enviar a la unidad de recolección de la evidencia, ya sea, zip, jazz, Pen Drive, disco rígido o cinta.

Para obtener el archivo de memoria virtual, pagefile.sys, en Windows NT, 2000 o

XP, se debe iniciar la computadora, con un disco de arranque en modo DOS, no se puede abrir la consola de DOS desde Windows, para descargar el archivo, porque el sistema operativo se encuentra utilizando este archivo y envía un error en el momento de efectuar la copia. El archivo se puede encontrar en el directorio raíz c:\, o en c:\winnt\system32 o en otra unidad de disco o partición. Para descargar el archivo se puede ejecutar el comando copy:

A:\copy c:\winnt\system32\pagefile.sys D:, en donde D:, puede ser la unidad de zip, jazz, pen drive, cinta o disco rígido.

A:\copy c:\pagefile.sys D:,

En el sistema operativo Windows 95, 98 o Millenium, el archivo de intercambio es win386. swp, desde la consola de DOS, ejecutar:

A:\copy c:\windows\win386.swp d:

Para visualizar el contenido es preferible utilizar cadenas de palabras claves con el fin de obtener alguna evidencia.

Herramientas

FileMonitor, http://technet.microsoft.com/en-us/sysinternals/bb89664

Con esta herramienta se puede visualizar la escritura de datos al archivo de intercambio.

Análisis de los datos de las unidades de CD-R y CD-RW - DVD y dispositivos con memoria flash

En las unidades de discos compactos también es posible recolectar evidencias. Para la vi- sualización de los datos se requiere de herramientas que permitan obtener información de las distintas sesiones de grabación de un disco compacto.

• CD/DVD Inspector, http://www.infinadyne.com/forensicsoftware.html, lectura, análisis, extracción y recuperación de archivos de la mayoría de los dispositivos ópticos. InfinaDyne provee software para diferentes agencias de investigación en Informática Forense e investi- gadores en Informática Forense. Para el informe pericial se captura la pantalla donde apa- recen las diferentes sesiones del disco

compacto. El producto de la misma empresa:

– AccuBurn-R for CD/DVD Inspector, genera copias idénticas de imágenes de CD y DVD creadas con CD/DVD Inspector.

• Flash Retriever Forensic Edition, recupera imágenes y archivos de cualquier tipo de dis- positivo flash –USB Pen Drive, tarjetas de cámaras fotográficas, de teléfonos, de MP3, entre otros–, crea imágenes bit a bit y genera la certificación matemática –hash–. http://www. infinadyne.com/flashretrieverforensic.html

Visualización de diferentes tipos de archivos

El perito informático forense requiere de herramientas para visualizar distintos tipos de archivos generados por diferentes aplicaciones, evitando la modificación de los datos de los archivos examinados ya que no poseen modos de edición.

• Quick View Plus, www.avantstar.com: Software comercial, permite la apertura de varios archivos al mismo tiempo, reconoce más de 200 tipos diferentes de archivos, incluyendo formatos de los sistemas operativos Windows, Linux, Unix y Macintosh, correo electrónico y de extensión ".msg".

• DataViz's, http://www.dataviz.com/index.html: Contiene el programa MacOpener, para ver archivos de Macintosh y Conversions Plus, en un solo paquete, permitiendo la lectu- ra de archivos de computadoras Mac, PC y de sistemas operativos Unix. También permite abrir archivos de correo electrónico y archivos adjuntos en forma simultánea, sin tener que copiar o extraer el archivo adjunto del mensaje.

– Conversions Plus, para computadoras Macintosh, permite visualizar archivos de apli- caciones Macintosh en sistemas operativos del tipo Windows.

• ThumbsPlus, www.cerious.com: permite visualizar distintos tipos de archivos de imágenes, seleccionando un directorio o dispositivo de almacenamiento y catalogando y mostrando to- das los archivos de imágenes hallados. Se puede seleccionar previamente el tipo de archivo de imagen a buscar y el programa genera una base de datos de imágenes. Este programa se pue- de ejecutar desde una unidad de zip, ejecutando la instalación e indicando la unidad lógica del zip como destino, luego se deben verificar los archivos creados en el directorio Windows durante la instalación, y éstos se deben copiar a la unidad de zip. De esta forma el programa se puede ejecutar en una computadora donde el relevamiento y análisis de los datos se debe hacer en el lugar del hecho. Disponible para Windows 2000, XP, 2003, 2008, Vista y Windows 7. Para cámaras fotográficas se puede utilizar el producto Digicam Plug-in.

• Filemon: En Windows, se puede descargar de http://technet.microsoft.com/es-es/sysin- ternals/bb896642, monitorea y muestra toda la actividad del sistema de archivos en tiem- po de ejecución. La información se puede capturar o enviar a un archivo para su posterior análisis. Permite visualizar la forma en que el sistema operativo Windows funciona, cómo las aplicaciones utilizan los archivos y librerías de enlace dinámico (DLL) o efectuar el seguimiento de problemas en el sistema operativo o en la configuración de aplicaciones. Se puede utilizar en los sistemas operativos Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, Vista, Windows 95, Windows 98 and Windows ME.

• dtSearch, www.dtsearch.com: Efectúa búsquedas muy rápidas de terabytes de texto –MS Office through 2010 (Word, Excel, PowerPoint, Access), OpenOffice, ZIP, HTML, XML/XSL, PDF, entre otros–, utiliza funciones de lógica difusa. Una de las características principales es la de buscar archivos de tipo ".pst" de Microsoft Outlook y archivos adjuntos, también para el correo electrónico Thunderbird. Genera un índice de cada palabra en el disco duro, ace- lerando la búsqueda de palabras claves dentro de los mensajes de correo. También puede buscar por sinónimos.

En Linux/ Unix, el comando find del sistema operativo, es una herramienta poderosa para efectuar búsquedas combinadas con otros comandos de filtrado de datos.

Buscar modificaciones en el sistema de archivos:

#find / -ctime -3 –type f –print0 | xargs -0 ls –l | less

-ctime, cambios en el archivo desde las últimas 3 horas

-type f, tipo de archivo regular

-print0, mostrar la ruta completa y si sobrepasa la línea continuar en el siguiente renglón.

|, pipe, tubería para conectar dos procesos en la misma línea de comando. xargs, -0, si tiene éxito, lee argumentos de la entrada estándar del comando. ls, lista el contenido del directorio, -l, utiliza el formato largo.

less, permite presentar la información por pantalla y avanzar y retroceder entre éstas.

Búsqueda de texto y palabras claves

Herramientas:

En Windows

Servicio de Índice, en las versiones de Windows NT, Windows 200x, XP y .Net, se encuentra este servicio que permite crear índices de todos los documentos y archivos del sistema, al ser un servicio se puede iniciar, detener o pausar. Efectúa búsquedas simples y avanzadas

dtSearch, www.dtsearch.com. Efectúa búsquedas muy rápidas en discos de gran capaci- dad, utiliza funciones de lógica difusa. Una de las características principales es la de buscar archivos de tipo ".pst" de Microsoft Outlook. Genera un índice de cada palabra en el disco duro, acelerando la búsqueda de palabras claves dentro de los mensajes de correo. También puede buscar por sinónimos.

Análisis del espacio no utilizado o no asignado

En el espacio no asignado o no utilizado de los dispositivos de almacenamiento es posible encontrar datos después de aplicar comandos tales como fdisk, format o mkfs, o eliminar deter- minados archivos, en Windows, con el comando del (Consultar Referencia de línea de coman- dos en el Ayuda de Windows) o rm en Linux o Unix.

La información que se encuentra en los espacios desperdiciados o no asignados no se ocul- ta intencionalmente en estos lugares, son datos que el sistema operativo deja huérfanos, espe- rando que sean sobrescritos en algún momento en el futuro.

El proceso de dar formato no asegura la eliminación de los datos existentes.

El perito informático forense debe tener especial cuidado cuando efectúa el almacena- miento de las pruebas porque puede crear su propio espacio desperdiciado en los archivos que genera, modifica, graba o elimina, estos archivos pueden contener espacio desperdiciado de otros archivos y agregarse a los archivos generados para la evidencia y ser visualizados a través de una herramienta de edición de hexadecimal. Por consiguiente se debe almacenar la infor- mación de la evidencia en dispositivos limpios, que no hayan contenido información previa, como, por ejemplo, en CD – DVD.

Áreas del sistema de archivo que contienen datos borrados o eliminados

Tipo de estructura de datos	Descripción	Técnica de recuperación de datos
Archivo	Archivos de aplicaciones (especialmente el caso de los archivos de Word, pueden contener datos perdidos del sistemas de archivos)	Examen mediante editor hexadecimal, o una herramienta de análisis forense de particiones o un archivo de imagen del disco rígido
Espacios desperdiciados	El último cluster de un archivo raramente es ocupado por completo, los datos provenientes del último uso de este cluster no son sobrescritos	Examen mediante editor hexadecimal, o una herramienta de análisis forense de particiones o un archivo de imagen del disco rígido
Bloques no utilizados	Clusters (bloques del sistema de archivos) que no están siendo usados, pueden contener datos eliminados (marcados como borrados)	Utilidad de recuperación de archivos (como la que trae el Coroner's Toolkit), editor hexadecimal, o una herramienta de análisis forense de particiones o un archivo de imagen del disco rígido
Particiones no usadas	Las configuraciones básicas de una computadora pueden no usar todo el espacio disponible en el disco rígido	Examen con editor hexadecimal de partición de la imagen de un disco rígido, o una herramienta de análisis forense que permita identificar la localización y tipo de todas las particiones. Debe usar las utilidades de partición para identificar la localización y tipo de particiones y verificar si ellas están utilizando o no todo el espacio de disco disponible
Pistas de inicio	La tabla de particiones y la información de arranque, se encuentra en pistas especialmente dedicadas que no son visibles a las utilidades de acceso a las particiones o sistemas de archivos	Herramienta de análisis forense o examen con un editor hexadecimal de la imagen completa del disco rígido

Espacio no asignado

Los clusters no asignados son los bloques que no están actualmente en uso por parte de un archivo. Los archivos en un disco rígido son constantemente cambiados de lugar. Cuando una aplicación modifica un archivo y lo sobrescribe, el archivo original modificado previamente es borrado y sus bloques son liberados es decir que quedan sin asignar y utilizables para futuras asignaciones para otros archivos. Hasta el momento en que estos bloques libres no asignados se sobrescriban, conservan el archivo original. Cuanto más alto sea el porcentaje de espacio libre en un sistema de archivo, mayor será la cantidad de archivos presentes no asignados antes de que sean sobrescritos.

Por lo tanto existe mayor espacio para información no visible u oculta. Algunas aplicacio- nes tienen su propio espacio interno desperdiciado. En el caso de Word 97, la aplicación vacía los datos perdidos en los clusters no asignados y los incorpora en los archivos “.doc” que genera el procesador de texto. Los datos no son visibles desde

el propio procesador de texto e ignora que de manera subrepticia se han incorporado datos perdidos dentro del archivo, pero se pue- den visualizar con un editor de hexadecimal.

Para el sistema operativo estos datos perdidos ya no existen en el sistema de archivo porque están incorporados a un archivo específico, aun cuando este archivo ".doc" es copiado o enviado por correo electrónico. Los espacios no asignados o parcialmente utilizados se pueden examinar en diferentes formas. La más conveniente es usar un software de Informática Forense para visua- lizar los datos. En un sistema operativo Unix, se puede visualizar una partición completa como un solo objeto, con un editor de hexadecimal se puede buscar o examinar a través de una parti- ción o en un disco duro. Se puede utilizar el comando grep o strings, pero no es muy conveniente. Si se utiliza una herramienta de búsqueda con palabras claves, tanto en Windows como en Unix, grep, sólo busca archivos individuales y no pueden ver los datos en los bloques no asignados.

Eliminación o borrado de información en el disco rígido

Los archivos eliminados no son borrados realmente. Los archivos son marcados para bo- rrar. Estos archivos permanecen en el dispositivo de almacenamiento secundario, hasta que nuevos datos sobrescriban físicamente el área donde se encontraban. Por ejemplo, en los sis- temas de archivos de tipo FAT cuando un archivo o directorio es eliminado, la primera letra del nombre del archivo es asignada con el carácter sigma ( ), por lo tanto los archivos se conservan intactos. Cuanto más rápido se recuperen los archivos eliminados, menor será el riesgo de so- breescribirlos con cualquier operación de entrada/salida del disco rígido.

La papelera de reciclaje (Recycle Bin) en Windows es un elemento que previene el borrado accidental de los archivos, los archivos permanecen en la papelera hasta que el usuario decida vaciar la papelera. La papelera captura solamente los archivos borrados del Explorador de Win- dows y de aplicaciones del paquete de oficina Microsoft Office. El borrado de archivos desde la línea de comandos y desde programas de terceras partes, generalmente no son enviados a la papelera. El proceso de la papelera de reciclaje crea un directorio que es diferente para cada usuario. El directorio se crea cuando el usuario borra un archivo por primera vez. Los conteni- dos de la papelera se pueden encontrar en el directorio de una partición (letra del disco rígido).

Encontrar los directorios ocultos de la papelera de reciclaje: C:\>echo

%systemroot%

C:\WINDOWS

C:\>dir recycler

Volume in drive C has no label Volume Serial Number is 5500-2626 Directory of C:\recycler

File Not Found

Listar los directorios ocultos de la papelera

C:\>dir /a recycler

Volume in drive C has no label Volume Serial Number is 5500-2626 Directory of C:\recycler

13/06/2004 08:11 p.m. <DIR> .

13/06/2004 08:11 p.m. <DIR> ..

16/08/2004 01:24 p.m. <DIR> NPROTECT

29/03/2003 11:03 p.m. <DIR> S-1-5-21-3787931800-1462124985-2256828832-1003

29/03/2003 10:22 p.m. <DIR> S-1-5-21-507921405-1563985344-854245398-1003

26/12/2003 10:24 p.m. <DIR> S-1-5-21-610489928-3332149871-147929544-1007

07/11/2004 12:01 a.m. <DIR> S-1-5-21-610489928-3332149871-147929544-1008

0 File(s) 0 bytes

7 Dir(s) 37.723.537.408 bytes free

C:\>

Al listar los archivos ocultos aparecen los subdirectorios de la papelera de reciclaje que es- taban ocultos, cada subdirectorio está basado en el identificador de seguridad del usuario (SID, Security Identification).

Se observa en el ejemplo un directorio para cada cuenta de usuario que haya eliminado un archivo, en este caso los usuarios son del tipo administrador. Al eliminar un archivo en la pape- lera de reciclaje puede aparecer con un nombre diferente (README.txt, cambia a Dc1.txt) pero la fecha y hora permanecen las mismas que en el archivo original.

C:\RECYCLER\S-1-5-21-610489928-3332149871-147929544-1008>dir

Volume in drive C has no label Volume Serial Number is 5500-2626

Directory of C:\RECYCLER\S-1-5-21-610489928-3332149871-147929544-1008
29/04/1996 02:40 p.m. 533 Dc1.TXT

1 File(s) 533 bytes

0 Dir(s) 37.716.107.264 bytes free

C:\RECYCLER\S-1-5-21-610489928-3332149871-147929544-1008>

En el objeto papelera de reciclaje, el archivo muestra el nombre original (README.txt) y agrega la fecha de eliminación del archivo. Por lo tanto debe existir un archivo que identifique el nombre verdadero del archivo borrado y la fecha de eliminación. En el artículo “Forensic Analysis of Microsoft Recycle Bin Records”, publicado por Keith J. Jones, del 1° de abril de 2003 y revisado el 6 de mayo de 2003, se efectúa el análisis de los registros de la papelera de reciclaje que se sintetiza a continuación:

En el directorio de la papelera de reciclaje (RECYCLER) existe un archivo oculto denomina- do INFO2, es un archivo binario que contiene la ubicación de cada archivo eliminado, nombre del archivo y fecha de eliminación. Cuando un usuario elimina un archivo desde el explorador de Windows, una copia del archivo es movida al directorio de la papelera de reciclaje. La ubica- ción del directorio depende de la versión del sistema operativo Windows.

Windows 95, 98, Millenium, con el sistema de archivo FAT32, C:\RECYCLED\INFO2. Windows NT, 2000, XP, con el sistema de archivo NTFS, C:\RECYCLER\<USER SID>INFO2.

Al mover el archivo a la papelera de reciclaje es renombrado a DC#.EXT, donde #, es un entero único, si se eliminan nuevos archivos este número ser irá incrementando, es un índice o referencia dentro del archivo INFO2 y EXT es la extensión original del archivo.

Si el archivo eliminado era CARTA.TXT, en la papelera estará renombrado como DC1.txt. Cuando se vacía la papelera de reciclaje, el archivo INFO2 es eliminado y un nuevo archivo IN- FO2 se vuelve a crear, es decir que el índice (#) se coloca en 1.

Estructura de INFO2

El archivo INFO2 debe tener la siguiente información para poder recuperar un archivo des- de la papelera de reciclaje:

• La ruta original del archivo

• El tamaño del archivo

• La fecha y hora en que el archivo fue movido a la papelera de reciclaje

• El identificador único del archivo en la papelera de reciclaje Ejemplo de la estructura de un archivo INFO2

Estructura de datos	Longitud (en bytes)	Bytes de desplazamiento
Tamaño del registro de la papelera	4	0xC
Nombre del archivo en la papelera	Variable, terminado en NULL	Inicio del registro+0x04
Identificador único del registro de la papelera	4	Inicio del registro+0x108
Número del dispositivo para el archivo en la papelera	4	Inicio del registro+0x10C
Fecha de eliminación	8	Inicio del registro+0x110
Tamaño físico del archivo eliminado	4	Inicio del registro+0x118

El archivo INFO2 se puede abrir en un editor de hexadecimal y ubicar estas estructuras. Cada registro en el archivo INFO2 es de 0x320 bytes de longitud.

El encabezado del archivo INFO2 aparece con 20 03 00 00, que se traduce a 0x320, que se encuentra en el byte de desplazamiento 0xC. El primer registro válido de la papelera de reciclaje se encuentra inmediatamente después del registro de información del tamaño de la papelera de reciclaje.

El nombre del archivo se ubica dos veces en el registro de la papelera. Existe una versión ASCII cerca del comienzo de un registro y una versión UNICODE cerca del final. Sería más fácil la salida de la versión ASCII, ubicada en el byte 0x04, después del comienzo del registro de la papelera de reciclaje.

La siguiente porción de información a identificar es el número único del índice. Si se en- cuentran varios archivos en la papelera y se comparan, el valor del índice se incrementará en 2.

El siguiente número parece ser el número del dispositivo donde se originó el archivo antes de ser movido a la papelera. Los datos están codificados utilizando el esquema 0x00, drive A, 0x01 drive B, y 0x02 drive C y así sucesivamente. Esta información se ubica en los bytes 0x10C desde el comienzo del registro de la papelera.

Para el perito es importante saber cuándo un archivo se movió a la papelera. El campo que contiene la fecha es 0x110 desde el inicio del registro de la papelera y de 8 bytes de longitud.

Luego de encontrar la fecha se debe traducir a un formato humano comprensible. Windows almacena la fecha y hora en el formato FILETIME, es decir, el número de pulsos (ticks), en incre- mentos de 100 ns desde la hora 00:00 del 1° de enero de 1601 (UTC). Dado que el resto del mundo utiliza la definición de tiempo de Unix, que es el número de segundos desde la hora 00:00 del 1° de enero de 1970, se debe traducir el formato FILETIME al formato Unix, con la siguiente ecuación:

$$(\text{Unix Time}) = A * (\text{NT Time}) + B$$

Dado que los pulsos (ticks) en FILETIME son intervalos de 100 ns, A es igual a 10-7 ns. B es el número de segundos entre el 1° de enero de 1601 y el 1° de enero de 1970, este valor ya fue calcu- lado y documentado en el desarrollo de software de Microsoft y es 11644473600.

El último campo contiene el tamaño del archivo. Este campo es 0x118 bytes desde el comien- zo del registro de la papelera de reciclaje. El tamaño del registro de la papelera no es exactamente el mismo que se visualiza con el comando dir. El archivo INFO2 debería ser múltiplo del tamaño del cluster del disco rígido.

Para visualizar el archivo INFO se puede utilizar herramientas como Rifiuti de Keith Jones de http://www.mcafee.com/us/downloads/free-tools/rifiuti.aspx, Internet Explorer History Viewer, Winhex, editores de hexadecimal.

Eliminación segura de los datos

No es posible efectuar un borrado real en el disco rígido. Siempre permanece una

imper- ceptible huella de la información previa al borrado. Los dispositivos magnéticos siempre dejan huella después de cada escritura, aun si se ha sobrescrito numerosas veces. La recuperación bit a bit de los datos que se encuentran en las pistas sobrescritas se puede realizar a través de microscopios especiales de electrones, siendo un proceso de costo muy elevado. Por lo tanto, hasta el momento y con la tecnología actual no es posible efectuar un borrado real de los me- dios de almacenamiento magnético.

Actualmente existen diversas técnicas de borrado seguro, acorde al tipo de información, el nivel de criticidad o el dispositivo donde se encuentre. El Departamento de Defensa de los Es- tados Unidos de Norteamérica (DoD) ofrece un conjunto de recomendaciones acerca de cómo limpiar o volver un dispositivo de almacenamiento magnético a su estado original de fábrica. Este procedimiento imposibilita con las técnicas conocidas hasta la fecha la recuperación de la información borrada. En enero de 1995, el DoD publicó un documento, denominado NISPOM (National Industrial Security Program Operating Manual), conocido también como DoD 5220.22- M, www.dss.mil/isec/nispom.htm, que describe un conjunto de procedimientos de seguridad industrial, entre ellos, el procedimiento de cómo eliminar datos contenidos en diferentes dis- positivos de almacenamiento, www.dss.mil/infoas/magnetic_tape_degaussing.doc. El Servicio de Seguridad y Defensa (Defense Scurity Service, DSS), desarrolló una Matriz de Limpieza y Res- tauración al estado original de fábrica de los dispositivos de almacenamiento, a partir del DoD 5220.22-M, en donde se describe la secuencia para eliminar o borrar completamente los datos en un determinado dispositivo, www.dss.mil/infoas/clearing_and_sanitization_matrix.doc. Peter Gutman, de la Universidad de Auckland de Nueva Zelanda, http://www.cs.auckland.ac.nz/, de- sarrolló un método de borrado seguro de 35 pasadas, que utilizan diversos programas de borrado de información. (Resumen disponible en la página personal del autor, http://www.cs.auckland. ac.nz/~pgut001/pubs/secure_del.html). Asimismo existen una serie de equipos de hardware de- nominados Degausser, que permiten volver el dispositivo de almacenamiento a su estado origi- nal de fábrica (www.datadev.com).

Por otro lado, existen laboratorios que se dedican a efectuar la recuperación de los datos y que poseen las herramientas y el ambiente necesario para efectuar la apertura física de los

1 Brian Carrier es doctor en Computación e investigador reconocido en informática o computación forense. Ha escrito varios libros entre ellos *File System Forensics Analysis* (Análisis Forense de sistemas de archivos). Addison Wesley. EE.UU., 2005. Para conocer sobre sus trabajos de investigación acceder a Digital Forensics Research Conference – Conferencia de Investigación forense

digital, http://www.dfrws.org/. El sitio del autor es http://www. digital-evidence.org/.

2 Estándar del Departamento de Defensa de EE.UU. de Norteamérica relacionado con la Limpieza y Desinfección de información en dispositivos de escritura DoD 5220.22-M.

3 dd, representa en inglés *duplicate disk*, duplicar disco.

4 Fecha de consulta 04-11-2011, http://www.nist.gov/index.html

5 Farmer, Dan – Venema, Wietse. *Forensic Discovery*. Addison Wesley Profesional. EE.UU., 2005.

6 Carretero Pérez y otros. *Sistemas Operativos – Una visión aplicada*, McGraw Hill, 2001.

discos y recuperación de los datos. Algunos fabricantes de discos rígidos autorizan y respaldan a determinados equipos de trabajo o empresas para que efectúen la recuperación de datos de discos dañados por agentes como el agua o el calor, o de platos dañados o rotos. Estos procesos suelen ser muy costosos, pero se suele compensar este valor con el de los datos a recuperar. Cuando no se tiene resguardo y la información almacenada en el dispositivo dañado es crítica, este proceso suele ser la mejor opción. Estas empresas suelen trabajar para la Justicia y recuperar evidencias. En EE.UU., Europa y Asia los servicios de recuperación pueden ser brindados por ONTRACK, **www.ontrack.com**. En Noruega existe el laboratorio Ibas, **www.ibas.net**, que ofrecen los servicios de recuperación de datos.

Existen factores potenciales que pueden sobrescribir los archivos eliminados, cuanto mayor sea la actividad del disco rígido o cuanto más tiempo esté ocupado, menor será la posibilidad de recuperar los datos eliminados, por ejemplo:

La creación de nuevos archivos en la partición.

Los archivos existentes aumentan de tamaño.

La instalación de un nuevo programa en la partición.

Las aplicaciones ejecutándose en la computadora puede actualizar la partición.

Si la partición almacena el directorio raíz, %systemroot%, el sistema operativo Windows puede modificar la partición para tareas de mantenimiento.

Si la partición contiene el cache del navegador de web, puede ser modificada cuando se reinicia el navegador.

Si el volumen contiene el directorio \temp, puede ser modificado con la instalación de programas.

Si la partición contiene un recurso de red compartido, los usuarios de la red pueden involuntariamente modificar el volumen cuando acceden a los archivos compartidos.

El sistema de INICIO/APAGADO, que incluye varios de los aspectos mencionados, puede reducir la posibilidad de recuperar los datos.

Análisis de datos ocultos

Para el ocultamiento de datos existen diversos mecanismos. Una de las herramientas

utilizadas es el cifrado de la información y se puede combinar con herramientas de ocultamiento de la información. A continuación se describen diversas técnicas para ocultar datos:

Técnicas de ocultamiento de información[1]

Tipo	**Técnica**	**Secuencia Metodológica**
Enmascaramiento: Los datos son visibles para todos, pero el contenido y el significado de éstos no es discernible	**Cifrado**	Identificar los datos Desencriptar
	Compresión	Identificar datos comprimidos Descomprimir utilizando el algoritmo adecuado

Tipo	**Técnica**	**Secuencia Metodológica**
	Códigos.	Decodificar mediante fuerza bruta o utilizar herramientas de

	Códigos.	criptoanálisis.
	Esteganografía.	Identificar el archivo. Desencriptar el archivo.
	Archivos ocultos. No son visibles con las herramientas estándar del sistema operativo.	Buscar características de los archivos ocultos. Buscar palabras claves en el sistema de archivos.
	Modificación de la extensión o tipo de archivo.	Buscar palabras claves en el sistema de archivos y / o anomalías. Ejecutar una herramienta que identifique el contenido de un archivo.
Ocultamiento de información La existencia y/o significado de los datos se encuentran ocultos, en archivos de texto no cifrados o dentro de la estructura de archivos, en archivos indistintos, o en el sistema de archivos solamente o fuera de la computadora.		Buscar palabras claves y / o anomalías en el sistema de archivos. Buscar en el sector de inicio. Buscar en los sectores reservados, inmediatamente después del MBR. Buscar en los sectores marcados como dañados.

	Ocultamiento. Los archivos pueden encontrarse en lugares inusuales.	particiones y en el espacio sobrante de la tabla de particiones. Buscar en todo el dispositivo, incluyendo los espacios no asignados a una partición activa.
	Archivos sin nombre. En Unix los archivos con enlace cero están asociados con ninguna entrada de directorio.	Ubicar todos los archivos con enlace cero, antes de apagar la computadora, o de lo contrario se perderán.
	Espacio desperdiciado. Espacio de intercambio. Espacio libre o no asignado.	Buscar palabras claves en todo el dispositivo de almacenamiento. Ejecutar programas de recuperación de datos eliminados.
	Tipo de partición. Al crear una partición, darle formato y luego cambiar el tipo de partición, cuando ya no se requiere el acceso a los datos, es una forma de ocultar la evidencia.	1. No confiar plenamente en la información que muestran las herramientas forenses, examinar los datos de la partición para distintos tipos de sistemas de archivos y sistemas operativos.

Tipo	Técnica	Secuencia Metodológica
	Almacenamiento de datos en dispositivos removibles o remotos. Como en una red LAN o Internet	Descubrir y examinar todos los dispositivos. Buscar evidencias de conexiones remotas.
	Flujo de caracteres. Capacidad del sistema de archivos NTFS de asociar o enlazar datos con un archivo determinado, ocultando su existencia a las herramientas de exploración y a los programas estándar del sistema operativo.	Verificar la existencia de flujo de caracteres o streams utilizando herramientas específicas para su detección. Obtener los datos de la computadora sospechada. Examinar los datos en un sistema operativo no dañado.
	Modificar el comportamiento de los comandos del sistema	Verificar la

Alterar el entorno, si bien los datos no se encuentran ocultos, las herramientas utilizadas para visualizar los datos son modificadas intencionalmente de forma tal que ciertos datos específicos no sean visualizados o encontrados en el sistema sospechado.	**operativo**	integridad de los comandos del sistema operativo. Obtener los datos de la computadora sospechada. Examinar los datos en un sistema operativo no dañado. Verificar la integridad de los módulos del sistema operativo.
	Modificar el sistema operativo	

Tipo: Enmascaramiento

Técnicas

Cifrado: El cifrado de documentos o criptografía es una ciencia muy antigua que se puede definir como la disciplina que estudia los principios, métodos y medios de ocultar la información contenida en un mensaje. Las técnicas clásicas de cifrado pertenecen a dos tipos denominados **sustitución** y **permutación/transposición**. En las primeras, los símbolos (caracteres o bits) del texto en claro, se reemplazan por otros, siguiendo una o varia reglas de sustitución. En las segundas, estos símbolos se reordenan para aparecer en posiciones distintas de las que tenían en el texto en claro.

Métodos:

Búsqueda física:

Inspección judicial, observar en los dispositivos como teclados, monitores, donde pueda aparecer la clave escrita.

Ingeniería social, averiguar la clave indagando al sospechoso o al personal del área.

Búsqueda lógica

Adivinación de la clave:

Por medio de diccionario de palabras claves basados en palabras comunes.

Por medio de palabras basadas en nombres, fechas o términos familiares al involucrado.

Por medio de la fuerza bruta, en forma metódica y secuencial probar todas las posibles claves.

Texto en claro de la clave en correos electrónicos o en documentos.

Análisis de tráfico, captura del texto en claro de la clave a través del tráfico de la red.

Texto en claro de la clave en las ubicaciones estándar de los sistemas operativos.

Criptoanálisis.

L0phtCrack, utiliza técnicas criptoanalíticas que permiten realizar un ataque de diccionario, basado en la permutación de las palabras del diccionario, o basado en la fuerza bruta, utiliza además diferentes conjuntos de caracteres. El tiempo de obtención de las claves dependerá del número de caracteres de la misma. **www.l0phtcrack.com**.

En Linux o Unix:

Obtener el archivo que se encuentra en \etc\shadow

Ejecutar L0phCrack, seleccionar el archivo shadow y especificar las opciones para la obtención de la clave.

En Windows NT:

L0phtCrack ha efectuado reingeniería del *hash* de Lan Manager que utiliza el

encriptado de una sola vía y es segmentado en tres porciones pequeñas que pueden ser reveladas, también obtiene los *hashes* de Windows NT más fuertes.

Base de datos de usuarios y claves

Obtener la SAM, a través de la utilidad ntfsdos, iniciando la computadora en modo DOS, copiar al disquete la SAM ubicada en \winnt\system32\config.

Ejecutar L0phCrack, seleccionar el archivo de la SAM y especificar las opciones para la obtención de la clave.

Otra opción sería verificar si existe un archivo de la SAM que se genera al efectuar un resguardo de la misma con el comando *rdisk /s.* El archivo SAM._ de resguardo generalmente no es eliminado y se puede copiar de la carpeta %systemroot%\repair. Para leerlo es necesario expandirlo, C:\expand sam._ sam. La herramienta L0phtCrack en sus últimas versiones lo hace automáticamente, por medio de la opción Import.

Pwdump2: Con accesos de administrador se puede obtener los *hashes* de las claves desde la base de datos del registro en Windows NT, 2000. Esta herramienta utiliza DLL (Dynamic Library Link) para cargar su propio código en el espacio de otro proceso que se ejecuta con privilegios de administración. Este código infiltrado realiza una llamada interna del tipo API que accede al SYSKEY –claves encriptadas, establece un encriptado de 128 bits, se puede habilitar desde el menú Inicio | Ejecutar syskey. Los *hash*es de las claves son encriptados por el System Key–, sin tener que desencriptarlas. El proceso en el cual se infiltra es lsass.exe, es decir, el subsistema de Autoridad de Seguridad Local (Local Security Authority), que almacena el inicio de sesión y las credenciales asociadas, utiliza el espacio de direcciones del proceso y el contexto del usuario, es decir el PID, el identificador de proceso del proceso lsass.exe. Pwdump2 se debe ejecutar en la máquina de donde se desea obtener las claves y tener privilegios de administrador. Si bien pwdump2 en sus últimas actualizaciones ejecuta una enumeración de los PID de lsass automáticamente, en forma manual se puede obtener el PID con una herramienta del Kit de Recursos de Windows NT, denominada pulist:

E:\pulist | find “lsass”

Lsass.exe36 NT AUTHORITY\SYSTEM

y luego ejecutar: E:\pwdump2 36

Lsadump2: Esta herramienta utiliza la misma técnica que pwdump2.

Ntpassword: En el caso de que no se pueda efectuar ninguna copia de la evidencia y no se pueda obtener la clave de acceso, es posible recurrir al cambio de la clave actual. Esta herramienta permite cambiar la clave**,** es una imagen de un disco de inicio, un pequeño kernel de Linux con soporte para particiones NTFS. La imagen del disco se copia con el comando rawrite. exe. Es importante considerar los riesgos del uso de esta herramienta que podrían dañar el sistema y desde luego la evidencia.

Ntaccess: de AccessData, solamente requiere el acceso físico a la computadora y un diskette de inicio de DOS, esta herramienta es de un costo considerable.

Gammaprog: Revela las claves de los servicios de correo del tipo web, como Yahoo, Hotmail y de POP, protocolo de correo entrante.

Hynopedia: Se conecta en forma remota al servidor de correo entrante de POP3 e intenta adivinar la clave una cuenta determinada.

John the Ripper: Es una aplicación para revelar claves muy popular en los sistemas operativos Unix, también puede obtener las claves de Kerberos, AFS (Andrew File System) y de Windows NT.

Mssqlpwd: Obtiene las claves del motor de base de datos de los servidores de Microsoft SQL.

PalmCrack: Funciona en dispositivos Palm PDA, y obtiene claves de Unix, Windows NT y de algunos routers de Cisco.

PGPPASS: Revela los anillos de claves PGP, el virus Calígula está diseñado para robar las claves de PGP y efectuar un FTPing de las mismas desde la computadora de la víctima a un servidor de Internet.

Slurpie: Revela las claves de Unix diseñado para trabajar en un modo distribuido, de esta forma la tarea de obtener las calves puede ser compartida por múltiples computadoras, el concepto es semejante al de la herramienta AccessData.

Webcracker: Revela las claves de los sitios web protegidos con claves por medio del método de fuerza bruta.

Aimpw: Revela las claves del servicio de mensajes instantáneos de AOL.

!Bios: Desencripta las claves utilizadas en los BIOS más comunes, IBM, American Megatrends, Award y Phoenix.

Zipcrack, PkCrack: revela las claves de archivos del tipo Zip o PKZIP.

Archivos protegidos con claves

En el análisis de un documento protegido con clave se sugieren aplicar los siguientes pasos:

Procedimiento

Verificar si se encuentra configurada la opción de crear copia de resguardo al guardar el documento, si es así, abrir el documento correspondiente con la extensión ".wbk" que no contiene contraseña de acceso. Si el archivo de resguardo no existe se deben utilizar herramientas específicas para la obtención de la clave.

Utilizar herramientas para la obtención de la clave. En el caso de Windows 95 o 98 las claves tienden a almacenarse en texto en claro.

– CAIN, permite obtener claves que se encuentran en texto en claro almacenadas en Windows, ya sea de acceso a cuentas de discado, de correo electrónico, páginas web o redes de Microsoft, archivos de tipo ".pwl" o ".dat". Además CAIN realiza pruebas de diccionario y es eficiente para la verificación de la clave por fuerza bruta. En los sistemas operativos Windows 9x, el caché de claves se puede estar deshabilitado en la base del registro:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Pol Network\DisablePwdCaching = 1. Esta herramienta permite descargar la LSA (Local Security Authority) en Windows XP y visualizar por ejemplo la clave un usuario local

31 00 33 00 31 00 33 00 61 00 7A 00 72 00 36 00 **1.2.1.3.A.z.R**.

Con Cain, http://www.oxid.it/cain.html, se puede exportar o descargar el *hash* de la máquina local o importarlo de un archivo de texto, o del archivo de las claves de usuarios de la SAM (Security Account Manager), o de un archivo generado por la aplicación L0phtCrack, con extensión ".lc". Un agente asociado a CAIN, denominado ABLE, ubicado en la computadora de la víctima puede ser accedida en forma remota para obtener las claves.

PASSWARE: http://www.lostpassword.com/ es otra herramienta para el paquete de oficina, archivos comprimidos de extensión ".zip" y correo electrónico:

Tipo: ocultamiento de información

Técnicas

Esteganografía: Proviene del griego *steganos* (protegido, oculto, cubierto) y se refiere a la práctica de ocultar información. Consiste en los procedimientos orientados a ocultar la existencia de un mensaje, no su contenido, como tintas invisibles, dibujos que bajo su apariencia ocultan informaciones, etc. En Informática consiste en el ocultamiento de la información dentro de los bits menos significativos de archivos de imagen, música, etc. Permite su publicación en la Web, sin que quienes lo accedan detecten la información, salvo que conozcan la situación precisa del esteganograma y su codificación. La esteganografía criptográfica encubre datos dentro de objetos no secretos que actúan de portador de los datos secretos u ocultos. Las aplicaciones de esteganografía utilizan dos métodos para encubrir los datos, uno es el de ocultar la existencia del archivo y el otro es el de cifrado.

Herramientas

Windows

S-Tools, **http://soft.softoogle.com/ap/s-tools-download-126.shtml**, es una herramienta de fácil uso.

Steganos, www.steganos.com, en el Ayuda, en la opción Antecedentes Técnicos se explica los métodos de Steganos: "utiliza los bits menos significativos de un elemento de datos para ocultar información en su interior. Un elemento de datos tiene 8 bits (1 byte) en un archivo de 8 bits, y 16 bits (2 bytes) en un archivo de 16 bits. Steganos, por ejemplo, utiliza los bits menos significativos de un archivo de ondas de 8 bits para ocultar los datos. El oído humano no puede distinguir estas ligeras modificaciones debido al ruido de fondo. En archivos de gráficos, los colores de los píxeles se modifican ligeramente, pero no lo suficiente como para afectar al que los está viendo".

Linux y Windows

outguess, http://www.outguess.org/info.php

Marcas de agua digital: Ocultan información en un archivo bitmap, es como si

fuera el sello o marca que se coloca en ciertos objetos donde se quiere proteger la autoría y propiedad intelectual, pero es invisible. En las copias color o las fotografías u otras obras de arte digital se aplican estas marcas. Este tipo de técnica puede ser utilizada en la corte en el ámbito civil como elemento de prueba para defender los derechos de autor. En EE.UU. para evitar la réplica de los originales se impuso para todos los fabricantes de copiadoras de color, la inclusión del ocultamiento de datos por medio de esteganografía en la salida impresa, lo que permite a la ley determinar cuál ha sido la máquina que efectuó la copia.

Espacio no asignado, desperdiciado y libre

Flujo de caracteres stream

La documentación de esta capacidad del sistema de archivos NTFS fue realizada en 1998 por Microsoft. Las particiones NTFS de Windows NT, XT, 2000 y 2003, tienen un flujo de caracteres primario predeterminado, uno de datos y otro el descriptor de seguridad. Pero existen flujo de caracteres opcionales o alternativos, denominados ADS (Alternative Data Stream). Las herramientas del sistema operativo pueden detectar solamente el stream primario pero no los alternativos, ya sean con nombre o sin nombre. El ocultamiento de datos en un archivo del tipo ADS se puede generar a través del siguiente ejemplo:

Crear un directorio en la unidad de disco C:\

C:\md ocultar

Cambiar al directorio ocultar,

C:\cd ocultar

Crear un archivo de texto pequeño,

C:\ocultar>echo “Este archivo contiene datos ocultos” > oculto.txt

Listar el contenido el directorio y verificar el tamaño del archivo oculto.txt

C:\ocultar>dir

Directorio de C:\ocultar

09/09/2004 08:29 p.m. <DIR> .

09/09/2004 08:29 p.m. <DIR> ..

09/09/2004 08:24 p.m. 40 oculto.txt

1 Archivo (s) 40 bytes

Agregar un flujo de caracteres al archivo oculto.txt, por ejemplo el listado del directorio del sistema operativo windows, la forma es "nombre_del_archivo:nombre_del_flujo_de_caracteres,

C:\ocultar>dir c:\windows > oculto.txt:agregado

Listar nuevamente el contenido del directorio y verificar el tamaño del archivo oculto.txt y compararlo con los resultados del punto 4. El tamaño del archivo es el mismo.

C:\ocultar>dir

Directorio de C:\ocultar

09/09/2004 08:40 p.m. <DIR> .
09/09/2004 08:40 p.m. <DIR> ..

09/09/2004 08:58 p.m. 40 oculto.txt

1 Archivo(s) 40 bytes

Verificar el contenido del archivo oculto.txt, debe contener la salida del listado del directorio de Windows efectuada en el punto 5.

Verificar el contenido del archivo oculto.txt sin el flujo de caracteres agregados:

C:\ocultar>more < oculto.txt

"Este archivo contiene datos ocultos"

Verificar el contenido del archivo oculto.txt con el flujo de caracteres agregados:

C:\ocultar>more < oculto.txt:agregado

Directorio de c:\windows 05/09/2004 10:05 p.m. <DIR> .

05/09/2004 10:05 p.m. <DIR> ..

29/03/2003 10:22 p.m. <DIR> addins

29/03/2003 10:22 p.m. <DIR> AppPatch 22/07/2004 12:50 p.m. 34cdplayer.ini

28/08/2002 11:00 p.m. 82.944 clock.avi

29/03/2003 10:22 p.m. <DIR> Config

-More --

Se pueden crear flujo de caracteres sin nombre, es decir no existe un archivo que lo contenga como en el punto 5.

C:\ocultar>echo “Este flujo de caracteres no tiene nombre” > :sin_nombre

Al listar el contenido del directorio ocultar no aparece. Ni el comando dir ni el Explorador de Windows detectan la presencia de este archivo:

C:\ocultar>dir

Directorio de C:\ocultar

09/09/2004 09:14 p.m. <DIR> .

09/09/2004 09:14 p.m. <DIR> ..

09/09/2004 08:58 p.m. 40 oculto.txt

1 Archivo(s) 40 bytes

Pero conociendo su existencia se puede visualizar el contenido del flujo de caracteres sin nombre:

C:\ocultar>more < :sin_nombre

“Este flujo de caracteres no tiene nombre” C:\ocultar>more < :sin_nombre

Se puede asociar o enlazar a un archivo un archivo ejecutable:

C:\ocultar>type c:\windows\explorer.exe >oculto.txt:exp.ex**e**

C:\ocultar>more <oculto.txt:exp.exe MZÉ

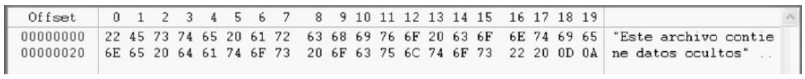
♥

♦

╕

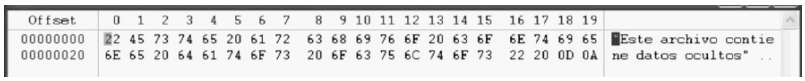
@

Archivo ocultar.txt sin flujo de caracteres



Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	
00000000	22	45	73	74	65	20	61	72	63	68	69	76	6F	20	63	6F	6E	74	69	65	"Este archivo contie
00000020	6E	65	20	64	61	74	6F	73	20	6F	63	75	6C	74	6F	73	22	20	0D	0A	ne datos ocultos" ..

Archivo ocultar.txt sin flujo de caracteres



Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	
00000000	22	45	73	74	65	20	61	72	63	68	69	76	6F	20	63	6F	6E	74	69	65	"Este archivo contie
00000020	6E	65	20	64	61	74	6F	73	20	6F	63	75	6C	74	6F	73	22	20	0D	0A	ne datos ocultos" ..

Técnica: Directorios y archivos no visibles en Linux o Unix

Herramienta

find, comando del sistema operativo para buscar información en diversos directorios como

/, /tmp, /dev.

#find . –type d –name “.*” –print0 | cat –A

Busca los archivos ocultos denotados con un ".", del tipo directorio, cuyo nombre comience con un "." y continúe con cualquier caracter y muestre el resultado en pantalla si tiene éxito y le envíe al comando cat, para visualizar el contenido en modo lectura con la opción –A, para mostrar todo el contenido. O con direccionarlo a un archivo de texto para su posterior análisis:

#find . –type d –name ".*" –print0 > /mnt/floppy/ocultos.txt

Para determinar si usuarios no autorizados están ejecutando aplicaciones en el sistema se debe buscar el identificador del usuario SUID, o del grupo SGID, del usuario root. Es necesario buscar en todos los directorios del sistema de archivos.

#find / –user root –perm -4000 –print0 | xargs -0 ls -l

#find / –perm -2000 –print0 | xargs -0 ls -l

#find / –perm -6000 –print0 | xargs -0 ls -l

En el directorio /dev, suelen ocultarse archivos que no corresponden a este directorio, es decir archivos que no son del tipo especial, como de bloques o caracter. En la siguiente búsqueda se intenta detectar archivos de tipo ordinario.

#find /dev –type f –print0 | xargs -0 ls -l

En el directorio del usuario pueden aparecer ejecutables, pero es necesario examinarlos para descartar cualquier tipo de duda.

#find /home –type f –print0 | xargs -0 file | grep executable

La búsqueda de palabras claves se puede efectuar buscando primero en el sistema de archivo completo con el comando de filtrado grep:

#grep intruso /dev/hda*

Y luego de ubicada la partición en donde se encuentra el archivo, efectuar una búsqueda específica:

#find /tmp –type f –print0 | xargs -0 grep intruso

od, comando de Linux o Unix que permite visualizar los archivos en formato octal en forma predeterminada y en ASCII, decimal, hexadecimal y otros formatos. Por ejemplo el contenido en el directorio /dev/null, siempre debería contener 0, la opción –c, indica el formato ASCII:

#od –c /dev/null

0000000

Tipo: Alteración del entorno

Técnica: Modificación del sistema operativo

La alteración del entorno del sistema operativo a través de la modificación de archivos del núcleo, de archivos binarios o de comandos producen una información que es visible al perito pero apócrifa. La modificación de archivos binarios en Unix es una tarea común, así como también en Windows NT. La herramienta Windows NT rootkits, difundida ampliamente, es un conjunto de archivos binarios del sistema, modificado, para brindar a los hackers puertas traseras ocultas que les permitan un acceso futuro a los sistemas que ellos mismos han comprometido. Tanto los sistemas operativos de Microsoft como los de Unix y Linux, utilizan librerías de enlace dinámico o DLL (Dinamic Link Library), estos archivos son accedidos en tiempo de ejecución, disminuyendo la cantidad de código redundante. Cuando una DLL se actualiza, todos los programas que hacen referencia a esta librería también se actualizan. El inconveniente de estas actualizaciones es que un cambio del tipo hostil a estos archivos o librerías compartidas afectarían a todos los ejecutables del sistema. Por lo tanto, cualquier actualización del código de un sistema operativo, debería ser manejada y autorizada por el personal de la administración del *software* de base. El análisis forense de la información debería efectuarse en todos los casos que sean posibles, sobre una imagen del sistema sospechado. Pero en los casos que se deba hacer sobre el mismo sistema operativo involucrado, se debe utilizar un dispositivo de inicio de sólo lectura en CD–ROM o disquete que sea confiable. Es importante y recomendable utilizar archivos binarios enlazados estáticamente. La creación de este tipo de archivos en el sistema operativo Solaris se torna problemática.

Herramientas

Tripwire, puede detectar cambios o diferencias entre los archivos binarios originales y los alterados. **http://www.tripwire.com/**

The Coroner's Toolkit (TCT), es una herramienta que permite generar una imagen para un disco compacto o CD–ROM, que contiene versiones enlazadas estáticamente de utilidades del sistema operativo y de informática forense.

Código malicioso o Malware

Se considera código malicioso u hostil al conjunto de líneas de código de diferentes lenguajes de programación que pueden incorporarse, dañar y/o modificar los programas de aplicaciones y de *software* de base instalados en una computadora produciendo un funcionamiento anómalo de todo o parte del conjunto y conseguir un control no autorizado sobre la computadora afectada. Este comportamiento puede o no ser detectado por el usuario final. La instalación de programas no autorizados por la administración del área de informática puede ser considerada como código dañino o malicioso. Diariamente se genera código hostil que se difunde por diversos medios, principalmente a través de los servicios que ofrece la red de redes, es decir Internet. El código malicioso tiene diversas características, a saber:

Métodos de invasión o ataque

Desde el interior, invade o ataca a la propia computadora en la que se encuentra incorporado.

Desde el exterior, invade o ataca en forma remota, a través de una red o de un acceso telefónico, alámbrico o inalámbrico.

Modos de control de la invasión o ataque

Manual: El código malicioso es manipulado y dirigido, en forma interactiva, por un ser humano.

Automático: El código malicioso actúa sin intervención del ser humano, acorde a los parámetros que le indica el propio código, se denominan robots o agentes.

Modo de distribución o impregnación

Autorreplicante:

Virus: Código dañino que requiere un programa portador para efectuar la

diseminación.

Gusanos: son siempre archivos ejecutables aislados, se copian a sí mismo en las diferentes computadoras de una red.

En algunos casos el efecto de un virus y de un gusano puede ser similar, por ejemplo, al utilizar el servicio de correo electrónico y distribuirse como un archivo adjunto, estos archivos al ser abiertos o ejecutados envían copias de sí mismo a otros usuarios cuyas direcciones de correo electrónico aparecen en la computadora que inicialmente recibió el código malicioso. (Virus: Melissa, Gusano: I Love You).

El código hostil autorreplicante puede utilizar un modo de control de la invasión de tipo automático o manual.

Una clasificación del código malicioso de *Computer Forensics, Incident Response Essentials*,[2]

es la siguiente:

Modos de control	**Método desde el interior**	**Método desde el exterior**
Manual	Manipuladores de registros o logs Utilidades que reemplazan el código binario original por un código hostil Herramientas de red de acceso remoto no autorizado (NetBus, BackOrifice, Internet Relay Chat –IRC–, agentes, robots)	Explorador de vulnerabilidades Denegación de servicio Ataques de desbordamiento de buffers.
	Virus (Melissa) Bombas de tiempo Binarios troyanos	Procesos zombies de distribución de denegación de servicio Agentes IRC

Autónomo

Objetivos del código hostil

El código hostil se apodera de la computadora que ha infectado o invadido para:

Acceder en forma remota

Las aplicaciones de control remoto pueden ser del tipo comercial como Symantec PCAnywhere o Citrix WinFrame, Microsoft posee una herramienta de administración remota System Management Server, SMS, pero no es lo mismo que estar administrando localmente la computadora. Por esta razón se requieren de herramientas comerciales como pcAnywhere o Citrix. Otras herramientas no comerciales como NetBus o Backorifice permiten el control remoto total e invisible de sistemas operativos como Microsoft Windows. El acceso o control remoto en los sistemas operativos Linux o Unix es factible a través de la aplicación Telnet.

Recolectar información o datos de la víctima

Los métodos para recolectar información pueden ser:

Exploración de vulnerabilidades, dirigido en forma remota y activa, ubica a las computadoras de una red e identifica las características de éstas.

Rastrear o husmear (sniff), dirigido externamente y pasivo, recolecta los datos visibles en un segmento de red, son aplicaciones específicas, una de sus funciones principales es obtener el nombre de usuario y la clave de acceso. En los sistemas operativos del tipo Windows, las claves de red están encriptadas utilizando el algoritmo de *hash* de una sola vía, esta técnica es fácil de quebrantar y por lo tanto los rastreadores obtienen la información que luego es traducida al par usuario/clave. En los servicios de FTP y Telnet la clave no se encripta, por lo tanto los rastreadores pueden obtener fácilmente la clave.

Explotación de datos, dirigido internamente y activo, busca datos específicos como las claves en una computadora, los sitios preferidos de navegación por Internet del usuario afectado.

Efectuar sabotaje

Los programas del tipo bombas lógicas o bombas de tiempo son utilizados para

efectuar sabotaje y son instalados por personas con acceso a información confidencial dentro de la empresa u organismo, provocando la alteración, modificación o destrucción de los datos. Las bombas lógicas son lanzadas ante la ocurrencia de un determinado evento o secuencia de eventos. Las bombas de tiempo son lanzadas en una fecha y hora determinada.

El mecanismo disparador de estas bombas verifica periódicamente, como si fuera un servicio, si la cuenta del administrador se encuentra activa. Si el administrador es en algún momento despedido de la empresa, la bomba automáticamente se dispara sin intervención del ser humano. Las bombas de tiempo pueden ser utilizadas para pedir rescate, forzando a la víctima a pagar y entonces desactivar la bomba.

Estos programas generalmente son diseñados para una única ocasión, es decir de un solo uso. Generalmente los programas de este tipo no son similares unos con otros. Son rutinas específicas de código oculto, incluidas en un programa personalizado, que se activan acorde a los requerimientos del propietario. Este tipo de código afectan el funcionamiento normal de los servicios, denegando su acceso, tales como el envío de numerosos mensajes falsos a una determinada cuenta de un pager, o los que aparecen en el uso del ICQ en los salones de conversación que obligan a desconectarse a los usuarios atacados, o en los que se incluyen como un código embebido en el correo electrónico y que al ser recibido por la víctima se ejecuta, aparecieron en 1998 con nombre de bombas de correo (mail bomb).

Efectuar denegación de servicio

La denegación de servicio del tipo distribuida (DDoS) introduce la mayor parte del código malicioso del ataque en las computadoras intermediarias, dificultando la detección de éste.

El ataque funciona a partir de la coordinación de ataques de múltiples computadoras dirigidos a una única víctima o a un único objetivo, impidiéndole a la computadora dañada ofrecer los servicios en forma normal a sus legítimos usuarios. Un solo agresor puede ejecutar un ataque de DDoS sin asistencia, influenciando a múltiples víctimas, denominadas zombies o esclavos, cada uno de ellos ejecutando un programa de denegación de servicio, instalado por el agresor. Para complicar el seguimiento de las huellas del origen del ataque, las víctimas zombies o esclavos son controladas por un programa maestro que funciona en otra computadora, víctima también del ataque. La inclusión del programa en las computadoras esclavas se realiza a través de un programa que automatiza el ataque en la computadora maestra, la cual busca computadoras con vulnerabilidades y le instala el programa agresor o servicio zombie en miles de computadoras por día. Estos ataques funcionan bajo el nombre de

Stacheldraht, Trinoo o Tribe Flood Network (Inundación de la red), han intentado utilizar como portador de los servicios zombies a los sistemas operativos Unix. Las computadoras hogareñas con acceso a Internet por medio de líneas de banda ancha (ADSL, Asymetric Digital Subscriber Line) son ideales para este tipo de ataque.

5. Eliminar huellas

Los agresores o intrusos luego de ejecutar un ataque o de invadir un sistema suelen eliminar sus huellas para no dejar rastro alguno de su accionar. Los sistemas operativos poseen un conjunto de herramientas para registrar diferentes eventos que se relacionan con la seguridad y con los errores producidos en el sistema durante su ejecución. Esta información puede ser eliminada por el intruso para no dejar rastro alguno, no se trata de ocultar información sino de modificar su significado. En otros casos pueden modificar el sistema de archivos substituyendo programas que aparentan ser originales. Al eliminar estos registros o sustituir programas se encuentra afectada la integridad y disponibilidad de la información para la administración del sistema.

Robar recursos

Los programas de tipo troyanos (relacionados con el caballo de Troya), acorde a lo expresado en el libro de *Computer Forensic, Incident Response Essentials*,[3] adquieren diversos significados, a saber:

Ruptura o infracción de la seguridad perimetral: Éste sería uno de los significados clásicos del programa troyano, el mecanismo funciona ubicándose en la computadora en forma intencional engañando a la víctima e infectándola. Ejemplos de este tipo de programas son el virus Melissa y el gusano I Love You. Algunas veces el programa troyano surge bajo la apariencia de un videoclip, pero en realidad es un programa de control remoto, también se pueden encontrar en los videos juegos o en los protectores de pantalla, la infección ocurre cuando se instala el programa o se ejecuta la aplicación misma.

Enmascaramiento: El programa ejecutable malicioso tiene el mismo nombre que el programa legítimo u original. La víctima que ejecuta el código malicioso no sería engañada, ya que estaría ejecutando un programa como lo hace habitualmente. Para instalar este tipo de troyano se debe tener acceso al sistema, rompiendo la seguridad perimetral.

Modificación: Como en el enmascaramiento se rompe la seguridad perimetral y se modifican los archivos ejecutables legítimos (se vuelven troyanos) infectándolos con un código malicioso, a diferencia con el programa troyano clásico, los nombres de los

ejecutables del código malicioso aparentan ser legítimos y aceptables.

Código malicioso no replicante: En ciertas ocasiones se considera al código malicioso de ejecución automática y de tipo no replicante como un programa troyano. Por ejemplo las aplicaciones de control remoto como NetBus y Backorifice serían considerados troyanos.

Sólo es aplicable este término en el momento en que atraviesa la seguridad perimetral, pero una vez instalado en el sistema ya no formaría parte de un programa troyano.

Engañar los mecanismos de control de acceso

Ciertos códigos maliciosos aprovechan y explotan automáticamente las vulnerabilidades de los sistemas y por lo tanto engañan a los mecanismos de control de accesos. Uno de los ataques más comunes de este tipo y que surge a mediados de 1960, es el desbordamiento de memoria, aparte de los de adivinar las claves (en forma manual o automática). Los programas que responden a solicitudes externas suelen ser vulnerables al ingreso de código malicioso. Si el dato que ingresa al sistema es mayor que la estructura de datos disponible para aceptarlo, puede ser posible insertar código de máquina que subvierta el propósito original del programa infectado e invocar a un programa no deseado desde el exterior, como puede ser una aplicación como el intérprete de comandos o shell.

Si el ataque tiene éxito el agresor goza de los privilegios que posee la aplicación infectada. Los objetivos principales son aquellas aplicaciones que son ejecutadas con el usuario administrador en el caso de Windows NT o 2000 o como root en Linux o Unix. El ataque de desbordamiento de memoria requiere de un conjunto de instrucciones de máquina, para poder explotar la vulnerabilidad, por lo tanto deben ser específicas para cada plataforma, para cada sistema operativo y para cada aplicación. Los ataques son orientados generalmente a las aplicaciones que ofrecen servicios de Internet.

En el caso de Unix o Linux pueden ser los servicios de nombres de dominio, DNS, o el servicio de información de red de Sun, NIS, el servicio de correo electrónico Sendmail de Unix o Linux, el servicio de impresión de Unix, que brinda también el servicio de impresión remota, LPR, el servicio de Web. En el caso de Windows NT se explota la vulnerabilidad del servicio de información de Internet, Internet Information Service, IIS o productos de terceros para esta aplicación. La vulnerabilidad que aprovecha el desbordamiento de memoria es la del propio lenguaje de codificación del sistema operativo o de las aplicaciones, es decir del lenguaje C.

Los programas de exploración de vulnerabilidades pueden ser utilizados con fines de auditoría de la seguridad del sistema o para explotarlas en forma maliciosa. Estas herramientas deben ser utilizadas tanto por los administradores de los sistemas operativos y de redes para verificar cuán vulnerable es su sistema y por los peritos informáticos forenses para detectar los diferentes tipos de ataques perpetrados o de elevada probabilidad de ocurrencia.

Efectuar ingeniería social

Ésta es una estrategia para la obtención de información sensible, utilizando como instrumento al ser humano. Cuando existe la posibilidad, esta estrategia se aplica antes de implementar cualquier otra acción sobre los recursos de *software* y /o *hardware*. Una de las técnicas más sencillas es que el intruso intente demostrar que pertenece al entorno de trabajo de la víctima y a partir de allí efectuar diferentes acciones, tales como planteo de interrogantes relacionados con la actividad rutinaria o normal de la víctima, quien sin cuestionar la autenticidad de la persona que realiza las preguntas, ya que la considera confiable, por haber demostrado superficial y amistosamente pertenecer al mismo entorno, le brinda la información requerida. Los intrusos pueden utilizar como medio de obtención de la información, el teléfono de la empresa, el fax, el correo postal o el electrónico, el chat, una página web, entre otros. La solución para la prevención de este tipo de accionar desinteresado, descuidado y en algunos casos mal intencionados de los empleados de la empresa u organización afectada, sería la de difundir por medio de la capacitación del personal las medidas de prevención y políticas de protección de la información, de manera tal que genere, en lo posible, un grado de responsabilidad y sentido de pertenencia a la organización, por medio de la concientización y compromiso responsable.

Por consiguiente la prevención debería redundar en un cambio de actitud que perdure en el tiempo y sea contundente**.**

Destruir, como único *fin en sí mismo y en modo indiscriminado*

Este objetivo está relacionado con la naturaleza humana intrínseca. El hombre como especie, reúne características que en algunos casos son semejantes a otras especies animales y en otros, le son totalmente propias. En este caso la satisfacción o placer del intruso es la de destruir la información sin importar a quién afecte y qué consecuencias pueda traer aparejadas. Este aspecto es difícil de corregir y evitar, tal vez la única solución sería su exterminación.

Análisis del correo electrónico

Los clientes de correo como Microsoft Outlook, Outlook Express, Netscape, Lotus Notes o Eudora, entre otros, al leer un correo electrónico pueden utilizar los protocolos de correo electrónico tales como POP –Post Office Protocol, puerto 110, RFC[4]1939, IMAP – Internet Mail Access Protocol, puerto 143, RFC 2060, MAPI – Microsoft Mail API. El correo electrónico entrante se almacena inicialmente en el servidor de correo, que ordena los correos en las casillas de correo individuales de cada usuario y acorde a las direcciones de correo electrónico. Los usuarios de correo POP pueden seleccionar la opción de descargar una copia de los mensajes desde el servidor o descargarlos sin dejar copia con la opción de borrarlos.

El RFC 822 –STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES–, define

el estandar para el formato de los mensajes de texto de Internet ARPA. El CCITT, Comité Consultivo Internacional Telegráfico y Telefónico (*Consultative Committee for International Telegraphy and Telephony*, que luego cambió a ITU-TS, International Telecommunications Union Telecommunication Standard Sector, formalmente denominado CCITT) definió otro estándar, el X.400, que describe el servicio de mensajes y el transporte de correo electrónico. Los siguientes RFC son complementarios del RFC 822:

RFC 1437 – The Extension of MIME Content-Types to a New Medium

MIME (*Multipurpose Internet Mail Extensions*, Extensiones de Correo Internet Multipropósito).

Son una serie de convenciones o especificaciones dirigidas a que se puedan intercambiar a través de Internet todo tipo de archivos (texto, audio, vídeo, etc.) de forma transparente para el usuario.

Una parte importante del MIME está dedicada a mejorar las posibilidades de transferencia de texto en distintos idiomas y alfabetos.

RFC 2045 – Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies –Formato del cuerpo de los mensajes en Internet.

RFC 2046 – Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types – Parte dos, Tipo de aplicación.

RFC 2047 – MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text – Parte tres – Extensiones del Encabezado del Mensaje para texto No ASCII.

RFC 2048 Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures [Parte cuatro: Procedimientos de registro].

El correo electrónico que ha sido leído o guardado para su posterior uso, se almacena en la computadora que está ejecutando el cliente de correo electrónico. En el caso de los protocolos IMAP y MAPI, los usuarios tienen o no la opción de dejar todos los mensajes en su servidor de correo electrónico. Las ventajas de dejar el correo electrónico en el servidor son las siguientes: permite a la organización centralizar todos los mensajes y efectuar el resguardo de los mismos y los usuarios pueden acceder a su correo electrónico desde cualquier computadora. El conocimiento de estos protocolos es importante para el análisis informático forense para determinar dónde se almacenan los mensajes:

Servicio de correo electrónico	**Protocolo**	**Análisis forense**
Almacenamiento solamente de correo entrante	Post Office Protocol, puerto 110, RFC 1939	Se debe acceder a la computadora para rastrear el origen de un mensaje
Almacenamiento de todos los mensajes, opcional	Código abierto MAPI Código propietario Microsoft Mail API (MAPI) Código propietario Lotus Notes	Las copias del correo entrante y correo saliente pueden almacenarse en el servidor o estación de trabajo y en resguardos en cintas o CD-ROM/DVD
	HTTP, protocolo	Los mensajes entrantes y salientes se almacenan en el servidor, con la opción posible de la descarga manual en la computadora.

Webmail, correo electrónico a través del web, envío y recepción	de transferencia de hipertexto, puerto 80, RFC 2854.	Permite la falsificación de la entidad del usuario del correo electrónico.

El correo electrónico saliente utiliza el protocolo de correo saliente SMTP (Simple Mail Transfer Protocol, puerto 25, RFC 2821). Los servidores de correo que aceptan correo electrónico y los retransmiten suelen denominarse Agentes de Transferencia de Correo (MTA, Mail Transfer Protocol). Los servidores SMTP de los proveedores de Internet reconocen los mensajes como dirigidos a los usuarios de su servidor local y los ubican en sus respectivas casillas de correo o los retransmiten a otros destinatarios.

El protocolo SMTP no posee una autenticación robusta, se puede utilizar para colocar cualquier información en los encabezados y falsificando las direcciones de origen y de retorno de los mensajes. Esta debilidad se puede solucionar con PGP (Pretty Good Privacy, RFC 1991, combinación de clave pública y cifrado convencional para brindar seguridad a los mensajes electrónicos y archivos) o S/MIME (Secure/Multipurpose Internet Mail Extensions, RFC 2311, brinda un modo consistente de enviar y recibir datos MIME [Multipurpose Internet Mail Extensions, que define el protocolo de representación de los mensajes], por medio de los servicios de seguridad criptográfica para las aplicaciones de correo electrónico: autenticación, integridad del mensaje y no repudio del origen –utilizando firma digital– y privacidad y seguridad de los datos –utilizando cifrado–). Los usuarios pueden almacenar el correo en las distintas carpetas predeterminadas del cliente de correo o crear sus propias carpetas. Para seguir el rastro de los mensajes de correo electrónico se deben analizar los encabezados del mensaje. Las funciones que cumple el encabezado son las siguientes:

Indican a los servidores de correo dónde entregar el mensaje.

Indican a las aplicaciones lectoras de correo electrónico cómo procesar el contenido de los mensajes de correo.

Ofrece un registro de la ruta seguida por el mensaje desde su origen hacia su destino – RFC 2076

Common Internet Messages Headers [Encabezados de Mensajes de Internet Comunes].

Características del encabezado de los mensajes:

Generalmente todos los campos del encabezado necesarios son generados por la interfaz de correo.

Algunos son opcionales y pueden ser añadidos por el usuario.

Otros campos son añadidos por el *software* de transporte de correo.

Por ejemplo, se puede ver que cada mensaje está precedido por una línea “From” (nota: sin dos puntos).

Ésta *no* es una cabecera RFC-822; ha sido insertada por el *software* de correo para facilitar la lectura a los programas que usen ese archivo.

Descripción del encabezado:

From:

De. Contiene la dirección de correo electrónico del remitente, y posiblemente el “nombre real”. Aquí se usa una variedad completa de formatos distintos.

De: aramirez@argentina.com

To:Ésta es la dirección de e-mail del destinatario. Si hay varias direcciones se separan por comas.

A:larellanogonzalez@yahoo.com.ar

Cc:

Con Copia. (carbon copy)

Ésta es una lista de las direcciones de correo que recibirán una copia textual del mensaje. Si hay varias direcciones, se separan por comas.

CC: informatica-forense@gruposyahoo.com

Bcc:

Cco: Con copia oculta. (Behind carbon copy)

Ésta es una lista de las direcciones de correo que recibirán una copia textual del

mensaje. La diferencia principal entre “Cc:” y “Bcc:” es que las direcciones listadas en el “Bcc:” no aparecerán en la cabecera del mensaje que se envía a cada destinatario. Si hay varias direcciones, se separan por comas.

Subject:

Es el **Asunto**, describe el contenido del mensaje en pocas palabras. Asunto: Informática-forense Encabezado de mensajes

Date:

Fecha, Indica la fecha y hora en que se envió el mensaje. Fecha: Fri, 14 Sep 2007 13:58:50 -0300

Reply-To:

Responder a, Especifica la dirección a la que el remitente desea que el destinatario le conteste. Esto puede ser útil si se tienen varias direcciones, pero se desea recibir la mayor parte del correo, sólo en aquella que se usa mas a menudo. Este campo es opcional.

Responder a: informatica-forense@gruposyahoo.com

Organization:

Organización. La organización que posee la máquina desde la que se ha enviado el mensaje. Si la máquina usada es la suya propia no incluya este campo, o bien indique “privado” o cualquier trivialidad sin sentido. Este campo no está descrito en ningún RFC y es completamente opcional. Algunos programas de correo lo soportan directamente, pero la mayoría no.

Message-ID:

Una cadena generada por el transporte de correo en el sistema remitente. Es única para cada mensaje.

Identificador del Mensaje

with ESMTP id 25556644C48

Received:

Cada nodo que procesa su correo (incluyendo las máquinas del remitente y el

destinatario) insertan este campo en el encabezado, dando el nombre del nodo, una identificación de mensaje, hora y fecha a la que lo recibieron, de qué nodo procede, y qué *software* de transporte ha sido usado. Esto se hace para conocer la ruta que ha seguido el mensaje:

Recibido de

Received:from [209.73.164.83] by n19.bullet.scd.yahoo.com with NNFMP; 04 Mar 2011 16:59:59 -0000

Message-ID:

El mensaje en sí mismo posee un segundo identificador que es transportado durante todo el trayecto del mensaje hacia su destino.

El Identificador del Mensaje – Message-ID, es asignado por el cliente de correo que creó el mensaje.

Este identificador permite buscar un determinado mensaje entre los registros de uno o varios servidores

Identificador del Mensaje

Message-ID:<56c2deea1100921f0f87d6cdf7afd662@wmx1.argentina.com>

X-cualquier-cosa*:* X-. Se utiliza para implementar características adicionales que aún no han sido incluidas en un RFC, o que no lo serán nunca.

X-Apparently-To:informatica-forense@gruposyahoo.com X-Priority:3X-Mailer:Argentina.com

X-Virus-Scanned:amavisd-new at argentina.com

X-Originating-IP:64.76.16.42X-eGroups-Msg-Info:1:12:0:0:0

MIME

La versión de formato MIME Multipurpose Internet Mail Extensions

1.0 version standard.

MIME-Version:1.0

http://rand-mh.sourceforge.net/book/overall/mimerg.html

Content-Type:

El juego de caracteres que se usa para representar la información. multipart/alternative, idéntico sintácticamente a multipart/mixed

Content-Type:multipart/alternative;
boundary=”b1_56c2deea1100921f0f87d6cdf7afd662“

Campo Received – Recibido

Es el campo más interesante para observar los pasos que sigue el mensaje desde su origen hacia su destino.

En cada paso que atraviesa el mensaje se agrega un nuevo encabezado Received que permite efectuar el rastreo o seguimiento de la ruta del mensaje.

La transferencia del mensaje se efectúa a través del MTA –Agente de Transferencia de Mensajes– de los servidores de correo por donde atraviesa el mensaje.

La comunicación entre servidores se efectúa a través del protocolo SMTP –Simple Mail Transfer Protocol– o ESTMP – Enhaced Simple Mail Transfer Protocol.

Received: –recibido– muestra el nombre de la computadora y dominio desde donde se envió el mensaje, este nombre puede ser falso, en cambio la dirección IP puede ser un poco más difícil de falsificar y es la que asigna el proveedor de Internet cuando se inicia sesión, la cuenta de acceso al proveedor y al servidor de correo puede ser falsa también.

El mensaje pudo ser enviado por una computadora en el mismo dominio que el servidor SMTP que retransmite el mensaje o no. Para verificar a quién pertenece la dirección IP y encontrar algún tipo de coincidencias entre el remitente y el servidor SMTP, efectuar un *who is* a la dirección IP que aparece en el campo Received.

Acorde a los resultados que devuelve este comando, que indica a quién pertenece la dirección IP, o a qué empresa u organización se le asignó el rango de direcciones IP que incluye la IP sospechosa, generalmente aparecen datos de los responsables del conjunto de direcciones IP, a veces pueden ser datos muy limitados, pero es importante continuar el seguimiento hasta llegar al proveedor de Internet o a la organización que posea la dirección dubitada.

El servidor SMTP cada vez que acepta un mensaje, coloca un nuevo encabezado *Received* al comienzo del mensaje antes de reenviarlo a otro servidor o a una casilla de correo local. El encabezado muestra dónde ha estado el mensaje, cuándo estuvo en un determinado lugar y cuándo fue entregado a su destinatario.

ESTRUCTURA DEL CAMPO RECEIVED

Received: from *string (hostname [host IP address]*

by *recipient host*

with *protocol id message ID*

for *recipient;*

timestamp

String: nombre del host del MTA emisor.

Hostname: nombre del host del MTA emisor si puede ser determinado por medio del dns inverso sobre la dirección IP.

Host ip address: La dirección ip del MTA emisor.

Recipient host: nombre del host del MTA receptor, algunas veces aparece seguido por la versión del software del MTA.

Protocol: El protocolo de transferencia de mensaje.

Message ID: un único *identificador para esta transferencia de mensaje que se puede encontrar en los archivos de registros en el servidor MTA receptor.*

Recipient: la dirección de correo electrónico del receptor.

Timestamp: la fecha y hora en que fue recibido el mensaje por el MTA.

El campo **FROM**: –de–, puede ser una dirección totalmente arbitraria y contener cualquier texto que el remitente desee configurar en su programa de correo electrónico.

Cuando se compara el encabezado *Received* y el encabezado *From* y se determina que no coinciden, esto se puede producir porque el usuario del correo electrónico configuró erróneamente el correo electrónico o porque el usuario está tratando de ocultar su identidad.

Se debe ejecutar el comando "nslookup" a cada uno de los dominios y obtener la información del contacto responsable del dominio, en caso de que exista tal dominio. Otra forma de comprobar su existencia es ejecutar el comando "Telnet" al dominio del correo SMTP y al puerto 25:

Telnet dominio.del.correoSMTP 25

Si el perito informático forense debe investigar un caso en nombre de una víctima, se le debe solicitar a la víctima que reenvíe los mensajes de correo electrónico sospechosos como archivos adjuntos. Si se reenvían directamente, los encabezados son reemplazados por los de la víctima y no los del sospechoso.

Los servidores de correo electrónico SMTP tienen la posibilidad de guardar los registros de todos los mensajes. Por lo tanto, los proveedores de Internet y de correo electrónico pueden ser consultados cuando se rastrea un mensaje. Dado el elevado volumen de tráfico de mensajes que manejan los proveedores de Internet, no suelen almacenar los registros por mucho tiempo, por lo tanto, cuando se efectúa el seguimiento de un mensaje se debe consultar lo más pronto posible al proveedor. Los registros de inicios de sesión ya sea por conexiones de banda ancha o discado telefónico, pueden brindar importante información para comprobar la evidencia.

Aspectos importantes a considerar en el análisis del encabezado del mensaje

El orden de lectura se realiza de abajo hacia arriba.

La cadena de caracteres que aparece delante de los () puede ser falsificada.

Los encabezados *Recibido* brindan información para determinar la ruta del mensaje.

Los campos de identificación única son asignados por cada MTA a través del recorrido de la ruta de entrega del mensaje.

El Identificador del Mensaje –Message ID– , es asignado por el cliente de correo que creó el mensaje.

Este identificador permite buscar un determinado mensaje entre los registros de uno o varios servidores.

Procedimiento

Analizar el primer encabezado *Received* (desde abajo hacia arriba).

Efectuar un *whois*, brinda información de la dirección IP, propietario del registro en ARINAmerican Registry for Internet Numbers –LACNIC (Latin American and Caribbean Internet Addresses Registry)– y DNS reverso de la dirección IP del hostname (lookup) el nombre asociado con la dirección IP. Nombre del contacto del proveedor y responsable.

Ídem con el encabezado del siguiente *Received* y los que correspondan.

Si no existe coincidencia entre los mismos el encabezado ha sido falsificado.

Efectuar el rastreo de SPAM por medio de los registros de los MTA y las direcciones IP.

Utilizar el identificador del mensaje generado en el servidor para encontrar coincidencias.

Herramientas para el análisis del encabezado de correo electrónico

Desde Internet:

www.network-tools.com, sitio que permite ejecutar los comandos (*whois*, nslookup, ping, trace, etc.) de verificación de direcciones IP, nombres de dominios, direcciones de correo electrónico, por medio de una página web.

Linux – Unix whois **dig**

Windows

A:\nslookup nombre.del.dominio

NetScanTools, se pueden ejecutar consultas avanzadas con el comando dig w/AXFR

Visualización de encabezados en diferentes clientes de correo electrónico

La visualización de los encabezados no aparece como una opción predeterminada en los clientes de correo electrónico. Para visualizar el encabezado del mensaje en:

Microsoft Outlook Express

Elegir el mensaje, con el botón derecho del mouse y seleccionar *Propiedades*.

Ficha General se muestra la información elemental del mensaje: Asunto, Remitente, Tipo, Ubicación (carpeta, por ejemplo: Bandeja de Entrada), Tamaño, Prioridad, Fecha y Hora de envío y recepción.

Para ver el contenido del mensaje y los encabezados, en la misma ventana, oprimir el botón Origen del Mensaje.

Se puede seleccionar el contenido de la ventana del código fuente del mensaje, copiarlo y analizarlo luego en un archivo de texto:

Con la herramienta de Internet **www.network-tools.com,** se puede verificar la validez y la existencia de una cuenta de correo electrónico, esta herramienta utiliza los comandos de consulta al servidor de correo y muestra los resultados obtenidos.

Con la herramienta **Telnet**, también se puede consultar la existencia del servidor de correo, verificando los puertos de POP3 y SMTP:

Telnet servidordecorreo.com.ar 25

Telnet servidordecorreo.com.ar 110

Microsoft Outlook Ver Encabezados. Ver Opciones.

En el área Opciones de entrega, Enviar las respuestas a, puede aparecer un nombre no real.

Para obtener la información concreta, oprimir “Ctrl A”, copiar y luego pegar el contenido en un archivo de texto y analizar el contenido.

Nestscape

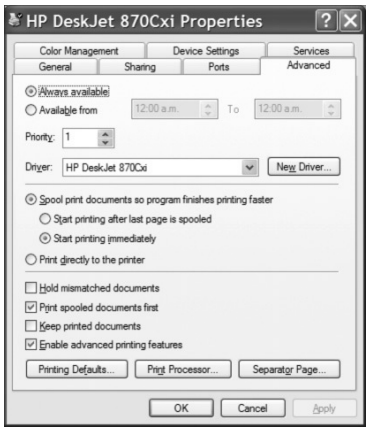
Opciones, Ver encabezados o Ver, Encabezados, Todos.

Eudora

Oprimir el botón de Blab, Blab, Blab.

Verificación de los archivos de impresión

Cuando se configura la impresora con la opción Mantener documentos impresos, desde la opción Propiedades, ficha Avanzada, se almacena una copia del documento impreso con la extensión ".EMF". Por lo tanto se deben buscar los archivos con extensión ".EMF" y analizar el contenido:



Análisis de código malicioso

El perito en informática forense debe conocer los sitios con información actualizada sobre código malicioso:

En el sitio **www.wildlist.org,** se encuentra un listado de los códigos maliciosos actualizados por la Organización Internacional.

Sitios de programas antivirus con la descripción de los distintos tipos de virus:

F-Secure, **www.f-secure.com,** McAfee, **http://www.mcafee.com/es/, Viruslist, www.viruslist.com/sp/**

Preguntas frecuentes sobre virus, **www.faqs.org/faqs/computer-virus**

Listado de aplicaciones y utilidades de exploración de vulnerabilidades, **www.packetstorm. security.com/sniffers**

Listado de código malicioso, **www.packetstorm.security.com/dirtree.htm**

Listado de programas de ruptura de claves y diccionarios, **www.packetstorm.security.com/ Crackers**

Herramientas de Antivirus

Se debe tener por lo menos dos o más versiones de programas antivirus actualizados.

www.symantec.com

www.panda.com

www.clamav.net

Herramientas de control remoto

Productos comerciales

PCAnywhere

Citrix Winframe

System Management Server

No comerciales

BackOrifice, www.nwi.net/~pchelp/bo/bo.htm

Netbus, http://www.netbus.org/

Herramientas exploradoras de red y de vulnerabilidades

SAFESuite, generado por Christopher Klaus, quien creó el primer explorador de vulnerabilidades por línea de comandos, denominado IIS, Internet Security System.

SATAN, System Administrator's Tool for Analysing Network, de Dan Farmer, surge en 1995, efectúa pruebas de un conjunto de direcciones de redes, en forma

activa y metódica, determinando si existen computadoras utilizando estas direcciones y si es así, verifica la existencia de vulnerabilidades. No obstante no es suficientemente poderosa para los hackers.

Nmap, www.nmap.org, es considerada una de las mejores herramientas de exploración de vulnerabilidades. Se caracteriza por actuar en forma escondida o clandestina y de difícil detección por parte de los administradores del sistema. Efectúa el seguimiento de las huellas del conjunto de protocolos de TCP/IP, específicamente de los números de puertos, enviando diferentes tipos de intentos de conexión a la computadora destino. Nmap detecta entre otros datos, la marca y versión del sistema operativo. Es una aplicación propia de los sistemas operativos Unix y Linux. Existe también para Windows NT. Es un producto de *software* libre.

Nessus, www.nessus.org, este explorador de vulnerabilidades es utilizado tanto por los hackers de sombrero blanco como negro. Es una herramienta de Unix y posee una interfaz de tipo Web para su ejecución. Es un producto de *software* libre.

Herramientas rastreadoras de la red o sniffers

Linsniff, es una aplicación de Linux que rastrea claves de los servicios de FTP, Telnet, *Rlogin*

y de las sesiones de correo electrónico.

Tcpdump, es una de las más comunes en los sistemas operativos Unix o Linux. Es una herramienta muy útil de diagnóstico para el análisis del tráfico de la red. Puede almacenar grandes cantidades de información, efectuar filtrados específicos de distintos tipos de datos.

Windump, tiene las características similares a la aplicación Tcpdump, pero es para los sistemas operativos Windows.

Readsmb NThash, rastrea claves de los archivos de sesiones de archivos e impresoras compartidas.

PPTP, rastrea claves de las sesiones de Microsoft de redes privadas virtuales, VPN, Virtual Private Network.

Icq_sniff, rastrea claves de sesiones del protocolo Internet Relay Chat.

Web_sniff, rastra claves de inicios de sesión a páginas web protegidas con claves.

Ebpd, es un servicio de claves de eBay, rastrea claves en forma más específica que un rastreador de web.

Herramientas detector de DDoS (denegación distribuida de servicio)

IDS, Sistema de detección de intrusos (Intruder Detection System), este tipo de aplicaciones son actualizadas y modificadas con frecuencia, acorde a la aparición de nuevas vulnerabilidades o tipo de agresiones, en SANS, **www.sans.org** se puede consultar sobre los nuevos o actualizados programas de IDS tanto para sistemas operativos Unix como para Windows.

Antivirus, programas diseñados para detectar código malicioso. Productos comerciales como Symantec, Panda, McAffee, Trends.

Herramientas bombas lógicas y bombas de tiempo

Este tipo de subrutinas ocultas no son detectables por las aplicaciones de antivirus. Si el programa no se borra a sí mismo luego de ejecutarse, una forma de detectar una bomba de tiempo sería la siguiente:

Utilizar la imagen de la copia del disco de la víctima.

Retroceder el reloj y determinar si el sistema regresa a su normal funcionamiento.

Detectar y eliminar (si es posible) el código malicioso.

Herramientas para el Registro de las acciones efectuadas por teclado y/o mouse

Simple Python Keylogger, http://sourceforge.net/projects/pykeylogger/, KeyLogger, para teclado y / o mouse, para ejecución en modo silencioso o no.

Estos programas permiten registrar las acciones realizadas por el usuario a través de los periféricos como el teclado o el mouse. Se efectúa en modo silencioso, el usuario no detecta la presencia de esta aplicación activa y se controla en forma remota. La información generada la almacena en registros o archivos de texto de fácil análisis. Esta herramienta es de gran utilidad cuando se desea verificar y comprobar cualquier tipo de actividad sospechosa en el sistema. Existen algunos programas simples como *key loggers* o recolectores de pulsaciones del teclado, que guardan información sobre las teclas que son presionadas, hasta otros que guardan imágenes de la pantalla que ve el usuario del computador, o hasta casos donde la máquina es controlada

remotamente.

Herramientas para eliminación de huellas

Después de acceder al sistema, el intruso no desea dejar huellas de su actividad y ejecuta una serie de aplicaciones para ocultar su presencia. A continuación se mencionan algunas de las posibles herramientas utilizadas por el atacante:

Unix Rootkits, en este paquete existen varias utilidades para limpiar los registros y ocultar evidencias de actividad no autorizada:

Wted.

Wtmp editor.

Zz, elimina la entrada del último registro.

Zap/zap2, sobrescriben el último registro de inicio de sesión con ceros. Cubre la pista pero no la oculta.

Cloak2, cambia los datos de inicio de sesión.

Clear, borra las entradas de inicio de sesión.

ACCTHandler, borra los registros de cuenta del sistema.

Unix rootkits, estas herramientas incrementan los privilegios, ocultan actividades o buscan información. Las herramientas de limpieza son utilizadas para manipular el entorno y ocultar la evidencia de la propia intrusión. Las de búsqueda de datos permiten obtener información para ampliar el ataque y las herramientas de modificación de archivos binarios alteran los archivos binarios correctos del sistema operativo, ofrecen una apariencia de funcionamiento normal del sistema, ocultando al administrador lo que está sucediendo realmente, no muestran información de su actividad y ocultan ciertas características en los archivos ejecutables del sistema para obtener controles de acceso.

Chkrootkit, www.chkrootkit.org, para sistemas operativos Linux o Unix, detecta un gran número de diferentes herramientas rootkits.

Para detectar código malicioso en archivos ejecutables, es muy importante que no se ejecute ningún binario desconocido, la única forma de ejecutarlo es en una computadora aislada de la red y con datos no relevantes. A continuación se muestran una serie de tareas para el análisis de código desconocido.

Procedimiento

Intentar leer el archivo

Verificar la fecha

Verificar el nombre

Buscar un código fuente en la misma computadora

Utilizar cadena de caracteres

Utilizar filtros como grep

Utilizar nm, una herramienta de programación para listar la tabla de caracteres

Buscar la asistencia de un programador

Ejecutar el código desconocido en un entorno controlado

Análisis de celulares, PDA, GPS

El análisis informático forense de estos equipos se puede realizar a partir de la información que se encuentra en:

Tarjeta SIM (Subscriber Identity Module [Módulo de identificación del Suscriptor], tarjeta inteligente con procesador especializado en el uso de equipos GSM (Global System for Mobile Communications [Sistema Global para Comunicaciones Móviles]), datos y datos eliminados.

Memoria flash de expansión

El tipo de información a obtener puede ser:

Información básica del dispositivo móvil: Esta información básica está presente en casi todos los dispositivos móviles sin importar la marca o modelo. Representa la información básica de la evidencia para todos los dispositivos. Incluye los siguientes conjuntos de datos:

Teléfonos y contactos del usuario

Registros de llamadas: realizadas, recibidas, perdidas

SMS. Contenidos y registros: enviados, recibidos, guardados

Calendario, agenda, tareas, listas de tareas por realizar

Información avanzada: Incluye todos los formularios y datos almacenados e información creada por el usuario asociada con otras funciones avanzadas del dispositivo. Incluyen típicamente:

Imágenes

Videosclips

Grabaciones de audio

Historial de navegación Web & WAP

Utilización de E-mail y contenido Conectividad Bluetooth

Documentos generados por diferentes aplicaciones de oficina: planillas de cálculo

Cualquier otra información contenida en las funciones avanzadas

Información borrada o eliminada: En muchos casos es posible obtener información básica y avanzada que aparece como borrada por el usuario. Esta información se obtiene directamente del dispositivo de memoria del equipo móvil.

Reconstruir en el laboratorio, si es posible, el entorno del delito o incidente

La reconstrucción es similar a la reconstrucción del hecho en Criminalística. Una opción es utilizar *software* de máquinas virtuales, tal como VMware, producto comercial, www.vmware. com o Virtual box, http://www.virtualbox.org/, de código abierto, tanto para la reconstrucción de los datos de una computadora en forma individual o en un entorno de red, por ejemplo, para simular en este caso los métodos de intrusión. La reconstrucción en el laboratorio con equipos reales es más recomendable que el uso de *software* de máquina virtual, en ambos casos la simulación o reconstrucción requiere de una serie de consideraciones previas, a saber:

La reconstrucción debe efectuarse siguiendo una secuencia planificada previamente, que incluya las evidencias recolectadas.

La reconstrucción de los eventos se debe realizar sobre la misma línea horaria,

especificada en la recolección de la evidencia, tanto del CMOS como la del sistema operativo, verificando las configuraciones de la fecha y hora. En algunos casos los datos de fecha y hora pueden ir variando, acorde a lo recolectado en la evidencia, y en la reconstrucción es necesario ajustar estos cambios para obtener una simulación más adecuada a la ocurrencia del hecho.

Los registros de eventos utilizan una línea de tiempo para indicar la ocurrencia de un evento. Por lo tanto debe existir una coherencia de esta línea horaria y la del sistema, para evitar conclusiones no pertinentes.

Durante la reconstrucción del hecho el perito informático forense debe registrar su propia tabla horaria para su análisis de la evidencia que está simulando, se puede utilizar GMT para la zona horaria, ya que el delito puede involucrar una serie de zonas horarias diferentes y de esta forma se toma un punto de referencia común, facilitando la tarea de la simulación y del análisis.

Según sea el caso a simular, se debe aislar el equipo, por ejemplo, no conectarlo a la red del laboratorio si la simulación no es específicamente de un incidente de red, evitando la generación de errores que no responden al hecho real.

Se debe trabajar sobre una copia de la evidencia o sobre un resguardo, donde las operaciones puedan ser reversibles, es decir, si se cometen errores o producen equivocaciones se puede volver al estado inicial restaurando la copia de resguardo.

Cada acción realizada debe ser documentada, así como, también los resultados.

Las operaciones que se realicen deben poderse repetir y obtener en cada repetición el mismo resultado, de lo contrario podrían esta variando los indicadores de la experimentación y por lo tanto analizando otra situación.

Una vez que se realizó la recolección de evidencia en la simulación, se debe intentar reconstruir los eventos por los que se produjo el delito o incidente.

Documentar la información obtenida en gráficos, diagramas, planillas de cálculo, para su posterior correlación.

Herramientas de software para la simulación virtual

Graficadores, Power Point, Flash

Realidad virtual –3D– Alice http://www.alice.org/, *software* de código abierto que ofrece múltiples objetos y posibilidad de incorporar y personalizar las aplicaciones o

escenas de simulación del lugar del hecho.

Simuladores para las Fuerzas de seguridad – Policía Virtual de la Universidad de Stanford

http://vhil.stanford.edu/mm/2008/police-lineup**.html**

VI Cotejo, correlación de datos y conclusiones

En esta etapa el perito informático forense genera las correlaciones pertinentes para emitir las conclusiones periciales, utilizando la información surgida del análisis e interpretación de los indicios probatorios y la obtenida, en el caso de que se haya realizado, de la reconstrucción y/o simulación del delito o del incidente. Es aquí donde el perito informático forense efectuará la integración de toda la información relacionada con el caso y donde reflejará sus propias aptitudes fundamentadas en el criterio, sentido común, experiencia, conocimientos académicos y capacidades intelectuales, tales como la habilidad para relacionar, transferir, integrar, acotar, deducir, inducir y descartar los datos obtenidos en las etapas periciales anteriores. El éxito del informe pericial se sustenta de manera considerable en la forma en que se establecen las correlaciones y se generan las conclusiones.

El cotejo de los datos implica efectuar comparaciones con los datos originales y los analizados en la evidencia para determinar modificaciones. Es importante efectuar el cotejo y la correlación de los datos en forma metódica, ordenada y precisa. Por lo tanto es necesario descartar aquella información que en la etapa de análisis no apareció como elemento anómalo. Podría ocurrir que luego del análisis de los datos, en esta etapa no se encuentren elementos probatorios incriminantes.

Técnicas posibles a utilizar para el cotejo y correlación de los datos

Tablas

Árboles de decisión

Matrices de decisión

Procedimiento para el cotejo y correlación de los datos Procedimiento

Disponer de toda la información verificada en la etapa de Análisis.

En el caso que la pericia sea originada por una orden judicial, se deberá efectuar una lectura previa de la causa para determinar los dichos de las partes intervinientes.

Ordenar la información disponible y desplegarla para su fácil acceso, específicamente toda aquella información que haya sido impresa.

Acorde a la lectura del material analizado y /o de la causa judicial, formular posibles hipótesis.

Determinar por cada hipótesis el conjunto de variables asociadas.

Utilizar la herramienta que el perito informático forense considere más adecuada para demostrar la hipótesis sugerida. Por ejemplo: elaborar una tabla colocando la hipótesis formulada, las variables asociadas, los datos de cada variable obtenidos en la etapa de análisis, si existe y la prueba indiciaria asociada.

Elaborar una tabla de decisión de la primera variable a cotejar dejándola fija, en la primera columna colocar todas las variables con las que se efectuará el cotejo y la correlación con la variable fija, en otra columna colocar los elementos comunes, en otra elementos derivados, en otra los elementos probatorios asociados, en otra la relación con la hipótesis, en otra las conclusiones del cotejo y correlación.

Aplicar el método del pivot (cada variable de la columna de variables, cotejarla y correlacionarla con la variable fija).

Documentar los resultados obtenidos en la columna de las conclusiones.

Efectuar esta tarea con todas las variables seleccionadas.

Determinar si la hipótesis propuesta ha sido comprobada, no comprobada o faltan datos.

Reunir las conclusiones obtenidas, en caso de que en el paso 8, se haya demostrado la hipótesis, de lo contrario reiniciar el procedimiento desde el paso 4.

A partir de este momento es posible generar las conclusiones.

Procedimiento para la elaboración de las conclusiones Procedimiento

Ordenar las conclusiones obtenidas en el procedimiento de cotejo y correlación.

Asociar a cada conclusión los elementos probatorios y la fundamentación asociada.

Documentar las conclusiones en el informe pericial.

Elementos a cotejar y correlacionar

A continuación se muestra un posible ejemplo de elementos a cotejar y correlacionar, el perito informático forense podrá modificarlo y mejorarlo acorde a los requerimientos periciales particulares. Se efectuarán cotejos y correlaciones de la información analizada en los dispositivos de almacenamiento volátil y no volátil.

Fecha y hora

Variable fecha y hora del sistema, obtenida en el momento de la recolección y cotejarla con:

La fecha y hora del CMOS.

La fecha y hora de modificación, creación, eliminación de archivos, hallados en la memoria volátil y en los dispositivos de almacenamiento secundario.

La fecha y hora de los archivos temporales, de intercambio u ocultos.

La tabla de procesos activos.

Los registros de eventos de seguridad, de aplicaciones y del sistema.

Tablas de enrutamiento

Variable Tablas de enrutamiento, si el incidente ocurre en un entorno de red, cotejar con:

Las rutas entre la computadora dubitada y el resto de las computadoras en la tabla de enrutamiento y las computadoras vecinas.

Las direcciones públicas o privadas de la tabla de enrutamiento, relacionadas con las que tiene asignada la empresa, para determinar, por ejemplo, si el incidente se relaciona con eventos generados desde la propia red interna de la empresa o desde el acceso de la red pública.

La topología lógica y física de la red de la empresa.

Tabla ARP

Variable Tabla ARP, si el incidente ocurre en un entorno de red, cotejar con:

La tabla de direcciones físicas con direcciones físicas de las computadoras vecinas y la propia dirección física de la computadora.

La dirección de origen físico con la de origen lógico, para determinar que la placa de red tiene la dirección física asociada con la dirección lógica que muestra la evidencia, para descartar cualquier modificación de la dirección física o modificación de la dirección lógica, tal como falsificar la dirección IP de la computadora dubitada para efectuar intrusiones.

La topología lógica y física de la red de la empresa.

Tabla de procesos activos

Variable Tabla de procesos activos, cotejar con:

Los servicios o programas por defecto que debe tener activo el sistema operativo dubitado en un estado de normalidad y correlacionarlos con el consumo de recursos de procesador, memoria, memoria caché, fallos de página. En algunos casos para descartar, por ejemplo, una denegación de servicio o uso de programas del tipo rootkit para emular los comandos reales del sistema operativo.

Los servicios o programas instalados en la computadora dubitada y de uso normal y correlacionarlos con programas o procesos activos no comunes y con posibles programas de código malicioso y con los archivos ocultos hallados. Acorde al tipo de código malicioso se determinará cuál o cuáles pudieron haber sido las modificaciones en el sistema y se relacionará con dichos datos.

Los recursos compartidos, en el caso de una red, por medio de la intercomunicación de procesos y correlacionarlo con los usuarios conectados en ese momento, con el esquema de permisos y con la lista de acceso. Para determinar si existieron intrusiones y qué posibles archivos o programas podrían haberse creado, modificado, borrado o accedido.

Los archivos temporales que generan los procesos y el consumo de recursos, de memoria, procesador y disco.

Los registros de eventos de seguridad, del sistema, de las aplicaciones y servicios activos y correlacionarlos con las estadísticas del sistema, los programas no comunes

o de código malicioso, con las conexiones de red activas, con los recursos compartidos y con los usuarios conectados.

El listado de puertos abiertos y de aplicaciones escuchando en dichos puertos, correlacionarlos con los usuarios conectados, los tipos de aplicaciones y la información ofrecida y con las políticas de la empresa y con la planilla del personal a cargo del área comprometida, con el listado del personal que fue despedido o renunció voluntariamente y con el horario de trabajo respectivo.

Los datos obtenidos, en el caso de haberse efectuado, de la simulación o reconstrucción del hecho.

El listado de palabras claves hallados en los dispositivos de almacenamiento volátil y no volátil y correlacionarlo con las aplicaciones no comunes o posibles programas de código malicioso o programas espías o de recolección de información personal.

Tipo de sistema operativo

Variable Tipo de sistema operativo, cotejarla con:

Las debilidades del código fuente propia del sistema operativo y relacionarlas con los procesos de inicio normal y con los programas propios del sistema operativo, para descartar la existencia de programas que emulen los comandos del sistema operativo como las herramientas rootkit.

El sector de arranque, con el esquema de particiones y correlacionarla con el tipo de sistema operativo, los programas de código malicioso, con el ocultamiento de información hallados en el análisis de la evidencia.

Sistemas de Archivos

Variable Sistema de Archivos, cotejarla con:

El listado de todos los archivos encontrados en el sistema, correlacionando la fecha y hora de cada uno con la obtenida del CMOS en la recolección de la evidencia.

Los archivos ocultos, eliminados o perdidos y relacionarlo con las palabras claves, con la fecha y hora de su creación, modificación, eliminación o acceso y correlacionarla con la fecha de sistema, relacionando el contenido con otros archivos

existentes y con los programas instalados.

Los archivos de intercambio o swap y relacionarlo con las palabras claves y las aplicaciones existentes en el sistema.

Las aplicaciones instaladas, con el listado de archivos encontrados en el sistema y relacionar las extensiones con las aplicaciones para determinar la presencia o no de programas de código malicioso.

Los archivos protegidos con claves, ya descifrados y correlacionándolos con las aplicaciones existentes en el disco y con los datos eliminados y /u ocultos.

Los archivos de cada usuario en el directorio raíz y en los subdirectorios, y compararlos con las aplicaciones existentes en el disco y con los archivos recuperados.

Los programas ejecutables definidos como sospechosos, y relacionarlos con técnicas de escucha telefónica, captura de teclas por medio de *hardware* o intercepción radial, captura de imágenes en forma remota, de escucha de celulares o pagers, de identificación oraciones o frases en binario de idiomas extranjeros, falsificación de tarjetas magnéticas archivos con extensión .vba, escritos en Visual Basic. Correlacionar la información con los archivos recuperados, con los archivos y /o datos ocultos hallados.

Resguardo de herramientas de hardware **y** software **utilizados en la pericia**

Cuando el perito informático forense emite las conclusiones de la pericia, debe realizar las tareas de cierre del caso investigado para proteger las evidencias utilizadas y para proteger su propio accionar profesional. Por lo tanto deberá:

Conservar una o más copias del informe pericial realizado, en el laboratorio y / o en otros sitios protegidos.

Almacenar los duplicados de la evidencia analizada, en recipientes que permitan su conservación en el tiempo, por ejemplo, discos rígidos, ópticos, zips, cintas.

Conservar todas las herramientas de *software* y *hardware* utilizadas en la recolección y análisis de la evidencia.

Resguardar las herramientas en el mismo recipiente que la evidencia duplicada

junto con toda la documentación generada y copia del informe pericial.

Identificar el recipiente con los datos de la pericia, nombre del cliente o número de juzgado, causa. Fecha de inicio de la pericia, fecha de finalización, responsables de la pericia. En el caso de su reapertura, indicar los fundamentos y el responsable.

Almacenar en el depósito del laboratorio o en el sitio que le haya asignado el perito o el equipo de trabajo, pudiendo utilizar un área de acceso restringido y protegido, dentro o fuera del laboratorio, como, por ejemplo, en la caja fuerte de un banco.

1 Kruse II, Warren y Heiser, Jay, Computer Forensic: Incident Response Essentials. 1° ed., Addison Wesley Professional. EE.UU., 2001.

2 Schweitzer, Douglas. *Incident Response, Computer Forensic Tool*. Wiley Publishing, EE.UU., 2003.

3 Schweitzer, Douglas. *Incident Response Computer Forensic Tool*, EE.UU., 2003.

4 http://www.rfc-es.org/, http://www.ietf.org/rfc.html

APÉNDICE 1
ESTUDIO DE UN CASO REPRESENTATIVO

Como ejemplo de implementación de las diferentes propuestas de este libro, presentamos un caso hipotético, aunque fundado en diversas situaciones reales en las que nos ha tocado intervenir.

En la actualidad, una gran parte de los contratos comerciales de mediano y bajo monto, se realizan utilizando medios informáticos.1 En especial el mensaje de correo electrónico. En este sentido les presentamos "El contrato de Brujas":

El día sábado 6 de febrero de 2010, a media tarde, un agricultor argentino que cultiva arándanos en la zona del delta y produce jugo a partir de sus frutos, envía un mensaje a un posible comprador ubicado en la localidad Belga de Brujas, con el que ya había realizado operaciones comerciales exitosas con anterioridad, avisándole de su disponibilidad de producto y el precio de venta (se ha producido la oferta, primera condición contractual).

El futuro comprador responde el mismo día, algunas horas más tarde, consultando sobre las condiciones de transporte, oportunidad y tiempos involucrados, manifestando su interés en adquirirlo en su totalidad, si las mismas son convenientes (aquí se inserta la discusión sobre la responsabilidad precontractual y las teorías doctrinarias asociadas).

El vendedor, en la mañana del domingo 7 de febrero, mediante otro mensaje, completa los datos requeridos y afirma que mantendrá reservada la mercadería durante cinco días, ya que los tiempos involucrados con el vencimiento de este producto son muy escasos.

El comprador, siguiendo la misma vía de comunicación, cerca del mediodía acepta la oferta (en este punto ya tenemos contrato, como fuente de obligaciones), que implica abonar el producto, contra entrega en su comercio de la localidad de Brujas.

Dos horas más tarde el vendedor confirma la recepción del pedido, acepta los términos y asegura el envío del producto de inmediato. Este envío se realizará el día lunes 8 a primera hora de la mañana.

Producido el envío y la recepción, el vendedor deja de tener noticias respecto del pago prometido. Luego de enviar al comprador varios mensajes de correo electrónico

reclamando el pago, que no son respondidos, concurre a nuestro estudio a consultar sobre las acciones a seguir para reclamar el pago.

A efectos de determinar la estrategia procesal a seguir, es necesario en primera instancia establecer algunos supuestos generales, que no son de solución sencilla:

En qué momento y lugar se perfecciona o concluye el contrato analizado, aceptado por el comprador mediante el mensaje de correo electrónico, enviado por el comprador el día domingo 7 de febrero al mediodía. Aun en el caso de adherir a la doctrina vigente respecto de la equivalencia entre el correo electrónico y el correo epistolar, al respecto la doctrina se divide en varias teorías:

de la declaración (o manifestación) por cualquier modo que ocurra,[5]

de la expedición (o emisión) del mensaje confirmando la operación,

de la recepción del mensaje confirmando la operación,

de la información, no bastando con la recepción, sino que requiere además que la aceptación haya llegado efectivamente a conocimiento del oferente.

Nuestro Código Civil, a partir del artículo 1154, adhiere a la teoría de la expedición ("*La aceptación sólo hace perfecto el contrato desde que ella se hubiere mandado al proponente")*. Aunque como la mayoría de las normas legales existen al menos dos excepciones a favor de la teoría de la información: En el artículo 1155 *"El aceptante puede retractar su aceptación antes de que haya llegado a conocimiento del proponente"* y en el artículo 1149 porque *"hay caducidad si el ofertante muere o se vuelve incapaz de haber sabido la aceptación"*. En síntesis en nuestro Código, si no hay retratación del aceptante, ni muerte o incapacidad del oferente (arts. 1155 y 1149) el contrato se perfecciona, desde el envío de la aceptación (art. 1154).

No obstante esta característica de nuestro Código Civil, se refiere exclusivamente a los contratos celebrados en país. Nada nos dice de la doctrina aceptada en Bélgica, ni de las relaciones comerciales normatizadas en tratados internacionales bi o multilaterales. De ahí la necesidad de analizar la legislación comparada y determinar la pertinencia real de litigar, la competencia y la jurisdicción asociadas a la misma y las posibilidad de arribar a un buen término para las pretensiones de nuestro consultante. Asimismo es necesario consultar normas comerciales que regulan esta actividad comercial en particular, en este caso las resoluciones y dictámenes de la CAPAB (Cámara Argentina de Productores de Arándanos y otros) que nuclea en nuestro país a la mayoría de los productores de *berries*, de distintas variedades y su homóloga Belga (en el marco de la CE). Este tema es sumamente interesante, pero

excede ampliamente a las intenciones de este libro. Para el caso que consideramos, daremos por perfeccionado el contrato ya que satisface los requisitos de todas las teorías descriptas.

Soslayada, pero no resuelta la cuestión anterior y otras relacionadas con las distintas responsabilidades parciales en cada etapa de la negociación[6] y particularmente con la jurisdicción donde presentaremos la demanda, pasaremos ahora a la producción de la prueba documental informática:

Desde el punto de vista de la prueba documental informática, la primera consideración a tener en cuenta es la necesidad de recolectarla, preservarla y certificarla, lo más pronto posible, ya que por las características antedichas de vulnerabilidad de la misma, en cualquier momento podría ser susceptible de modificación o destrucción por medios locales o remotos, de manera culposa o dolosa, dejándonos sin herramientas probatorias útiles a la hora de presentar la demanda.

La tarea descripta requiere de varias componentes relacionadas y concurrentes: se debe preservar el derecho a la privacidad de los actores involucrados, que contrariamente a lo que podría parecer son tres: el oferente, el aceptante y el ISP (proveedor de servicios de correo electrónico).

En esta etapa sólo es posible actuar sobre los datos almacenados en equipos informáticos del oferente exclusivamente,

En cuanto a sus referentes que obran en poder del ISP, deberán ser ser requeridos, al momento de presentar la demanda, como prueba de informes.

Respecto de los datos obrantes en equipos del aceptante, no pueden ser legalmente accedidos sin orden judicial y como se encuentran en servidores alojados fuera del país (no obligatoriamente en Bélgica, ya que muchas empresas por razones de seguridad informática y financiera, resguardan sus activos informáticos en países considerados “seguros”, respecto de la misma) requieren de un complejo mecanismo internacional, que implica exhortos y otros mecanismos de compatibilización normativa jurídica.[7]

Para efectuar la tarea referida, se requiere la concurrencia de varios actores, a saber: el propietario de la información a recolectar, certificar y resguardar, el técnico que realice la operación, una autoridad certificante de la misma, en nuestro caso un escribano público de la matrícula. Los pasos para realizarla son: determinar fecha y hora de la tarea (con la celeridad que esto implica).

Constituidos en el lugar se debe labrar el acta correspondiente:

Registrar la autorización expresa de nuestro cliente para acceder a sus activos informáticos, con las restricciones que juzgue conveniente establecer, de esta autorización se debe dejar obligatoriamente constancia en el acta.

Proceder a la recolección de todos los mensajes de correo electrónico intercambiados por las partes, descartando los que no tengan relación y pertinencia con los hechos a demandar.[8]

Recolectados los mensajes en presencia del escribano, se resguardan en un medio de almacenamiento externo (generalmente en un CD o DVD, por su comodidad de transporte y operación).

Se procede a su cierre lógico y físico (mecanismo que los sistemas de grabación ya tienen incorporado), para evitar su modificación *a posteriori.*

Se realiza una rutina de firma electrónica sobre los archivos resguardados (utilizando un digesto, basado en una función de *hash o hashing*).6

Se generan las copias necesarias a partir del CD o DVD original producido. Es muy importante tener en cuenta que cualquiera de las copias generada (en las condiciones de preservación procesales y técnicas establecidas), tiene el mismo valor probatorio, ya que no se tratan de copias similares, sino idénticas entre sí. Recordemos que la informática forense se basa entre otros en el principio de identidad impropio (de copias idénticas), que hace indistinguible la copia respecto de su original, ya que un bit, no es similar o igual, sino idéntico a otro bit.

Se resguardan en sobres y se entregan a los actores que lo han requerido (generalmente una copia para el escribano, una para presentar ante el futuro tribunal interventor, otra para el abogado patrocinante y una o dos para el cliente).

Se entregan las copias y se inicia la cadena de custodia correspondiente.

Todas las operaciones realizadas deben ser descriptas e incluidas en el acta protocolar realizada por el escribano en especial los resultados obtenidos mediante el *hashing* efectuado (que no es otra cosa que una cadena numérica).

Se protocoliza el acta y con esto termina el procedimiento de recolección de prueba documental informática, la que luego será presentada junto con la demanda.

A partir de este momento y ya con la prueba resguardada, se comienzan

negociaciones previas a la presentación de la demanda. Debemos recordar que en este caso particular, la mayoría de los comerciantes prefieren un mal negocio comercial, antes que un buen resultado jurisdiccional. La realidad mercantil nos señala que quien fracciona y vende jugo de arándanos en Europa, pretende mantener su clientela y si bien la dilatación del pago (no demasiado oneroso en términos comerciales relativos) puede resultarle momentáneamente beneficioso (la famosa bicicleta comercial que parecemos haber inventado los argentinos, pero que en realidad es bastante frecuente en todas partes), a la larga deberá pagar y preservar la relación o buscarse otro proveedor con los riesgos que esto implica, especialmente considerando las preferencias de su clientela cautiva, que ha se ha acostumbrado a la calidad del producto (cualquiera que ella fuere). En cuanto al vendedor, necesita colocar su producto y mientras logre su objetivo (cobrar), tal vez vea cumplida su pretensión (una especie de medida autosatisfactiva prejudicial). De ahí que estos reclamos es conveniente iniciarlos por medios alternativos de resolución de conflictos y el primero y más evidente es la negociación por parte del abogado patrocinante.

Al presentar la demanda, se acompaña la documental informática recolectada. Esta tarea debería incluir la firma de la cadena de custodia, por parte de quien recepciona los elementos informáticos resguardados. Sin embargo, constituye un auténtico problema en la práctica. Los empleados de barandilla no conocen los protocolos de preservación y transporte de la prueba, normalmente se niegan a firmar, manifestando que alcanza con la recepción de la demanda y la prueba adjunta, en el mejor de los casos, en otros lisa y llanamente se niegan a aceptarla. Para empeorar las cosas, este problema no mejora con la solicitud de concurrencia de las autoridades del tribunal. Si respetamos la naturaleza y condiciones particulares de la documental informática, su operación correcta desde el punto de vista criminalístico e informático sería la siguiente:

Firmar la cadena de custodia (quien entrega y quien recibe), trasladando de esta manera la responsabilidad por su integridad al tribunal interventor, que deberá resguardarla de manera adecuada.

Si el tribunal estima necesaria la apertura del sobre lacrado y sellado, confeccionado por el escribano, este acto debería ser documentado mediante el acto y acta protocolares correspondientes (una diligencia de apertura de prueba) y una vez constatado su contenido, vuelta a cerrar. De este hecho también se debería dejar constancia en el formulario de cadena de custodia. Sin embargo, no se comprende la necesidad de realizar semejante operación. El contenido del sobre ha sido certificado por un escribano, con lo que goza de la credibilidad de un documento público. El *hash* obra en la etiqueta del sobre, el lacre está intacto, el contenido referido en un acta notarial que acompaña al mismo. ¿Qué sentido tiene en esta etapa del proceso abrir el

sobre? Lo ideal sería que dicha apertura se realizara en el momento apropiado que determine el titular del Juzgado o su representante procesal, acorde a las necesidades del proceso.[9]

Simultáneamente, con la entrega de la documental informática, en la demanda se debe incluir una prueba de informes al ISP, para que certifique los mensajes de correo recolectados, su origen, destino y hora GMT. Esta prueba es imprescindible y complementa la tarea de recolección previa. Todos y cada uno de los mensajes contenidos en el CD o DVD deben ser avalados por el proveedor de servicios (ISP), de esta manera su confiabilidad estará asegurada. La solicitud de esta información no transgrede norma legal, ni jurisprudencia alguna, ya que no consiste en informar datos sensibles de los interlocutores, sino en determinar la veracidad en cuanto al momento de intercambio de mensajes, su origen y destino. Es equivalente a solicitarle a una empresa de provisión de servicios telefónicos, constancia de la fecha y hora de comunicación entre dos líneas telefónicas.

En la misma demanda y en subsidio debe solicitarse la correspondiente prueba pericial informático forense, cuyos puntos de pericia principales serán:

Determinar si existe correspondencia entre los elementos recolectados y presentados como prueba documental informática y el informe realizado por el proveedor de servicios (ISP).

Determinar si los archivos que contienen los mensajes de texto preservados ha sido modificado desde su resguardo (comprobación de correspondencia directa entre dichos archivos y el *hash*, que se realizara en el momento de la recolección y que obra en el sobre que contiene el CD o DVD y en el acta el escribano).

En caso de resultar positiva la tarea anterior, describir en detalle, el origen, destino, hora de envío, el objeto (*subject)* y contenido de los mensajes recolectados.

En caso de resultar negativa la tarea de cotejo con el *hash*, establecer la fecha cierta o probable de dicha modificación (esta tarea sólo sirve para deslindar responsabilidades, ya que relaciona la modificación con el momento en que fue alterada de manera culposa o dolosa y normalmente no tiene demasiada pertinencia para la causa, porque no se puede establecer la autoría de dicho accionar).

Sólo resta utilizar las tres pruebas (documental informática, de informes y pericial), en respaldo de nuestra estructura argumental estratégica y táctica.

En el caso que nos ocupa y antes de presentar la demanda, tomamos contacto con el comprador, por supuesto, por medio de un mensaje de correo electrónico, donde le

explicamos la situación imperante y su posible devenir, destacando las características de la prueba recolectada, su pertinencia, las responsabilidades económicas, el deterioro al prestigio financiero, el daño a la imagen comercial, las cargas procesales y la imposibilidad de seguir manteniendo la relación comercial con el vendedor, que provocaba y provocaría este incumplimiento contractual. El comprador, restablecido el diálogo epistolar electrónico con el vendedor, luego de algunas negociaciones y concesiones mutuas, se allanó a las pretensiones de nuestro patrocinado. Se efectuó el pago, mediante una transferencia de fondos virtual (de cuenta a cuenta bancaria). El casó llegó a feliz término y no fue necesario litigar. Actualmente siguen realizando operaciones similares, al parecer con satisfacción mutua.

Es de destacar que este tipo de controversia se encuentra en proceso de crecimiento geométrico, cada vez hay más contratos comerciales que se perfeccionan por este mecanismo u otros similares. Todo aquel que prueba y obtiene resultados satisfactorios, desde la compra de un libro a una Librería Virtual estadounidense, mediante el uso de una tarjeta de crédito, en plan de cuotas, que es enviado desde Francia y se recibe en el hogar, hasta los casos contractuales, como el que nos ocupa, seguramente vuelve a repetir la operación, al menos hasta el primer disgusto. En la actualidad hay contratos que se celebran directamente por medio de una conversación digital en línea *chat,* cuyo origen y destino pueden ser dos computadoras personales de escritorio, *notebooks, netbooks* y hasta teléfonía móvil (teléfonos celulares). Nuestra experiencia nos indica que la mayoría de las controversias que puedan resultar de esta operatoria, finalizan en la etapa prejudicial, por medios alternativos de resolución de conflictos. No obstante, siempre es necesario actuar profesionalmente como si el litigio fuera inevitable, algo que, por el contrario, la mayoría de las veces ocurre con los contratos realizados dentro de la jurisdicción nacional (comprador de vinos en Buenos Aires y vendedor en La Rioja, para nombrar un ejemplo real, que no pudo ser resuelto por otro medio alternativos y finalizó en un proceso judicial).[10]

La expansión de los medios de comunicación portátiles y las necesidades de interacción remotas presentan a los operadores un panorama en el futuro cercano, que los llevará indefectiblemente a involucrase en este tipo de problemática, ya sea como patrocinantes de terceros o como potenciales litigantes a título personal. El asesoramiento empresarial o particular, conlleva la necesidad de la inmediatez, es probable recibir una consulta legal, referida a la validez de ciertas condiciones contractuales, en el mismo momento en que se está formalizando y que dicha consulta llegue directamente a nuestro correo electrónico o a nuestro teléfono móvil. De manera similar, puede contener todos los elementos de un contrato de patrocionio, proponerse, aceptarse, perfeccionarse y cumplirse por este medio. Ésta es una realidad tecnológica a la que el derecho deberá adaptarse y que requiere de la normativa correspondiente de manera inmediata. El futuro tecnológico es imprevisible, la

realidad nos abruma y nos supera. El mecanismo de generación de leyes debe ser participativo, ningún especialista puede pretender haber accedido a "la verdad" respecto de la problemática informática como género y de las pruebas documental y pericial relacionadas como especie. La tarea de crear leyes relacionadas con la gestión informática en todos sus aspectos[11] no debe quedar sólo en manos de los legisladores, sino que requiere la inclusión de operadores del derecho, especialistas en Criminalística y sus homólogos informáticos.

5 Por ejemplo el aceptante le comenta a su contador que ha decidido adquirir el producto y que se preparen para su fraccionamiento y distribución.

6 Por ejemplo, qué efectos y obligaciones genera entre ambas partes la decisión unilateral (pero no discutida por el a la sazón potencial comprador) del vendedor, respecto de reservar el producto durante cinco días, en espera de la respuesta. ¿Qué hubiera ocurrido si el comprador se hubiese retirado de la negociación? ¿Genera esto responsabilidad de resarcir al vendedor por la pérdida de oportunidades, en especial tratándose de un producto perecedero como el que nos atañe? También son temas para la discusión doctrinaria que trascienden a este trabajo.

7 Es un tema poco claro, sobre el cual no hay acuerdo doctrinario y que requiere de un análisis transdisciplinario profundo, que no parece cernirse sobre nuestra realidad jurídica, al menos por el momento. No obstante por la particular característica del derecho de reaccionar muy *a posteriori,* de los cambios tecnológicos, en algún momento deberá producirse. Es una manifestación clara de la contraposición de dos principios: *derecho a la privacidad vs. derecho a la jurisdicción.*

8 De ahí la necesidad de analizar exhaustivamente la prueba recolectada en el momento de efectuar la tarea, para evitar que se filtren mensajes espurios referidos a otros temas, que pudieran generar responsabilidades por daños, al ser agregados sin relación con los hechos controvertidos (por ejemplo, un mensaje de simple salutación entre las partes, que pudiera contener información sensible o dañina contra la imagen personal o comercial de una de las partes).

9 En la práctica ocurre que el empleado de barandilla, con absoluto desparpajo, sin ningún cuidado técnico especial, sin respetar protocolo legal, criminalístico o informático alguno, aun frente a nuestra queja expresa, rompe el sobre, constata que contiene un CD o un DVD y lo vuelve a colocar en su interior, dejando el sobre abierto, la prueba expuesta y sin hacer caso alguno del formulario de cadena de custodia que lo acompaña, formulario éste que en el mejor de los casos se niega a firmar y nos lo devuelve o simplemente lo arroja al cesto de papeles. Aunque parezca exagerado esta forma de actuar constituye la norma y no la excepción, con la que tendremos que lidiar a diario, si queremos que la misma mantenga alguna utilidad procesal. Por supuesto, la prueba así manipulada, podrá ser impugnada, por cualquier experto medianamente formado, simplemente porque fue violada la cadena de custodia y es imposible asegurar la confiabilidad de la información contenida (basta con cambiar el CD o el DVD). Es cierto que siempre resta la copia en poder del escribano, pero su recuperación implicará una serie de trámites, que atentan contra la economía procesal y nada nos asegura que esta copia sufra un tratamiento diferente al que soportara la que entregamos en primera instancia. Estas acciones son equivalentes a recibir una muestra biológica para determinar ADN, preservada en un recipiente refrigerado, abrir el recipiente, extraer el frasco con la muestra, quitar el lacre y el tapón,

sacudirla un poco para ver qué contiene, guardarla destapada en cualquier cajón del Juzgado y devolver el recipiente refrigerado o arrojarlo a la basura. Nuevamente surge la necesidad del trabajo transdisciplinario, especialmente en la formación técnica de los involucrados en las referidas tareas.

10 Litigio que por otra parte no llegó a una sentencia judicial referenciable, ya que una de las partes, luego de una ardua negociación (también por medio de mensajes de correo electrónico), se avino a las pretensiones de la otra y quedó zanjada la cuestión, si bien más de hecho que de derecho. Es por esta razón entre otras, que resulta tan difícil obtener referentes judiciales, donde se haga evidente la pertinencia y aceptación de la prueba documental informática, como parte de la documental anexada a la demanda o sus documentos asociados (contestación de la demanda, reconvención, etc.).

11 En particular es imprescindible la formulación de una ley que reglamente la profesión, su importancia y criticidad la tornan necesaria, al igual que la ley de ejercicio de la medicina o la abogacía. La inclusión específica de la prueba documental informática, en los Códigos de Procedimientos, también es consecuencia de esta necesidad de revisión legislativa.

APÉNDICE 2
PROCEDIMIENTO ANTE LA REQUISITORIA PERICIAL

Toda pericia se realiza sobre la base de una necesidad manifiesta. Sin embargo, el origen de la requisitoria puede ser variado, podemos diferenciar:

Pericias ordenadas por un tribunal de Justicia: En este caso el Juez es quien decide ordenar la pericia.

Ésta puede ser solicitada en etapa de instrucción o de sentencia en los casos de delitos penales y hasta el cierre de la causa para dictar sentencia, puede ser motivo de revisión o ampliación.

En este caso el perito cuenta con el respaldo del tribunal y su labor se facilita desde el soporte legal, ya que actúa por y para el juez.

En el caso de los juicios civiles, es menos probable la interacción directa del juez para solicitar una pericia. El juicio civil se caracteriza por la participación activa de las partes, por medio de sus abogados. Por esta razón, la mayor parte de las veces las medidas probatorias son solicitadas por el abogado del actor o de la demandada. En algunas jurisdicciones, la prueba de cada una de las partes se desglosa del expediente en los llamados "Cuadernos de Prueba".1[12]Estos cuadernos de prueba son cuerpos del expediente separados físicamente del mismo, circunstancia que suele generar inconvenientes a la hora de efectuar la consulta del expediente en ocasión de la aceptación del cargo. Por esa razón, al solicitar el expediente, el perito debe consultar en barandilla, si existen Cuadernos de Prueba y en ese caso revisarlos, porque la requisitoria pericial puede obrar en el Cuerpo Principal del Expediente (Demanda, Contestación de Demanda, Reconvención, Contestación de Reconvención) o en alguno de los precitados cuadernos.

Pericias ordenadas por un tribunal de Justicia a solicitud de la Fiscalía, del abogado defensor o de las partes.

En los juicios penales esta tarea se centra en la fiscalía o el abogado defensor. El perito por razones éticas debería recibir la solicitud a requerimiento del juez y no relacionarse con el fiscal o el abogado defensor. De esta manera se aseguraría la imparcialidad de la opinión. En la práctica se vuelve imposible actuar de esta manera y se hace necesaria una relación directa con los antedichos. Se generan reuniones a efectos de clarificar los puntos periciales e indefectiblemente estas reuniones aportan

puntos de vista parcializados de los hechos ocurridos, con o sin intención por parte de quienes interactúan. Lo cierto es que los seres humanos no pueden desprenderse de sus preconceptos y actuar de manera objetiva, cualesquiera sea el cargo que ocupen.

En materia civil, la solicitud de pericias por las partes es la norma y no la excepción. El juicio civil estimula el accionar de las partes, les fija términos estrictos para presentar la prueba y establece condiciones especiales para el tratamiento de la misma. En razón de lo novedoso de las pericias informático forense, es normal que los puntos de pericia aparezcan poco claros, confusos o directamente inentendibles. El perito no debe aceptar puntos periciales que reciten frases como la siguiente: “las pericias de rigor”, ya que dejan en sus manos el control de la prueba, convirtiendo indirectamente al experto en parte del expediente, lo que se contrapone con la naturaleza de la prueba pericial. En estos casos es conveniente en el momento de aceptar el cargo, solicitar aclaratoria de dichos puntos (véase el modelo de nota en los anexos). Debería evitarse de esta manera el contacto con el abogado de la parte que solicita la pericia, no obstante, los usos y costumbres hacen que esta tan pretendida independencia, autonomía y objetividad pericial en la práctica no sea respetada, ya que es frecuente el llamado de los abogados al perito, ya sea para abonar el adelanto para gastos, o efectuar consultas, o porque simplemente cuando son notificados del pedido de aclaratoria llaman al perito para explicarle qué pretenden y que les diga cómo escribir los puntos de pericia. Es decisión del perito y de sus parámetros éticos el establecer la justa medida de esta relación para evitar ser influenciado por una de partes en detrimento de la otra (la imparcialidad no es una característica propia del ser humano, sino un objetivo al cual tender a partir de nuestra concepción profesional y moral).

Pericias solicitadas por particulares: En este caso, el perito debe actuar de manera especialmente minuciosa, no sólo está en juego su prestigio, sino también su libertad.

La solicitud puede tener diversos motivos, entre ellos:

Actuar como consultor técnico en una causa determinada. En este caso los riesgos son mínimos, porque se debe actuar de igual manera que siendo perito de oficio.

Actuar como consultor técnico, para solicitar medidas previas o preliminares, generalmente *in audita altera pars*; es un tema delicado porque está en juego el derecho de defensa de la contraparte, para mayor dificultad, la contraparte no está presente en el acto de recolección de la prueba y como máximo está siendo representada por un tercero, que difícilmente comprenda la naturaleza de las operaciones técnicas en proceso.[13]

Actuar como asesor técnico, para reunir información sobre los activos informáticos

en una empresa, que involucran datos en poder de dicha empresa o de sus empleados. Éste es un caso complicado y sumamente riesgoso.[14]

Actuar como asesor técnico, para eliminar activos informáticos de manera segura y sin posibilidad de recuperación por medios informático forenses.[15]

Actuar como asesor técnico respecto de operaciones que luego pueden derivar en actos delictivos (delitos informáticos propios e impropios). En este caso, si se logra probar el accionar, difícilmente el experto escape a la imputación por participación necesaria (primaria o secundaria) en el delito que fuere.[16] Reiteramos, siempre hay profesionales dispuestos a todo, pero muchos de ellos terminan observando a la sociedad tras las rejas.

Al ser consultado sobre la posibilidad de realizar una pericia informático forense en una empresa, negocio, institución o local privado, es necesario analizar en profundidad la requisitoria. Escuchar primero la propuesta y luego recién aportar los datos técnicos que la avalen o la rechacen.

Explicar luego los requisitos legales necesarios para efectuar la pericia. Señalar cuáles son válidos y cuáles constituyen una invasión ilegítima a la privacidad del sospechado o lo afectan de manera tal que se pueda constituir un delito, una transgresión a un código o reglamentación en particular, o una actitud antiética para los principios de la empresa, del solicitante o del perito.

Finalizada la explicación y justificación legal, ante la solicitud pericial, se informará al solicitante sobre la pertinencia o no de realizar las tareas técnico periciales pretendidas. El perito puede aceptar o negarse a realizarlas, pero debe evitar dar detalles técnicos sobre los procedimientos a emplear para resolverla, aunque esta pregunta es prácticamente inevitable por parte del solicitante.

El punto anterior es crítico, no se trata de ocultar conocimientos para proteger la impunidad, sino de evitar transgredir la ley por acción indirecta u omisión.

Si el perito acepta la tarea, es suficiente con que el cliente conozca las bases periciales mínimas, para facilitarle al perito el ingreso y el acceso a la prueba documental informática a resguardar. De esta manera se evita que interactúe con la prueba y la modifique de manera intencional o no.

Si la prueba es modificada y luego esta modificación es comprobada *a posteriori,* al ser interrogado, nuestro cliente afirmará que hizo los cambios apoyado en los conocimientos que le aportamos en su momento. Aunque este hecho, en general, no

llegue a producirnos acciones legales en contra de nuestro accionar, nuestro prestigio quedará sumamente afectado. No hay manera de evitar pensar que se trató de una connivencia entre nuestro cliente y nosotros.

Si el perito no acepta la tarea, el cliente, como es natural, intentará buscar a otro profesional que lo haga. Pero si no lo consigue seguramente apelará a su propio ingenio e intentará poner en práctica lo que le enseñamos. Se repetirá entonces la situación señalada en el punto anterior.

Tenga siempre en cuenta que la figura del cómplice es sumamente peligrosa para su accionar, pero aun en el caso en que los conocimientos aportados a quien cometa la falta (o el delito), lo hayan sido sin intención, esta culpa, no deja de ser evidente. Por otra parte, siempre pesa sobre su cabeza la espada del "partícipe necesario (primario o secundario)" y su prestigio, honor y libertad penden de hilos muy delgados. En todos los casos lo mejor es hablar lo menos posible con las partes o los clientes y por el contrario ser sumamente claro, específico y detallado respecto del tribunal interventor.

Es imprescindible analizar en profundidad el objetivo final de la tarea pericial solicitada por un particular a veces será obtener pruebas para una acción legal (lo menos frecuente), otras tendrá por objetivo lograr un trato ventajoso al despedir a un empleado, evitar el fraude económico o el espionaje y muchas otras accionar contra alguien por simple competencia, envidia o rencor. Usted decide, acorde a sus principios éticos, si actuará o no en cada caso, pero siempre debe decidir sobre conocimientos ciertos de los hechos relacionados.

Por último, recuerde que usted puede actuar como asesor de seguridad, sin inconvenientes y dentro de marcos legales y normativas regulatorias claras. Sin embargo, en todo momento debe considerar la separación entre *enseñar para proteger* y *enseñar para transgredir* (o delinquir). Los peritos sabemos que gran parte de nuestro accionar depende de la ignorancia del delincuente. Si el delincuente es experto en el área pericial referida, puede actuar con antelación modificando la prueba para que le resulte beneficiosa y no condenatoria. El sentido común siempre será su mejor auxiliar a la hora de decidir.

12 CPCCN. "Cuadernos de Prueba. Art. 380. En la audiencia del artículo 360 el juez decidirá acerca de la conveniencia y/o necesidad de formar cuadernos separados de la prueba de cada parte, la que en su caso se agregará al expediente al vencimiento del plazo probatorio. *(Artículo sustituido por art. 2° de la Ley N° 25.488, B.O. 22/11/2001.)"*

13 Ésta es una ocasión en la que entran en colisión dos derechos, como mínimo, el derecho a la jurisdicción, por parte de quien pretende resguardar la prueba que confirma su argumentación, a fin de alcanzar la pretensión judicial demandada o por demandar y el derecho de quien posee la información a preservar y disponer de ésta. Ya hemos tratado este tema, pero siempre es bueno reiterar que la información en poder de un tercero no puede ser accedida sin autorización expresa judicial, se trata de una invasión a la privacidad de dicho tercero, equivalente a la violación de domicilio o de correspondencia, de ahí los recaudos a considerar. Al solicitar la medida previa el abogado debe hacer notar la naturaleza, entidad y alcance de su solicitud, explicitando si la información a recolectar se encuentra en poder de su cliente, de la contraparte o de un tercero, para que el juez ordene las medidas que considere necesarias (aprobar o denegar el pedido en forma total o parcial). Muchos operadores del derecho ignoran esta circunstancia, por lo que el perito debe aclararle estos temas para que la excepción jurídica establecida por el juez tenga el alcance necesario y suficiente como para acceder estricta y restrictivamente ni más ni menos a la prueba pretendida.

14 Ahora el problema principal reside en establecer cuáles activos informáticos pertenecen a la empresa y cuáles son propiedad exclusiva de cada empleado. Respecto de los primeros, basta con la autorización (siempre por escrito yreservándose una copia de la misma, ante futuras eventualidades) del dueño de la empresa o su representante legal (apoderado, departamento jurídico, gerente general nacional en las multinacionales o su equivalente nacional), no es suficiente con la autorización de un empleado caracterizado de la misma, cualquiera sea su nivel de decisión. Respecto de los datos propietarios pertenecientes a un empleado, es necesaria la autorización expresa por escrito del mismo o una orden judicial autorizando la irrupción. Algunas empresas pretenden que la autorización es implícita porque las herramientas informáticas que la procesan o resguardan son de propiedad de la empresa, esta afirmación no tiene sustento legal alguno (la jarra puede ser de cualquiera, pero el vino que contiene es del que lo pagó). Otra forma de atacar el mismo problema, consiste en afirmar que el empleado firmó un convenio de confidencialidad y/o de libre disponibilidad de sus archivos informáticos. Este tema es sumamente delicado, es cierto que un contrato entre partes es siempre válido, pero para que esta validez se pueda aducir, el contrato debe ser celebrado por las partes en igualdad de condiciones y con posibilidad de decidir. De ahí el profundo cuestionamiento sobre los contratos de adhesión (uno no decide las condiciones contractuales al solicitar electricidad, una línea telefónica o un servicio de televisión por cable), la desigualdad de las partes es evidente y hay abundante jurisprudencia al respecto. El contrato de confidencialidad firmado por el empleado es nada más y nada menos que un tipo particular de contrato de adhesión, donde el empleado debe optar por firmar o no trabajar. Esta afirmación será siempre aducida por el abogado del empleado en el momento de discutir la validez en la recolección de los datos que lo perjudican. A lo ya dicho se debe agregar que en caso de duda existe un principio general en derecho laboral que expresa algo así como *in dubio pro operario*, que inclina indefectiblemente la balanza hacia el empleado. Es importante que la responsabilidad del experto siempre sea deslindada hacia quien solicita la medida, que se le explique con claridad la entidad jurídica de estos actos, para que decida si desea proseguir o no. Si el experto sigue teniendo dudas, lo mejor que puede hacer es renunciar a la acción solicitada. Entendemos con claridad que a veces en su deseo de colaborar algunos profesionales se exceden en sus atribuciones (lamentablemente lo comprueban cuando el aparato jurídico se apunta hacia ellos y otros lo hacen por simple desidia o falencias éticas, cada uno sabe lo que hace, pero luego no puede afirmar que desconocía la trascendencia de sus actos (un perito es siempre un testigo experto).

15 En este caso en particular, la decisión técnica es sencilla y la decisión personal es compleja. En cuanto a lo técnico es condición necesaria y suficiente el utilizar alguna técnica de borrado seguro certificada por entidades internacionales (normas del FBI) y la tarea se realiza sin inconvenientes. El

problema personal ya es sumamente complicado, puede darse el caso en que la información a borrar (caso muy frecuente en los estudios profesionales de abogados, contadores y otros profesionales), consista en datos sensibles de un cliente o información de una causa. Las razones son múltiples, por ejemplo, en los organismos estatales suele haber información clasificada (reservada, confidencial, secreta o estrictamente confidencial y secreta), al producirse los recambios tecnológicos, las computadoras son entregadas a instituciones de bien público que las recuperan y emplean para su propio servicio (escuelas, centros de atención social, etc.), en este caso los reservorios de información, normalmente discos rígidos fijos magnéticos, deben ser "limpiados" de datos que pudieran ser aprovechados con fines espurios por terceros interesados en el tema. Éste es uno de los casos en que la tarea del experto está perfectamente justificada, se trata de un acto legal y legítimo. Sin embargo no siempre las cosas son tan transparentes y podemos caer en una participación necesaria por eliminar una prueba decisiva para una acción judicial de cualquier tipo. Una solución practicada por ciertos expertos consiste en no realizar la tarea, sino en explicar cómo realizarla (descargan alguno de los aplicativos comerciales del tipo *"Steganos Security Suite"*, hacen que el cliente adquiera la licencia correspondiente y le explican cómo emplearlo, incluyendo algunos otros servicios como valor agregado, caja fuerte digital, correo cifrado, etc.). Aquí la cuestión se vuelve dudosa y puede terminar de cualquier manera. Producido el hecho y destruida la prueba, quien es interrogado sobre la manera en que la realizó, explicará al juez que lo hizo siguiendo las instrucciones que el experto le brindó. Si el juez actúa estrictamente, la cadena causal tiene como eslabón ineludible al experto que asesoró (de contrario su cliente nunca podría haber realizado el borrado seguro de los datos) y por lo tanto es un partícipe necesario (además quien borró los datos es normalmente el acusado y no agrega nada a su acusación, pero no en cuanto al experto se convierte en partícipe necesario). Normalmente los jueces hacen la vista gorda y oídos sordos ante esta circunstancia, salvo que la misma sea demasiado evidente o muestre un accionar doloso pro delictivo (no es lo mismo asesorar a un abogado sobre cómo borrar un directorio con datos de sus clientes, que explicarle a un conocido delincuente cómo acceder a un sistema informático bancario y recuperar los nombres de usuario y las claves de los clientes de dicho banco). Este accionar siempre está suspendido en la cuerda floja, nuevamente será decisión personal del experto el nivel de riesgo que asume, asumiendo por supuesto las responsabilidades que conlleva.

16 Código Penal de la Nación Argentina. PARTICIPACIÓN CRIMINAL

"ARTÍCULO 45. L os que toma sen pa r te en la ejecución del hecho o presta sen a l autor o autores u n au x i l io o cooperación si n los cua les no habr ía pod ido cometerse, tend rá n la pena establecida pa ra el del ito. En la misma pena incurrirán los que hubiesen determinado directamente a otro a cometerlo.

ARTÍCULO 46. Los que cooperen de cualquier otro modo a la ejecución del hecho y los que presten una ayuda posterior cumpliendo promesas anteriores al mismo, serán reprimidos con la pena correspondiente al delito, disminuida de un tercio a la mitad. Si la pena fuere de reclusión perpetua, se aplicará reclusión de quince a veinte años y si fuere de prisión perpetua, se aplicará prisión de diez a quince años.

ARTÍCULO 47. Si de las circunstancias particulares de la causa resultare que el acusado de complicidad no quiso cooperar sino en un hecho menos grave que el cometido por el autor, la pena será aplicada al cómplice solamente en razón del hecho que prometió ejecutar.

Si el hecho no se consumase, la pena del cómplice se determinará conforme a los preceptos de este artículo y a los del título de la tentativa.

ARTÍCULO 48. Las relaciones, circunstancias y calidades personales, cuyo efecto sea disminuir o excluir la penalidad, no tendrán influencia sino respecto al autor o cómplice a quienes correspondan. Tampoco tendrán influencia aquellas cuyo efecto sea agravar la penalidad, salvo el caso en que fueren conocidas por el partícipe.

ARTÍCULO 49. No se considerarán partícipes de los delitos cometidos por la prensa a las personas que solamente prestaren al autor del escrito o grabado la cooperación material necesaria para su publicación, difusión o venta."

APÉNDICE 3
EL MÉTODO SISTÉMICO (RESUMEN)

La metodología de análisis de sistemas,[17] puede dividirse en diferentes ramas, acorde a las necesidades del sistema informático en desarrollo. Es necesario aclarar que la Informática pretende realizar el tratamiento de la información. En nuestra realidad espacio temporal de principios del siglo XXI, la computación en general y la computación basada en silicio en particular, constituyen el instrumento o herramienta más adecuada para los fines de la Informática. Lo contrario no es verdadero. Antes de que se inventaran las computadoras de silicio ya existían técnicas de análisis de información basadas en otros elementos menos sofisticados y actualmente ya se utilizan computadoras biológicas (ADN o proteínas), cuánticas y basadas en distintas fuentes de radiación no electrónica (fotones, partículas), que hacen prever un futuro informático si no prescindente, al menos coexistente con la computadora de silicio. La Informática en ese sentido trasciende a la computación. No así al análisis de sistemas de información.

Entre las diferentes metodologías aplicables al análisis de sistemas de información podemos destacar principalmente las siguientes:

Metodología Aplicaciones

Análisis estructurado Programación estructurada Ingeniería de la Información Bases de datos

Orientación a objetos Programación orientada a objetos

Específicas Computación de ADN, de proteínas, cuántica, fotónica, etc.

De entre las metodologías enumeradas, la que mejor se adapta al problema criminalístico, relacionado con la investigación de la prueba informático forense, es el Análisis estructurado en razón de:

El orden de realización de las distintas etapas de esta metodología, es aplicable a la sucesión de eventos que se producen durante el desarrollo de las actividades periciales

informático forenses.

La etapa de relevamiento de la información aporta instrumentos y herramientas lógicos y físicos, perfectamente adaptables a las diligencias previas a la ejecución de la inspección ocular propiamente dicha.

Los modelos de análisis de la información, asociados con esta metodología, pueden ser perfectamente adaptados al procesamiento de los datos relevados en el lugar del hecho o detectados en los soportes de información analizados. Recordemos que una vez efectuada la labor pericial de recoleccion de datos, es necesario ordenarlos, relacionarlos, evaluarlos e interpretarlos con finalidad reconstructiva. El contar con modelos apropiados para esta labor facilita notoriamente la tarea pericial.

Visión sistémica de la investigación

Si consideramos que una investigación no es otra cosa que una serie de actividades tendientes a resolver un problema específico y acotado, podemos inferir que la metodología sistémica es una de las más apropiadas y actualizadas para encarar dicha tarea. Esta visión aparecerá a todo lo largo de nuestro curso y es el fundamento de la planificación metodológica de cualquier investigación que se decida iniciar.

La visión sistémica será el sustrato sobre el cual se apoyarán tanto el *análisis*, como el *diseño* y la *implementación* de la investigación. Los métodos clásicos de *inducción, deducción* y *abducción*, todos ellos reunidos en el *método científico*, constituyen herramientas ineludibles y básicas a la hora de investigar, pero la planificación general es sistémica.

En general es posible reducir los pasos de la metodología de sistemas para una investigación a cuatro etapas: a) Análisis, b) Diseño, c) Implementación y d) Retroalimentación, adecuadas al siguiente esquema general:

Análisis

Determinación del alcance y propósito de la investigación.

Objetivos de la investigación.

Especificación de objetivos.

Determinación de variables.

Funciones principales a resolver.

Aspectos de funcionamiento.

Restricciones metodológicas y técnicas.

Investigación operativa.

Diseño

Estimaciones del proyecto de investigación.

Datos históricos a reunir.

Técnicas de estimación.

Estimaciones.

Riesgos del proyecto de investigación.

Análisis del riesgo.

Identificación.

Estimación.

Evaluación.

Gestión del riesgo.

Opciones de aversión al riesgo.

Procedimientos de supervisión del riesgo.

Planificación

Estructura de descomposición de tareas (Diagramas de flujo de actividades)

Red de tareas.

Diagrama temporal (Gantt).

Tabla de recursos.

Personas.

Equipos.

Especiales.

Personal.

Estructura de equipos.

Información de gestión.

Implementación

Ejecución de la investigación.

Mecanismos de seguimiento.

Mecanismos de control.

Retroalimentación.

Determinación de nuevos interrogantes.

Planificación de nuevas investigaciones.

Entrevista previa o licitación

La primera tarea que se relaciona con el desarrollo de un sistema de información computable, consiste en una entrevista con el futuro cliente o con la participación en una licitación con sus correspondientes especificaciones técnicas.

Estos hechos dan lugar a dos situaciones diferentes:

Sistema a pedido de un cliente: En este caso deberemos actuar profesionalmente en dos sentidos, como analistas de sistemas y como asesores del cliente. Quien nos contrata no siempre tiene conocimientos profundos de Informática y por lo tanto la entrevista sirve especialmente para interpretar el pedido del cliente, establecer qué cosas son factibles y qué cosas son producto de su imaginación o de una mala interpretación de otros sistemas que ha visto en funcionamiento.

Una vez realizada la entrevista, el analista de sistemas sabe aproximadamente a qué atenerse y puede generar un modelo aproximado del sistema solicitado.

Este caso se parece mucho a la solicitud de nuestra labor como peritos informático forenses, por parte de clientes particulares (empresarios, industriales, profesionales), que desean utilizar nuestros servicios para clarificar determinados hechos puntuales que los afectan. Estos hechos pueden estar relacionados o no con actividades delictivas por parte de empleados de nuestro cliente. Es imprescindible que le hagamos comprender qué cosas podemos hacer, qué cosas podemos hacer sólo a partir de una orden judidial y qué cosas no debemos hacer en ninguna circunstancia. Esto evitará que participemos voluntariamente en la ejecución de un delito por ignorancia en la requisitoria del cliente (somos testigos expertos, no podemos alegar ignorancia de la ley). Es necesario explicarle con claridad la naturaleza de nuestra tarea, nuestras capacidades y limitaciones (especialmente las legales) y de qué manera podemos actuar para brindarle una solución factible, legítima y legal. Muchas veces esta entrevista terminará en una decisión del cliente que hará innecesaria nuestra labor pericial (decide echar al empleado por los métodos previstos y sin acusaciones o hacer una denuncia policial, penal, civil o administrativa o simplemente dejar de lado el problema, para no enfrentarse con mayores dificultades). Es cierto que hemos perdido un trabajo remunerado, pero también lo es que hemos evitado movernos al borde de la ley, lo que también es extensible a nuestro cliente. No estamos tratando un problema ético (que siempre dependerá del individuo en cuestión), sino un problema legal, la figura del partícipe necesario, casi siempre nos alcanza, si no ajustamos nuestro accionar estrictamente al marco legal correspondiente. En general requiere medios de certificación externa de nuestra actividad. Ej.: *"Siempre es conveniente labrar un acta en presencia de un escribano público, a efectos de dejar constancia de las actividades realizadas, material evaluado y origen de la requisitoria, para deslindar responsabilidades posteriores".*

Licitación: En este caso una empresa solicita un determinado sistema informático y por diversos medios genera pliegos que establecen estrictamente la estructura del sistema, sus prestaciones, sus componentes físicos (edilicios y de harware), lógicos (programas) y de recursos humanos (capacitación y soporte técnico). Es el caso ideal para el profesional. Tiene todo definido y sabe a qué atenerse. Todo es cuestión de competir en relación con los tiempos de desarrollo, la capacidad tecnológica y los precios. Una vez obtenida la licitación, ninguna de las partes debería tener dudas respecto de las actividades a desarrollar.

En nuestra labor informático forense, este caso se parece específicamente a la designación como perito oficial o como perito de oficio. Somos llamados para resolver una cuestión pericial perfectamente determinada por orden del tribunal interventor y generalmente a pedido de las partes. La requisitoria pericial obrante en autos es determinante de nuestra actividad, sus autorizaciones y limitaciones. Normalmente nos aporta las herramientas necesarias para realizar nuestra tarea, con el

auxilio de las Fuerzas de Seguridad (Fuerza Pública), que nos brindarán cooperación, asistencia y seguridad física, durante el desarrollo de nuestras tareas periciales. En estos casos podemos desentendernos un poco de la problemática legal en lo formal y dedicarnos plenamente a nuestra actividad profesional.

No obstante, los casos planteados en el apartado anterior son casos puros e ideales, pocas veces nos encontraremos con ellos, debemos considerar los casos mixtos que dan lugar a distintas situaciones diversas, pero previsibles:

Somos llamados para actuar como consultores técnicos o peritos de partes (a solicitud de las partes). Aunque nuestra actividad profesional debería ajustarse estrictamente a la tarea pericial, es indudable que a la vista general no aparecemos tan imparciales, como ante la designación oficial o de oficio. Somos peritos (expertos), pero el grado de credibilidad se resiente. En estos casos debemos actuar con sumo cuidado, ya que los ojos del tribunal y de las partes involucradas estarán fijos en nuestra tarea y prontos a atacar sus vulnerabilidades. En estos casos la interacción con el abogado de la parte que solicita la pericia es inevitable, pero deberíamos restringir nuestras reuniones a las necesarias para comprender la naturaleza de la requisitoria pericial solicitada, clarificarla y sugerir al perito los puntos específicos de pericia necesarios para demostrar su punto de vista.

Somos llamados para actuar como peritos oficiales o de oficio, pero la requisitoria pericial es poco clara. Esto es bastante frecuente. La carrera de abogacía no forma específicamente a sus estudiantes en la naturaleza de la labor pericial (entendiéndose como tal todas las especialidades criminalísticas), por lo tanto las requisitorias periciales se fundan generalmente en el análisis de casos similares y jurisprudencia y terminan siendo simples copias con pedidos generales y poco específicos. En general si trabajamos en fuero penal, las requisitorias son claras, pero en el fuero civil suelen ser sumamente ambiguas. En estos casos al solicitar aclaración, los mismos empleados en el mostrador, nos sugieren tomar contacto con el abogado. Esta práctica no es recomendable, ya que implica una entrevista con el abogado de partes, que por supuesto intentará influir en nuestra visión previa de los elementos a evaluar. Por otra parte, es probable que necesitemos adelantos para gastos (las pericias se pagan mucho tiempo después de realizadas y suelen resultar incobrables), lo mejor es solicitarlo al tribunal interventor. Todo contacto con el abogado de partes afectará nuestra credibilidad.

Si nos atenemos a la normativa legal, el perito no debería tener contacto con las partes, salvo que sea llamado como perito de partes. Esta forma de actuar asegura la imparcialidad del perito, que actúa realmente sin condicionamientos previos, limitándose a analizar la requisitoria pericial y los actuados hasta el momento de la

misma. Sin embargo los tribunales se encuentran sobrecargados de tareas, las pericias en el fuero civil, son generalmente a instancia de las partes y las diligencias necesarias para clarificar los puntos de pericias entre otras, si son efectuadas por medio del tribunal, retrasan sobremanera el diligenciado de los expedientes. Esta razón no debería ser suficiente para incentivar los contactos entre los peritos y los abogados, pero lamentablemente son la única solución efectiva implementable. Cada profesional, según sus propios criterios éticos, sabrá cómo reaccionar ante estas circunstancias.

Resumiendo: Antes de comenzar la tarea pericial es necesario reunir la mayor cantidad de información posible, esto se logra realizando un profundo estudio de los autos que motivan la requisitoria pericial (en caso de ser designados como peritos oficiales o de oficio) y/o mediante la entrevista de las personas que hayan solicitado la tarea (para los casos de ser nombrados peritos de partes o de un cliente particular).

Relevamiento de la información

La metodología de análisis de sistemas implica una serie de etapas. La primera de ellas consiste en el relevamiento de la información disponible. Este relevamiento será consecuencia de la lectura de los autos y/o de la entrevista con las partes o cliente de referencias.

El tratamiento de esta información implica:

Reunión de la información. Se refiere específicamente a la toma de notas, apuntes, grabaciones y cualquier otro método de registro, que nos permita analizar la información relevada, *a posteriori* y con fines únicamente de recopilación.

Clasificación de la información. En general se emplean dos métodos sucesivos, un ordenamiento por temas (situación edilicia, componentes electrónicos de almacenamiento, procesamiento y distribución de la información, componentes lógicos de los sistemas analizados, recursos humanos que interactúan con el sistema) y un ordenamiento posterior por fecha, que permiten obtener una visión clara sobre la evolución del sistema a analizar.

Interpretación de la información. Implica una integración funcional de los elementos anteriores. Es muy similar a un DER, pero con ciertas modificaciones, las burbujas representan los elementos clasificados en el punto 2, mientras que las flechas que las unen señalan las relaciones entre los distintos componentes del sistema.

A partir del punto anterior es necesario realizar una estimación de las acciones a realizar para acceder a la prueba, identificarla, resguardarla y trasladarla hasta nuestro laboratorio. Esta estimación debe ser realizada en forma ordenada y con una clara planificación de tiempos y recursos involucrados (fecha y hora de la irrupción o acceso al lugar, recorridos probables, recursos de apoyo como ser Fuerzas de Seguridad, escribanos, fiscales, abogados). Es conveniente realizar un diagrama de Gantt para este punto de la tarea. Este Gantt debe ser complementario de un Diagrama PERT general para el desarrollo de la actividad pericial en su totalidad, considerando los tiempos necesarios para cada tarea y los vencimientos legales involucrados (plazo máximo de entrega de la pericia, solicitud de postergación, etc.).

Selección de la metodología de análisis

Por lo expuesto anteriormente, se hace evidente que la metodología a utilizar en la casi totalidad de los casos es el Análisis estructurado, adaptado a la metodología pericial:

El análisis estructurado se basa en una serie de diagramas que permiten realizar un seguimiento claro de los diferentes estados y etapas que afectan a la información procesada.

En este punto es necesario utilizarlo como herramienta de modelado de datos. Al llegar al lugar es imprescindible efectuar modelos orientados a comprender claramente los mecanismos que obran en la estructura analizada. Al respecto debemos efectuar:

Un diagrama de flujo de datos con el mayor detalle posible.

Un diagrama de comunicaciones (redes) por donde circula la información accedida.

Un diagrama de almacenamiento de información (considerando recursos locales, remotos y dispositivos de resguardo *backup* de la información).

Un inventario detallado de los componentes físicos *hardware* que interactúan en el procesamiento de la información.

Seguidamente es necesario realizar un modelo de flujo de control, las especificaciones de control y procesamiento. Este modelo es de suma utilidad para comprender las responsabilidades en la manipulación, procesamientos, distribución o resguardo de la información, a partir de la prueba indiciaria informático forense.

Generación del modelo conceptual

El primer modelo a desarrollar es el modelo conceptual. En el caso específico de la Informática Forense, este modelo conceptual debe reunir los distintos aspectos involucrados con la investigación propuesta, a saber:

Componentes edilicios, instrumentos, programas y recursos humanos involucrados.

Relaciones *a priori*, deducidas a partir del análisis previo de la causa, los comentarios de los restantes peritos y las manifestaciones de las partes.

Con los elementos anteriores se desarrolla un modelo tentativo en el que se debe conceptualizar al más alto nivel y con un mínimo detalle la visión general de la problemática propuesta.

Consiste en un modelo general de comportamiento y relaciones entre las entidades involucradas en la investigación propuesta.

No pasa de ser un gráfico previo, tentativo, perfectible y que seguramente se modificará como consecuencia de la investigación en desarrollo.

Generación de los modelos complementarios

El modelo conceptual aporta al informático una visión general, y a vuelo de pájaro, de la problemática analizada, no obstante no es suficiente para analizar la información en detalle, ni para interactuar con otros peritos presentes en el lugar, por esta razón es necesario realizar otros modelos complementarios con un mayor nivel de detalle, como ser:

1. Modelo edilicio: Consiste en la reunión de los componentes planimétricos y fotográficos, que permitan situar de manera adecuada las pruebas periciales analizadas o secuestradas. Se deben incluir los sistemas físicos de control de acceso y los mecanismos de seguridad física y lógica detectados. Debe complementarse con una descripción somera de la posible secuencia temporal de detección, relevamiento, protección y secuestro de la prueba.

2. Modelo de red: Es complementario del anterior y determina los componentes, posiciones y relaciones entre los elementos de conectividad del sistema analizado.

3. Modelo de datos: Describe las estructuras de datos detectadas y sus

interrelaciones. Incluye las descripciones de alto nivel de las estructuras lógicas de administración de datos (Intra- net, Extranet, VPN, etc.).

4. Modelo de seguridad: Es imprescindible y describe los componentes de seguridad detec- tados. Es necesario diferenciar entre los componentes de seguridad generales de la red (Fi- rewalls, antivirus y otras estructuras de seguridad) y los componentes individuales de pro- teccion (Steganos, AntiSpy, Adaware, antivirus, sistemas de borrado seguro). Cuanto más abundantes sean estos últimos elementos, más dificil será nuestra tarea y más cuidadosos debemos ser.

5. Documentación complementaria: De ser posible, solicitar la documentación de los siste- mas en uso en el lugar, incluyendo los manuales de administración y de usuarios. Siempre que esté disponible deben consultarse las políticas de seguridad establecidas (formales e informales) y su grado de implementación y auditoría.

Programación y codificación

En este punto se analizarán las aplicaciones y programas particulares del sector analizado. Es de suma importancia comprobar las correlaciones existentes entre la documentación del sistema aportada y el funcionamiento de las aplicaciones en particular. Esta actividad se evi- dencia particularmente relevante, ya que implica la detección de posibles modificaciones por parte de los usuarios del sistema, a efectos de vulnerar mecanismos de seguridad implemen- tados, evitar el cumplimiento de normas, eliminar trazas de la actividad realizada y toda otra circunstancia que facilite la impunidad delictiva.

No siempre el único involucrado es el usuario final. Si estamos en presencia de espionaje industrial es normal que exista una estructura de recursos humanos (explícita o implícita) que por diversas razones participa de los hechos (problemas monetarios, resentimientos, envidias, competencias, etc.). Como la prueba informático forense posee características propias que la re- lacionan con las metodologías sistémicas involucradas, deben ser consideradas desde un punto de vista particular. En Criminalística, en general, cuanto más individual es un delito, más difícil resulta obtener pruebas de éste. El asesino al volante de un auto hurtado, sin patentes o con pa- tentes falsas, que altas horas de la noche se aproxima a un solitario paseante sin ninguna relación más que la casualidad, lo apuñala y luego abandona el vehículo, arroja el arma desde un puente, vuelve a su vida normal y no reincide, es prácticamente imposible de detectar. Sin embargo el caso anterior es muy hipotético, la actividad criminal es efectuada por hombres, los hombres son falibles, descuidados

y charlatanes en diversa medida. Un secreto entre dos, es lo mismo que ningún secreto. Pero en Informática Forense la actividad delictiva de un individuo aislado deja trazas conducentes en un único sentido, mientras que la actividad asociada genera distin- tos caminos de investigación. Esta diversificación complica aún más la investigación informá- tico forense y se suma a la característica única de la prueba consistente en su indeterminación ante las copias (una copia no es igual, sino idéntica al original).

Por estas razones es necesario analizar en profundidad las modificaciones efectuadas sobre el software de base o de aplicación, que permitan inferir la comisión de un delito o el ocultamiento de sus rastros.

Prueba y ejecución en paralelo

En esta etapa es necesario controlar los procesos que se encuentran en estado de produc- ción y funcionamiento definitivo y aquellos que forman parte del desarrollo, ya sea que estén funcionando en paralelo o no.

Nuestra actividad pericial puede hallarse restrigida a un equipo en particular o involucrar diferentes componentes del sistema analizado. En ambos casos es necesario analizar el sistema en su totalidad, con la máxima profundidad posible. Esta requisitoria se funda en un viejo con- cepto que establece que el todo suele ser superior a la suma de las partes. De la misma manera en que un avión es algo más que la suma de las partes, ya que puede volar y las partes aisladas no, un sistema informático es una entidad interrelacionada con componentes físicos, lógicos y humanos.

Esta interacción, puede generar modificaciones a la estructura y cronologías supuestas a priori. El establecer que determinada conexión de red permite el acceso a la máquina cuestio- nada, no sólo por parte del administrador, sino también por otras personas, puede implicar que ciertas pruebas han sido “plantadas” en el lugar, con el objeto de inculpar a determinada perso- na. De la misma manera una vía de de acceso al sistema, accidentalmente abierta (por ejemplo, una carpeta compartida con todo el mundo) puede ser un error atribuible a la impericia de un empleado, o una puerta abierta intencionalmente por otro o un elemento generado por el pro- pietario de ese puesto de trabajo, a efectos de deslindar su responsabilidad, generando al menos una duda razonable sobre la autoría de los hechos investigados (puede funcionar como puerta de entrada, como puerta de salida o como coartada entre otras posibilidades).

Si existen aplicaciones particulares en funcionamiento, compare las mismas con las que obran en otras máquinas del sector o del ámbito analizado. Compruebe las diferencias entre las distintas personalizaciones, opciones y seteos. Trata de formarse un perfil de usuario del sospechoso o de las personas involucradas, incluyendo al acusador y los posibles testigos. Si usted es coherente con su profesión, debe intentar revenir los hechos ocurridos de la manera más precisa posible e integrarlos en un argumento comprobable (el guión de la reconstrucción del hecho, grado de participación y responsabilidades de los distintos actores detectados).

Capacitación, supervisión y soporte de la aplicación

Reúna toda la información disponible respecto de la capacitación de los actores en el área informática (cursos, carreras, especializaciones, certificaciones). No siempre la primera impresión es valedera. Detrás de un simple operador de computadora personal puede usted encon- trarse con un experto hacker o con un hábil delincuente informático.

La delincuencia no tiene preferencias sexuales, culturales, formativas, sociales o económi- cas. Una prueba evidente de esto los constituyen los delitos relacionados con abusos sexuales de menores. En una gran mayoría se producen dentro de la familia, involucrando todos los niveles de parentesco reconocidos, esto se hace extensivo al ambiente escolar y a los entornos religiosos. No siempre el abuelito que sostiene en la rodilla a la nietita es tan dulce, ni tan inocente, ni tan cariñoso como parece (al menos en el sentido en que lo estimarían los padres). A esto se suma la natural aversión del ser humano hacia la verdad, la mayoría prefiere autoengañarse, antes que reconocer la homosexualidad de un hijo, o su afección a las drogas o su carácter de delincuente. En muchos casos las personas prefieren callar y disimular para preservar la imagen de la familia aun a costa de la salud física y psíquica de sus hijos. Si transferimos estos hechos, la principal regla es “no prejuzgar”. Cuando actuamos como peritos todos son culpables hasta que com- probemos su inocencia. No existen los “tontos” a priori, ni todas las secretarias son torpes para operar los sistemas, es preferible pecar de desconfiado, antes que ser engañado en el origen de una prueba real o supuesta.

Una vez establecido el perfil probable del sospechoso y su entorno, busque identificar sus rasgos principales en las diferentes personalizaciones que ha hecho de las herramientas que utiliza. Busque testimonios creíbles y desinteresados, no descarte a las personas relacionadas por un motivo distinto del específicamente informático (porteros, cuidadores de playas de es- tacionamiento, telefonistas), todos pueden ser

una fuente de información adecuada que agre- gue datos de interés a la investigación o permita avanzar en ésta.

Es necesario entrevistar e interactuar con los responsables del soporte técnico del área, in- tentando determinar las razones principales de consulta del usuario en particular, los proble- mas que ha tenido, las fallas de hardware y software que ha denunciado. El resultado alcanzado luego de analizada la falla y la solución implementada en cada caso. Especialmente en lo re- lacionado con transgresiones de seguridad intencionales o dolosas. Pida y escuche la opinión de quien realiza el soporte técnico, pero no la crea a pie juntillas, recuerde que el delincuente tiende a disimular su personalidad y sus características psicológicas particulares, con el objeto de pasar lo más inadvertido posible. Cuando un empleado manfiesta a voces ser un hacker, generalmente no lo es. El auténtico hacker y su contrapartida el cracker, no se "agranda" por adelantado, prefiere hacerlo al finalizar su tarea.

De la misma manera, entreviste a las personas responsables de la auditoría de sistemas. Solicite la documentación correspondiente a los resultados de las últimas auditorías. Analícelos en profundidad, especialmente las violaciones "accidentales" de seguridad que involucren al sospechoso. También debe analizar las que no involucren al sospechoso, para establecer si se encuentran intrínseca o extrínsecamente relacionadas. Sospeche de toda relación directa con el imputado, analice la información que transmite y la que envía. Si se lo permiten y no trans- grede normas legales o de la empresa, lea e interprete la correspondencia del sospechoso en busca de elementos probatorios complementarios. Recuerde que como profesional usted se ha sometido voluntariamente a un código de ética. La información personal de las personas que haya accedido debe mantenerse como "secreto profesional" y no se considerará salvo en rela- ción con el hecho investigado. Aunque suene violento, recuerde que "usted es un investigador y un experto al servicio de la ley, no un alcahuete".

Retroalimentación

Cuando finalice con las tareas anteriores revise nuevamente el modelo conceptual que efectuara en la primera etapa y a partir de él la totalidad de los pasos que hemos descripto. No podemos decirle cuántas veces deberá realizar estas revisiones. Dicha cantidad está relaciona- da con su propia experiencia profesional y con el grado de complejidad de los hechos inves- tigados. Sea paciente, actúe sin prisa pero sin pausa y trate de mantener en todo momento la imparcialidad. Si los hechos llegan a afectarlo de manera particular y nota que está tomando parte en el asunto, es preferible que

abandone el caso. Si prosigue en éste y se deja llevar por sus sentimientos, es muy probable que arribe a conclusiones y resultados erróneos, prejuiciosos, parciales, incompletos y/o tendenciosos.

La retroalimentación no termina nunca. Cada vez que repasamos nuestras labores pericia- les en el pasado nos damos cuenta de más cosas que deberíamos haber ampliado o realizado de otra manera. No obstante, usted debe ponerle un punto final a la investigación y debe expresar esta decisión por escrito. De esta manera será responsable de los datos adquiridos hasta el mo- mento de dar por terminada la investigación, pero no de los posteriores.

Síntesis

Como ya dijimos es posible reducir los pasos de la metodología de sistemas para una in- vestigación a cuatro etapas: a) Análisis, b) Diseño, c) Implementación y d) Retroalimentación, adecuadas al siguiente esquema general:

1. Análisis

a. Determinación del alcance y propósito de la investigación.

b. Objetivos de la investigación.

i. Especificación de objetivos.

ii. Determinación de variables.

iii. Funciones principales a resolver.

iv. Aspectos de funcionamiento.

v. Restricciones metodológicas y técnicas.

vi. Investigación operativa.

2. Diseño

a. Estimaciones del proyecto de investigación.

b. Datos históricos a reunir.

c. Técnicas de estimación.

d. Estimaciones.

e. Riesgos del proyecto de investigación.

i. Análisis del riesgo.

ii. Gestión del riesgo.

1. Identificación.

2. Estimación.

3. Evaluación.

1. Opciones de aversión al riesgo.

2. Procedimientos de supervisión del riesgo.

f. Planificación

i. Estructura de descomposición de tareas (Diagramas de flujo de actividades)

ii. Red de tareas.

iii. Diagrama temporal (Gantt).

iv. Tabla de recursos.

v. Personal.

3. Implementación

1. Personas.

2. Equipos.

3. Especiales.

1. Estructura de equipos.

2. Información de gestión.

a. Ejecución de la investigación.

b. Mecanismos de seguimiento.

c. Mecanismos de control.

4. Retroalimentación.

a. Determinación de nuevos interrogantes.

b. Planificación de nuevas investigaciones.

Estos puntos deben ser tenidos en cuenta específicamente antes de cada investigación en general y de cada pericia informático forense en particular. Algunos aparecerán como redun- dantes o innecesarios acorde a las características del trabajo a desarrollar, pero no podemos ignorar su existencia. Son las herramientas que nos permitirán efectuar un trabajo sistémico metodológicamente estructurado y sistemáticamente fundamentado.

17 Para ajustar el vocabulario, consideraremos como sistema a *un conjunto de elementos relacionados*. Algunos autores agregan que debe tener un objetivo, motivo o fin determinado. No compartimos esa idea en su totalidad, ya que el concepto de finalidad es una concepción puramente humana. Los planetas han girado alrededor del Sol desde mucho tiempo antes que aparecieran las leyes de Kepler. Estas leyes son un modelo humano para representar e interpretar el movimiento planetario, pero la realidad es que los planetas se mueven simplemente, como se mueven los planetas (con o sin leyes que los expliquen). La matemática es una herramienta de modelado humana y nada más que eso. Sin embargo en lo referente a este capítulo, nos referimos a sistemas de información, por lo general, implementables computacionalmente. (No al sistema digestivo, ni al sistema nervioso, ni al sistema solar.)

APÉNDICE 4
INFORMACIÓN COMPLEMENTARIA

Requisitoria pericial

Al respecto recordemos que la requisitoria puede provenir de:

1. Una autoridad judicial, en caso de actuar como peritos oficiales. En este caso las restriccio- nes son mínimas ya que nos hallamos insertos en un organismo oficial de apoyo a la inves- tigación judicial. La única caracterísitica especial a tener en cuenta es que la aceptación del cargo se da por sentada con la designación como perito.

2. Una autoridad judicial, en caso de actuar como perito de oficio. En este caso es necesario considerar:

a. Poseer un domicilio legal dentro de la jurisdicción del tribunal que lo designa. La solu- ción más común entre los peritos es alquilar una casilla de recepción de corresponden- cia, en algún lugar próximo a la sede judicial. Este servicio casi siempre está disponible en manos de particulares u oficinas especializadas que por muy poco dinero alquilan su dirección para recibir correspondencia (de todo tipo de profesionales relacionados con la labor judicial) y que generalmente incluyen el aviso de recepción de cédulas u otros documentos oficiales por medio de correo electrónico, por teléfono o por consulta en línea en una página electrónica. Es la solución más adecuada para evitar las posibles pérdidas de documentación, extravíos o atrasos en la notificación de llegada, que vie- nen implícitas en la colaboración gratuita de un familiar o amigo que viva en la zona.

b. Términos legales para aceptar el cargo. Normalmente usted será requerido con un plazo de aceptación del cargo de tres días hábiles. No obstante este hecho no es de aplicación general, especialmente en las jurisdicciones establecidas en el interior del país, donde la disponibilidad de peritos no es la norma, sino la excepción. En definitiva en estos casos lo normal es que primero se tome contacto con el perito por diversos medios (el telefónico constituye la norma) y cuando éste concurra al tribunal, se le entregue la no- tificación y la aceptación del cargo en un mismo acto. Esta falta de personal capacitado en determinadas áreas periciales hace que muchas veces se llamen peritos de otras ju- risdicciones y que el domicilio legal quede fijado en el

despacho o la casa particular del abogado que solicitó la pericia. Es una especie de designación híbrida, ya que implica la actuación como perito de oficio, pero de hecho se instituye como perito de partes.

c. Plazo para el despacho de la designación. Una vez aceptado el cargo, el expediente pasará a despacho (será diligenciado por el juzgado), para confirmar la designación y establecer el término para realizar la pericia. En la práctica profesional realizada en el Gran Buenos Aires, este despacho suele tardar aproximadamente una semana, no excediéndose de los diez días. A partir de ese momento el expediente (o el cuaderno de prueba involucrado) volverán a estar disponibles y usted podrá retirar los elementos sub peritia y de ser necesario la documentación complementaria asociada. Existen pla- zos legales para la realización de la pericia, no obstante los mismos pueden ser extendi- dos a pedido del perito, pero este pedido debe ser siempre formal y por escrito.1

d. Adelanto para gastos: Es normal que entre el momento de realizar la pericia y el mo- mento de defenderla pase un tiempo considerable (a veces un par de años o más). Los honorarios del perito son fijados de diferentes maneras y constituyen una atribución del tribunal correspondiente. No siempre constituyen una retribución adecuada, res- pecto del trabajo y de los gastos de los peritos. Por lo tanto es conveniente que solicite un adelanto para gastos, nada de mucha importancia, pero sí el dinero suficiente para su movilidad y para los desembolsos que implica la labor pericial (fotografías, impre- sión, papel, etc.).

e. Confidencialidad y resposabilidad sobre los elementos recibidos en custodia. Usted es el único responsable por el traslado y protección de los elementos a peritar. Ya hemos sugerido con anterioridad, pero reiteramos la conveniencia de realizar una copia del elemento cuestionado en el juzgado y devolver de inmediato éste, evitando su custodia efectiva. La posibilidad de modificación accidental de la información contenida en un soporte probatorio original es una espada de Damocles sobre nuestra cabeza, trate de quitársela lo más pronto posible. Es cierto que esto requiere de instrumental que a ve- ces no está disponible para todos los peritos (por lo menos una notebook y los periféri- cos necesarios para realizar la copia del disco y el hash que la certifique). Si no tiene otra opción traslade la prueba a su casa, manipúlela sólo lo imprescindible, trabaje siempre sobre una copia, guárdela en un lugar protegido, fuera del alcance de todos sus colabo- radores y en las adecuadas condiciones de protección antimagnética y de los agentes naturales agresivos externos (especialmente la familia y los amigos).

3. Usted ha sido designado por la autoridad judicial como perito de parte o consultor técnico a solicitud y propuesta de una de las partes. En este caso la problemática de

los adelantos para gastos y los honorarios dejan de constituir un problema (aunque nada es seguro y a veces los más confiables son los que menos pagan), pero la credibilidad de sus dichos ya no es tan contundente. Es el momento no sólo de ser, sino de parecer. En todos los actos involucrados con la designación, que por supuesto incluyen la aceptación del cargo y las demás diligencias establecidas para el párrafo anterior, debemos ser muy estrictos, serios y formales. La más mínima duda en el accionar científico, tecnológico, técnico y ético, serán utilizadas para atacar el informe pericial e impugnarlo. De más está decir que es conve- niente manipular la prueba lo menos posible y describir estrictamente el estado de ésta en el momento de la recepción y particularmente en el momento de la devolución. Cualquier sospecha, real o supuesta, que sea considerada como posible por el tribunal interventor a sugerencia de la otra parte, dará por tierra con todo nuestro esfuerzo técnico e intelectual.

1 En la labor realizada en algunas jurisdicciones de la provincia de Córdoba, resultaba normal que un perito que residía en Villa Allende (particularmente en aquellas especialidades escasas, a la sazón, como Dactiloscopía o Ba- lística) y que se encontraba inscripto en los tribunales de la capital cordobesa, fuese convocado por los tribunales de Río Cuarto o Río Tercero, al no disponer de esas especialidades en sus respectivos listados. En ese caso al con- currir el perito (era conveniente llegar temprano) lograba en un mismo día aceptar el cargo, que se diligenciara de inmediato este hecho y retirar los elementos a peritar en el mismo momento, incluyendo una excepción temporal en los plazos para entregar la pericia. Es decir el juez tiene atribuciones suficientes como para administrar ciertos plazos legales (no todos, ya que muchos implican la libertad o la incomunicación de una persona) para facilitar la labor pericial.

Actúe de manera ordenada, estricta, clara, pero sobre todas las cosas transparente. No sólo su prestigio, sino la validez del informe pericial, dependen de su actitud profesional.

4. Usted ha sido llamado a efectos de asesorar a una empresa o a un particular respecto de algún tema específico. En este sentido, suelen mezclarse distintos aspectos de la tecnología informática. Es muy posible que el asesoramiento implique temas de seguridad informáti- ca, algunos de los cuales puedan resultar en actividades específicas de Informática Forense. El requirimiento específico puede partir del cliente o puede ser inducido directa o indirec- tamente por el perito convocado. En realidad, pocas personas conocen las incumbencias de la Informática Forense, incluidos en este grupo algunos de los peritos en dicha especia- lidad. El principal problema en esta metodología de trabajo es que muchas veces la requisi- toria pericial surge como consecuencia del asesoramiento realizado y no precede a éste.

En general, la calidad de asesor del perito lo exime de sanciones legales, si como conse- cuencia de su asesoramiento un tercero transgrede la ley. Puede ocurrir que el experto sea llamado para asesorar, y al realizar el asesoramiento y como consecuencia del mismo des- cubre, que en caso de efectuar realmente el trabajo solicitado y/o necesario para satisfa- cer el requerimiento, puede llegar a transgredir la ley o a violar su propia ética profesional, debido a las condiciones ilegales o ilegítimas en que debería realizar su labor. En conse- cuencia se niega a hacerlo, pero ya ha brindado información suficiente como para que el entonces ya "ex cliente", pueda actuar por su cuenta. Lo hace y cuando es requerido por la Justicia, manifiesta que lo hizo por consejo de usted. Tenga en cuenta que el Código Penal establece:

Título VII - Participación criminal

Art. 45. "Los que tomasen parte en la ejecución del hecho o prestasen al autor o autores un auxilio o cooperación sin los cuales no habría podido cometerse, tendrán la pena establecida para el delito. En la misma pena incurrirán los que hubiesen determinado directamente a otro a cometerlo".

Art. 46. "Los que cooperen de cualquier otro modo a la ejecución del hecho y los que pres- ten una ayuda posterior cumpliendo promesas anteriores al mismo, serán reprimidos con la pena correspondiente al delito, disminuida de un tercio a la mitad. Si la pena fuere de reclusión perpetua, se aplicará reclusión de quince a veinte años y si fuere de prisión perpetua, se aplica- rá prisión de diez a quince años. (Texto originario conforme a la ley 23.077.)"

Art. 47. "Si de las circunstancias particulares de la causa resultare que el acusado de com- plicidad no quiso cooperar sino en un hecho menos grave que el cometido por el autor, la pena será aplicada al cómplice solamente en razón del hecho que prometió ejecutar. Si el hecho no se consumase, la pena del cómplice se determinará conforme a los preceptos de este artículo y a los del título de la tentativa."

Art. 48. "Las relaciones, circunstancias y calidades personales, cuyo efecto sea disminuir o excluir la penalidad, no tendrán influencia sino respecto al autor o cómplice a quienes corres- pondan. Tampoco tendrán influencia aquella cuyo efecto sea agravar la penalidad, salvo el caso en que fueren conocidas por el participe. (Texto conforme a la ley 11.221, de fe de erratas.)"

Art. 49. "No se considerarán partícipes de los delitos cometidos por la prensa a las personas que solamente prestaren al autor del escrito o grabado la cooperación material necesaria para su publicación, difusión o venta."

No sea ingenuo, todos somos valientes en la charla de café, pero cuando llega el momento de declarar ante un tribunal el valor decae y es mucho más fácil echar la culpa a otro que asu- mir la propia responsabilidad. Siempre que alguien pueda quitarse el lazo de encima y pasarlo a otro, lo hará. En este sentido, la mejor herramienta es el silencio profesional. Si es llamado a asesorar sobre un tema relacionado con la seguridad informática u otro tema, que deviene en una solución informático forense, limítese a escuchar y mantenga la boca cerrada, salvo para efectuar las preguntas necesarias que le permitan comprender o intuir la realidad oculta tras la solucitud efectuada. Siga los consejos populares: "no se agrande" y "en boca cerrada no entran moscas", ya que la mosca que le puede entrar suele ser sumamente tóxica para su libertad, tran- quilidad y prestigio profesional.

Evite hablar sobre las técnicas específicas de su profesión. Si ha decidido actuar como ase- sor hágalo, pero siempre mediante un informe escrito, respaldado por una solicitud igualmente escrita "las palabras se las lleva el viento, pero a veces a los papeles también", nunca la preven- ción será suficiente. Actúe con cautela. Una letra de tango acude en nuesto auxilio: "no me gusta avivar giles, que después te dan la contra", en este caso no existen giles, sino delincuentes, cuan- to más sepan respecto de las técnicas de obtención, manipulación, análisis e interpretación de la pueba indiciaria informático forense, más posibilidades tendrán de actuar con impunidad, lo que en definitiva va en contra de su profesión. Escuche más de lo que habla y observe más de lo que escucha. Si los delincuentes tuviesen una profunda formación criminalística (en dactilos- copía, rastros, balística, documentología, etc.) sus probabilidades de delinquir impunemente se incrementarían en gran medida. De hecho, no hay mejor escuela del delito que la cárcel. Tal vez no se haya logrado el ideal constitucional del artículo 14 "…Las cárceles de la Nación serán sanas y limpias y para seguridad y no para castigo de los presos detenidos en ellas…", pero en su labor educativa demuestran ser muy eficientes, aunque no precisamente en beneficio de la sociedad.

Si como consecuencia de su asesoramiento se requiere su trabajo profesional informático forense específico y ha decidido hacerlo, entonces, tome todas las medidas necesarias para deslindar responsabilidades, exija una requisitoria formal escrita e indiscutible legalmente. No transgreda la ley por acción u omisión, recuerde que nunca podrá alegar desconocimien- to. Cuando se analiza la relación entre la obligación del perito a decir verdad como testigo y la idéntica obligación de limitarse a los puntos de pericia, la contradicción se torna evidente. Pero este hecho no es excepcional en materia jurídica, sino todo lo contrario. La jurisprudencia es un claro ejemplo de esta dicotomía, como dijeramos anteriormente, el mismo Beccaria lo había notado cuando escribió "…vemos los mismos delitos castigados de manera diferente por el mismo tribunal en tiempos diferentes, por haber consultado no a la voz

constante y fija de la ley, sino a la errante inestabilidad de las interpretaciones".

Usted nunca tendrá la seguridad absoluta de estar protegido por la ley, ya que aunque se manifieste de esta manera y la gran mayoría de los legisladores se rasguen las vestiduras ante la realidad, lo cierto es que no siempre la ley tiene por objeto proteger al ciudadano y mucho me- nos al perito. Su vulnerabilidad está en directa relación con su conocimiento de la ley. Usted ha decidido actuar en el ambiente jurídico, puede adaptarse al mismo o morir en el intento, pero no puede darse el lujo de ignorarlo.

Entrevista aclaratoria: Una vez establecida la pertinencia de la actividad pericial a realizar y como primera medida de ésta, debemos reunir, clasificar, evaluar y seleccionar la mayor can- tidad de información posible que nos auxilie en nuestra tarea. Al respecto es necesario integrar dos marcos ya definidos con anterioridad: el marco científico y el marco sistémico.

La labor de recolección de información debe ser estrictamente científica, pero metodoló- gicamente sistémica. Esta labor respecto de la prueba indiciaria informático forense, tendrá su principal punto de acción durante la inspección judicial que se insertará exclusivamente en el marco criminalístico y en el marco específico informático forense. Sin embargo, para alcanzar los resultados pretendidos es necesario haber realizado una adecuada planificación previa. Tal vez la batalla no sea menos cruenta, pero seguramente será más previsible si disponemos de suficientes datos antes de embarcarnos en la lucha propiamente dicha.

La entrevista previa con las partes involucradas en la pericia es característica del accionar pericial frente a un cliente potencial o a un asesoramiento relacionado. Pero también puede co- rresponder a una citación, especialmente en los tribunales penales, donde el juez o el secretario citan al perito para proponerle participar en una inspección judicial en determinado lugar. En este último caso la entrevista será más restringida, ya que raras veces podrá interactuar con las partes para que le allanen el acceso a la prueba pretendida.

En cuanto al caso del cliente, la entrevista permite recolectar toda la información posible. Es conveniente que se realice en su propia oficina o en un ambiente neutral, nunca en el lugar donde suponemos que se realizará la recolección de pruebas propiamente dicha. Esto se debe a varias razones, entre ellas:

1. Seguramente usted será reservado en sus dichos (ya hemos visto la conveniencia de que lo sea), pero no todo el mundo es igual, su futuro cliente tal vez lo haya hecho llamar por medio de su secretaria, que no siempre es todo lo confiable, discreta y silenciosa que sería deseable. Su irrupción en el lugar implica indirectamente su

identificación como potencial enemigo y dicha identificación puede proyectarse al grupo involucrado o a los clásicos ob- servadores no involucrados, pero sumamente curiosos y con una clara e innata tendencia periodística. Esto puede generar acciones preventivas que destruyan las pruebas que usted pretende detectar, ya sea porque los sospechosos saben cómo eliminarla o porque dispo- niendo de tiempo para asesorarse sobre cómo hacerlo.

2. Recuerde que el tiempo es un factor primordial, pero que, en general, velocidad no implica atolondramiento. Mientras su futura labor permanezca entre las sombras, usted puede to- marse un tiempo para planificar la acción (un tiempo, no toda la vida). Por el contrario una vez descubierta la posibilidad de ser investigados por los sospechosos, la acción debe ser inmediata. De ahí que cuanto menos lo vean por la empresa o lugar de recolección de prue- bas, antes de la inspección judicial, mejor para usted y mejor para los resultados periciales esperados.

3. Por otra parte, al sacar al futuro cliente de su entorno habitual, en general lo induce a ser más objetivo. La visualización del área donde cree que está siendo engañado o estafado, in- centiva su emotividad y en general lo vuelve más agresivo, más elocuente y menos racional. El analizar el tema fuera del entorno le permitirá abstraerse de las emociones y concen- trarse en sus preguntas.

Al planificar los tiempos de la entrevista tenga en cuenta:

1. La personalidad del entrevistado, esto es sumamente útil, ya que permite prever el rumbo previsible que tomarán los acontecimientos.

2. Identifique los temas generales a tratar y el período de tiempo necesario para interactuar ante las posibles derivaciones de dicha entrevista.

3. Prepare un cuestionario de preguntas para realizar a su cliente con una serie de preguntas generales y aplicables a cada caso y con una serie de preguntas específicas variadas, acorde al desarrollo de la entrevista.

4. Las preguntas deben realizarse siguiendo una estricta metodología de análisis de sistemas y cuando usted finalice su entrevista deberá poder realizar un análisis de alto nivel de los sistemas informáticos involucrados. Incluyendo las estructuras edilicias, componentes físi- cos, lógicos y humanos involucrados, normas de seguridad, controles de acceso, diagrama de red, diagrama de datos, cursogramas de actividades, distribución física del personal, or- ganigrama de la empresa y toda otra información que pueda facilitar la planificación de las acciones necesarias para acceder al lugar, recolectar la prueba, protegerla y trasladarla al lugar de análisis.

5. Siempre y en toda circunstancia tenga en cuenta el marco legal en que se encuentra traba- jando.

Dibujo pericial complementario

Croquis ilustrativo

Los croquis ilustrativos y las fotografías son recomendados por todos los Códigos de Procedimientos en el accionar de los jueces, fiscales, sumariantes, investigadores y peritos durante la etapa de instrucción. Lo que la ley busca es que la inspección judicial pueda aclararse más aún con la confección de un plano o dibujo del lugar del hecho o diseño de los efectos o la persona; es decir, ilustrar al magistrado que deba juzgar lo más claramen- te que sea factible para que se pueda formar una idea exacta de los hechos. En lo posible se realizará en escala, especialmente en hechos graves. A título de ejemplo y para mayor claridad diremos que en ella un centímetro en el papel equivale a un metro. Es preferible colocar las referencias en el frente de la hoja y no en la parte posterior, esto facilita la lectu- ra del croquis. Puede usted utilizar papel de cualquier tamaño, aunque recomendamos los cuadernos cuadriculados autoperforados de tamaño A4.

Si bien los croquis clásicos son impresos, nada impide utilizar las herramientas infor- máticas a nuestra disposición y el soporte digital de éstos, con los adecuados requisitos le- gales incluyendo una identificación específica, mecanismos de certificación legal o digital (hash, firma electrónica).

También, a veces, es necesario confeccionar dos croquis o más. Uno, panorámico, y otro, más amplio, del lugar que más interesa para poder fijar mejor los detalles importantes. Por ejemplo, en caso de un secuestro de disco en el interior de una empresa, haremos un plano completo de ésta (en papel o digital) y otro de la habitación donde se encontraba el disco.

El croquis con abatimiento de paredes (en cruz) es de gran importancia en casos graves producidos en un lugar cerrado, es decir, en el interior de una habitación, salón, etc. En él no sólo tendremos el piso, sino también las paredes “abatidas”, donde podremos señalar las circunstancias que más nos interesan y el lugar o altura exactos; por ejemplo, de co- nexiones, cableados, equipos de conectividad o distribución, etcétera.

Es conveniente prepararlos en color negro; pero es oportuno y útil utilizar otros co- lores, marcando y destacando aquellos elementos de interés. De allí la conveniencia del empleo de las herramientas informáticas de graficado clásicas (graficadores) o

específicas (aplicaciones específicas, como ejemplo: visio o herramientas CAD). En los casos que fuera necesario señalar circunstancias en el techo de la habitación o lugar del hecho, se confeccio- nará lo que se denomina croquis en cruz larga. Para ello la parte correspondiente al techo se agregará sobre una de las paredes, preferentemente la superior.

En la confección de los croquis es muy necesario el uso del escalímetro (de escala). Se denomina así una regla de espesor, triangular, con cinco escalas diferentes, pero más la de 1:1, que es igual a la de nuestro sistema métrico decimal. Mediante su uso es fácil reducir en escala cualquier dibujo. En caso contrario, utilizando una regla común, igualmente se puede confeccionar el croquis en escala reduciendo, por ejemplo, cada metro a un centímetro; así tendremos el croquis efectuado en una escala de 1:100. Se deberá dejar especificada la escala empleada. En los comercios del ramo existen escalímetros pequeños (de 10 centímetros de longitud), resultan sumamente útiles en el momento de graficar. Las herramientas computa- cionales facilitan esta tarea en grado sumo.

En general se torna imprescindible agregar una representación gráfica del lugar inspeccio- nado. Como ya dijimos, lo ideal es poseer un equipo fotográfico estereométrico digital y todos sus problemas habrán terminado. Es necesario comprender que la fotografía sirve para docu- mentar el lugar, pero no es suficiente para determinar todas las relaciones entre los elementos observados. De ahí la necesidad de realizar representaciones gráficas. Para efectuarlas se deben observar los mismos requisitos que para el acta de secuestro, si es posible en presencia de testi- gos y antes de modificar cualquier elemento del lugar. Este último requisito no siempre puede cumplirse, ante el ingreso previo o simultáneo de otras personas ajenas a la labor pericial (pe- riodistas, empleados, curiosos, colaboradores espontáneos (bien o mal intencionados).

Condiciones esenciales

Tenga en cuenta que las condiciones esenciales que deberá reunir este gráfico son:

1. Fidelidad: Es decir deben adecuarse lo más estrictamente posible a la realidad observada.

La creatividad es privilegio de los artistas, pero en este caso no es recomendable.

2. Claridad: Debe ser fácilmente interpretable, sin mediciones ni nombres ambiguos. Debe- mos ponernos en la situación del lego, que no estuvo en el lugar.

3. Legibilidad: Debe poseer dibujos y textos lo más destacados posibles, de manera

que no impliquen una dificultad agregada a la falta de visión (real y ostensible o disimulada) de quienes deben analizarla, especialmente el tribunal interventor (tenga en cuenta que la edad incrementa la dificultades visuales).

4. Nitidez: Los gráficos y dibujos relacionados con el hecho deben destacarse con claridad sobre el fondo que les da sustento. El uso de colores o resaltadores en su formato físico o computacional es la mejor solución para este requerimiento.

Elementos

Debe poseer los siguientes elementos:

1. Título: En la parte central superior del gráfico, para facilitar su identificación.

2. Orientación: Si le es posible dibuje junto al mismo una cruz orientada con los cuatro puntos cardinales. En caso contrario se interpretará que la parte superior del gráfico co- rresponde al Norte.

3. Colores: Si dispone de ellos debe usarlos. No existe una norma al respecto, deberá emplear el sentido común. Esto le permitirá, entre otras cosas, separar entre sucesos que guarden cierto orden cronológico, identificando con un color cada situación y permitiendo de esta manera hacer un correlato escrito posterior, comprensible y fácilmente identificable para el lector (especialista o lego).

4. Nombres: Siempre paralelos a la base de la hoja, con excepción de las calles laterales que se escribirán según el margen derecho de la hoja (como si rotara el gráfico 90 grados en el sentido de las agujas del reloj). En las calles es conveniente indicar el sentido de circulación del tránsito. Si se trata de autopistas, carreteras o rutas, indicar en cada extremo, de dónde provienen, hacia dónde se dirigen (localidades más próximas) y si es posible la distancia a dicha localidad. Recordemos que si el experto ha trabajado de manera adecuada, su des- cripción comenzará con la aproximación al lugar de inspección, su acceso al predio, al edificio y al lugar de recolección específico de la prueba indiciaria pretendida.

Dibujos auxiliares

En la representación gráfica militar se clasifican una serie de gráficos diferentes. Esta cla- sificación, si bien no es directamente aplicable al dibujo pericial, es

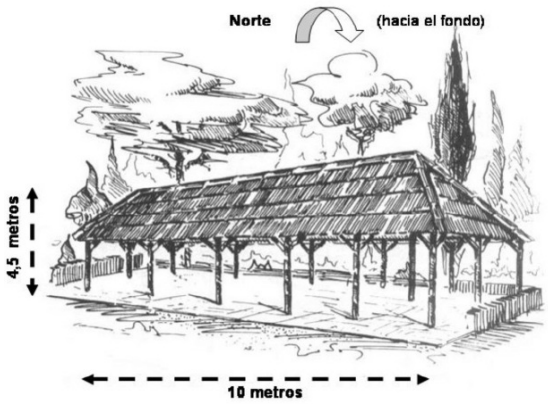
sumamente útil en el mo- mento de hacer una representación gráfica y referirse a la misma. Aporta un muy interesante vocabulario técnico específico:

1. Esquicio:

Será la representación gráfica de una zona pequeña del terreno (en nuestro caso la situa- ción de la finca involucrada y sus alrededores), sin escala, o a escala aproximada. Sirve para aclarar un texto y para reemplazar una descripción larga y complicada. Si se emplea en una situación con escaso tiempo disponible, se realizarán a mano alzada y las medidas se aprecia- rán a simple vista, en caso contrario se podrán agregar los datos que se puedan comprobar. No lleva referencias, todos los datos se anotan en el mismo gráfico. Registra de manera simple y rápida la situación de un lugar, que puede ser modificado de inmediato (un choque de au- tomóviles con heridos) y sirve como ayuda memoria en una etapa posterior.

2. Esquicio panorámico:

Es la representación de perspectiva de una zona del terreno, tal cual aparece ante el ojo del observador. Es ideal para representar fachadas de edificios, especialmente si frente a no- sotros aparecen jardines o desniveles difíciles de representar de otra manera. Debe registrar- se la flecha que indica el Norte o el punto cardinal hacia el que está observando quien lo efectúa, esto permitirá orientar rápidamente el dibujo. En general se dibuja sin escala, pero se dibujará una regla horizontal y una vertical que indiquen las distancias y alturas relativas (aproximadas). Es preferible no escribir en el dibujo y utilizar referencias. Es necesario indicar el punto específico donde se hallaba situado el observador, para poder repetir la experiencia a futuro. No debe confundirse con el corte vertical de una habitación o edificio, se trata de un dibujo a mano alzada, aproximado y sin medidas estrictas, es el recurso inmediato y directo para describir lo que el observador estaba viendo y documentando. Puede reemplazar a la fo- tografía panorámica en ciertas situaciones en que por falta de elementos (cámara) o razones de visibilidad escasa (neblina, oscuridad) u otras que puedan surgir, se hace necesario descri- bir el entorno frente al observador y no se cuenta con otros elementos.

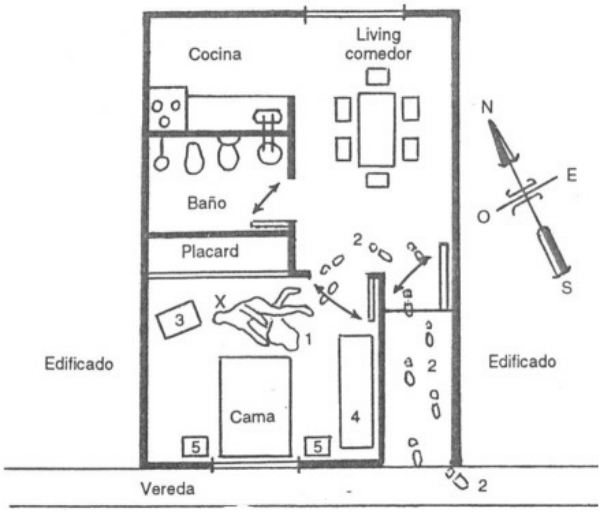


Ejemplo de esquicio panorámico.

3. Croquis:

Éste será nuestro auxiliar predilecto. Representará gráficamente una zona pequeña, a es- cala. Para realizarlo bien deberá adoptar una actitud paciente, metódica, minuciosa y orde- nada. La observación crítica del lugar será su mejor aliada, el sentido común, su capacidad de relacionar elementos dispersos, su creatividad y su inteligencia, le permitirán realizar una labor útil para la individualización posterior de los elementos detectados, su orientación re- lativa y su empleo probable.

Ejemplo de croquis



Calle Chile N° 1313 Escala: 1:75 Referencias:

x: Posición de la víctima (masculino, adulto, vestido con ropas íntimas femeninas).

1. Mancha de sangre.

2. Huellas de pisadas (cada vez más difusas al alejarse).

3. Televisor, filmadora y equipo de video con CD secuestrado.

4. Cómoda con ropas femeninas.

5. Proyectores de luz estroboscópica.

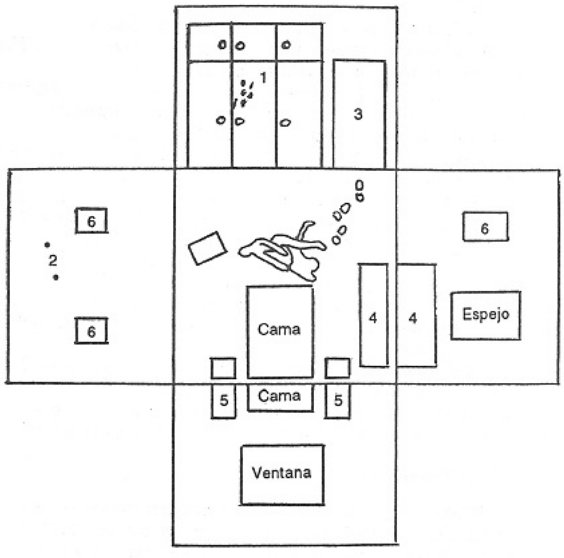
Firma del testigo 1 (aclaración, DNI, teléfono) Firma del testigo 2 (aclaración, DNI, teléfono)

Buenos Aires, 13 de diciembre de 2004.

Firma del perito

Ejemplo de croquis

(con abatimiento de paredes)



Escala: 1:75. Referencias:

1. Marcas de perdigones en la puerta del ropero.

2. Ídem anterior en la pared.

3. Puerta hacia el pasillo central de la vivienda.

4. Cómoda.

5. Proyectores.

6. Cuadros de fisicoculturistas.

Firma del testigo 1 (aclaración, DNI, teléfono) Firma del testigo 2 (aclaración, DNI, teléfono)

4. Gráfico:

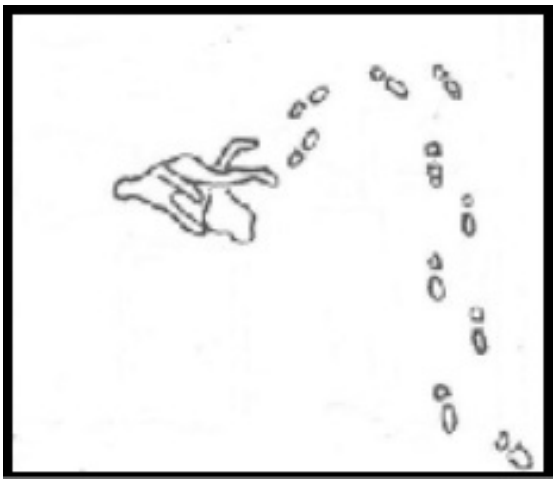
Buenos Aires, 13 de diciembre de 2004.

Firma del perito

Es la representación de los elementos relacionados con el hecho investigado. Contendrá todos los elementos probatorios directos o indirectos que el perito considere necesarios para investigar los hechos. Se realiza con prescindencia de la edificación y del mobiliario (salvo en las áreas que sea imprescindible destacar, por ejemplo, impactos en paredes, huellas dac- tilares en muebles). Si se efectúa en papel transparente y a escala constituirá en calco, es- to mismo puede efectuarse utilizando herramientas computacionales (escáner, capturas de pantallas, graficadores, procesadores de texto, etc.).

5. Calco:

Es un tipo de dibujo de suma utilidad, pero en general de empleo a posteriori. Poseyendo un plano del edificio es posible realizar un croquis sobre material transparente, que luego se pueda superponer al mismo e identifique rápidamente los elementos referidos. Esto parece algo obsoleto, pero recordemos que si hemos hecho bien las cosas, nuestro croquis realizado en el lugar del hecho puede ser capturado con un escáner y superpuesto al plano de la finca, (también capturado de la misma forma). Los medios electrónicos facilitan el trabajo manual, pero no modifican el concepto teórico, en este sentido un calco electrónico podrá ser de gran ayuda en el momento de defender la pericia.



Ejemplo de gráfico

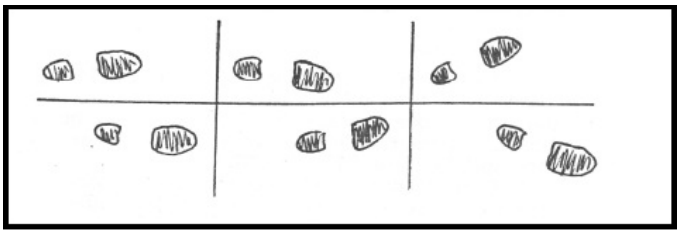
(calco si empleamos papel transparente)

6. Mapa, carta de situación o plano del edificio o finca:

Nos brindarán el soporte necesario para ajustar nuestra escala previa. De ser posible, es conveniente contar con aproximaciones de mayor a menor que faciliten la identificación del lugar del hecho al lector. Por ejemplo, vista general del barrio (destacando la manzana), am- pliación de la manzana (destacando la finca), plano de la edificación (destacando la habita- ción), plano de la habitación con superposición de calco de los elementos involucrados en la investigación (la prueba indiciaria).

7. Otros gráficos auxiliares:

Todo tipo de dibujo que usted considere útil para la comprensión de los actos realizados durante la inspección judicial y los elementos involucrados en los mismos.



Retrato del paso (reconstrucción gráfica)

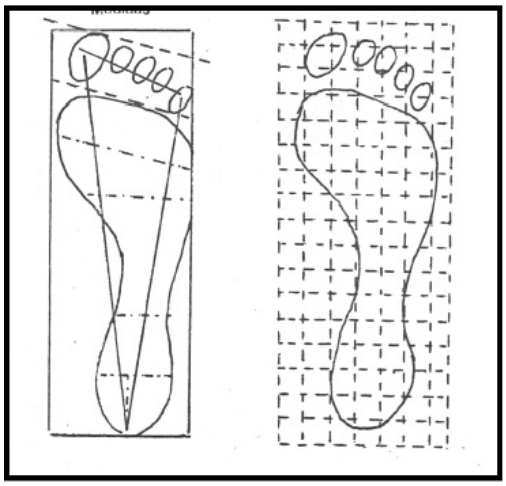


Gráfico de huella de pie desnudo

(colocar medidas externas, internas, alineación de los dedos, anomalías, etc.)

Podemos diferenciar las pericias normales de las de carácter urgente que no requieren las formalidades de requisitos legales establecidos para las de orden general, es decir, notificación al perito y aceptación del cargo, y notificación a las partes para que si lo creen conveniente las presencien, formulen las observaciones que crean necesarias y/o nombren peritos a sus cos- tas. Las pericias que se deban realizar en un tiempo normal están rodeadas de estas garantías legales, pero en caso de urgencia algunas acciones se simplifican, ya que de otro modo no se dispondría del plazo correspondiente para practicarlas.

Generalmente, los instrumentos utilizados para la consumación de delitos son de uso prohibido, y por lo tanto deben ser secuestrados y decomisados luego de haber servido co- mo elementos de prueba, sin embargo, en el caso específico de la pericia informático foren- se, dichos elementos probatorios no sólo son de uso legal, sino que suelen ser imprescindi- bles para el funcionamiento normal de una empresa determinada. Por eso debemos estar preparados para realizar copias en el lugar sin interferir (o interfiriendo lo menos posible con el normal funcionamiento de la empresa y sus negocios u operaciones asociadas).

El único que puede determinar el secuestro de un elemento y su traslado desde el lugar inspeccionado es el juez de instrucción o el fiscal de la causa, respectivamente, acorde a la jurisdicción donde se realiza la inspección. Todos los Códigos de

Procedimientos pretenden dar seguridad a los elementos secuestrados con el fin de que no puedan ser sustituidos por otros, falsificándose de esa manera los medios de prueba, pero recordemos que la prueba informático forense almacenada en archivos es idéntica al original.

"El decomiso no recae en el valor de los instrumentos: sino en los instrumentos y efectos mismos. Constituye una pena particular que no puede ser alterada por el juez, debiendo enten- derse que son instrumentos del delito los objetos utilizados intencionalmente para ejecutarlo o intentarlo. Por efectos del delito se entiende a los que resultan de su comisión, sea porque el ilícito los ha producido o bien porque el delincuente los ha obtenido mediante el delito. Sirva como ejemplo del primer caso de esos efectos la moneda falsa, y del segundo, la cosa robada" (Núñez, t. II, p. 445).

"La ley con esta norma establece el distingo de que la confiscación no puede recaer sino so- bre aquellos objetos empleados como instrumentos, y de ahí que el decomiso no sea aplicable a los delitos culposos. Sólo pueden ser objeto de decomiso los instrumentos del ilícito y los efectos provenientes del mismo. Pero no es aplicable al producido total del delito, ni a los objetos roba- dos pertenecientes al propietario, ni tampoco a lo que el delincuente obtuvo como efecto prove- niente del delito. A alguno de los partícipes deben pertenecer los objetos. Se tiene que distinguir el decomiso del secuestro porque éste tiene carácter procesal y sirve para que el juez asegure pruebas o haga cierto los resultados del juicio" (Soler, t. II, pp. 398 y 399).

"Corresponde devolver a su dueño el instrumento empleado para realizar el hecho denun- ciado si éste no constituye delito" (CAC, 20-4-1934; FCAC, t. II, p. 37).

"Secuestrada una cosa en poder de un tercero que no se encontraba procesado, quien invoca algún derecho sobre la misma, puede ser entregada durante el proceso al propietario originario" (CNP, 27-4-1954; "ED", 8-568).

"No basta, para que un acta sea inválida, que quien la redacte incurra en faltas de orto- grafía o demuestre fallas culturales, ya que esa deficiencia no permite conjeturar malicia de parte de quien la labra y que incurra en falsedades, máxime si no afecta a la comprensión de lo sentado en dicho instrumento" (Cám. 3° La Plata, S-II-1974-144, t. 1).

"Si un acta de secuestro no fue firmada por la persona en cuyo poder fueron hallados los efectos –en la especie, por encontrarse desvanecida– ni tampoco por testigos, a raíz de la na- turaleza y lugar del procedimiento, la diligencia no es nula, debiéndose apreciar su mérito, eficacia e idoneidad en cuanto su concordancia con otras pruebas acredite su realidad y vera- cidad" (Cám. Apel. San Martín, causa 7406, en "DJBA" del 12/4/82).

"El secuestro es un acto procesal y su validez y eficacia se rigen por las normas del derecho procesal penal y no por los preceptos del Código Civil" (Cám. Apel. San Martín, causa 7406, en "DJBA" del 12/4/82).

"El art. 99 (actualmente 107) del CPP también requiere –como el 97 (actualmente 105)– que la diligencia sea firmada por la persona en cuyo poder se hubieren encontrado, y si bien admite la firma de dos testigos, lo es en defecto de aquélla –sea que no se encuentre presente, sea que se niegue a firmar–, correspondiendo dejar constancia en el acta de cualquiera de esas circunstancias para sustituir la firma del interesado por la de dos testigos" (Cám. 3°, La Plata, S- II-1971, t. 1).

"Debe decretarse la nulidad de un acta de secuestro cuando ésta no contenga la firma del in- fractor y a la vez careciera de la firma de dos testigos, ya que ambas suplirían la de aquél" (Cám. Apel. Morón, 6/9/73, en "Sensus", t. X, p. 626).

Fotografías durante la inspección judicial

El fotógrafo es el primer perito que necesita la instrucción y el que debe trabajar "pega- do" a ésta. Es lógico de que si bien antes de tocar o remover algo es necesario no pisar sin antes observar detenidamente, también lo es documentar el lugar del hecho tal cual se en- cuentra al llegar, en la misma forma en que fue encontrado. Primero se fotografiará lo que se considere conveniente documentar y luego se realizarán las demás pericias, secuestros, etcétera.

En muchos casos, aunque es importante la toma de fotografias que reflejen fielmente detalles que podrían pasar inadvertidos, como, por ejemplo, la posición exacta de los equipos involucrados, de ninguna manera esto reemplaza el croquis, en el cual se pueden determinar fehacientemente las distancias. Si las fotografías las realiza un tercero, dicha circunstancia debe figurar en el acta. En todos los casos debe detallarse el instrumental utilizado (lentes de macro, cámaras digitales, teleobjetivos ópticos o digitales, zoom, etc.) y de ser necesario sus mecanismos de operación (por ejemplo, ante el uso de equipos de fotografía digital estereométrica) y sus principios dfuncionamiento.

APÉNDICE 5
MANUAL DE AUTOPSY



http://www.sleuthkit.org/autopsy/ Versión 2.21, desarrollado por Brian Carr**ier**

Traducción al castellano, adaptación y notas del traductor:

Prof. Ing. María Elena Darahuge

Curso de Experto en Informática forense

Universidad Tecnológica Nacional – Facultad Regional Avellaneda Argentina

Introducción

La herramienta de gestión de pericias de Informática Forense Autopsy, desarrollada por Brian Carrier y accesible desde el sitio http://www.sleuthkit.org/autopsy/, es un programa con licencia GNU General Public License.

La ejecución de Autopsy requiere de la instalación previa del conjunto de herramientas Sleuth Kit.

Autopsy se puede ejecutar en sistemas operativos Linux, Unix y en entornos Microsoft Windows.

En el caso de que se desee ejecutar en sistemas operativos del tipo Microsoft Windows se deberá instalar previamente un emulador del sistema operativo Linux o Unix. En este manual se describirá la forma de instalar, configurar y acceder a la

interfaz de emulación del sistema operativo Linux denominada Cygwin.

Este manual está orientado para los estudiantes del Curso de Experto en Informática forense de la Universidad Tecnológica Nacional – Facultad Regional Avellaneda.

En el presente manual se irá actualizando e incorporando aspectos relacionados con los comandos que utiliza Autopsy, especialmente Sleuth Kit y aspectos conceptuales relacionados con los sistemas operativos y sus gestores.

Cualquier sugerencia, duda, error u omisión que los lectores observen en el presente manual y deseen efectuar comentarios al respecto, podrán ser enviadas a: Prof. Ing. María Elena Darahuge, darahuge@yahoo.com.ar.

Emulador Cygwin

Instalación – Configuración y Acceso

Cygwin es un entorno semejante a Linux para Windows y consta de dos partes:

Una librería (cygwin1.dll) que actúa como una capa de interfaz de programación (*API*

-*Application Programming Interface*) de emulación, brindando una sustancial funcionalidad de tipo Linux API.

Un conjunto de herramientas las cuales proveen un entorno gráfico semejante a Linux.

Instalación de Cygwin:

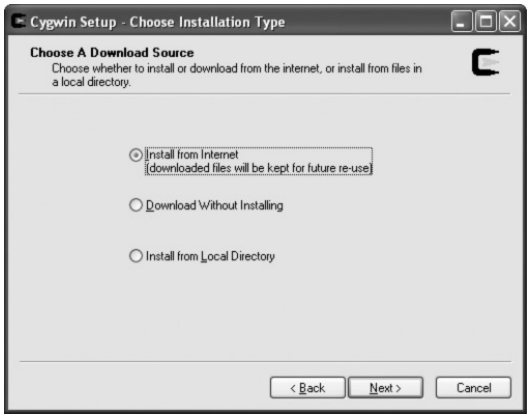
A continuación se listan los pasos a seguir para la instalación de Cygwin en Windows:

Se puede descargar de Internet una guía de instalación de Cygwin de Charles Lucas de la siguiente url: http://www.sleuthkit.org/sleuthkit/docs/lucas_cygwin_v1.2.pdf

Descargar el emulador Cygwin, desde www.cygwin.com, guardar el archivo "setup.exe" en una carpeta de Descargas en Windows.

Ejecutar el archivo "setup.exe", aparece un cuadro de diálogo que pregunta si se

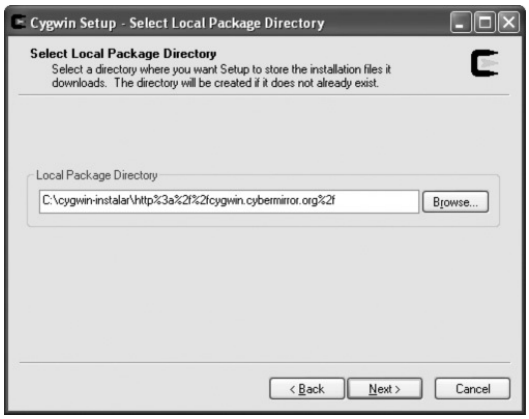
desea instalarlo desde Internet, descargarlo sin instalar o Instalarlo desde un directorio local (esta opción se selecciona en el caso de que se haya elegido “Descargar sin Instalar”. En este caso se selecciona la primera opción:



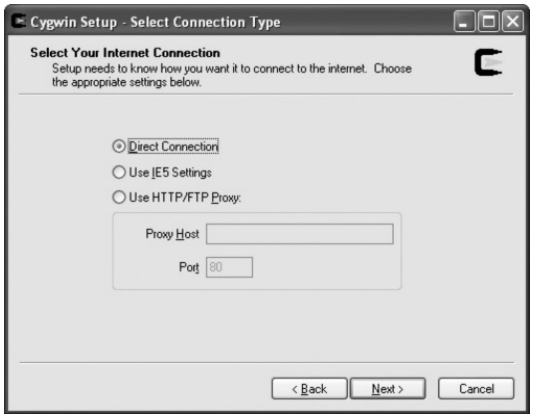
A continuación solicita el directorio de instalación, generalmente el disco C:\ y el directorio “cygwin” aparece como la ruta predeterminada, pero se puede seleccionar otro dispositivo. Además se debe seleccionar si se “Instala para todos los usuarios o solo para el actual” y el “Tipo de archivo de texto predeterminado”. En este caso se seleccionan las opciones como aparecen en la siguiente imagen:



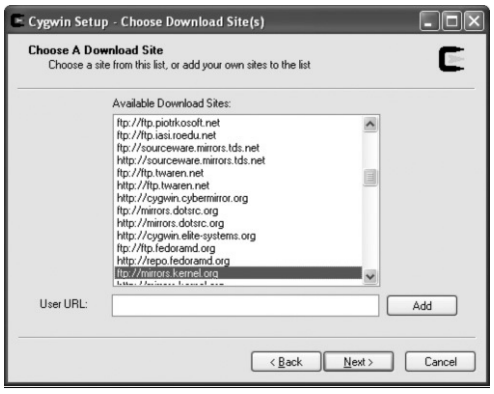
A continuación se debe seleccionar el directorio para los paquetes de instalación “packages”.



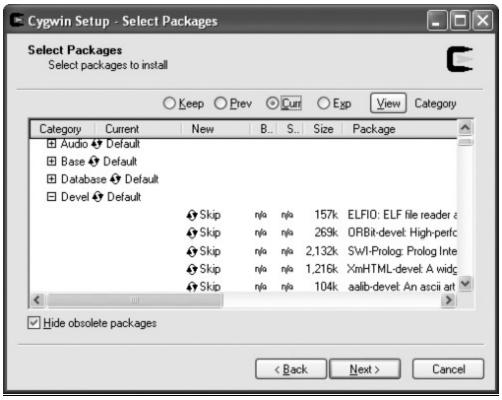
El siguiente paso es seleccionar el tipo de conexión de Internet “Directa, Utilizando la configuración del Internet Explorer o Utilizando un servidor Proxy http o ftp”:



El setup pregunta por el lugar desde dónde descargar los paquetes, se debe elegir uno, por ejemplo: ftp://mirrors.kernel.org:



Luego se deben seleccionar los paquetes específicos para Autopsy y Sleuth Kit, como se indica a continuación:



En “Devel” seleccionar: gcc C compiler, hacer clic en Skip y aparece el número de versión y a continuación agregar estos paquetes:

gcc: C compiler

gcc-g++: GCC C++ compiler

make: La versión GNU version de la utilidad “make”

patchutils: Conjunto de programas que trabajan con archivos de paquetes

En “Interpreters” seleccionar:

perl: Larry Wall’s Practical Extracting and Report Language

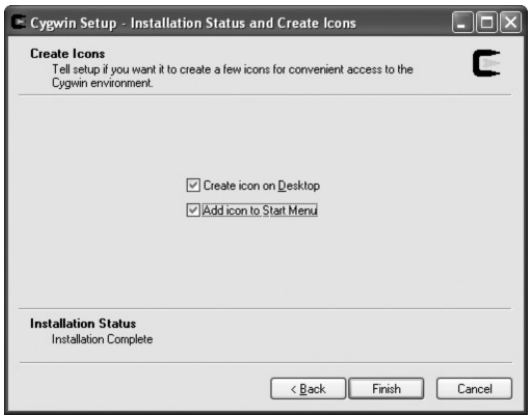
En “Libs” seleccionar:

openssl: The OpenSSL Runtime Environment

openssl-devel: The OpenSSL Development Environment

A continuación comenzará la descarga de los paquetes, esto puede llevar un tiempo considerable dependiendo del sitio seleccionado de la descarga de los paquetes y del ancho de banda de la conexión a Internet.

Al finalizar la descarga se puede seleccionar las opciones de: “Crear un acceso directo en el escritorio y Agregar un Icono en el Menú Inicio”.



La instalación de Cygwin presenta las siguientes carpetas y archivos:

bin, cygdrive, dev, etc, home, lib, tmp, usr, var

Cygwin.bat y Cygwin.ico



Ejecución de Cygwin y acceso al intérprete de comandos (shell):

La ejecución de la aplicación se puede realizar desde tres lugares posibles:

En el directorio seleccionado para la ubicación de Cygwin, ejecutar el archivo "Cygwin.bat"

Ejecutar el acceso directo creado en el Escritorio de Windows

Desde el Grupo de Programas, Inicio → Programas → Cygwin, seleccionar el ícono de "Cygwin Bash Shell"

A continuación aparece una consola de Dos donde se muestra el indicador del intérprete de comandos, conformado por: el usuario predeterminado de la sesión actual de Windows, el símbolo de @ y el nombre de la computadora:



Instalación de Sleuth Kit:

El conjunto de herramientas de Sleuth Kit es necesario para la ejecución adecuada de Autopsy. La descarga de Sleuth Kit se puede realizar desde la siguiente url: http://sourceforge.net/ projects/sleuthkit/files/sleuthkit/3.0.1/

La versión que se debe descargar es "sleuthkit-3.0.1.tar.gz"

Guardar el archivo en el directorio de cygwin: /usr/local

Acceder al directorio /usr/local, desde la consola de Cygwin, ejecutando el comando *"cd / usr/local"* y luego oprimir la tecla "enter"

Para comprobar que se encuentra en el directorio /usr/local, ejecutar el comando "*pwd*", que debe devolver /usr/local



A continuación se debe utilizar el comando *"tar"* para desempaquetar y descomprimir los archivos contenidos en "*sleuthkit-3.0.1.tar.gz*", para no ingresar todo el nombre del archivo a descomprimir, se puede escribir el comando y sus parámetros y a continuación las primeras letras de sleuth y oprimir luego la tecla "tab" para completar el nombre del archivo.

tar xvfz sleuthkit-3.0.1.tar.gz



Para instalar Sleuth Kit se debe ingresar al directorio creado con el comando anterior: "*cd sleuthkit-3.0.1" y* oprimir la tecla "enter".



Para instalarlo se deben ejecutar los siguientes comandos:

./configure, (punto barra **.**/configure)una vez finalizado devuelve nuevamente la línea de comando.

make

make install

De esta forma quedan instaladas las herramientas de Sleuth Kit en Cygwin.



Instalación de Autopsy:

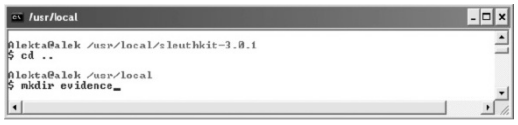
Previamente a la instalación de Autopsy se debe crear una carpeta denominada "evidence", que será requerida en el momento de la instalación de Autopsy, al preguntar la ubicación de la carpeta "Evidence locker".

La carpeta se debe crear con el comando "*mkdir*".

Para subir un nivel desde el directorio "sleutkit-3.0.1",

Ejecutar el comando "cd .." y dar "enter"

Crear la carpeta "evidence" con el comando: "mkdir evidence"



Descargar Autopsy 2.21, desde la siguiente url: http://sourceforge.net/projects/autopsy/ files/autopsy/2.21/autopsy-2.21.tar.gz/download

Guardar el archivo en el directorio de cygwin: /usr/local

Acceder al directorio /usr/local, desde la consola de Cygwin, ejecutando el comando *"cd / usr/local"* y luego oprimir la tecla "enter"

Para comprobar que se encuentra en el directorio /usr/local, ejecutar el comando "*pwd*", que debe devolver /usr/local A continuación se debe utilizar el comando *"tar"* para desempaquetar y descomprimir los archivos contenidos en "*autopsy-2.21.tar.gz*", para no ingresar todo el nombre del archivo a descomprimir se puede escribir el comando y sus parámetros y a continuación las primeras letras de "autop" y oprimir luego la tecla "tab" para completar el nombre del archivo.

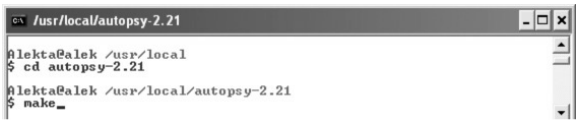
tar xvfz autopsy-2.21.tar.gz



Para instalar Autopsy se debe ingresar al directorio creado con el comando

anterior: "*cd autopsy-2.21" y* oprimir la tecla "enter".

Ejecutar el comando "make"



Luego, durante la instalación, pregunta dónde se encuentran las librerías de "Perl" y se debe ingresar manualmente la ruta: "/usr/local/sleuthkit"

Luego pregunta si se instalarán los paquetes de *hash* de "NSRL", responder "no"

A continuación solicita al ruta del directorio de "Evidence Locker", ingresar la ruta "/usr/ local/"

Si no aparecen errores devolverá el indicador del intérprete de comando.

Descripción general de Autopsy

El navegador forense de Autopsy es una interfaz gráfica para la ejecución de los comandos de las herramientas forenses y estándar de las utilidades de Unix. Permite realizar el análisis de volúmenes y sistemas de archivos sobre los sistemas operativos Unix y Windows.

Los datos se almacenan en un directorio dentro del "*Evidence Locker"* (Casillero de Evidencia), el cual se especifica en el momento de la instalación o al ejecutar el programa. Visualizar en el ayuda la opción "Gestión de casos" (Case Management) para mayor información. En el modo normal, Autopsy importa un archivo de una imagen de un disco o partición. En el modo "en vivo", Autopsy puede analizar un sistema en ejecución y no almacena ningún dato en el disco rígido local.

El navegador posee las siguientes opciones:

Archivos – Files: Permite examinar el archivo de la imagen como un sistema de archivo y visualizar los contenidos de los archivos y directorios. En este modo se muestran también los archivos borrados y Alternate Data Streams (Flujo de caracteres) de imágenes de sistemas de archivos NTFS. Se pueden ordenar los archivos y directorios según sus metadatos (descriptores de archivos).

Metadatos – Meta Data: Permite analizar el archivo de la imagen examinando las estructuras de los metadatos o descriptores de archivos. Se puede seleccionar la dirección de una estructura de metadatos (hipervínculo) y visualizar los detalles de la estructura. Este modo es muy útil para examinar las estructuras no asignadas y obtener todos los detalles acerca de los archivos asignados (incluyendo todas las unidades de datos y otra información tal como los valores de hash MD5).

Unidad de Datos – Data Unit: Permite visualizar las unidades de datos por número de bloque. Esto resulta de mucha utilidad cuando se realizan búsquedas o exploración de los metadatos. Los contenidos de los bloques pueden ser mostrados en formatos diferentes: ASCII, hexadecimal o a través de cadenas (strings) de caracteres. Permite visualizar la estructura de metadatos que tiene el bloque asignado, si es que existe alguno, junto con el nombre de archivo, si es que existe.

Búsquedas de palabras claves – Keyword Search: Busca en un archivo de imagen utilizando el comando "grep" para una determinada cadena de caracteres o expresión regular. El resultado será una lista de unidades de datos que tienen la cadena. Cada unidad de datos puede ser seleccionada para visualizar los contenidos.

Detalles de la imagen – Image Details: Presenta un listado acerca de los archivos o volumen de sistema. La salida de este modo depende de los sistemas de archivos. Ejemplos de los datos del sistema de archivo incluyen la fecha de la última activación, la ubicación en donde se activó por última vez y un detallado listado de información de grupos de bloques o de los contenidos de la Tabla de Asignación de Archivos.

Integridad de la imagen – Image Integrity: La integridad de los datos puede ser validada en cualquier momento al seleccionar esta opción. Utiliza el valor que se encuentra en el archivo "md5.txt" para identificar si se ha sido modificado algún dato durante el proceso de análisis de la imagen.

Actividades de la línea de tiempo del sistema de archive – File Activity Timelines: Autopsy puede crear una línea de tiempo de la actividad de un archivo basándose en los tiempos de Modificación, Acceso y Cambios (MAC-Creados en los sistemas de archivos FAT/NTFS). La línea de tiempo tendrá detalles acerca de los contenidos borrados y asignados. La línea de tiempo resultante puede ser visualizada dentro de Autopsy o utilizando otras herramientas de visualización (Advertencia: muchos navegadores de Internet no manejan muy bien grandes tablas de archivos como las de líneas de tiempo, por lo que se recomienda utilizar un editor de texto para visualizarlas).

Categorías de tipos de archivos – File Type Categories: Autopsy puede ordenar los archivos en una imagen basándose en sus tipos de archivos. Por ejemplo, todos los

archivos JPEG y GIF serían identificados como imágenes y también todos los archivos ejecutables. Este modo ignora archivos que son encontrados en las bases de datos de hash de archivos conocidos como buenos, identifica archivos que se encuentran en la base de datos de archivos conocidos como malos, e identifica archivos que tienen una extensión que no es consistente con su tipo de archivo.

Generación de Informes – Report Generation: Cada una de las técnicas mencionadas anteriormente permite generar un informe. Este informe lista la fecha, el valor de hash md5, el nombre del perito informático forense y cualquier otra información en un formato del tipo texto. Estos informes pueden ser utilizada para mantener un registro cuando han sido encontrados bloques de datos eliminados o borrados.

Ejecución de Autopsy en Cygwin

Luego de instalar las herramientas de Sleuth Kit y el programa Autopsy se encuentra en condiciones de ejectuar la aplicación en el emulador Cygwin. Los pasos a seguir son los siguientes:

Acceder a Cygwin:

Ejecutar el ícono del acceso directo del escritorio o del grupo de programas o el archivo Cywin.bat, en el directorio raíz **C:\cygwin**



Cambiar al directorio de Autopsy

$ cd /usr/local/autopsy-2.21

Ejecutar el comando de Autopsy (punto barra **./autopsy)**

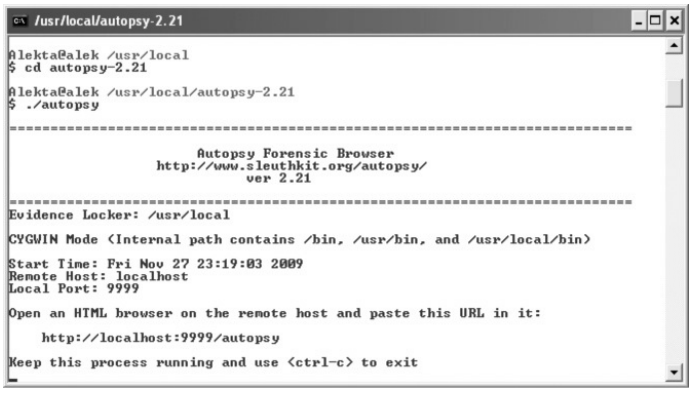
$ ./autopsy

Nota: Si aparece el error: ·“ERROR: Sleuth Kit (or local) file executable missing”, se debe editar y modificar el archivo “config.pl” que se encuentra en el directorio autopsy-2.21, accediendo desde el Explorador de Windows, completando la ruta que

se muestra a continuación:

i. Colocar en $FILE_EXE = '/usr/local/bin';

A continuación aparecerá el siguiente texto:



Abrir una ventana en el navegador de Internet e ingresar la url indicada en la aplicación:

http://localhost:9999/autopsy

Para salir de la aplicación de Cyqwin, oprimir **<ctrl-c>,** en la consola de Dos.



Creación de un caso en Autopsy

Nota: computadora es lo mismo que host.

Descripción:

Autopsy organiza las imágenes basadas en un caso y una computadora o host de la cual provienen. Un caso contiene uno o más hosts –computadoras–, un nuevo caso debería ser creado para cada investigación. Cada host puede contener una o más imágenes, las cuales corresponden a los discos o particiones de la computadora o host.

Creación de un nuevo caso

(Véase Issue 2 de The Sleuth Kit Informer)

En el menú principal –al inicio–, seleccionar New Case [Nuevo Caso].

Ingresar el nombre del caso, acorde a una nomenclatura previamente determinado por el PIF.

El nombre del caso debe ser un nombre de directorio válido (sin espacios, sin símbolos)

Opcionalmente, ingresar una breve descripción del caso

Ingresar el nombre del o los PIF que participan de la investigación. Esto se utilizará para auditar los registros, no para autenticación.

Un directorio con el mismo nombre que el caso se creará en el directorio Evidence Locker [Casillero de Evidencia].

Para cambiar el nombre del caso es suficiente con renombrar el nombre de la carpeta.

Ejemplo:

electrónico

Agregar un Nuevo Host. Una computadora debe ser creada en el Caso.

Seleccionar el caso que fue recientemente creado de la galería de hosts.

Seleccionar “Agregar Host” e ingresar el nombre del host.

Ingresar una breve descripción del host.

Ingresar la zona horaria (véase listado en

http://www.timeanddate.com/worldclock/)

Ingresar la desviación horaria, cantidad de segundos que el sistema está desfasado del un reloj sincronizados.

Al agregar el host se creará un directorio en el directorio del caso y subdirectorios en el host para las imágenes, información de salida, registros e informes.

Si no se agrega la zona horaria, por defecto se tomará la hora del sistema de la computadora en donde se ejecuta Autopsy.

Opcional, agregar la ruta de la base de datos de los *hash*es. Autopsy utiliza las bases de datos de *hash* de tres formas:

Análisis de las clases de tipos de archivos – File Type Category Analysis: Identificar los archivos malos e ignorar los archivos correctos.

Análisis de los metadatos (datos que describen otros datos) Meta Data Análisis: Las bases de datos de *hash* pueden utilizarse para identificar un archivo desde la ventana de Visualizar metadatos. Si la base de datos está configurada, el *hash* de un determinado archivo puede leerse presionando el botón de Ver –Lookup–. Las tres bases de datos pueden visualizarse de esta forma. Esta visualización puede aparecer en el modo de Análisis del archivo –File Análisis–, seleccionando la dirección del metadato en la ventana de listado de directorios.

Gestor de base de datos de Hash Hash Database Manager: Desde la vista de Galería de Host -Host Gallery se puede ingresar al Gestor de Base de Datos de Hash. Aquí es donde se puede indexar la base de datos y ejecutar una búsqueda simple en cualquiera de las bases de datos.

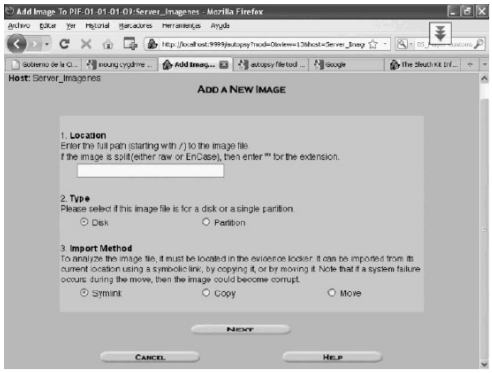
Las bases de datos de *hash* son utilizadas para identificar rápidamente los archivos buenos y erróneos utilizando el MD5 o SHA-1. Autopsy utiliza tres tipos de base de datos de *hash* para ayudar al PIF a reducir los números de archivos que necesita analizar. (Véase Anexo 1 – Creación de Base de Datos de *Hash*.)

Ejemplo:

cipal de Base de Datos Solaris de Windows 2003

hash/win2k.txt *hash*/win_hack.txt

Agregar una Nueva Imagen: Las imágenes deben agregarse al host,



Seleccionar el host que se agregó recientemente de la Galería de Host [Host Gallery].

Seleccionar Agregar archivo de imagen [Add Image File], se abre un nuevo formulario.

En el cuadro de texto ingresar la ruta donde se encuentra la imagen, si la imagen está separada por volúmenes, la extensión debe estar ordenada en base al orden del archivo. Colocar un * en la extensión del nombre del archivo donde los números o letras están

–(../image.*). El archivo de imagen puede ser un disco completo o de una partición en particular. Se debe elegir una de las dos opciones. Antes de analizar la imagen, la imagen deberá ser ubicada en el casillero de evidencia. Aparece una opción para crear un acceso directo –symbolic link– de la ubicación actual, para copiar el archivo, o para moverlos de su ubicación actual a la del directorio de evidencia. Elegir uno de los dos métodos:

Image Path: /mnt/sys1/disk2.*
Type: Disk
Import Action: symlink

Si se importa una imagen por volúmenes la próxima ventana confirmará el orden de las imágenes. Luego de esto la próxima ventana le permitir especificar o calcular el *hash* para el archivo. El *hash* será de todo el archivo y si la imágenes es de

volúmenes, entonces el *hash* será de todos los volúmenes combinados. Si se importa una imagen con volúmenes, Autopsy tratará de determinar el tipo de sistema de archivo. Se le deberá indicar también el punto de montaje. Esto es solamente con fines de presentación de la información que al imprimirse aparece con la ruta completa de los archivos.

Si la imagen es un disco, Autopsy listará todas las particiones y tratará de determinar el sistema de archivo en cada una. Tiene la opción de no importar una partición y de cambiar el tipo de sistema de archivo.

Valores MD5: Cada host tiene un archivo de texto md5.txt que contiene el valor MD5 para los archivos en ese directorio. Autopsy utiliza este archivo para validar la integridad de los archivos. En forma predeterminada, cuando un archivo se importa en Autopsy, los *hash* MD5 se volverán a calcular.

Subdirectorios del Host Host Subdirectories. Cada host tiene un directorio de imágenes –images– y un directorio de salida –output–. Toda la información generada por Autopsy es guardada en el directorio de salida –output–, para permitir al directorio de imágenes tener permisos restrictivos y prevenir la modificación accidental de las imágenes, este directorio tiene los permisos de escritura no configurados.

Opción Analize Analizar



Después de agregar el host y la imagen, aparecen las opciones para efectuar el Análisis de la información de la imagen.

Al oprimir el botón Analize, aparece la siguiente ventana, con las opciones de:

File Analysis – Análisis de Archivo

Keyword Searchs – Búsquedas de palabras claves

File Type – Tipo de archivo

Image Details – Detalles de la Imagen

Meta Data Metadatos

Data Unit – Unidad de Datos

Help Ayuda

Close – Cierre del Host



Análisis de archivos File Analysis.

El modo de análisis de archivos le permite analizar una imagen desde el archivo y directorios respectivos, como si estuviera en la propia computadora, mostrando también los archivos borrados, contenido de los archivos y directorios, permite efectuar un análisis básico binario al extraer las cadenas ASCII del archivo binario. Los archivos pueden también ser seleccionados por cualquier campo.



Listado de directorio -Directory List, el lado izquierdo de la ventana tiene cuatro opciones principales:

Búsqueda en el directorio Directory Seek

Búsqueda por nombre de archivo -File Name Search

Ocutar y expandir directorios Hide / Expand Directories

Mostrar todos los archivos borrados Show All Deleted Files

En forma predeterminada el listado de directorio no es mostrado cuando se ingresa primero de este modo. Al expandir el botón de Directorios aparecerá la lista completa. El número de símbolos "+" representa la profundidad del directorio. Sólo se expanden de a un directorio.

Seleccionando el vínculo de todos los archivos borrados –All Deleted Files–, en la imagen se desplegarán del lado derecho de la ventana.

Existe un cuadro de texto donde un nombre de archivo o directorio puede ser ingresado y se desplegará del lado derecho. Esto facilita pasar de un directorio a otros sin tener que ir a través del listado. Ej., para buscar la carpeta "windows\system32", se puede ingresar esta cadena en el cuadro de texto en vez de desplegar todos los directorios.

Existe otro cuadro de texto donde se puede ingresar una parte del nombre de un archivo y aparecerán todas las coincidencias. (No utilizar palabras como ´.´. ´*´.. que forman parte del código del lenguaje de programación –Perl– en que fue escrita la aplicación). La búsqueda es sensible a las mayúsculas. Para encontrar todos los archivos que poseen una extensión .JPG, se puede escribir "\.jpg". O para encontrar todos los archivos que empiezan con un punto: "^\.".

Contenidos del Directorio Directory Contents. La ventana en el extremo superior derecho contiene los contenidos del directorio. En un sistema de archivo, un directorio almacena unidades de datos en un disco y completa las unidades de datos con estructuras que contienen el nombre del archivo y la dirección de las estructuras de metadatos. Esta vista analiza la estructura del nombre de archivo en un directorio. Se completa seleccionando un directorio del lado izquierdo de la lista o un directorio dentro de la misma ventana. Las entradas pueden ser vueltas a seleccionar haciendo clic en cualquiera de los valores del encabezado. Los encabezados de las columnas poseen la siguiente infomación:

del: su selección representa un archivo borrado. Existen dos tipos:

Una entrada en rojo, significa que la estructura del nombre de archivo no está asignada y la estructura de metadatos a la que apunta está también desasignada. Esto es lo que se espera de un archivo borrado recientemente. Se puede confiar que los

datos que se están buscando siempre y cuando la estructura de metadatos no fue asignada y desasignada desde el último borrado.

Si el color es un rojo más oscuro, la estructura de metadatos ha sido reasignada y es posible que los datos no sean confiables.

Type – Tipo: Esta columna contiene el "tipo" de archivo o directorio que es. Existen dos tipos de valores:

El primero (dir), es el tipo de acuerdo a la entrada en la estructura de directorio, que es donde se encuentra ubicado el archivo.

El segundo (in), es el tipo de acuerdo a la estructura de metadatos. Éste debería ser el mismo, salvo para los archivos borrados. Ambos son asignados para ayudar al PIF a identificar si un archivo borrado ha sido reasignado o no. Por ejemplo, si el tipo de estructura del metadato es diferente que la del tipo de nombre de archivo, es posible que uno de las estructuras fue reasignada a un nuevo archivo.

Name – Nombre: El nombre de un archivo o directorio. Haciendo clic en el nombre se muestra el contenido del archivo, en la parte inferior de la ventana o el contenido del directorio en la misma ventana. Para los archivos borrados, ningún enlace aparecerá si la dirección de la estructura de metadatos ha sido borrada o limpiada. Para identificar el destino de un acceso directo en Unix, hacer clic en la dirección al final de la columna. Nota: el nombre no será un acceso directo si la medida del archivo es 0 o si la estructura de metadatos es desconocida.

Modified Time – Fecha y Hora de Modificación: Esta columna aparece para los sistemas de archivos de Unix y NTFS. Muestra la última fecha y hora en que fue realizada la última modificación del archivo. Es decir, cuándo fue la última vez en que la información fue escrita en las unidades de asignación del archivo. En Unix, la función utimes() puede modificar este valor fácilmente.

Written Time – Fecha y Hora de Escritura: Esta columna aparece para los sistemas de archivos FAT y se corresponde con la fecha y hora en que el archivo fue escrito por última vez. De los tres tiempos (Fecha y Hora), éste es el único requerido por la especificación FAT.

Accessed Time – Fecha y Hora de Acceso: Esta columna contiene la fecha y hora del último acceso al archivo. En una imagen FAT, este valor es opcional y solamente se corresponde exactamente con el día (no horas o segundos). Este valor puede modificarse con la función utimes() en Unix.

Changed Time – Fecha y Hora de Cambio: Esta columna existe para los sistemas de archivos de Unix y NTFS. Es la última fecha y hora que el estado de un archivo (o metadato) cambió. Esto es diferente de la fecha y hora de Modificación, porque Modificado se relaciona con los datos del archivo y Cambio se relaciona con los datos descriptivos de un inodo en Unix o con el los cambios en el descriptor de archivo o entrada en la Master File Table en NTFS. Este valor no puede cambiarse con la función utimes() en Unix.

Created Time – Fecha y Hora de Creación: Esta columna aparece para los sistemas de archivos de NTFS y FAT. Es la fecha y hora de cuando fue creado el archivo. De acuerdo con la especificación FAT, es una fecha y hora opcional.

Size – Tamaño: El tamaño del archivo. Si la medida de un archivo es 0, no se mostrará ningún enlace con el nombre del archivo.

UID – Identificador de Usuario: El Identificador de Usuario del Propietario del archivo.

GID – Identificador de Grupo: El Identificador de Grupo del Propietario del propietario del archivo.

Meta Data – Metadato o descriptor de archivo: Los nombres de las estructuras de archivos contienen un puntero a la estructura de metadatos que describe al archivo. Esta columna contiene la dirección de la estructura. Seleccionando este valor se mostrará los detalles en la ventana inferior. Si el valor es inválido, entonces el vínculo al archivo no existe. Si esto es porque fue borrado el nombre del archivo que tiene una estructura de metadatos con un estado de asignado, una cadena de reasignación existirá para identificar esto. El tamaño informado por la estructura de metadatos es muy importante con el uso de Sleuth Kit, el cual utiliza este valor para identificar cuántas unidades de datos se deben mostrar. Si esta medida es 0, pero la estructura de metadatos aún apunta a los bloques de datos, no serán mostradas. Se puede forzar a Autopsy para que muestre los valores, seleccionando la dirección del metadato utilizando la opción “force” (forzar). Para observar un archivo en una de las bases de datos de *hash* seleccionar la dirección del metadato. Esta vista ofrece una interfaz con las bases de datos.

El botón Add Note (Agregar Notas): es un vínculo que le permitirá efectuar comentarios acerca de este directorio y tenerlo guardado en su archivo personal de notas.

El botón Generate MD5 List (Generar Lista de MD5): es un vínculo que generará los valores MD5 para cada archivo en el directorio y le permitirá guardarlo como un

archivo de texto. Usando base de datos de huellas digitales, facilita la verificación de los archivos que fueron modificados por un atacante o intruso.

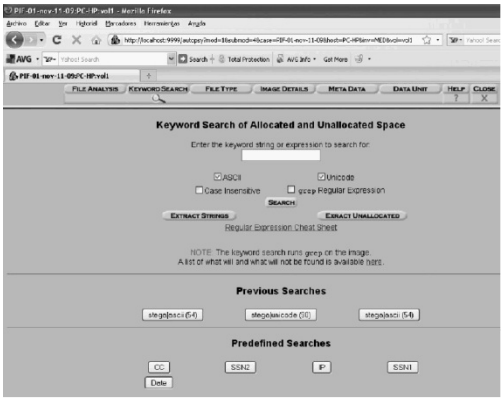
La ruta en la parte superior de la ventana tiene hipervínculos que permiten cambiar a un directorio anterior.

File Contents – Contenidos de los archivos: El lado inferior derecho de la ventana muestra los contenidos de un archivo específico. Los contenidos pueden ser en formato binario (el navegador no mostrará mucho del archivo si éste no es ASCII) o a través de cadenas o strings. La opción de strings es útil para un análisis rápido de un archivo binario. También se muestra el tipo de archivo. Para determinar el tipo de archivo utiliza los valores del encabezado y pie del formato del archivo (*Véase estructura de los archivos, Sistema Operativo, Una Visión Aplicada*, Carretero Pérez, McGraw Hill). Si el archivo es una imagen o HTML, aparecerá una opción para visualizar los datos en su forma interpretada (una foto o una página web en vez del formato binario). Cualquier HTML que se visualice será procesado en un entorno seguro que no carga imágenes y no permitirá conectarse a un sitio remoto. Para ver la imagen original, seleccionar la opción Export (Exportar) y abrir un documento HTML en otro ventana del navegador. (Ver issue #1 of The Sleuth Kit Informer.)

La opción Report (Informe), crea un archivo ASCII que contiene los contenidos del archivo así como también información respecto del *hash* MD5 y fechas.

La opción Export (Exportar) extrae el archivo fuera de la interfaz del navegador de forma tal que se puede guardar y visualizar localmente y aplicar otras herramientas para el análisis del archivo.

La opción Add Note (Agregar Nota) permite incorporar observaciones del PIF en el registro de notas para futuras referencias.



Opción Keyword Search – Búsqueda de palabras clav**es**

Keyword Search – Búsqueda de palabras claves:

Este modo busca en una imagen una cadena de caracteres especificada. Es particularmente útil para buscar contenidos eliminados. Para disminuir el tiempo de búsqueda un archivo del tipo "strings" –cadena– puede servir como índice. Este archivo contendrá solamente la cadena ASCII en la imagen. Autopsy indicará la creación de un archivo de datos no asignados si es que no existe uno. Éste es útil para recuperar datos eliminados. Si la cadena se encuentra en este archivo, Autopsy informará la ubicación en la imagen original.

Entering the String Ingresar la cadena: Ingresar la cadena o expresión regular dentro del cuadro de texto. Autopsy permite buscar tanto por una cadena específica o utilizando el estilo del comando "grep" para las expresiones regulares. Una búsqueda no sensible a las mayúsculas se puede seleccionar, de lo contrario será sensible a las mayúsculas. Se puede buscar también seleccionando que la cadena sea en formato ASCII o Unicote. Unicote es más común en los sistemas Windows que en Unix. Si se seleccionan ambos tipos, se harán dos búsquedas. Si no se ha seleccionado ninguna cadena o datos no asignados, no efectuará la búsqueda.

El botón Load Unallocated Image o Load Allocated Image sirven para cambiar entre dos tipos de archivos si ambos han sido generados.

Autopsy puede realizar búsquedas predefinidas – "Predefined Searches".

Viewing the Results – Ver los resultados: Después de que se ha realizado la búsqueda en la imagen, una lista de coincidencias aparecerán del lado izquierdo. Cada unidad de datos que contiene la cadena de datos se encuentra en la lista para cada ocurrencia. Si se utiliza una expresión regular, la ubicación exacta no será mostrada. Si la búsqueda fue hecha en un archivo de datos no asignado, aparecerá una opción próxima a cada dirección para ver también el original. Al realizar esto se revela el inodo que tiene asignado.

Previous Searches – Búsquedas previas: Los resultados son guardados en un archivo de manera que se pueda leer fácilmente sin tener que realizar la búsqueda nuevamente.

Regular Expressions – Expresiones regulares: Se puede utilizar el comando "grep" para las expresiones regulares de la búsqueda. Para buscar un par de palabras diferentes se pude utilizar el comando "foo | " (pipe).

Comando "grep" (filtrar)

Caracteres de Escape

Autopsy utiliza el commando “grep” para buscar en la imagen, pero requiere valores de escape si se requiere buscarlos. Autopsy automáticamente ignora estos caracteres si la búsqueda se hizo con expresiones no regulares. Los valores de escape son:

\

.

[

^

$

‘

*

inicial Expresiones regulares**:**

Las siguientes expresiones tienen significado especial para el comando “grep”.

[A-Za-z]: Cualquier letra mayúsculas o minúsculas

[:alpha:]: ídem anterior

[0-9]: Cualquier número

[:digit:]: ídem anterior

[0-9A-Za-z]: Cualquier letra mayúsculas o minúsculas o número

[:alnum:]: ídem anterior

[:space:]: Cualquier espacio en blanco

Para especificar cuántas veces puede aparecer una ocurrencia, se utiliza lo siguiente:

?: Opcional y puede ocurrir solo una vez

*****: Opcional y puede ocurrir más de una vez

• +: Requerido y puede ocurrir más de una vez

Para especificar más de una cadena para coincidir, se debe utilizar el signo de pipe "|" Ejemplos

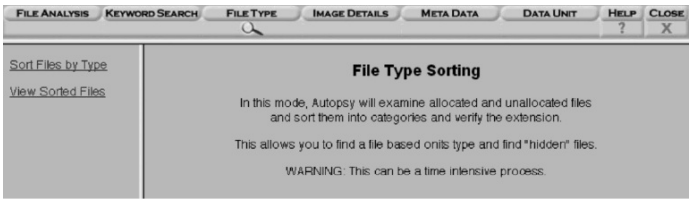
Para buscar "Jane Smith" o "Jack Smith": (Jane)|(Jack) Smith

Para asegurar las coincidencias un espacio se inserta entre el nombre y el apellido: (Jane)|(Jack)[:espacio:]Smith

Para buscar "Jane Smith" o "Jane Anne Smith": Jane(Anne)? Smith

o: Jane([:espacio:]Anne)?[:espacio:]Smith

Opción File Type – Tipo de Archiv**o**



Opción File Type – Tipo de Archivo:

El análisis de los sistemas de archivos de imágenes grandes puede ser muy desalentador. Una forma de identificar los archivos que deberían ser examinados es ordenar los archivos por tipo. De este modo Autopsy permitirá ordenar los archivos en una imagen por tipo y excluir los archivos conocidos, para reducir datos. También permite marcar archivos que se conoce como dañados.

Procedimiento: El documento ordenado en el directorio de "docs" del Sleuth Kit tiene más detalles de la información, pero dará una descripción general a través de la interface de Autopsy.

El primer paso: es Ordenar –Sort– la imagen. Existen varias opciones para elegir cuándo realizar esto. La herramienta "sorter" de Sleuth Kit efectuará el ordenamiento. Existen dos acciones que "sorter" puede hacer: ordenar los archivos por tipo y validar

las extensiones. En forma predeterminada Autopsy realizará ambas acciones. Si no se desea realizar ambas desmarcar una de las opciones. En el ordenamiento existen dos opciones:

La primera: es guardar la salida. Por defecto, detalles acerca de cada archivo será agregado a una categoría de archivo. Por ejemplo, una imagen JPG tendrá la dirección del metadato y nombre de la imagen guardado en el archivo images. Al seleccionar la opción Save –Guardar–, un directorio se creará por cada categoría y una copia de los archivos será guardada. Esto puede requerir gran cantidad de espacio en disco (tanto como el tamaño de la imagen original).

La segunda opción: es guardar los tipos de archivos desconocidos. Existen archivos de configuración que contienen reglas acerca de los tipos de archivos más comunes. Si el archivo no se encuentra contemplado dentro de la regla, es agregado como archivo desconocido. Si esto no se desea, seleccionar la opción "Not Save Unknown", No guardar desconocidos.

Durante el proceso de ordenamiento, la herramienta "sorter" examinará la extensión del archivo. Si el tipo de archivo es conocido, tiene extensiones conocidas, y el archivo no tiene una de esas extensiones, será agregado a un archivo denominado "mismatch" –error de coincidencia–. Si esta opción no se desea se debe desmarcar.

Hash Databases – Base de datos de Hash: Una forma de reducir datos es utilizar las bases de datos de *hash*. La herramienta "sorter" puede utilizar tres bases de datos de *hash* diferentes. Cada una puede ser configurada con Autopsy y utilizadas en otras fichas del menú.

NIST NSRL: (National Software Reference Library) http://www.nsrl.nist.gov/ contiene *hashes* de sistemas operativos confiables y de programas. Esto se utiliza para ignorar los archivos conocidos. Los archivos que se encuentran en el NSRL no se incluirán en las categorías de archivos (para reducir el tiempo cuando se revisan los archivos). Si el archivo está en el NSRL y no tiene una extensión errónea, será registrado como un archivo especial.

Ignore Database – Ignorar Base de Datos: Esta base de datos debe ser creada por el usuario y agregada al host. Es similar a la del NSRL, contiene *hashes* de archivos bien conocidos. Serán ignorados de la misma forma que aquellos de las bases NSRRL.

Alert Database – Base de datos de Alerta: Esta base de datos debe ser creada también por el usuario y agregada al host. Contiene *hashes* de archivos que son conocidos de ser erróneos o malos y deberían ser identificados si se encuentran en la imagen. Esto incluiría los rootkits conocidos o fotografías. Las coincidencias de estas

bases de datos se encuentran en el archivo “alert” –alerta–.

Output – Salida: No existe forma de ver la salida del archivo dentro de Autopsy. Todos los datos pueden hallarse en el directorio de “output” –salida–, del host. Un directorio es creado por la salida del comando “sorter”. Véase el arcahivo index.html que contiene los enlaces a los otros archivos.

Referencias – Issues 3, 4, y 5 de The Sleuth Kit Informer uso de la herramienta “sorter”.

Image Details – Detalles de la I**magen**

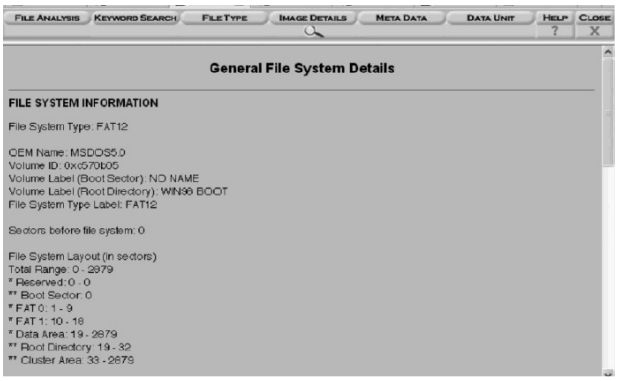


Image Details Detalles de la imagen:

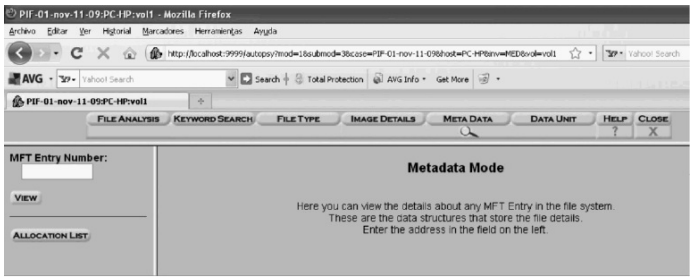
Algunas veces existen detalles de una imagen que no se corresponden con ningún archivo en particular. Estos detalles pueden encontrarse en este modo, el cual brinda un detalle general de la imagen y por consiguiente variará dependiendo del tipo de sistema de archivo.

FFS & EXT2FS: Para los sistemas de archivos Unix, este modo contendrá los detalles del superbloque. Esto generalmente incluye Fecha y Hora en que fue montado el sistema y cualquier bandera especial. También tiene el rango de las direcciones de inodo y direcciones de fragmentos. Para una avanzada recuperación de archivos, se puede también identificar el grupo sobre los detalles de la estructura del disco. Esto puede ser útil para restringir dónde se efectúa la búsqueda de datos. Los archivos se asignarán en bloques y fragmentos en el mismo grupo de Cilindros o Bloques tal como se encuentra su inodo, su atención puede ser orientada hacia ésta area

restringida.

FAT: Para los sistemas de archivos FAT, este modo contendrá la Tabla de Asignación de Archivo. Tendrá los clusters que pueden ser seleccionados para visualizar su contenido en el modo de análisis de Data Unit –Unidad de Datos–. O, si el archivo está fragmentado, el puntero puede ser seleccionado y la pantalla enlazará con la próxima cadena de cluster.

NTFS: La única información para una imagen NTFS es el tipo numérico asociado con los atributos. Estos valores pueden ser dinámicos y esta área identificará los que son para el sistema de archivo.



Opción Meta Data M**etadatos**

Metadata Analysis – Análisis de Metadatos o Descriptores de archivos:

Este análisis permite al PIF visualizar los detalles de las estructuras de los descriptores de archivo. La estructura de metadatos se encuentra en la estructura del disco que contiene los detalles del archivo como: fechas y horas, punteros a las unidades de asignación de datos. Los sistemas de archivos FFS (Fast File System) y EXT2FS (Second Extended File System), los denominan como estructuras inodo (sistema de ficheros que almacenaba la información del acceso a los archivos como una lista plana en disco, dejando al margen toda la información jerárquica de los directorios – Dennis Ritchie). Los sistemas de archivos NTFS lo denominan entradas en la MFT (Master File Table) o entradas de archivos, y en los sistemas de archivos FAT los denominan entradas de directorio. Este modo es útil para la recuperación de datos y para obtener una detallada visión del archivo.

Input – Entrada: Para visualizar los contenidos de una estructura, ingrese la dirección en el cuadro de texto del lado izquierdo y seleccionar Display (Mostrar). El

botón Allocation List (Lista de Asignación) puede ser utilizado también para visualizar el estado de asignación de las estructuras de metadatos en grupos de 500.

View – Ver: El detalle de la estructura se muestra del lado derecho. Típicamente la estructura de metadatos no tiene el nombre del archivo que usa esa estructura, por lo que Autopsy tratará de ubicar el nombre del archivo. Este proceso es lento en un sistema de archivos FAT, por lo que no se realiza en forma predeterminada.

File Type – Tipo de archivo: Es dado por la salida de la herramienta "file". Esta herramienta utiliza cualquier información del encabezado del archivo para determinar de qué tipo es, junto con el valor MD5.

Si Autopsy ha utilizado las bases de datos de *hash*, entonces se puede seleccionar sobre cuál base de datos buscar el archivo.

El resto de la información variará dependiendo del tipo de sistema de archivo. En general el estado de asignación dará el tamaño el tamaño y cada una de las unidades de datos asignada. Un hipervínculo será creado para cada unidad en donde se mostrará su contenido.

La opción Report (Informe) produce un informe en ASCII con la estructura detallada, con los valores de *hash* MD5 y las fechas.

La opción View Contents (Véase contenidos) muestra los contenidos de los datos asignados como un gran archivo.

La opción Export (Exportar) permite guardar los datos en un archivo.

La opción Add Note (Agregar Nota) permite al PIF agregar comentarios acerca de la estructura de forma tal que pueda ser utilizado en otra oportunidad.

Aclaraciones acerca de NTFS y FAT:

NTFS tiene un diseño muy diferente de los sistemas de archivos Unix y la estructura de metadatos se direccionan en forma distinta. Típicamente tienen la forma por ejemplo: A-B-C, 88-128-3. El valor A es la dirección del archivo en la Tabla Maestra de Archivos (MFT – Master File Table), por ejemplo 88. Esto es semejante al valor de inodo en Unix. Cada archivo tiene varios atributos, incluyendo al menos uno en archivos para los datos. El valor B, es el tipo de atributo. En la mayoría de los casos el atributo de datos tiene un tipo de 128, así es comúnmente visto. Si se quiere

ver el atributo del nombre de archivo, se puede especificar aquel tipo y ver los contenidos (lo cual puede ser muy tedioso). El valor final C, es el Identificador (Id). Cada atributo tiene un único valor de Id. De esta manera, si existen múltiples atributos con el mismo tipo, se puede especificar el tipo.

FAT no ofrece direcciones para la entrada de directorio. Las entradas de directorios pueden ser almacenadas en cualquier parte del disco. Se almacenan en el cluster asignado al directorio padre. Esto es diferente de lo que ocurre en NTFS o Unix, donde las estructuras están en una amplia tabla que no se mueve. El problema del direccionamiento se solucionó brindando una dirección a cada área de 32 byte en el área de datos, tanto si los datos son o no una entrada de directorio. Esto facilita la búsqueda de una dirección y la recorre cuando se han creado nuevos archivos. La desventaja es que no todas las direcciones son posibles, por lo que es más probable que se visualicen los saltos en los valores de la dirección.

Opción Data Unit – Unidad de D**atos**



Data Unit Analisis – Análisis de la Unidad de Datos:

Permite al PIF visualizar los contenidos de una unidad de datos individualmente. El término Unidad de Datos es genérico y se utiliza para describir las áreas del disco que son utilizadas para almacenar datos. Cada sistema de archivo denomina a cada unidad de forma diferente (Fragmentos, Clusters). Este modo es muy útil cuando se recuperan y analizan datos eliminados.

Input – Entrada: Para ver los contenidos de una dirección específica, ingrese la dirección en el cuadro de texto del lado izquierdo de la página. En forma predeterminada, solamente una única unidad de dato será mostrada. Para ver más de

una unidad en forma consecutiva ingresar el número en el cuadro de texto inferior.

Es común extraer los espacios no asignados de la imagen de un sistema de archivo y analizarla en busca de datos borrados. La herramienta “blkls” (listado de bloques) de Sleuth Kit permite extraer estos datos. Los datos se encontrarán en el archivo “blkls”, el próximo paso sería encontrar su ubicación en la imagen original y examinar los datos circundantes. Para realizar esto simplemente habrá que calcular qué unidad de datos encontró el dato (dividiendo el desplazamiento del byte del dato de interés por la medida de la unidad de datos (la cual se encuentra en Image Details

– Detalles de la Imagen). Ingresar la dirección dentro del cuadro de texto original y seleccionar el tipo Unallocated –No asignado–. Éste encontrará y mostrará la dirección original de la ubicación del dato previa eliminación. Si Autopsy reconoce la infomación de “blkls”de la imagen, entonces podrá cargarla en cualquier momento seleccionando la opción Load Unallocated (Cargar desasignados), de esta forma se podrá examinar cualquier unidad de dato.

La herramienta Lazarus formaba parte del TCT. Analiza la porción de datos e identifica qué tipo de archivo es y trata de agrupar consecutivamente los tipos. Lazarus enumera sus datos de salida iniciando con el número 1. Por consiguiente, en vez de substraer 1 cada vez que se desea visualizar una unidad de datos identificada por Lazarus, simplemente seleccionar el cuadro de verificación.

Oprimir el botón de Ok para desplegar los contenidos de la dirección del lado derecho de la ventana.

El enlace Allocation List – Lista de Asignación: Muestra el estado de asignación de las direcciones en intervalos de 500.

El botón View – Ver: Luego de ingresar la dirección de la unidad de datos, los contenidos se mostrarán en el lado derecho. Se pueden utilizar filtros para visualizar los datos en diferentes formatos (cadena de caracteres, hexadecimal, ASCII). Por cada formato se puede generar un Report – Informe, de esta forma quedan guardados los contenidos y metadatos en un registro.

El botón Export Contents – Exportar Contenidos: Se utiliza para guardar los contenidos localmente.

La opción Add Note – Agregar Nota: permite al PIF agregar comentarios acerca de la estructura de forma tal que pueda ser utilizado en otra oportunidad.

El tipo de archivo también se muestra, el cual es identificado al ejecutarse la salida

del comando “file” –archivo– de Sleuth Kit.

Autopsy intentará encontrar la estructura de metadatos que asignó la unidad y despliega ambas, su dirección y un nombre de archivo. El proceso es muy lento para los sistemas de archivos FAT, por esta razón este proceso no se ejecuta en forma predeterminada.

Aclaraciones sobre el sistema de archive FAT

Sleuth Kit and Autopsy no utilizan clusters para el tratamiento de las imágenes con sistema de archivo FAT. Solamente se utilizan sectores. Esto se fundamenta en que FAT no empieza direccionando clusters hasta que muchos sectores se encuentren dentro del sistema de archivo.

Si los clusters fueran usados para direccionar unidades de datos, entonces no habría forma de direccionar los sectores en la FAT y en la FAT secundaria. Por consiguiente, se utilizan sectores para todas las direcciones. NTFS cambia la forma en que se direccionan los clusters y no tiene este problema.



Timeline Mode – Modo Línea de T**iempo**

Timeline Mode – Modo Línea de Tiempo:

Para algunas investigaciones la creación de una línea de tiempo de una actividad puede ser útil para identificar lugares donde el análisis debiera empezar. Por supuesto que la fecha y hora podría ser modificada por un atacante, por lo que no son totalmente confiables. Pero Autopsy puede crear una línea de tiempo de la actividad

del archivo. Los archivos tienen por lo menos tres tiempos asociados con ellos. Los detalles de cada tiempo varía con el tipo de sistema de archivo.

Los siguientes tiempos existen para los sistemas de archivos Unix (EXT2FS & FFS):

Modified – Modificado: Cuando el archivo de datos fue modificado por última vez.

Este tiempo puede ser modificado utilizando la función utimes(). Este tiempo se preserva un archivo "tar", por lo que es posible tener M tiempos de archivos antes de que sean introducidos al sistema.

Accessed – Accedido: Cuando el archivo de datos fue accedido por última vez. Este tiempo puede ser modificado utilizando la función utimes().

Changed – Cambiado: Cuando el estado (inodo-data) de un archivo fue cambiado por última vez. Este tiempo no puede ser configurado utilizando la función utimes() .en Unix (pero será con figurado cuando utimes() es utilizado para modificar otros valores).

El sistema de archivo EXT2FS también tiene un tiempo de Deleted –borrado–, pero no se muestra en la línea de tiempo.

El sistema de archivos FAT tiene los siguientes tiempos:

Written – Escrito: Cuando un archivo fue escrito por última vez. Éste es el único tiempo requerido en el sistema de archivos FAT.

Accessed – Accedido: Cuando el archivo fue accedido por última vez, solamente es preciso respecto del día (no en minutos). Es un valor opcional, así que algunos sistemas operativos pueden no actualizarlo.

Created – Creado: Cuando el archivo fue creado. También es opcional, así que algunos sistemas operativos pueden no actualizarlo. De hecho, muchas instalaciones de Windows tienen un C-Time de 0 para directorios tales como C:\\Windows C:\\ Archivos de Programa.

El sistema de archivo NTFS tiene varios tiempos, cuatro de los cuales son utilizados en la línea de tiempo. Estos tiempos son reunidos en el atributo \$STANDARD_INFORMATION

Written – Escrito: Cuando el archivo fue escrito por última vez.

Accessed – Accedido: Cuando el archivo fue accedido por última vez.

Changed – Cambiado: Cuando la entrada MFT fue modificada por última vez.

Created – Creado: Cuando el archivo fue creado.

Procedimiento para crear una línea de tiempo: Se realiza en dos pasos.

El primer paso: Extrae y guarda los datos requeridos de cada una de las imágenes de los sistemas de archivos. En este paso se almacenan los datos específicos de cada sistema de archivo en un formato genérico. Históricamente (el formato de TCT), este archivo se denominaba el archivo principal o cuerpo.

El segundo paso: Utiliza el archivo principal o cuerpo como la entrada y genera una línea de tiempo en ASCII de la actividad del archivo entre dos fechas específicas. La línea de tiempo resultante puede ser vista en Autopsy o en un editor de texto.

Generación del archivo principal o cuerpo (body): El metadatos del archivo debe ser extraído de la imagen del sistema de archivo y guardado en el archivo principal o cuerpo. Existen tres tipos de archivos de los cuales se puede extaer datos:

Archivos asignados – Allocated Files: Son los archivos que se visualizan con los comandos “ls” o “dir”, listar directorio, en un directorio, es decir, que son los archivos que poseen una estuctura de nombre de archivo asignado.

Archivos No asignados – Unallocated Files: Son los archivos que han sido borrados, pero a los que Sleuth Kit puede acceder. Los archivos en esta categoría incluyen archivos huérfanos, los cuales son archivos que no tienen más nombre, pero cuyos metadatos aún existen. Si un nombre de archivo eliminado apunta a una estructura de metadatos asignada, entonces el nombre dirá reasignado (realloc), al lado del mismo.

Pasos para crear el cuerpo (body) del archivo:

Seleccionar las imágenes para analizar de la lista en la parte superior.

Luego, seleccionar qué tipo de datos se desea extraer, en forma predeterminada se extraen todos los tipos.

Posteriormente, identificar el nombre del cuerpo (body) del archivo a crear. El archivo se creará en el directorio como “output” (salida) y una entrada se agregará en el archivo “config”(configuración) del host.

Puede elegir a continuación la opción de calcular el valor de *hash* MD5 del Nuevo

archivo.

Creación de la línea de tiempo: La siguiente ventana permite crear una línea de tiempo base en el recientemente creado archivo principal o cuerpo (body). O se puede seleccionar la opción del lado izquierdo del menú. El rango de fechas debe ser seleccionado así como también el nombre del archivo de línea de tiempo. La línea de tiempo resultante utilizará la zona de tiempo especificada para el host.

Si las imágenes son de un sistema de archivo de Unix, entonces los archivos de claves y de grupo puede ser utilizados para cambiar el UID, identificador de usuario, y el GID, identificador de grupo a los nombres actuales. Si la partición del directorio root existe en el host, seleccionarla de la lista deplegable y Autopsy encontrará el contenido de los archivos /etc/passwd y /etc/group.

La línea de tiempo se creará en el directorio output (salida).

Aparece la opción de calcular el valor de *hash* e MD5 del nuevo archivo.

Visualización de la línea de tiempo: La línea de tiempo se puede visualizar en Autopsy. Las líneas de tiempo suelen ser muy grandes y pueden tener miles de líneas. Los navegadores de HTML no pueden manejar adecuadamente tablas de este tamaño y típicamente tienen problemas para procesarlas. Por consiguiente, Autopsy solamente mostrará las líneas de tiempo de mes por vez. Sería más fácil abrir una Terminal del intérprete de comandos y examinar la línea de tiempo en un editor de texto o por páginas con los comandos “less”o “more”.

El enlace “summary”(resumen) mostrará una página que contine un resumen mensual de actividad. Muestra cuántos sucesos ocurrieron en aquel mes y lo vincula con los detalles. Esto permite obtener un alto nivel de visualización del momento en que ocurrieron por última vez una gran cantidad de actividades.

Elementos de las columas: Las siguientes columnas se encuentran en la línea de tiempo (en orden).

Date and time – Fecha y hora: de la actividad. Si se dan fechas, entonces la actividad ocurrió en el mismo momento que la entrada previa con un tiempo.

Size – Tamaño:. El tamaño del archivo.

Entry Type – Tipo de entrada: Las letras “m”, “a”, “c” y “b” existirán para identificar cuáles de los tipos de actividad le corresponde. La “m” es para tiempos modificados. “a”, es para tiempos de aceso y “c” es para tiempos cambiados y “b” es

para determinar la fecha de creación.

Mode – Modo:

UID. Muestra el identificador de usuario o nombre de usuario. Si el archivo de clave fue ingresado cuando la línea de tiempo se creó, entonces la columna debería tener sólo nombres.

GID – Identificador de Grupo. Muestra el identificador de Grupo o Nombre de Grupo. Si el archivo de grupo fue ingresado cuando se creó la línea de tiempo, entonces la columna tendrá sólo nombres.

Meta Data Address – Direcciones de Metadatos: Las direcciones de entrada de inodo o MFT para el archivo asociado.

File Name – Nombre de archivo: El nombre del archivo y el destino del acceso directo o enlace simbólico. Las entradas eliminadas tendrán ("deleted") o eliminada al final del nombre y las entradas eliminadas que apuntan a una estructura de metadato asignada tendrán ("realloc") o reasignada.

Image Integrity – Integridad de la Imagen

Verificación de Integridad – Integrity Check:

Es muy importante validar siempre la integridad de las imágenes durante el análisis. Autopsy utiliza el algoritmo MD5 para la validación de imágenes y de otros archivos que son creados por Autopsy.

El archivo "md5.txt", contiene los valores del MD5 para los archivos en un determinado directorio. Los valores son agregados al archivo cuando las imágenes del sistema de archivos son importadas dentro del sistema o cuando Autopsy crea el archivo.

Este modo permite al PIF calcular el valor MD5 si no fue creado antes y validar la integridad. Cuando se selecciona el botón de Image Integrity – Integridad de la Imagen de la ventana del Host Manager – Gestor del Host, todos los archivos serán mostrados con sus respectivos valores MD5 si es que son conocidos. Aquí cualquier imagen puede tener su valor verificado o se creará un nuevo valor.

Event Sequencer Secuencia de sucesos

En muchas investigaciones, la evidencia no se encuentra en el orden en que fue

creada durante el incidente. La opción de Comentarios –Notes– de Autopsy permite al PIF realizar observaciones acerca de ciertos archivos, pero no sirve para colocar un conjunto de sucesos en el orden correspondiente.

La Secuencia de Sucesos permite al PIF realizar comentarios y observaciones de las partes de la evidencia. Cada observación debe tener una fecha y hora asociada al mismo. Para los archivos y metadatos, la fecha y hora puede ser una o más tiempos de MAC. Otras observaciones pueden tener tiempos ingresados en forma totalmente manual. El secuenciador de sucesos ordenará los sucesos después de que fue ingresado de forma tal que el PIF pueda rápidamente identificar dónde existen desajustes en los resultados.

Agregar un suceso: Para agregar un evento para un archivo, directorio o una estructura de metadato, seleccionar el botón "Add Note" (Agregar Comentario). En la parte inferior existen unos casilleros de verificación que permiten que se genere un suceso o evento para cada uno de los tiempos de un archivo. La opción de "Standard note"(Comentario estándar) no tiene que ser generada si no es necesario.

Para agregar un suceso de otra fuente: Acceder desde el menú "Host Gallery"(Galería del Host) a la opción "Event Sequencer"(Secuenciador de Eventos o sucesos), donde la imagen se encuentra listada. En la parte inferior de la ventana existe un área donde el nuevo suceso o evento puede ser agregado.

La fuente del evento o suceso se mostrará cuando el nombre de archivo de un evento se muestra normalmente. Ejemplos de este tipo incluyen las entradas en los registros de un firewall o e informes de la mesa de ayuda.

Visualización de la secuencia de eventos o sucesos:

El botón de "Event Sequencer" (Secuenciador de eventos) se encuentra en la "Host Gallery" (Galería del Host). Esta ventana muestra los eventos o sucesos que son ordenados por fecha. Los sucesos que corresponden a un archivo, directorio o estructura de metadato tendrán tanto como [M-Time], [A-Time], o [CTime] en la aclaración que muestra en qué hora se generó un evento. Si se selecciona el nombre se mostrarán los contenidos del archivo o directorio.

Hash Database – Base de datos de Hash

Las bases de datos de *hash* se utilizan para identificar rápidamente archivos conocidos buenos y malos utilizando los valores de verificación de MD5 o SHA-1. Autopsy utiliza tres tipos de bases de datos de *hash* para ayudar al perito informático

forense a reducir el número de archivos que deben analizar.

La Biblioteca de Referencia de Software Nacional (National Software Reference Library -NSRL) del Instituto Nacional de Estándares y Tecnología (Nacional Institute of Standards and Technologies – NIST), contiene los hashes de los archivos que se encuentran en los sistemas operativos y en las distribuciones de software. Estos archivos se conocen como archivos buenos ya que provienen de fuentes confiables y están normalmente en los sistemas autorizados. Cuando se analizan los archivos de una imagen, estas bases de datos pueden ser utilizadas para ignorar archivos porque se asume de que son conocidos y por consiguiente no relevantes. La ubicación de las bases de datos se configura en el momento de la instalación de Autopsy. La biblioteca de referencia NSRL se puede obtener del sitio de NIST en www.nsrl.nist.gov.

La opción Ignorar Base de datos (Ignore Database) es una base de datos que el perito informático forense debe crear. Es similar a la del NIST NSRL, en ella se encuentran loa archivos que se conocen y consideran buenos y pueden ser ignorados si el périto elige esta opción (solamente es aplicable cuando se encuentra en la opción de “Análisis de Categorías de Tipos de Archivos “ (File Type Category Analysis). Los ejemplos de archivos en esta categoría incluyen sistemas binarios para construcciones estándar de programa. Visualizar la opción “Creación de Base de Datos” (Database Creation), para obtener información sobre la creación de esta base. Su ubicación se configura cuando el host es creado y puede ser editada en el archivo de configuración del host.

La Base de datos de Alerta (Database Alert) es una base de datos que debe crear el périto informático forense. La base de datos contiene los *hashes* de archivos conocidos como malos. Existen archivos que un perito desea saber si se encuentran en el sistema. Los ejemplos de estos archivos incluyen *rootkits* o fotografías no autorizadas. Cuando se utliza la opción “Análisis de Categorías de Tipos de Archivos” (File Type Category Analysis), estos archivos se guardarán en un archivo especial. Visualizar la opción “Creación de Base de Datos”(Database Creation) para obtener información acerca de la creación de las bases de datos. Su ubicación se configura cuando el host es creado y puede ser editada en el archivo de configuración del host.

Usos de las bases de datos Database Uses

Autopsy utiliza las bases de datos de tres maneras:

Análisis de las Categorías de Tipos de Archivos (File Type Category Analysis)

Las bases de datos de *hash* son utilizadas para identificar los archivos conocidos como malos e ignorar los archivos conocidos como buenos.

Análisis de los Metadatos (Meta Data Analysis)

La base de datos de *hash* pueden ser utilizados para identificar un archivo de vista de metadatos. Si la base de datos están configuradas, el *hash* de un archivo determinado puede ser observada presionando el botón "*lookup"*. Las tres bases de datos pueden ser utilizadas en esta vista. Esta vista puede visualizarse desde el modo Análisis de Archivo (File Analysis) seleccionando la dirección del metadato en la ventana del listado de directorio.

Gestión de base de datos de Hash (Hash Database Manager)

Desde la vista de Galerías de Host (Host Gallery), se puede ingresar a la Gestión de las Bases de Datos de *Hash*. En este lugar se puede reindexar la base de datos y ejecutar una búsqueda simple de cualquiera de las bases de datos.

Actualmente, Autopsy sólo le permite al perito informático forense buscar dentro de las bases de datos. No le permite al perito crear base de datos con facilidad, pero a continuación se describe el procedimiento (el cual es bastante simple):

Autopsy utiliza la herrmienta *"hfind"*, del Sleuth Kit para realizar las búsquedas. Esta herramienta requiere que la base de datos se encuentre indexada de esta forma se puede ejecutar una búsqueda rápida utilizando un algoritmo de búsqueda binaria (en vez de una búsqueda secuencial más lenta, tal como lo realizaría la herramienta *"grep*"). Cuando se actualiza la base de datos (o se crea), debe ser indexada. Esto puede realizarse en Autopsy en el Gestor de Base de Datos de *Hash* (se debe recordar que la base de datos ya debe estar configurada).

La biblioteca NSRL del NIST, obviamente, no necesita ser creada, pero debe ser indexada antes de utilizarse.

Para crear una base de datos del *hash*, se debe crear un archivo con de mismo formato que utiliza el comando "*md5sum*". El *hash* tiene el siguiente formato: espacio en blanco y el nombre del archivo.

Por ejemplo: c4a6761b486de3c6abf7cf2c554289e5/bin/ps

Se debe crear un archivo con este formato para cada línea (no necesita estar ordenado). Por ejemplo, si se tiene un sistema confiable se puede crear una base de datos de *hash* de los archivos binarios de ese sistema utilizando la siguiente línea de comando:

```
# md5sum /bin/* /sbin/* > bin-md5.db
```

Después de la creación, la base de datos de *hash* debe ser indexada y ordenada (esto incluye la biblioteca NSRL). Las bases de datos serán indexadas por medio del uso de la herramienta *"hfind*". La base de datos NSRL se indexará con la siguiente línea de comando:

hfind -i nsrl-md5 PATH_TO_NSRL/NSRLFile.txt

La base de datos creada con *"md5sum*" será indexada con: la siguiente línea de comando:

hfind -i md5sum bin-md5.db

O si Autopsy tiene este archivo configurado desde el momento en que se agregó el host, entonces puede ser indexada por medio del Gestor de base de datos de *hash* (*Hash* Database Manager).

Configuración en Autopsy

Las bases de datos de Alerta y la de Ignorar se almacenan en el archivo de configuración del host con los encabezados de "exclude_db" y "alert_db". Por ejemplo:

alert_db "/usr/local/*hash*/bad.db"

Las entradas a la base de datos se pueden editar en cualquier momento. La base de datos NSRL se configura en el archivo "config.pl" en el directorio donde Autopsy fue instalado. Utiliza la siguiente variable: $NSRLDB. Por ejemplo:

$NSRLDB = "/usr/local/*hash*/nsrl/NSRLFile.txt".

En base de datos se puede editar, agregar y eliminar registros en cualquier momento, pero se debe reiniciar Autopsy.

Véanse referencias en los Issues 6 y 7 de The Sleuth Kit Informer donde se analizan las bases de datos de *hash*es.

Referencias

Bootable Linux CDs: http://www.sleuthkit.org/links.php

cryptcat

http://sourceforge.net/projects/cryptcat/

dcfl-dd

http://sourceforge.net/projects/biatchux/ netcat

http://www.securityfocus.com/tools/137

NIST CFTT Test Results for Disk Imaging Tools: dd http://www.ncjrs.org/pdffiles1/nij/196352.pdf

Splitting the Disk:

The Sleuth Kit Informer Issue #2 http://www.sleuthkit.org/informer/sleuthkit-informer-2.html#split

UNIX Incident Verification with The Sleuth Kit:

The Sleuth Kit Informer Issue #10 http://www.sleuthkit.org/informer/sleuthkit-informer-10.html#verify

Updated on 1/15/04 to fix the meaning of DCFL. Copyright © 2003 by Brian Carrier. All Rights Reserved

Anexo I Herramientas de Sleuth Kit

Las herramientas Sleuth Kit están divididas en 4 categorías.

La primera muestra información de sistemas de archivos completos y sólo contiene el comando “fsstat”.

El segundo grupo comienza por “d” y nos permite acceder a los datos almacenados en archivos como: “dcalc”, “dcat”, “dls”, y “dstat”.

Sleuth Kit proporciona las siguientes herramientas para información del tipo metadatos almacenada en ínodos: “icat”, “ifind”, “ils”, e “istat”.

Los comandos en el 4º grupo comienzan con “f” y están diseñados para tareas de nivel de archivos como la creación de listas y búsqueda de archivos.

El comando “mactime” muestra los eventos cronológicamente en un sistema.

Los comandos “file” y “sorter” clasifican los archivos en la imagen del disco duro por tipo.

Anexo II Comando: sorter

Función: Ordena los archivos de una imagen en categorías según el tipo de archivo. Ejemplos:

Ejecutar “sorter” sin bases de datos *hash*:

sorter -f ntfs -d data/sorter images/hda1.dd

sorter -d data/sorter images/hda1.dd

sorter -i raw -f ntfs -o 63 -d data/sorter images/hda.dd

Ejecutar “sorter” e incluir la biblioteca NSRL, una exclusión y una base de datos *hash* de alerta:

sorter -f ntfs -d data/sorter -a /usr/*hash*/rootkit.db -x

/usr/*hash*/win2k.db -n /usr/*hash*/nsrl/NSRLFile.txt images/hda1.dd

Para identificar imagenes utilizando el archivo “images.sort”:

sorter -f ntfs -C /usr/local/sleuthkit/share/sort/images.sort -d data/sorter -h -s images/ hda1.dd

APÉNDICE 6
RELACIONES CON LA PRUEBA INDICIARIA NO INFORMÁTICA

Expertos en Balística

Se divide la Balística en interior, exterior, interna y de arribo o efecto. En la interior se estudian los fenómenos que se producen dentro del arma al ser disparado el proyectil; la exterior analiza lo relativo al proyectil desde que sale de la boca del cañón del arma hasta que llega al punto de impacto, en la interna la trayectoria dentro del cuerpo de la víctima (corresponde al médico legista), siendo la caída del proyectil, o el choque de ésta contra un blanco lo que se denomina balística de efecto.

El experto deberá buscar puntos de la trayectoria para identificar la posición del tirador, por lo que no debemos modificar muebles, ventanas o persianas que puedan aportar elementos de juicio. También buscará vainas y proyectiles, sueltos o alojados en muebles y paredes: no debemos moverlos de su lugar, salvo que tengamos la firme sospecha de su desaparición, ante la ausencia de los peritos correspondientes.

en caso de ser imprescindible el secuestro y protección de éstos, se debe documentar la posición exacta de los elementos secuestrados, su descripción técnica y su ampliación macrofotográfica, no se deben limpiar los vidrios provenientes de una perforación por proyectil, ya que permiten identificar la dirección de origen de dicho proyectil.

Armas

No deben ser manipuladas, a fin de evitar la desaparición de posibles impresiones digitales. La forma más común de levantar las armas de fuego es por el arco del guardamonte. La imagen televisiva del empleo de un lápiz o bolígrafo por el cañón es de alto valor iconográfico, pero nada más. Sería interesante observar a un individuo no familiarizado con el uso de armas, tratando de levantar una Ingram M10, cargada y lista para disparar, manipulándola con un lápiz. La seguridad debe ser su preocupación principal. Si como consecuencia de su impericia se produce un disparo y resulta herido o muerto uno de los asistentes al acto, no creemos que la explicación basada en la visión de una serie de televisión deje conforme a la víctima o a sus

deudos. La posibilidad de encontrarnos con armas en condiciones de disparo es escasa, pero no nula, aprender a manipularlas es un deber ético del perito y su inoperancia al respecto no se condice con los requisitos de idoneidad esperados en un profesional de la investigación delictiva. No resulta tan infrecuente en hechos violentos encontrar proyectiles dentro de equipos informáticos, que han escapado a la revisión de los expertos, en estos casos es imprescindible informar a los mismos. Si no se encuentran presentes, informar a la autoridad a cargo, pedir autorización y secuestrarlos siguiendo las normas de protección de cualquier activo informático previo (nunca emplear pinzas en la manipulación de proyectiles, ni forzar su extracción si está incrustado en un objeto).

Las armas blancas deben ser levantadas por los costados de la "s", lo que permite una toma segura y firme y evita riesgos de lesiones propias o por caída. Las armas de fuego o blancas, de ser factible, serán colocadas en cajas de cartón o similares a fin de evitar su manoseo y facilitar el traslado. Siembre descargadas y en el caso de las armas de carga automática con sus cerrojos abiertos y sujetos en dicha posición mediante un precinto plástico.

Proyectiles

En lo posible se levantarán con los dedos enguantados, sujetándolos por los extremos, se los envuelve con gasa y cinta adhesiva, protegiendo la periferia de los mismos. Se los debe rotular e identificar adecuadamente. En lo posible incluir el calibre de los mismos, recordemos que:

Nombre popular	mm	Pulgadas	Largo de vaina
Cuarenta y cinco	11,25	.45	23 mm
Nueve (en pistolas)	9	.38 .380 .357	19 mm 17 mm
Treinta y ocho (revólveres)			
	7,65	.32	21 mm 53 mm
	6,35	.25	11 mm
Veintidós	5,56	.22	10 mm 73 mm

En el caso de escopetas o pistolones, los mismos tienen una numeración de calibre especial de arrastre histórico. En su momento y a efectos de unificar los calibres de las armas, se recurrió a una unidad de peso: la libra. Se tomaba una libra de plomo, se construía una esfera con dicha libra, el diámetro de dicha esfera era el correspondiente al calibre 1. Si se dividía la esfera en dos (media libra) y con cada trozo de plomo resultante, se construían sendas esferas, el diámetro de cada una de ellas correspondía al calibre 2 y así sucesivamente. Por eso el calibre 12 (esferas por libra) es mayor que el calibre 16 (esferas por libra). Se describirá asimismo si es de plomo desnudo o encamisado, si presenta deformaciones, si se encuentra fragmentado, etcétera.

Las vainas servidas requieren mayores cuidados; es necesario proteger la parte posterior (culote), ya que en ese lugar se encuentran las huellas del espaldón, el botador y la aguja percutora, que permitirán identificarla con el arma empleada. Si han sido secuestradas del tambor de un revólver o del cargador de una pistola, debemos dejar constancia del hecho. Idéntico tratamiento debemos utilizar para los cartuchos de bala intactos secuestrados.

Si es imprescindible retirarlos de un mueble, lo mejor es dejar la tarea a los expertos, si esto no es posible es preferible romper un sector relativamente amplio que lo contenga y evitar los daños por actuar directamente sobre el proyectil. Es decir conviene recortar alrededor y mandar el conjunto, sin intentar retirar el proyectil, dejando esa tarea para el correspondiente laboratorio.

Ropas

Cuando presenten deflagración de pólvora se tratará de evitar el hacerles dobleces, con el propósito de no producir desprendimiento. En el acta de inspección judicial, según corresponda, se efectuará un detalle minucioso de ellas: calidad de tela, color, forma, etiquetas, etc.

Cuando presenten manchas de sangre o estén impregnadas con ella, se ventilarán, previamente de su remisión a pericia, en un lugar aireado, preferiblemente fresco, y donde no reciban tierra ni elementos extraños de ninguna naturaleza. Para su envío serán acondicionadas de la mejor forma a fin de evitar, como se dijo, el desprendimiento de la pólvora deflagrada.

Huellas plantares (Retrato del paso) y de vehículos

La Pelmatoscopía se dedica específicamente al estudio, revelado y clasificación de las huellas de pies, calzados, desnudos y con medias. Nuestras acciones al respecto deben tender a documentar fotográfica y gráficamente la posición de las mismas, dejando el levantamiento y traslado en manos de expertos, ya que las técnicas utilizadas para dichas tareas son demasiado complejas para que las realice el neófito y requieren de elementos e instrumental adecuados al efecto. Es conveniente fotografiar con iluminación oblicua y flash. Las consideraciones referidas a huellas humanas se aplican de igual manera a las huellas de vehículos.

Huellas dactilares

También en este caso es preferible dejar la tarea a un experto, no obstante si la huella es muy visible (manchas de sangre, pintura, grasa, etc.) es conveniente documentarlas, realice varias macrofotografías, desde distintos ángulos, con iluminación oblicua y siempre con el uso de flash.

En general se clasifican en visibles (las antes descriptas) y latentes o invisibles, que se forman por la aparición de los exudados cutáneos fisiológicamente normales, originados por las glándulas sebáceas y sudoríparas. Ambas materias, es decir, la sebácea y sudorípara, se depositan en forma de gotitas en las crestas papilares, las que al tomar contacto con otras superficies reproducen el dibujo papilar. Este proceder se origina tanto con las crestas papilares como con las palmares y plantares.

Es importante tener en cuenta que no todos los cuerpos o materias son receptores aptos para registrar y conservar estas impresiones. Los mejores son los que tienen superficie lisa, pulimentada o lustrosa y relativamente limpia. Entre ellos podemos citar el vidrio, cristal (mientras no haya dibujos diminutos labrados), loza, porcelana, hojalata esmaltada, aluminio, cobre y elementos de barro cocido con superficie vidriada. En menor escala, las podemos encontrar en celuloide, marfil, hueso, ebonita, plástico, metal lustroso, barnizado, niquelado, plateado o pavonado, y en papeles, cartulinas y cartón que no tengan granos ni rugosidades. Es digno de destacar que estas huellas son de notable nitidez y, por lo tanto, las más importantes para cuidar, ubicar y trasplantar.

Ante la imposibilidad de deteminar *a priori* el lugar de ubicación de las huellas dactilares, es preferible limitarse a tocar lo menos posible (especialmente las superficies lisas y pulidas) y trabajar en todos los casos con guantes (preferentemente de cirugía).

También entre ellas se ubican las que se denominan *moldeadas,* que se originan cuando el individuo apoya débilmente sus dedos, palmas o planta del pie en elementos no endurecidos o próximos al punto de fusión, tales como materias plásticas, betún, cerámica escayola, masa de pan, velas calentadas por la mano, cera de moldear, material de construcción no fraguado, lacre, masilla, etcétera.

Tal como ya lo expresamos, no es aconsejable el transporte de objetos que presenten huellas digitales, pero cuando ello fuera *imprescindiblemente necesario* se tomarán todas las previsiones posibles para evitar contacto con ellas en su manipulación, así como en el embalaje que se efectúe.

Manchas de sangre

Hay manchas de sangre que por su magnitud se ven a simple vista. Pero hay también algunos elementos maculados (sucios o manchados) que no se perciben inmediatamente, y para detectarlos es necesario el empleo de una lupa cuando los elementos puedan ser transportados a la luz del día, más aún a la luz directa del sol y variando la incidencia de los rayos. Todo elemento manchado debe ser sospechado de interés criminalístico y documentado.

Para describirlas podemos clasificarlas en:

Manchas de proyección (gota, salpicadura).

Manchas por escurrimiento (charco, reguero, goteado).

Manchas por contacto (impresiones sangrientas de manos, pies, etc.).

Manchas por impregnación (embebimiento de prendas textiles, etc.).

Manchas de limpiamiento (del arma, de las manos en un paño, etc.).

Con respecto a la sangre enviada al laboratorio se puede, en general, solicitar lo siguiente:

Si se trata de sangre.

Si es sangre humana o de determinado animal.

Grupo sanguíneo al que corresponde.

Si se puede determinar de qué parte del cuerpo proviene.

Si se encuentran mezclados con ella otros elementos. En caso afirmativo, de cuáles se trata.

Método empleado en cada estudio.

Manchas varias (material fecal, meconio, calostro, semen, orina), pelos, fibras naturales o artificiales

Igual tratamiento que las manchas de sangre.

Documentos

Deben secuestrarse y remitirse en el estado que se encuentran, no deben ser plegados para evitar complicaciones al perito en documentos en el análisis de las zonas de contacto entre los dobleces y el texto del documento.

Suposiciones a priori

Finalizada la inspección podemos tener una hipótesis de cuál fue el hecho ocurrido y de qué forma pudo haberse producido. Pero es aconsejable no basarse solamente en esta hipótesis, aferrándose a la misma; el buen investigador debe prever todas las posibilidades. Ante la duda es conveniente sospechar de todo y de todos. Es preferible no suponer y limitarnos a sacar conclusiones fundadas en hechos comprobables. Es imposible actuar de manera objetiva, pero nada impide que lo intentemos.

APÉNDICE 7
LA ESTRUCTURA LÓGICA DEMOSTRATIVA EN LA LABOR PERICIAL

Demostración lógica y tecnológica de las conclusiones alcanzadas

Cuando usted haya finalizado con el tratamiento de la prueba habrá logrado, sin duda, ciertas comprobaciones experimentales y teóricas que debe volcar en el informe pericial para justificar sus conclusiones. En este punto debe realizar dos tareas formales que le permitirán demostrar sólidamente la pertinencia de su informe:

Separe las demostraciones experimentales de la estructura lógica demostrativa.

Separe en oraciones individuales y sin nexos (ni “o”, ni “y”) las conclusiones alcanzadas.

A partir de estos elementos ejecutaremos una pseudo tarea demostrativa que conferirá consistencia a la demostración. Recordemos que la estructura demostrativa consiste en:

Recolectar información.

Plantear un problema.

Generar una hipótesis (solución *a priori* del problema).

A partir de la hipótesis formular la variable principal.

Determinar los indicadores o variables secundarias necesarios para comprobar o negar la variable principal.

Transformar las variables secundarias en premisas (mediante demostraciones lógicas, teóricas o prácticas, conceptuales o experimentales, según sea el tipo de variable elegida).

A partir de las premisas construir un árbol binario demostrativo silogístico, que deberá converger en la variable principal, demostrando la hipótesis.

Concluir afirmando la hipótesis (o negándola o afirmándola en grado de probabilidad).

Bueno, nosotros actuaremos exactamente al revés para construir la demostración. Como ya hemos alcanzado la o las conclusiones, deberemos realizar todo el procedimiento de atrás hacia delante para construir nuestro árbol demostrativo.

Usted deberá generar un árbol demostrativo por cada conclusión alcanzada. Luego a veces será posible unificar todas las conclusiones en una integración única y otras veces no. Si se logra, esta integración no es nada más que la reconstrucción del hecho. Fíjese que si aplicamos esta estructura a un ambiente multidisciplinario pericial, nos permitiría efectuar una reconstrucción coherente y fírmemente fundamentada desde las distintas disciplinas participantes.

No obstante, nos referiremos en exclusividad a la pericia informático forense. Observe que estamos tratando de armar una estructura lógica coherente, para sobre ésta construir nuestra demostración. Una de las fallas más comunes en los peritos es pretender limitar la demostración a los resultados experimentales. Luego, en el momento de intentar defender la pericia, se quedan de inmediato sin argumentos, ya que nadie está interesado en los números o experiencias realizados, no los entienden, no quieren entenderlos o no tienen ganas ni paciencia para estudiar lo necesario para entenderlos. Por lo tanto toda demostración experimental es sensible y vulnerable a la oratoria y mucho más a la retórica.

Esto no indica que sus experimentos no sirvan, de hecho son la base de toda la demostración, pero deben ocupar el lugar que les corresponde dentro del discurso, para ser válidos y contundentes.

¿En qué momento debo utilizar las demostraciones prácticas y los resultados de los estudios periciales específicos? Únicamente en el momento de transformar las variables secundarias en premisas. Analicemos la acción completa:

He llegado a una conclusión. Ej.: Los fragmentos de archivo detectados en el disco son suficientes para demostrar la existencia de la fotografía X (hemos podido reconstruir el ochenta por ciento de un archivo .JPG, con una imagen pornográfica de las que normalmente aparecen en Internet).

Ahora debo encontrar las premisas. Ej.: Utilizaré como premisa la correspondencia de cada fragmento con el archivo original. Supongamos que he reunido ocho fragmentos. *“El fragmento identificado como 8.JPG, es parte del archivo total.JPG”.*

A partir de estas nueve premisas generaré nueve variables secundarias o

indicadores. Ej.:

"¿Es el fragmento indentificado como 8.JPG, una parte del archivo original total.JPG?".

Ahora tengo ocho variables secundarias. A partir de las mismas construyo mi variable principal. Ej.: *"Son los ocho fragmentos reconstituidos a partir de la información obrante en el disco, parte de un archivo* únic*o, al que llamaremos total.JPG".*

En base a la variable principal construyo mi hipótesis. Ej.: *"Es posible a partir de los fragmentos de archivos detectables en el disco reconstruir una imagen pornográfica de las actualmente obrantes en Internet".*

Partiendo de la hipótesis propongo el problema (en realidad éste debería ser un punto de pericia). Ej.: *"Es posible determinar si el empleado m, posee archivos pornográficos en su computadora".*

Bueno, ya estamos en condiciones de realizar nuestra demostración completa:

Recolectar información. Lo hicimos a partir de las herramientas informáticas aplicadas al disco sometido a pericia.

Plantear un problema. *"Es posible determinar si el empleado m posee archivos pornográficos en su computadora".*

Generar una hipótesis (solución *a priori* del problema): *"Es posible a partir de los fragmentos de archivos detectables en el disco reconstruir una imagen pornográfica de las actualmente obrantes en Internet".*

A partir de la hipótesis formular la variable principal (una variable binaria cuantitativa, es decir mensurable, tal que si se demuestra, queda demostrada la hipótesis): *"Son los ocho fragmentos reconstituidos a partir de la información obrante en el disco, parte de un archivo* únic*o, al que llamaremos total.JPG".*

Determinar los indicadores o variables secundarias necesarios para comprobar o negar la variable principal: *"¿Es el fragmento identificado como 8.JPG, una parte del archivo original total.JPG?"* (esto debemos hacerlo con cada uno de los ocho fragmentos detectados).

Transformar las variables secundarias en premisas (mediante demostraciones lógicas, teóricas o prácticas, conceptuales o experimentales, según sea el tipo de

variable elegida): *"El fragmento identificado como 8.JPG, es parte del archivo total.JPG"* (éste es el punto crítico, debo hacerlo por separado con cada una de las variables, en nuestro caso lo determinamos por poseer todos el mismo número de identificador de archivo, ya sea de entrada en la FAT, o el mismo número de i.nodo en Unix o Linux, ésta es la parte experimental, ya que cada demostración experimental permite afirmar o negar una variable y transformarla en premisa).

A partir de las premisas construir un árbol binario demostrativo silogístico, que deberá converger en la variable principal, demostrando la hipótesis. Ej.: *Ahora reúno las premisas por pares en silogismos válidos.*

Razonamiento Uno (estructura utilizada: conjunción P, Q, entonces P y Q)

Premisa 1: El fragmento 1.JPG, es parte del archivo total.JPG (porque posee el número de inodo 17724).

Premisa 1: El fragmento 2.JPG, es parte del archivo total.JPG (porque posee el número de inodo 17724)

Conclusión: Los fragmentos 1.JPG y 2.JPG, forman parte del archivo total.JPG. (Premisa 9)

Razonamiento Dos (estructura utilizada: conjunción P, Q, entonces P y Q)

Premisa 3: El fragmento 3.JPG, es parte del archivo total.JPG (porque posee el número de inodo 17724).

Premisa 4: El fragmento 4.JPG, es parte del archivo total.JPG (porque posee el número de inodo 17724).

Conclusión: Los fragmentos 3.JPG y 4.JPG, forman parte del archivo total.JPG. (Premisa 10)

Razonamiento Tres (estructura utilizada: conjunción P, Q, entonces P y Q)

Premisa 5: El fragmento 5.JPG, es parte del archivo total.JPG (porque posee el número de inodo 17724).

Premisa 6: El fragmento 6.JPG, es parte del archivo total.JPG (porque posee el número de inodo 17724)

Conclusión: Los fragmentos 5.JPG y 6.JPG, forman parte del archivo total.JPG. (Premisa 11)

Razonamiento Cuatro (estructura utilizada: conjunción P, Q, entonces P y Q)

Premisa 7: El fragmento 7.JPG, es parte del archivo total.JPG (porque posee el número de inodo 17724).

Premisa 8: El fragmento 8.JPG, es parte del archivo total.JPG (porque posee el número de inodo 17724)

Conclusión: Los fragmentos 7.JPG y 8.JPG, forman parte del archivo total.JPG. (Premisa 12)

Razonamiento Cinco (estructura utilizada: conjunción P, Q, entonces P y Q)

Premisa 9: Los fragmentos 1.JPG y 2.JPG, forman parte del archivo total.JPG. (Por razonamiento Uno)

Premisa 10: Los fragmentos 3.JPG y 4.JPG, forman parte del archivo total.JPG. (Por razonamiento Dos)

Conclusión: Los fragmentos 1.JPG, 2.JPG, 3.JPG y 4.JPG forman parte del archivo total.JPG. (Premisa 13)

Razonamiento Seis (estructura utilizada: conjunción P, Q, entonces P y Q)

Premisa 11: Los fragmentos 5.JPG y 6.JPG, forman parte del archivo total.JPG (Por razonamiento Tres)

Premisa 12: Los fragmentos 7.JPG y 8.JPG, forman parte del archivo total.JPG (Por razonamiento Cuatro)

Conclusión: Los fragmentos 5.JPG, 6.JPG, 7.JPG y 8.JPG forman parte del

archivo total.JPG (Premisa 14)

Razonamiento Siete (estructura utilizada: conjunción P, Q, entonces P y Q)

Premisa 13: Los fragmentos 1.JPG, 2.JPG, 3.JPG y 4.JPG, forman parte del archivo total.JPG (Por razonamiento Seis)

Premisa 14: Los fragmentos 5.JPG, 6.JPG, 7.JPG y 8.JPG, forman parte del archivo total.JPG (Por razonamiento Seis)

Conclusión: Los fragmentos 1.JPG, 2.JPG, 3.JPG, 4.JPG, 5.JPG, 6.JPG, 7.JPG, y 8.JPG, forman parte del archivo total.JPG.

Es decir todos los fragmentos forman parte del archivo total.JPG, que como puede verse es una imagen pornográfica de las que habitualmente se encuentran en Internet.

Por lo tanto hemos comprobado la variable principal, lo que demuestra la validez de la hipótesis propuesta, pudiendo concluir que:

"Los ocho fragmentos encontrados en el disco sometido a pericia corresponden a un único *archivo que hemos denominado total.JPG, que contiene una imagen pornográfica de las que habitualmente se encuentran en Internet."*

APÉNDICE 8
LA REDACCIÓN FINAL

Analicemos estrictamente el trabajo anterior:

Desde el punto de vista lógico demostrativo es estricto y se basa en silogismos de validez universal.

Se ha mantenido la estructura estricta silogística (dos premisas y una conclusión).

El árbol demostrativo es consistente.

El pasaje de variables secundarias a premisas está sustentado por una tarea experimental, demostrable y fácil de repetir para cualquier otro perito.

La demostración es impecable. Sin embargo, el mundo no es tan fácil y el mundo de las demostraciones legales menos todavía. Si usted presenta la estructura anterior seguramente no podrán discutirle nada desde el punto de vista lógico, pero ¿usted cree que sus interlocutores entenderán la demostración? No debe sobreestimarlos son personas corrientes, la lógica estricta no forma parte de sus actitudes, de sus pensamientos, de su profesión, ni de su vida de relación.

Ahora viene el golpe de galera. Los pasos anteriores usted no los hizo para volcarlos en el informe pericial. Si es necesario puede discutirlos con cualquier técnico o persona que emplee adecuadamente el sentido común y la lógica (una minoría selecta de las personas). Usted debe hacer los pasos anteriores. Usted debe construir la estructura demostrativa, pero para estar seguro de su trabajo y para evitar ataques formales a su demostración. Es tiempo de que utilice los componentes lógicos anteriores en un discurso claro, conciso, fácil de interpretar y válido para el resto de los mortales que no se encuentran en la minoría referida, ni tienen intención alguna de ingresar a la misma. Ej:

"A partir de la requisitoria pericial encomendada: Determinar si en el disco rígido secuestrado por personal policial y sometido a pericia, se pueden encontrar rastros de imágenes pornográficas, que permitan inferir que el empleado JFK, se dedicaba en su tiempo de trabajo a bajar archivos pornográficos desde su acceso a Internet, el perito que suscribe ha podido establecer que: (en este punto hemos determinado el problema).

A partir de los fragmentos de archivos borrados que han podido ser recuperados del disco 'sub peritia' y seleccionados ocho de los mismos por poseer el mismo identificador de i-nodo (identificación del sistema operativo que asegura la pertenencia a un mismo y único *archivo), es posible suponer que los mismos se correspondan con una* única *imagen que llamaremos total.JPG, por no ser posible determinar su nombre original y en la cual aparece una imagen pornográfica, de las que habitualmente se encuentran en diversos soportes, entre otros en Internet* (en este punto hemos definido la hipótesis y la variable principal).

*Relacionados los ocho fragmentos seleccionados, ha sido posible establecer que los mismos poseen un elemento en común: el número de i-nodo de identificación y por lo tanto corresponden a un único archivo (*acabamos de definir las variables secundarias y las transformamos en premisas).

Reunidos los ocho fragmentos en un único archivo, se pudo reconstruir el ochenta por ciento del denominado total.JPG, que obra en impresión adjunta y que como S Sa puede comprobar de visu, es una imagen pornográfica de las que pueden encontrarse en distintos soportes, entre otros en Internet.

El discurso anterior a simple vista no pasa de ser uno de los discursos técnicos propios de un perito más consustanciado con su profesión que con el arte de sostener, invertir, subvertir, modificar o reinventar la prueba que caracteriza a la retórica del derecho. Sin embargo, estudiemos los puntos ocultos tras su sencilla redacción:

La conclusión indica la existencia de una imagen pornográfica en el disco analizado.

Esta conclusión está sostenida por la experiencia irrefutable (mismo número de i-nodo).

La construcción de la demostración es un árbol binario, basado en silogismos estrictos y perfectamente reconstruible a partir del discurso generado.

Cada una de las comprobaciones está sustentada en un tipo de silogismo válido (conjunción).

Nada hemos dicho respecto de la autoría de la tarea de copiado del archivo. Dijimos que estaba en el disco, ahora bien: si lo puso el empleado JFK, lo plantó la policía o había quedado como residuo de otro empleado anterior, no lo hemos afirmado ni negado.

Hemos dicho que la imagen se corresponde con las que suelen aparecer en distintos

soportes, entre otros en Internet. Si efectivamente fue bajada de Internet o copiada de otro lado, no ha sido afirmado ni negado.

Le tendimos una excelente trampa a un retórico, orador o argumentador desprevenido o que no sea lo suficientemente estricto.

Esta aparente robustez en la demostración es muy útil para armar el discurso defensivo y siempre permite actuar en consecuencia, simplemente porque se trata de un discurso basado en una estructura silogística estricta. Sin embargo, tiene sus puntos débiles, los que por supuesto son muy difíciles de determinar por parte de un adversario lego en su especialidad. En la demostración que hicimos el punto flojo lo constituye el hecho de afirmar que porque ocho fragmentos posean el mismo número de i-nodo, corresponden a un mismo archivo. ¿Es esto cierto?

¿Piénselo? Recuerde cómo actúan Linux o Unix al borrar un archivo. Piense en la posibilidad de reasignación de un i-nodo. Considere la existencia de archivos de tipo link hard. ¿Cabe la posibilidad de que no lo sea? Dejamos esta respuesta en sus manos. Y además suponiendo que no lo sea, ¿esta probabilidad es tan importante como para hacernos dudar de nuestra conclusiones? Éstos son los puntos débiles y difíciles de responder. No debe preocuparse demasiado, su oponente en general tratará de luchar en el campo que conoce: el de la retórica y usted debe defenderse en el mejor campo antirretórico posible: la ironía, la burla, el ridículo, para poder lograrlo hemos recurrido a la estructura lógica, ésta debe ser su mejor aliada.

Generación del informe pericial

Es el momento de integrar los diferentes marcos que dan soporte a su trabajo pericial a saber. El informe debe estar basado en una estricta metodología científica con las modificaciones sistémicas y criminalísticas que la actividad requiere. Debe emplear una demostración lógica estricta y una redacción adecuada al informe a presentar. Las herramientas utilizadas en las experiencias practicadas deben corresponder estrictamente a su función informática y a su pertinencia pericial. La totalidad del informe debe evidenciarse como inserto en un adecuado marco legal. Su estructura ya ha sido tratada en profundidad en esta obra:

Preparación de la defensa escrita/oral

La preparación de la defensa del informe pericial es un proceso arduo y complejo, donde el acervo cultural del perito juegan un rol de importancia primordial. Esta defensa será soportada por una adecuada redacción y una profunda preparación para su defensa oral. Respecto de esta última nos ocuparemos más adelante en el apéndice correspondiente especialmente dedicado a la misma. En cuanto a la redacción, es necesario considerar que se trata de un proceso de comunicación que posee los siguientes componentes:

Un emisor, el autor del documento.

Un medio de transmisión, el documento mismo (impreso, con resguardo electrónico firmado digitalmente).

Un canal de comunicación, la red de distribución del documento y su puesta a disposición del tribunal.

Un receptor y destinatario, el personal del Juzgado que utiliza la información presentada como complemento probatorio de la reconstrucción del hecho supuesta y propuesta como resolución del caso investigado.

El perito es a la vez receptor y productor de documentos, esto lo obliga a generar sus propias consideraciones al respecto.

La redacción se entiende en el sentido de poner por escrito cosas sucedidas, acordadas, observadas, comprobadas o pensadas con anterioridad.

En la redacción podemos distinguir los siguientes elementos:

El sujeto redactor y su entorno.

El instrumento esencial de la redacción, el lenguaje.

El proceso de redacción en sentido amplio y en sentido estricto.

El resultado final de la redacción o informe pericial propiamente dicho.

Se requiere, una buena preparación, paciencia, dominio del lenguaje, buena definición y correcta concatenación de la información. La composición es el arte de desarrollar un tema. Sus etapas son la invención o búsqueda de ideas(reconstrucción del hecho *a priori)*, la disposición o forma de ordenación y la alocución o defensa mediante el uso de la palabra.

Para efectuar la redacción es necesario esquematizar las ideas y planificar el guión

general orientado a las conclusiones. Es necesario redactar con precisión, se deben preferir las palabras y frases concretas y con significado, evitando las exposiciones vacías o de relleno.

Se deben tener en cuenta cuatro aspectos para mantener el orden y el enlace debido de las palabras dentro de las frases: la concordancia (entre género y número de sustantivo y adjetivo y de número y persona entre verbo y sujeto), el régimen (relación preposición-verbo), la construcción (considerando el orden gramatical, el orden lógico, la claridad y la armonía) y la puntuación.[1]

El párrafo tiene una definición delimitada físicamente, es simplemente el trozo escrito entre dos puntos y aparte consecutivos, o entre un encabezamiento del escrito y el primer punto y aparte. El dominio de la redacción del párrafo consiste en la habilidad para darle la estructura adecuada a cada circunstancia. Se puede empezar afirmando la idea principal y luego justificarla o exponer la justificación y luego llegar a la idea, y también combinar ambos procedimientos. El párrafo debe mantener cohesión entre sus oraciones. Este método de ida y vuelta, constructivo y reconstructivo del proceso de demostración, ya ha sido propuesto y analizado con anterioridad en este mismo capítulo.

El capítulo es un resultado del conjunto de párrafos referidos a un mismo aspecto del tema tratado. Cada uno debe tener su guión propio, orientado y centrado en el guión general del trabajo. Es recomendable una cierta uniformidad en la extensión de los capítulos. *"En eso creo yo que está la perfección del estilo, en decir ni más ni menos lo que se quiere decir, y en decirlo con exactitud"* (Azorín).

La redacción pericial debe reunir: claridad, sencillez, precisión, sinceridad, originalidad, inteligencia práctica, rigor y sistematización.

Evitar las generalizaciones sin base empírica seria (inducción).

Inferencias siempre fundamentadas.

Evitar el dogmatismo.

Analizar objetivamente las cuestiones doctrinales, le gusten o no.

Sea objetivo en todos sus análisis.

Descomponga las ideas, distinguiendo sus aspectos principales.

Separe entre hechos y opiniones.

Mantenga una actitud científica, pericial, sistémica y criminalística humilde.

Piense detenidamente cada punto a desarrollar, luego actúe sin demora.

Sea sistemático en la planificación y redacción.

Prepare esquemas, planes y guiones.

Desarrolle las ideas sucesivamente sin solapamientos.

Descanse cuando lo necesite, el esfuerzo prolongado disminuye la eficiencia.

Respecto del lenguaje y del estilo de redacción debe considerar: utilizar un lenguaje técnico en su disciplina y convencional en todos los casos, que sea variado, con estilo personal, inteligente y ágil. Evite la lentitud, destaque sólo los puntos principales, elimine las aclaraciones, incisos y adjetivos innecesarios, utilice los sinónimos (evite las redundancias), asegúrese el correcto empleo de preposiciones, adjetivos, adverbios, partículas, gerundios, no abuse de las expresiones comunes "por tanto", "por consiguiente", tenga en cuenta los párrafos y capítulos, coloque los adverbios y complementos cerca del verbo, en lo posible mantenga el orden gramatical, ponga en primer lugar el complemento más corto y que se identifique claramente al sujeto de referencia, evite las largas cadenas de palabras técnicas o las derivaciones extensas de una palabra, evite el uso del oxímoron, puede resultar incomprensible o contradictorio (palabra formada por elementos contrapuestos como "agridulce").

El punto debemos dividirlo en: a) punto y seguido, sirve para separar temas distintos que, sin ser próximos, no son tampoco lejanos, o se emplea para enfocar desde otro punto de vista un tema que se ha tratado en el ámbito anterior, o para fraccionar por su excesiva longitud o ante una dificultad de redacción, un mismo punto de vista,

b) el punto y aparte, separa ideas que guardan una relación lógica lejana y c) el punto final separa ideas remotas entre sí, más lejanas, como ocurre entre los temas de distintos capítulos, o finaliza el trabajo.

Las notas son advertencias, explicaciones, comentarios o noticias de cualquier clase que en los manuscritos van fuera del texto, ya sea al margen de los folios, al fin de la obra o de cada una de sus divisiones con una llamada en el lugar del texto que corresponda, las citas son la presentación textual o resumida de ideas de otros autores que sirven de apoyo al investigador, se contraponen a lo que dice o proporcionan mayor información.

En general las citas pueden clasificarse en ideológicas o resumidas y textuales. Las notas se pueden colocar al pie de página, en los márgenes, al final del capítulo o al final del trabajo. Respecto a las citas textuales, se deben disponer:

Incorporadas al texto, entre comillas y luego de dos puntos.

Situadas aparte, separadas del texto del autor. Algo útil en caso de citas largas.

Para consignar las referencias bibliográficas de la obra existen dos formas:

de cita nota, la referencia se coloca como nota al pie de página o al final del capítulo o de la obra,

autor y fecha, se elimina la cita nota y en su lugar se consigna en el texto, después de la cita y entre paréntesis, el nombre del autor y la fecha de la obra citada luego de punto y coma y la página.

Reglas para las citas

Literatura crítica (sólo cuando con su autoridad corroboran una afirmación nuestra).

La cita supone que comparte la idea citada (si no es así, debe ser aclarado).

Las citas de fuentes primarias deben hacerse del original o de la edición más acreditada.

Los autores extranjeros deben citarse en su idioma original con su correspondiente traducción.

Las citas deben ser exactas y completas, para admitir el cotejo.

Las citas deben ser selectas.

Se deben evitar las citas de segunda mano.

Las referencias bibliográficas de las citas deben ser precisas.

Si es necesario se puede recurrir a la transliteración, entre obras escritas con alfabetos distintos del latino, por ejemplo, griego antiguo o ruso, manteniendo la correspondencia entre ambos alfabetos.

La posredacción

Consiste en las operaciones posteriores a la redacción destinadas a perfilar, completar y dar forma definitiva al informe. En el caso de los informes de investigacion, implica la revisión y la aprobación por el director de la investigación, además es conveniente darla a leer a especialistas amigos y escuchar sus sugerencias. En nuestro caso particular implica la revisión técnica profunda del producido pericial, de ser posible debe ser realizada por un tercero, ya que tendemos a pasar por alto nuestros propios errores y faltas de claridad en la exposición.

Respecto de la presentación

La presentación debe ser artística y armoniosa, si no es posible al menos correcta y limpia.

Debe ajustarse a las normas legales y a las formas en uso en el foro judicial considerado en general y en la jurisdicción específica en que desarrolla sus tareas. Estos detalles son especialmente tenidos en cuenta por los letrados.

Debe mantenerse la uniformidad formal previamente establecida.

Respecto de la forma de presentación

Para el papel, en general, tamaño A4.

Márgenes uniformes en blanco a derecha (3,5 cm), izquierda (1,5 cm), arriba y abajo (2 cm).

Inserte su propio encabezado, genere un logo, aporte un aspecto formalmente profesional a su trabajo.

Sangrías o espacios en blanco antes de empezar los capítulos y párrafos.

Espacios proporcionales de separación entre líneas, párrafos y títulos.

Disposición de los títulos de capítulos y parágrafos.

Pautas adecuadas a seguir respecto de los destacados de palabras o frases y escritura de números, mayúsculas, abreviaturas y siglas.

Numere las hojas e identifique el informe en el pie de página. A tal efecto lleve un registro de las informes periciales, asignando un número de pericia específico e irrepetible a cada uno. Para evitar dejar en evidencia un carácter de neófito numere e incluya el año (si usted coloca Informe pericial N° 1, todo el mundo sabrá que es su primera pericia, por lo menos en esa jurisdicción, si coloca 1/04, evita tal disquisición, recuerde que nunca debe aportar armas gratuitas a sus oponentes).

Numere los renglones escritos del informe (todos los procesadores de texto actualmente en uso cuentan con esta función). Al finalizar deje constancia de la cantidad de páginas del informe y del número de renglones escritos que lo componen.

Mayúsculas: Usarlas al principio de la palabra, al empezar la oración. En los restantes casos, ante la duda, preferir las minúsculas.

Números y fechas: Usarlos con moderación, una norma admitida es escribir en letras los adjetivos numerales del cero al veinte y las cifras redondas, las fechas con números y es preferible no poner genitivos “20 abril 1953”, en lugar de “20 de abril de 1953”.

Abreviaturas y siglas: Las primeras son palabras abreviadas o con menos letras, las siglas en cambio, son palabras formadas con las iniciales de varias palabras. Las primeras llevan punto al final, las segundas no deben llevarlo y todas sus letras se escriben con mayúsculas. En las tesis y trabajos científicos no es conveniente utilizar abreviaturas, cuando las siglas son muchas se suele ofrecer un índice de siglas o incluirlas en el glosario.

Comillas, paréntesis y corchetes: Podemos distinguir tres tipos de comillas:

inglesas dobles (“ ”), para las citas textuales,

inglesas simples (‘ ’), para textos que van dentro de otros más amplios también entre comillas,

francesas (« »), para diferenciar textos por alguna razón especial, por ejemplo para distinguir el significado de una palabra.

Los paréntesis sirven para separar de ámbitos más amplios oraciones, frases o

palabras, en sentido aclaratorio o secundario. Los corchetes se utilizan para distinguir los paréntesis dentro de los paréntesis más extensos, las palabras reemplazadas por conjeturas o las aclaraciones del autor dentro de dicho texto.

Bastardilla o itálicas, según Umberto Eco se destacan:

Las palabras extranjeras de uso no común o no castellanizadas.

Los nombres científicos de animales, plantas, etc.

Los términos técnicos que se quieran destacar.

El enunciado de tesis o demostraciones finales.

Los títulos de libros, poemas, diarios, revistas, películas, canciones y óperas.

Entrega formal del informe pericial

Antes de efectuar la entrega formal del informe pericial realizado, es necesario controlar que se hayan efectuado las siguientes tareas (es conveniente agregar a cada informe pericial un pequeño volante con el detalle de la actividades realizadas, para poder efectuar un seguimiento real de todas las pericias en trámite de manera sencilla y efectiva):

Confección del informe pericial en formato digital.

Corrección con fundamentos científicos, criminalísticosy sistémicos de las operaciones realizadas.

Control de la lógica asociada con la demostración planteada.

Corrección sintáctica y ortográfica del texto digitalizado.

Corrección de estilo (redacción adecuada, eliminación de redundancias y errores de dicción, adecuación del lenguaje utilizado a los conocimientos esperados entre los lectores, eliminación de elementos superfluos, inclusión de aclaraciones y notas a pie de página, adecuación del glosario y toda otra tarea que contribuya al perfeccionamiento literario del escrito desarrollado).

Impresión de una copia para corrección.

Lectura del informe realizado por un tercero.

Corrección final acorde a la lectura anterior.

Generación de una copia digital en soporte removible (disquete o CD) que se entregará junto con la pericia impresa en papel.

Ejecución de un *hash* de la copia digital realizada.

Inclusión del *hash* de la copia digital, como un archivo adjunto en el soporte digital a entregar junto con el informe escrito. Este archivo conteniendo el *hash* de la pericia debe ser firmado por la clave privada del perito.[2]

Impresión del original para ser entregado y una copia para el perito.

Confección es impresión de un resumen del trabajo (síntesis al estilo de los "abstracts" de las obras literarias), el que será incluido en una ficha, que será archivada con fines de búsqueda rápida posterior. Al respecto, resulta muy útil la confección de un pequeño formulario de resumen, resguardado en una carpeta (directorio) especial.

Finalizadas estas tareas, se efectuará la entrega formal del informe pericial en el tribunal que la solicitara. Se entregará al Juzgado:

El original impreso del informe pericial efectuado.

Una copia digital del informe en soporte removible (disquete o CD)

La totalidad de los elementos sometidos a pericia.

La totalidad de los documentos entregados en custoria al perito (expedientes, cuadernos de prueba, actas, etc.)

Se solicitará el sellado, firma y fecha de recepción por parte del empleado del Juzgado que lo recibe, en la última hoja de la copia de la pericia (que contendrá un detalle de todos los elementos devueltos, incluyendo la copia digital del informe y el *hash* adjunto)[3] los elementos agregados y los elementos devueltos.

1 El punto y coma sirve para separar oraciones no análogas pero sí con una proximidad de sentido entre sí.La coma separa elementos análogos del ámbito: palabras, frases, oraciones e indica entre ellas una relación lógica de semejanza.Los dos puntos se pueden distinguir en tres grupos: a) separa ideas

próximas lógicamente, de las cuales la última, precedida por los dos puntos constituye una aclaración, consecuencia o resumen de las precedentes, b) se emplea luego de los tratamientos de cortesía o de jerarquía, c) antes de una cita textual.

2 En el cierre y elevación del informe pericial, deje constancia expresa de los archivos que han sido adjuntados al informe en formato digital (en lo posible en soporte óptico del tipo CD-ROM) y el pedido expreso de que dichos elementos sean desglosados de la causa y reservados en la secretaría a efectos de preservar una copia digital certificada por el perito, asegurando su integridad y no repudio.

3 El *hash* del informe pericial en formato digital conforma parcialmente la firma digital del mismo por parte del perito. En este punto se produce un problema de inconsistencia lógica que debemos solucionar. En efecto, si hacemos el *hash* del informe digitalizado y luego pretendemos incluirlo en el informe, al hacerlo modificamos el informe y debemos hacer un nuevo *hash*, que provocaría la modificación del primero y… (resultado paradójico por ser un círculo vicioso). Para resolver este problema, una vez finalizada la corrección definitiva del informe pericial, lo grabamos en el soporte elegido y efectuamos el *hash* sólo del archivo. Este *hash* lo incluimos en un archivo de texto y lo ciframos con nuestra clave privada, incluyendo nuestra clave pública (o certificado digital otorgado por alguna autoridad certificante) en otro archivo y entregamos estos elementos al Juzgado.

Las ventajas de actuar de esta manera son evidentes, ante la posibilidad de pérdida o extravío del informe escrito entregado.

El *hash* y la firma digital del informe (con inclusión de su clave pública o mediante un certificado digital), nos asegurará la integridad y autoría del mismo y constituirá un elemento de prueba indiscutible, ante futuros inconvenientes legales (robo de hojas, extravío de informes, modificaciónes de textos, inclusiones o sobreescrituras espurias, etc.) Se recomienda grabar todos los elementos a remitir en un disco óptico (CD-ROM, nunca utilice CD del tipo RW), dado el escaso costo de los mismos. Cerrar la sesión, para evitar inclusiones en dicho CD y grabar los informes en algún formato que reduzca la posibilidad de fraude Ej.: Acrobat de sólo lectura con clave de acceso.

La seguridad que estamos aportando a nuestro informe digital nunca será suficiente y por lo tanto debemos complementarla con toda otra medida que nos parezca adecuada (permisos y atributos de sólo lectura para los archivos incluidos y demás mecanismos de seguridad disponibles en el SO o en programas de aplicación). Respecto de la validez legal de este procedimiento, si bien los Códigos de Procedimientos no especifican nada en particular, la validez de la firma digital está asegurada por la Ley de Firma Digital (25.506) y su uso ya ha sido especificado en varios Cuerpos Legales.

Ej.: Art. 224 (modificado por ley 25.434) del CPPN al referirse al allanamiento de morada "…(Incorporado por ley 25.760) En caso de urgencia, cuando medie delegación de la diligencia, la comunicación de la orden a quien se le encomiende el allanamiento podrá realizarse por medios electrónicos. El destinatario de la orden

comunicará inmediatamente su recepción al Juez emisor y corroborará que los datos de la orden, referido en el párrafo anterior, sean correctos. Podrá usarse la firma digital. La Corte Suprema de Justicia de la Nación o el órgano en que ésta delegue dicha facultad, reglamentará los recaudos que deban adoptarse para asegurar la seriedad, certidumbre y autenticidad del procedimiento".

APÉNDICE 9
LA DEFENSA ORAL

La defensa ante el tribunal

Esta parte de la pericia constituye una de las más difíciles de planificar por parte del perito, es necesario tener en cuenta:

Casi siempre nuestra pericia será beneficiosa para algunos y perjudicial para otros.

Aquellos que vean afectados sus intereses por nuestras conclusiones tratarán de rebatirlas o al menos de reducir su peso probatorio.

Las circunstancias anteriores implican la necesidad de las partes involucradas o de sus representantes legales de impugnar la pericia. (Casi toda pericia es impugnable por algún motivo formal o de fondo, por lo tanto casi toda pericia termina siendo impugnada por alguien.)

Prepararse para la respuesta a la impugnación es una de las tareas del perito y depende de su capacidad profesional y de la estricta fundamentación científica, lógica, criminalística y metodologíga de las conclusiones alcanzadas.

Por otra parte el perito será llamado siempre en la etapa de sentencia (y a veces en la de investigación), para ratificar sus dichos y conclusiones en presencia del tribunal.

Ante esta realidad, el perito debe prepararse para ejercer una defensa adecuada de su labor profesional. Consideramos tan importante este punto, que hemos agregado un anexo específico referido al entrenamiento para la defensa escrita u oral, ya que la oralidad comienza a ser la regla y no la excepción en la modalidad utilizada para los juicios en nuestro país.

Esto puede llegar a complicarse aún más si se impone el juicio por jurados que establece nuestra Constitución Nacional y que hasta el momento no ha sido implementado, salvo parcialmente en algunas provincias, genera:

Los jueces, debido a su labor tienen una profunda experiencia en el análisis e interpretación de la prueba pericial, tal vez no reconozcan las operaciones técnicas implicadas, pero saben a qué atenerse, respecto de la pertinencia de la prueba y su implicancia dentro del juicio.

Por el contrario los jurados están constituidos por personas generalmente sin formación legal, que tienden más a dejarse convencer por la oratoria que por una técnica que no comprenden, que les parece oscura, les requiere un esfuerzo intelectual y les genera rencor o envidia (*"lo que no se conoce se teme, se odia o se envidia, en ese orden")*, por lo que la dialéctica y la retórica se convierten en armas fundamentales en el arsenal demostrativo del perito en cualquier especialidad criminalística.

La defensa oral de un informe pericial es un tema delicado y que involucra una serie de elementos que escapa al análisis estricto que hemos propuesto en este manual. En efecto, el perito se encontrará en una situación muy especial, en un entorno poco habitual y con reglas de juego diferentes de las habituales en el ambiente científico-tecnológico.

Planifique su defensa de la misma manera en que planificó su investigación. Es necesario tener en cuenta algunos detalles que aunque triviales contribuyen a aumentar sus posibilidades de éxito. Quienes hemos tenido la fortuna de peregrinar por diversas salas de audiencias y en distintos entornos judiciales, hemos podido establecer algunas reglas generales que pueden serle de utilidad. Las mismas no se incluyen de manera alguna en la formación pericial sino son el producto de la recopilación de experiencias personales compartidas con otros expertos, en similitud de circunstancias:

No es bueno que su vestimenta demuestre una posición económica demasiado solvente.

En general no se espera que el profesional triunfe demasiado. Al parecer el científico creíble no debe poseer, ni aparentar riqueza. Este simple hecho implicaría reconocer que existen personas capaces de pensar, deducir, evidenciar un alto poder de abstracción y con estos elementos ganar dinero.

La realidad nos indica que el saco y la corbata son los uniformes de rigor. Es un hecho fácilmente comprobable que los empleados y jefes de bajo nivel utilizan saco y corbata como parte de su pseudo imagen profesional. Un ambo de colores clásicos y escaso precio, constituirán su mejor tarjeta de presentación y se ajustarán a la perfección a la imagen esperada. Respecto de las mujeres, la vestimenta no tiene importancia, si en la barandilla son atendidas por un adscripto a la masculinidad, siempre serán recibidas, en caso contrario siempre serán criticadas.

Evite las vestimentas excéntricas. Entre la excentricidad y el ridículo sólo hay un paso y este paso lo determina el poder. Si usted ha aparecido en la tapa de *Fortune*, *Nature*, *Times* o *Playboy* y utiliza un moño violeta con pintas amarillas o un sombrero

de tul, será considerado excéntrico. Si usa estas prendas, pero su más importante aparición en público fue la fotografía de su nacimiento en el álbum familiar, su imagen será simplemente absurda.

No utilice ropas que estén en desacuerdo con su edad cronológica (no la que surge de su imaginación o deseos personales). La juventud y la belleza son una cuestión estética y no un problema de actitud o de manera de pensar, como suelen sugerirlo los comerciales televisivos.

Evite los ingresos impactantes y las actitudes desafiantes. Ingrese a la sala con naturalidad, espere a que le indiquen dónde debe sentarse y cuando lo hagan muéstrese ligeramente sorprendido. Esto aumentará su aspecto inexperto y relajará los ánimos a su alrededor.

Tenga en cuenta en todo momento que entre quienes lo observan seguramente se encontrarán su o sus potenciales interlocutores y que éstos estarán pensando: *"este tecnicucho ni se imagina lo que le espera"*, mientras conserven esa sensación usted tendrá todas las posibilidades de actuar ante un interlocutor desprevenido y si actúa adecuadamente, no necesitará repetir este accionar (sumamente riesgoso en caso de ser reiterado, pocos tropiezan dos veces con la misma piedra).

En el tribunal oral, usted ocupará una posición central en la sala y esto no es casual. Estará siendo interrogado por especialistas en interrogatorios, no por especialistas en su área pericial. Estará sentado en medio de un entorno en el mejor de los casos indiferente y casi siempre francamente hostil. Su presencia en general será una molestia objetiva o subjetiva para la mayoría de los presentes. Estará frente al tribunal rindiendo cuentas de su labor pericial, en medio de ciertas condiciones generales que intentaremos detallar, a efectos de que no ejecute lo que todos hemos pensado la primera vez que pasamos por este trance: salir corriendo, volver a casa, cerrar la puerta, desconectar el teléfono y soltar al perro.

La legislación vigente: Usted está actuando como testigo, le comprenden las generales de la ley, desde el Código de Fondo (Falso Testimonio), el Código de Procedimientos particular de la Jurisdicción en que se desarrolló la pericial, las leyes complementarias y la jusrisprudencia relacionada con el tema sub peritia y su entorno legal. Estos elementos pueden jugar a su favor si usted los utiliza adecuadamente, para ello debe conocerlos. Es imprescindible que conozca a fondo no sólo la legislación de fondo, sino especialmente y en particular la legislación de forma aplicable en el lugar y sus leyes asociadas y de ser posible alguna jurisprudencia establecida ante casos similares.

El público asistente: Usted está de espaldas al público, donde existen intereses

particulares, muchos de los cuales son contrarios o contradictorios con su informe pericial. Pocas personas, salvo los especialistas (abogados, procuradores, estudiantes de leyes) concurren voluntariamente a presenciar un juicio. La mayoría de la población se conforma con el resumen televisivo correspondiente. Por lo tanto, en general, quienes están presentes, pretenden una decisión judicial favorable a sus intereses. Ya sea que la sentencia afecte intereses familiares, de amistad, de venganza, económicos, la visión de los concurrentes al acto, casi nunca es imparcial. Nunca debe esperar apoyo por parte de estos espectadores, pero tampoco debe dejarse influir por sus reacciones (voces, gritos, insultos, cada vez más frecuentes y tolerados).

El tribunal interventor: No sólo se trata de un organismo destinado a evaluar hechos, sino que de hecho es un tribunal evaluador y en el presente caso el evaluado es usted. El tribunal tiene muy claro su rol, conoce su poder decisional, de ninguna manera se supone frente a iguales (el juicio entre pares, al parecer sólo funcionó en la poesía y por un período limitado, en la Mesa Redonda del rey Arturo, hasta el asunto ese de Lanzarote y Ginebra, que cambió definitiva las reglas de juego). En ese contexto el tribunal que se sabe todopoderoso hace un acto implícito de reconocimiento de ignorancia: deben consultar a un supuesto experto, sobre un tema del que no conoce lo suficiente. Este hecho no es demasiado propicio para los integrantes del tribunal, ni muy positivo para sus egos particulares. Recordemos que estamos en presencia de hombres. Los hombres en general, siempre creerán poder opinar sobre cualquier tema en particular, con la solvencia de un experto.

El tribunal de ninguna manera acepta su superioridad como experto en ningún campo. Si se trata de un tema que conoce de oídas, por referentes familiares, afectivos, amistosos o simple curiosidad, usted tiene muchas probabilidades de ser ignorado en aquellas afirmaciones que se opongan a la creencia del juez. Es un simple tema de confiabilidad, desde que nacemos confiamos más en nuestros afectos, entorno familiar, amigos y colegas. En definitiva, cambiar las creencias es muy difícil y resulta mucho más complicado si intentamos hacerlo desde un lenguaje científico o tecnológico.

El fiscal: Su accionar suele ser bastante aséptico, en general podemos esperar una actitud espectante o indiferente. Si nuestra pericia aporta elementos que justifiquen sus afirmaciones para implicar al acusado, nos hará las preguntas estrictas y necesarias para respaldar su petición. No participará demasiado salvo para interrogarnos buscando confirmación sobre los aspectos que le interesen. Por el contrario si nuestra pericia contradice sus afirmaciones, podemos esperar un accionar bastante lógico y sumamente procedente. Discutirá los puntos en duda que lo favorecen, pero lo hará desde una actitud profesional y estricta, donde dependeremos de nuestros conocimientos técnicos y no de nuestra capacidad histriónica. Además tendremos un

aliado: el abogado defensor.

El abogado defensor: Ésta es una relación sumamente dificultosa de planificar. El abogado defensor, debe defender a su cliente, está obligado materialmente a hacerlo. Esta defensa es independiente de la calidad humana del acusado y de la autoría del mismo sobre los hechos imputados. Por lo tanto, siempre toma su tarea con el fervor profesional que le merece. Si nuestra pericia aporta datos a favor de su defensa, será un excelente aliado, intervendrá en nuestra defensa en contra del fiscal, justificará nuestros errores discursivos y apoyará nuestras conclusiones. Por el contrario, si la pericia aporta elementos en contra de su cliente, será un enemigo feroz, del que debemos defendernos con nuestras propias armas y sin esperanza de alianza o ayuda externa alguna. Éste es el peor de los casos. Por lo tanto es necesario que nos preparemos y nos entrenemos. Nuestra única aliada será nuestra capacidad dialéctica y una decidida actitud retórica. El soporte científico, criminalístico y tecnológico ya lo hemos adquirido, la retórica depende de nosotros. Recuerde que:

En este mundo traidor, nada es verdad ni mentira, todo es según el color del cristal con que se mira. (El hombre como especie, es un sofista especializado en la búsqueda del poder para obtener placer, no un filósofo altruista.)

Usted no es un auxiliar de la Justicia (un bien difícil de definir y sobre el que es prácticamente imposible arribar a un acuerdo entre dos personas, mucho menos en una sociedad cosmopolita y polifacética como la nuestra), sino por el contrario un auxiliar de la ley (la ley no siempre tiene que ser justa, más aún, es casi imposible que lo sea, por su propia naturaleza basada en el consenso de quienes detentan el poder). Usted debe ajustar su discurso a la norma legal, no a sus convicciones personales, científicas o tecnológicas.

El discurso se basa en capacidades adquiridas generalmente mediante la lectura. Este proceso de integración de vocabularios incrementa la disponibilidad de conceptos para integrar en la argumentación oral. Cuanto más vocablos conocemos, más variantes oratorias podremos crear y expresar. Si quiere mejorar su dicción, incremente su lectura. En lo personal pensamos que las personas piensan como escriben y hablan como piensan (de ahí las dificultades de comunicación intergeneracional).

La lucha se presenta entre usted y un abogado entrenado para argumentar. Él tiene la ventaja oratoria (no siempre la suficiente capacidad retórica) y la desventaja en conocimientos específicos periciales. Su caso es inverso. El abogado difícilmente se interesará por los temas primordiales de su actividad pericial y con las ciencias involucradas en los mismos. Intentará llevar la discusión al campo legal, o de

conocimiento vulgar, porque allí se siente superior. Usted nunca podrá llevarlo a su campo de conocimiento, principalmente porque requiere de un lenguaje específico que no conocen los restantes integrantes del acto testimonial. Por otra parte, los demás tampoco están interesados en conocer los detalles de una ciencia que aparece como aburrida, tediosa, más propia de "ratas de laboratorio" que de personas normales, bellas, inteligentes y divertidas como todos deberíamos ser o al menos tender a ser. Pero precisamente estos hechos pueden jugar a su favor. Nadie y mucho menos el abogado espera que usted lo enfrente en su propio terreno (recuerde a Alejandro y Napoleón), la mejor defensa es un ataque y si logra dividir, casi seguro vencerá.

Generalmente, el discurso del abogado está destinado a convencer al tribunal (ya que no tenemos juicio por jurado, pese a lo que pueda decir la Constitución Nacional), atraer la simpatía de los concurrentes y demostrar su superioridad frente a un técnico obcecado y de escasas luces. La estrategia debe orientarse a lo formal no a lo protocolar que constituye el punto débil en la oratoria de nuestro interlocutor.

No es cierto (o es muy raro) que el operador con el que interactúa conozca profundamente la ley y sus implicancias, ni que sea un experto doctrinario legal.

Fundamenta sus dichos en una preparación más o menos superficial del tema, ya que no deberá explicar los fundamentos legales ante sus pares y hará lo posible para que el resto no los entienda. Esta afirmación no constituye una descalificación de la tarea legal técnica, simplemente, al igual que otras profesiones, el impulso inicial estimulado por la vocación y la novedad de la tarea encarada se va diluyendo con el tiempo y de a poco se convierte en hábito y luego en rutina. Esto mismo pasa en nuestra profesión, se hacen tantas pericias, se tiene que atender tantos temas a la vez, que llega un momento que uno supone que sabe.[4] Éste es el peor enemigo de todos, el suponer que sabemos, porque nos hace confiados y por lo tanto vulnerables. De ahí que recurrentemente utilicemos las mismas técnicas una y otra vez, como si se tratara de una clase muchas veces repetida. Es por eso que el operador con el que interactúa raras veces realizará su discurso a partir de una metodología formal estricta (formalidad que sólo aportan la lógica, los mecanismos inductivo-deductivos en tiempo real y el correcto manejo de las estructuras silogísticas).

Recuerde que el punto más doloroso de la anatomía humana es el ego. Nadie quiere hacer el ridículo, mayoritariamente pretendemos ser llamados por nuestros títulos reales o supuestos y siempre buscamos la aprobación explícita o implícita. Aun en la supuesta modestia de decir: *"no me diga doctor, llámeme Hugo, nomás"*, se da por sentado con claridad que: *"soy doctor y me dejo llamar Hugo, por usted, no por nuestra igualdad, sino por mi condescendencia".* Diríjase siempre al tribunal con el respeto que se merece (o que cree merecer). Los tratamientos tales como Su Señoría,

Vuestra Señoría, etc. no por anticuados han dejado de tener validez y aportan un aspecto de colaboración sumisa, que siempre será bienvenido desde el estrado. Por el contrario, los abogados, en general, necesitan ser llamados doctores (tengan o no un doctorado).[5] No pierda de vista que el tribunal también está integrado por abogados.

Si detecta una actitud hostil por parte de un abogado, apunte a donde duele, diríjase a él, como a un par o subalterno, nunca lo llame doctor, hable a él o de él, en tercera persona *"como dijo el abogado X"*, *"pese a lo que evidencia desconocer el abogado X, respecto de..."*, trátelo como lo haría con un estudiante que no entiende nada, fínjase comprensivo ante sus falencias, corríjalas de manera extensiva, lenta, recalcitrante.

Una técnica simple para defenderse de un discurso agresivo es:

Escuche atentamente lo que su contraparte expone.

No lo interrumpa.

Adopte una imagen reconcentrada y atenta. Por ejemplo, incline levemente la cabeza, observe a su interlocutor con los ojos entrecerrados. Nunca y por ningún motivo mire en este momento al tribunal, no busque comprensión, ni complicidad; no la encontrará.

Recuerde, que la mayoría de los presentes son abogados y por lo tanto tienen una afinidad profesional inevitable e innegable con su interlocutor. Usted debe revertir esta situación logrando establecer una brecha entre el tribunal y su adversario verbal. Esto no lo logrará buscando complicidad, sino haciendo notar que los argumentos de su interlocutor no son lógicamente sostenibles o resultan *"un poco raros"*. Si usted lo consigue, el tribunal pondrá distancia subconsciente con su interlocutor. Lo reconocerá aun como un par, pero como un par de menor nivel (algo así como la llamada *vergüenza ajena*) y si bien no se inclinará de su parte, al menos adoptará una actitud de neutralidad, ideal para el triunfo de la ciencia sobre la retórica.

Ante los intentos de desacreditación verbal discursiva, afirme con la cabeza (esto tranquilizará a su interlocutor y le restará contundencia argumentativa), él supondrá que se encuentra ante un oponente de menor valía y le aportará a usted una ventaja competitiva sumamente útil.

Mientras tanto, busque, detecte y recuerde las generalizaciones o particularizaciones en que basa su interlocutor sus argumentos.

Ahora replique:

Ante las generalizaciones deduzca: Busque un caso particular absurdo e irrisorio y expóngalo con aire de ingenuidad. No existe norma sin excepciones y esta circunstancia, siempre jugará de su parte.

Ante las particularizaciones induzca: Argumente las mismas hacia una generalización del mismo tipo anterior (absurda o ridícula). Como a partir de un hecho aislado, siempre es posible alcanzar generalidades inconsistentes, otra vez la lógica argumentativa jugará de su parte.

Si frente al empleo del método anterior su interlocutor intenta explicar o contradecir sus dichos, se meterá en un berenjenal argumentativo de naturaleza tal que difícilmente logrará salir airoso de la contienda.

Usted debe alcanzar (mediante el entrenamiento adecuado) la capacidad de argumentar por el absurdo, pero con soporte teórico científico real o supuesto y con un soporte lógico estricto.

Su lado flojo es la retórica, el lado flojo de su interlocutor es el desconocimiento técnico pericial. Recuerde que no puede esperar piedad, defensa externa, ni ayuda divina alguna, su interlocutor está preparado para destruirlo. No crea, ni suponga que se trata de una animadversión personal. Así como su tarea pericial es intentar analizar la prueba para modelar los hechos sucedidos y realizar una reconstrucción de los mismos, la tarea del abogado consiste en cumplir con su misión de defender a un cliente (abogado defensor) o de implicar a un acusado (fiscal). El determinar la verdad material de lo ocurrido puede ser una consecuencia de estas tareas técnicas, pero no el objeto principal, que acorde con la moderna doctrina penal coloca en primer lugar la observación estricta del debido proceso, protegido constitucionalmente. Si como consecuencia de su labor técnica legal gana la contienda y obtiene la absolución del imputado (defensor) o la condena del mismo (fiscal), su tarea ha sido correctamente realizada, los medios y la argumentación son simples herramientas en esa tarea.

Usted debe buscar imitar esa actitud dentro de su propia tolerancia ética y en aras de establecer la verdad técnica material, pero está circunstancia no estará sometida a su decisión, sino a la pericia del abogado que enfrenta y a las armas que esté dispuesto a utilizar para vencer retóricamente (utilizando no sólo la oratoria, sino principalmente la dialéctica, por la indudable contundencia lógica que implica).

La regla es *destruir e iterar*. Una vez que logre desarmar o ironizar uno de los argumentos de su interlocutor, no permita que los espectadores lo olviden. Cada vez que deba discurrir nuevamente adopte un aire reflexivo y haga referencia a dicha situación, como si hubiese quedado asombrado o *shockeado*, ante el error argumental esgrimido por su interlocutor. Cuanto más itere, más furioso se pondrá su interlocutor

y mejores serán sus posibilidades. No es necesario destacar que todo nuevo error destacado por el mismo medio debe ser agregado a esta iteración y que su imagen debe aparecer cada vez más asombrada ante estos errores (desde su lógica actitud paternal de científico, técnico, maestro, evaluador y compresivo profesional).

Puede ocurrir que usted no gane, pero seguro logrará emparejar los términos de la discusión y a partir de ese momento tal vez logre comunicar (transmitir) lo que ha demostrado científica, tecnológica y técnicamente en el informe pericial.

Si usted tiene suficiente paciencia y elocuencia podrá revertir el proceso y lograr que la ciencia se imponga sobre el discurso. Para ser un buen argumentador alcanza con conocer profundamente su especialidad y restringirse a un análisis discursivo crítico estricto, lógicamente fundamentado y gramaticalmente estructurado.

No se permita una actitud prejuiciosa ante las reglas enumeradas. Usted no está mintiendo respecto de sus conclusiones periciales. Usted ha desarrollado su labor empleando una metodología estricta, con un soporte técnico adecuado y con toda la objetividad que puede desarrollar. Por el contrario lo están atacando en aspectos que nada tienen que ver con su idoneidad profesional. Ante este ataque, toda defensa dentro de los límites de la legalidad y la legitimidad es válida. Sólo después de destruir los argumentos distractores de su interlocutor podrá presentar su trabajo profesional, con la solvencia que usted es capaz de lograr. Sólo entonces logrará acaparar la atención de su audiencia, para justificar sus conclusiones.

Usted sabe, usted puede, usted debe cumplir con su labor de perito, no permita que lo eliminen discursivamente.

“Sus mejores referentes en este aspecto deben ser los sofistas, nunca los filósofos.”

Reglas de argumentación generales

Reconocer lo explícito como explícito: Para que pueda haber argumentación hay que tomar en serio lo que se afirma por ambas partes. Las intenciones o lógicas ocultas no deben contar para la evaluación del argumento. No admita las afirmaciones absurdas. Contra los dogmáticos, nada mejor que la ironía y cinismo.

Buscar argumentos de calidad (respecto de nuestro nivel): Es necesario enfrentarse a la mejor argumentación posible. Si nuestro interlocutor no posee conocimientos, capacidades o habilidades dialécticas para defender su punto de vista, nosotros (al

preparar la defensa), debemos preverlo de todas formas. La calidad de nuestros argumentos depende de la calidad de los argumentos de nuestros interlocutores. Prepárese para luchar contra pares o fuerzas superiores.

Ser minucioso: No se apure a tomar partido. La mayor parte de las discusiones reales se plantean entre puntos de vista que tienen ciertos criterios interesantes de analizar. Es imprescindible percibir la complejidad del problema y entender la diferencia entre los argumentos. En definitiva, no subestime a su interlocutor.

Ser realista: No se debe ocultar la evidencia, ni ignorar los contraejemplos, las contradicciones y las excepciones en nuestra argumentación. Ni siquiera cuando nuestro interlocutor no lo haya descubierto. Recordemos que a corto o largo plazo, esa evidencia se hará visible y destruirá nuestra argumentación.

No personalice la discusión: Distinga entre la argumentación y el interlocutor. Debemos considerar que estamos ante un intercambio de ideas y no ante un choque entre dos personas. No obstante, siempre es bueno atacar a fondo. En general cuando alguien pierde una discusión no se queda tranquilo, sino que acumula veneno para la próxima. Si ha logrado vencer una vez, no deje que el otro lo olvide. Si no desequilibra a su interlocutor al menos lo enfurece y cuando nos enfurecemos la adrenalina nos hace más rápidos para reaccionar, lo que no condice con la buena argumentación.

Responsabilidad argumental: Algunos autores opinan que: *"cuando argumentamos ante otros estamos contribuyendo a crear una cultura de la discusión. Si nuestra manera de discutir es malintencionada y poco rigurosa estaremos contribuyendo a crear una mala cultura. Si nuestra manera de discutir es leal y rigurosa, estaremos contribuyendo a construir una mejor. Somos responsables de los beneficios o daños que causemos"*. Esta forma de pensar sería excelente si los hombres poseyeran una moral en común (más aún alcanzaría con que poseyeran una moral común y la aplicaran en su vida cotidiana). La realidad indica que cada hombre tiene diferentes morales y utiliza diferentes éticas ya sea que el hecho analizado lo afecte en persona, a sus afectos, a quienes no conoce o a sus enemigos. El hombre apareció evolutivamente como un predador y por eso se encuentra en el extremo superior de la cadena alimentaria. A este hecho natural se le suma una enorme capacidad intelectual, respecto de los demás animales y también entre componentes de su misma especie. Esta capacidad intelectual ha permitido la aparición de un componente competitivo excelente y generador de cultura: *la hipocresía*. Es posible que lo mejor sea intentar ser lo más responsable posible en nuestra argumentación reflexiva, y luego, en el campo de la discusión, como en la vida, muchas armas son válidas.

Reglas para evaluar argumentaciones de los interlocutores

Identificar claramente los conceptos, procedimientos y/o actitudes defendidos en la argumentación.

Reformular dichos elementos dándoles el mayor grado posible de claridad y precisión. Eliminar lo que sea irrelevante o accesorio.

Separar los argumentos principales de los argumentos secundarios. Normalmente al formular una argumentación se sigue un camino en forma de árbol binario invertido, donde cada argumentación secundaria se va desarrollando para construir la estructura argumentativa de la síntesis final. Para detectar los argumentos secundarios durante el análisis del discurso es suficiente con prestar atención a los conectivos lógicos (por lo tanto, entonces, en consecuencia, podemos inferir, se deduce, debido a... etc).

Identificar falacias formales (por la estructura lógica), no formales (por el contenido o valor de verdad de la afirmación) y las paradojas, que afectan a la argumentación propuesta. Establecer cuáles de las afirmaciones conceptuales, procedimentales o actitudinales son afectadas por estas fallas en la construcción lógica de los argumentos.

Buscar formas alternativas de reestructurar la argumentación para escapar a las falacias y paradojas. A continuación explicarlas con claridad y aspecto comprensivo. Esta actitud generalmente descoloca al interlocutor, genera ira y adrenalina, le cerramos los caminos, si utiliza la nueva argumentación, debe reconocer la certeza de ésta o quedar “enganchado” de su argumentación previa falaz o paradójica, con lo que habremos logrado nuestro propósito.

Si nuestro interlocutor utiliza nuestra nueva argumentación, habremos demostrado nuestro punto. En realidad hemos logrado la tarea que pretendíamos desde el principio.

Por tanto su interlocutor ya no tiene muchas salidas y si por segunda vez acepta sus argumentos y recomienza la discusión, no tendrá otra alternativa que admitir la derrota de sus argumentos (esto es sumamente hipotético, lo más frecuente es que se aferre tercamente a sus afirmaciones o trate de quitarles importancia o defenderlas a ultranza).

Reglas para construir nuestras propias argumentaciones

Ordenar y presentar cada argumento separado de los demás (no mezclar, ni superponer fundamentos). Construir la argumentación en forma de silogismos categóricos estrictos, de ser posible denominarlos individualmente (asignarles un nombre específico) para luego utilizarlos en la estructura demostrativa.

Diferenciar con claridad las premisas y la conclusión de cada argumento. Siempre es preferible utilizar la estructura silogística clásica (dos premisas y una conclusión), con una excepción al formular la conclusión final (si los argumentos secundarios han sido correctamente demostrados, luego es posible reunirlos en un único proceso racional integrador). Sin embargo, es mucho más estricto (y mucho más lento) realizar esta construcción por pares de premisas en una estructura de árbol binario invertido.

Sea conciso, claro y estricto en la formulación de los argumentos. No agregue comentarios o complementos eruditos. Es importante para no correr el riesgo de equivocarnos en esta argumentación. Tiene sus excepciones, pero no sería legítimo comentarlas en esta obra.

Calcular el tiempo del que disponemos y sobre esta base elegir los argumentos a emplear.

Un argumento bien desarrollado es preferible a tres argumentos apenas esquematizados.

Verificar la compatibilidad, interrelación y coherencia entre los argumentos a utilizar para evitar contradicciones entre los elementos de nuestra propia argumentación.

Controlar el uso del lenguaje. Definir los temas centrales, evitando cambiar su significado dentro del mismo discurso. Recordemos que todos los conceptos son ambiguos y en general dependen del contexto en que son empleados. Evitar las ambigüedades y vaguedades, no utilizar juicios de valor y tener cuidado con el uso de los conectivos lógicos (y, o, por lo tanto, entonces, si). Siempre es posible cambiar esta regla, si nos es útil a la argumentación.

Utilizar una estructura demostrativa natural y fácilmente comprensible para quien nos lee o escucha (adecuarnos al nivel cultural del interlocutor, sin exagerar), somos profesionales académicamente formados y esa característica personal, no debe ser abandonada.

Independizar los argumentos del contenido. Es decir comprobar la pertinencia

lógica del silogismo empleado, dejando entre paréntesis el valor de verdad de las premisas utilizadas o de la conclusión alcanzada.

Comprobar fehacientemente los datos experimentales o estadísticos empleados en la argumentación. No utilizar argumentos de autoridad. En ese sentido, si queremos ser buenos argumentadores es necesario que alcancemos un profundo manejo de la estadística y sus herramientas (con los mismos datos, distintas herramientas y relaciones, es posible demostrar la validez de asertos contrarios, los sofistas y la dialéctica son los ejemplos históricos más contundentes al respecto).

Considerar seriamente las objeciones que se plantean a nuestros argumentos por anticipado, para adelantarnos a la argumentación previsible por parte del otro contendiente. Esto es válido aun en el caso en que decidamos atacar mediante una actitud irónica o cínica, para intentar desacreditar lógicamente a nuestro interlocutor. Aunque no sea visible de inmediato, no existe nivel de abstracción más profundo que el exigido para burlarse (seriamente) de los hechos. Los individuos poco dotados intelectualmente entienden poco, discuten mucho y gritan mucho más. Los mediocres entienden un poco, discuten y gritan en menor medida. Los expertos entienden, afirman y argumentan en temas particulares. Los sabios entienden, no afirman, pero argumentan en temas particulares y generales (tienen conciencia de su propia ignorancia, cuanto más aprenden más ignorantes se reconocen: *"sólo sé que no sé nada"*). Los genios entienden, no afirman, ni argumentan, salvo para burlarse de la realidad. Esto es evidente, muchos escriben, pocos escriben bien, pero son sumamente escasos lo que pueden escribir con humor. Por esta razón comenzamos a escribir en prosa, luego intentamos con la poesía y muy pocas veces llegamos a trabajar con el humor (es más difícil crear un buen chiste que un buen cuento).

La defensa ortodoxa

Algunas técnicas de retórica han demostrado su eficiencia a lo largo de los años, pasando al folklore popular en forma de bromas y respuestas ridiculizantes y absurdas, pero sumamente eficientes a la hora de emplear la dialéctica.

Las lagunas pasajeras

Si nos vemos antes la necesidad de definir o argumentar respecto de determinado tema que implique el uso de sustantivos y adjetivos, deberíamos hacer precisamente eso: definir y argumentar en forma estricta. Sin embargo, para poder hacerlo es necesario contar con una extensa cultura, con un muy amplio vocabulario y con una

excelente memoria. De nada sirven los dos primeros elementos si no podemos utilizar el último, en el momento adecuado y con la correspondiente relación e inserción en el tema. Muchas veces nos retiramos de una discusión en la que hemos sido vapuleados y un par de horas más tarde, ya tranquilos, nos damos cuenta de que deberíamos haber respondido tal o cual cosa ante determinada argumentación, pero ya es tarde.

Lo mismo ocurre con la evocación de palabras, a medida que transcurren los años nos apa- recen "lagunas" o espacios en blanco en medio de una frase, que ni siquiera implican el re- cordar palabras de uso poco frecuente. Por el contrario nos olvidamos de palabras comunes, simples, de uso cotidiano y quedamos tartamudeando y diciendo "esa... ese... ¿cómo se dice...?", está última solución es absolutamente impropia, en el mejor de los casos el interlocutor se nos quedara mirando o aportará una serie de palabras que en general no tendrán ninguna relación con lo que pretendíamos afirmar. Para empeorar las cosas, si este olvido se produce en medio de una argumentación o discusión importante, ante un rival capacitado, podemos darnos por perdidos, nunca recibiremos ayuda, ni comprensión por parte de nuestro interlocutor, posible- mente se quede atento, esperando y gozando nuestro desconcierto.

Sin embargo estas falencias pueden ser empleadas perfectamente a nuestro favor:

1. Si nuestro interlocutor sufre uno de estos "períodos en blanco" y trata de recordar mientras balbucea, tartamudea o se muestra desconcertado, tome la palabra y haciendo como que quiere ayudarlo satúrelo de palabras contradictorias y desordenadas que nada tengan que ver con lo que usted supone que quiere decir.

2. Muéstrese asombrado ante el enrojecimiento de su interlocutor y si éste enfurecido le dice que se calle porque no lo deja pensar o lo confunde, retome este argumento a su favor, señale la intolerancia de su interlocutor que no acepta su sana ayuda, su tendencia a la violencia y con- tinúe golpeando. Su enemigo habrá bajado la guardia, su profundidad argumentativa habrá sido distorsionada ante lo absurdo de la situación, éste será el momento de pasar al ataque.

3. Si por el contrario es usted quien sufre una "miniamnesia", busque el sinónimo que se le presente primero y complete la frase. Si no consigue un sinónimo complete la frase con la primera palabra que se le ocurra. En general pasará inadvertido, como la mayoría de los seres humanos somos locuaces, pero cuasi sordos a los dichos del otro, sólo quedará la sen- sación de "una frase rara", "algo extraño en los argumentos", pero por simple desinterés es difícil que alguien le exija aclaraciones por varias razones, entre ellas:

a. En general nos escuchan con la misma atención que al tránsito de fondo, por lo que no tienen la seguridad de que hubo un error y: si nadie dice nada, yo no voy a ser

el primero en hacerlo.

b. La generalidad humana es abúlica y masificable, para pedir aclaraciones es necesario adoptar una actitud proactiva, tomar la iniciativa y con la probable excepción de su inter- locutor, el resto de la audiencia no está dispuesta a realizar un movimiento que los ponga en evidencia y del cual no estén absolutamente seguros. Por esta razón es conveniente derivar siempre las preguntas para el final de una conferencia, de esta manera, la pregun- ta aguda, suspicaz, colocada en el momento y contexto oportunos, se convierte en una simple insolencia o actitud desubicada al final de la charla, precisamente por la falta de contexto (el chiste es inmediato y espontáneo, o se convierte en simple impertinencia).

No obstante, si pese a todo su interlocutor le pide que aclare la frase, hágalo con otras pala- bras y asunto terminado. Si su interlocutor es lo suficientemente obstinado, persistente o inteli- gente como para exigir la repetición de la frase textual, corre el riesgo de que usted simplemente admita que no lo recuerda exactamente, pero que por favor se lo recuerde, con esto la pelota ha cambiado de lugar otra vez. Cuanto más dure esta discusión más nervioso estará su interlocu- tor y más lejos de su óptimo argumentativo.

Las metáforas

A medida que se incrementan los conocimientos de un individuo, cuanto mayor es su ha- bilidad y disponibilidad para la lectura, más frecuente es el uso que hará de las metáforas en su oratoria. El lenguaje se hace más florido e interesante, no obstante es un arma de doble filo. Es preferible que al menos en la defensa judicial evite el uso de metáforas.

1. Ante una metáfora (o frase clásica o refrán) de su interlocutor, actúe como si no fuera capaz de entender su cabal sentido, sino sólo una descripción textual, ortográfica y gramatical- mente estricta. Esto hace perder sentido a la metáfora y por supuesto logra el desconcierto y el enfurecimiento de su interlocutor.[6] Y seguramente logrará rabia, o explicaciones absur- das o risas entre los concurrentes o cualquier otra reacción distractora respecto de la fuerza argumentativa que se nos opone.

2. Si usted comete el error de utilizar una alegoría y es atacado por el método anterior, respire profundamente (entienda que ha cometido un error), espere a que su interlocutor se calle y luego haga una extensa, profunda, lenta y recalcitrante explicación del sentido de la me- táfora y la poca capacidad de su interlocutor para

interpretar la belleza y profundidad de la oratoria incluida en la misma. Si es bastante paciente y actúa con precisión y eficiencia, seguramente alcanzará su objetivo, pero a costa de haber distraído fuerzas de su objetivo principal. Estas contiendas parciales en general no aportan gran cosa y por el contrario aumentan nuestra fatiga intelectual al tener que trabajar en dos frentes al mismo tiempo.

4 La esfera del conocimiento: Suponiendo que el conocimiento es una esfera virtual, que nos rodea, a medida que incorporamos conocimientos su volumen aumenta. Es decir cuanto más agregamos, más sabemos. Sin embargo, la superficie de la esfera (límite entre lo conocido y lo desconocido) también crece proporcionalmente. Por esa razón nos surgen más y más dudas y en realidad nos hace menos seguros de nosotros mismos a la hora de afirmar algo. Simplificando, cuando más aprendemos más ignorantes nos sentimos. Si esto no ocurre, algo anda mal, o bien estamos estancados intelectual, profesional y académicamente o nos está invadiendo la soberbia que casi siempre termina en pedantería.

5 No se deje engañar por la supuesta existencia de una acordada de la SCJN que legaliza este tratamiento. Nunca una norma de menor nivel puede modificar a una de mayor nivel, según la pirámide de Kelsen. Si una acordada pudiera dejar sin efecto la aplicación de una ley de fondo de la Nación (en este caso el artículo 247, segundo párrafo del Código Penal), la seguridad jurídica de nuestra patria no estaría en duda, sería inexistente. Se podría por este mecanismo crear grupos de ciudadanos con privilegios especiales, fuera del control legal, una especie de fueros diplomáticos exclusivos para una profesión. Hemos tenido componetes de la Corte de muy variada ideología, pero nunca se ha dado el caso de semejante transgresión legal, al menos durante la vigencia del Estado de Derecho. Cuando le refieran la precitada acordada, por favor pida que la identifiquen con claridad (de la misma forma en que se referencia la jurisprudencia, con fecha, número, origen y oportunidad de ésta), verá que todos prometen conseguirla y acto seguido olvidan el tema.

6 Por ejemplo: “ladran Sancho, señal que cabalgamos”, se puede responder con “¿usted piensa que emplear una frase del Quijote, que nada tiene que ver con su argumentación, nos hará distraer del verdadero objetivo de esta discusión? En realidad el hecho de escuchar ladridos sólo implica que hay perros y no estamos tratando sobre cánidos y ...”

Las respuestas estrictas

Si su interlocutor se muestra especialmente capacitado limítese a responder e interpretar cada frase o palabra con la misma técnica empleada en el párrafo anterior. Es decir interprete de manera textual y conforme a las reglas idiomáticas. Los resultados en general son sumamente contundentes.

Practique con su entorno, con sus compañeros, amigos o simplemente con las personas que se contacta a diario. Ante la pregunta de un transeúnte "¿tiene hora?" responda "sí" y permanezca impasible, observe las reacciones de su interlocutor:

La mayoría repetirá la pregunta pensando que usted no entendió nada, reitere la respuesta y observe nuevamente.

Algunos comprenderán de inmediato el sentido de la "cuasi broma" y cambiarán la pregunta "¿me la puede decir?" "sí".

En general esto pasa porque nuestra permanente actitud impostada en las relaciones humanas nos hace sumamente sociables y evitamos dar órdenes. Simplemente bastaría con decir "dígamela" y se terminaron los subterfugios. Pueden responderle "no quiero", pero ya estamos tratando del tema pretendido.[1]

Consideraciones prácticas para la argumentación oral

A modo de síntesis podemos generalizar:

Generalice los dichos de su interlocutor para obtener un resultado universal absurdo (inducción).

Intente detectar un resultado particular absurdo (deducción).

Busque las contradicciones lógicas entre los atributos.

Aproveche la ambigüedad de los conceptos.

Destruir e iterar.

Entrénese permanentemente.

1 Si usted tiene ganas de divertirse un rato, pruebe de responder cada pregunta, saludo o frase sin ningún tipo de relación y transferencia, podrá comprobar que en general desconcierta a sus interlocutores:

"Hola, ¿cómo estás?" "Sentado."

"¿Cómo te llamás?"

"No me llamo, ¿para qué me voy a llamar?, si siempre estoy, en general me llaman." "Bueno, ¿cómo te llaman?"

"Che, gordo, vení."

Y de esta manera *ad infinitum*.

APÉNDICE 10
GLOSARIO COMPLEMENTARIO BÁSICO

Ambigüedad: La condición de una palabra con más de un significado se llama polisemia o ambigüedad (ejemplo: vela) *Todas las palabras son vagas y potencialmente ambiguas.*

Autorreferencias y paradojas: Las autorreferencias lingüísticas pueden conducir a paradojas:

todo lo que decimos en este libro es falso.

Características accidentales o concomitantes: Son agregados cuya presencia resulta irrelevante para definir el objeto.

Características definitorias: Partes de la descripción de un objeto que integran el criterio de uso del mismo.

Clases de lenguaje:

natural,

artificial (técnico: lenguaje natural con términos técnicos),

formal (álgebra, binario).

Colofón: Una proposición lógica siempre es una afirmación, porque cuando digo *"Juan no es futbolista"*, estoy afirmando que Juan no es futbolista.

Esto es muy importante, porque el lenguaje no nos permite la negación, sino la afirmacion de la negación.

Es necesario aclarar que el llamado lenguaje técnico, a veces deja de serlo para convertirse en la simple deformación idiomática, por ejemplo, el vocablo "libertad" (tan grandilocuente y universalmente aceptado), como capacidad de opción es imposible, ya que no es posible "no elegir", cuando decidimos "no elegir", estamos "eligiendo no elegir" (principal objeción lógica al concepto de libertad, que implica que el hombre en realidad está condenado a elegir y no puede escapar a esta condena, sólo deja de elegir cuando muere).

Muchos errores gramaticales gruesos se insertan en el supuesto lenguaje jurídico, el ejemplo más evidente es “penas privativas de la libertad”. El lenguaje técnico se conforma con lenguaje natural más términos técnicos, pero sin escapar a las normas de formación del lenguaje original.

Comunicación: Emisor, mensaje y canal. Requiere además un código (por ejemplo un idioma).

Componentes de la Semiótica: Sintaxis, semántica y pragmática.

Concepto y clasificación: Al identificar delimitamos la realidad y hasta podemos asignar un nombre propio al elemento identificado.

Definición: Definir una palabra es indicar su significado (describirla de manera exhaustiva, empleando sus componentes definitorios y de ser necesario sus diferencias con otros similares). Consiste en separar una porción del mundo para poder darle nombre propio.

Definiciones denotativas o extensionales: Nombrar a toda la clase de los mismos: ¿Qué es un planeta? Mercurio, Venus, Tierra, Marte, Júpiter, Saturno, Urano y Neptuno. (Plutón no, porque ha sido reclasificado como planeta enano, junto Caronte, Nix e Hidra).

Definiciones intencionales o por designación: ¿Qué es un planeta? Un cuerpo celeste, opaco que describe una órbita periódica alrededor del Sol y brilla al reflejar su luz.

Siempre se puede cambiar la definición, gracias a la ambigüedad y vaguedad de las palabras.

Los políticos son ladrones. Illia era político y no era ladrón. Illia no era un verdadero político.

Definiciones ostensivas: Indicar mediante ejemplos.

Definición persuasiva: Usar el poder de la palabra para lograr adhesiones y obtener ventajas. Nos mostramos como demócratas y tratamos como totalitarios a los que no coinciden con nuestra ideas. *(Todos sabemos que algo superior debe existir, bueno* ése *es el dios que les propongo, deben darme dinero para construir su reino, si no lo hacen serán excluidos del mismo.)*

Definiciones verbales: Comunican el significado de una palabra a través de otras

palabras.

Denotación y designación: (Frege) denotación o extensión y designación o intensión o connotación. La conducta es producto de un criterio. El criterio forma el concepto. El criterio de una palabra de clase se llama designación. Por ejemplo obelisco es la denotación de todos los obeliscos, mientras que es la designación de un pilar alto, de base cuadrangular, alto, puntiagudo, etc. La palabra cíclope tiene designación, pero carece de denotación (al igual que quimera o hipogrifo).

Diacrónico: Dinámico, examina la evolución de la lengua a lo largo del tiempo.

Elementos del lenguaje:

signos primitivos (palabras),

reglas de formación (*el perro ladra*, no es válido: *el ladra perro)*, no se aplican a los lenguajes formales,

reglas de derivación (permiten derivar una expresión en otra, como en la voz pasiva). **Enfoque sincrónico de la lengua:** Observar la lengua desde el punto de vista estático. **Fuente del significado:** Nosotros cambiamos el modo de nombrar una determinada cosa.

Función ideológica: La creencia en significados inherentes a la realidad (definiciones reales) facilita la aceptación de la definición persuasiva al protegerla contra las críticas obvias.

De ahí la necesidad de discutir las bases del discurso, si uno las deja pasar, luego es sólo cuestión de construir alrededor y cualquier cosa puede ser demostrada (según el interés del orador, el llamado y reconocido: poder de la retórica).

Habla: Acto individual, por medio del cual la lengua se manifiesta.

Idioma:

hablado,

gestual,

pictórico,

onomatopéyico.

Identificación y significado: El Sol es el Sol para todos, cualquiera sea la palabra que lo denomine, pero el significado de las cosas depende de nuestra interpretación (nos gusta o no, nos atrae, etc.)

Lengua: Sistema de signos y reglas que sirven a una comunidad lingüística.

Lingüística: Estudia los lenguajes naturales.

Metalenguaje descriptivo: Cuando se hace referencia a las normas, por ejemplo en una clase de derecho: *la presente ley no debe considerarse válida.*

Metalenguaje prescriptivo: Se refiere a normas (una señal de tránsito: *respete las señales)*

Niveles de lenguaje:

es objetivo cuando el lenguaje es motivo de la investigación,

se llama metalenguaje a aquel en que se formulan los resultados de la investigación.

Oraciones y proposiciones: La proposición es el significado de la oración, una vez abstraído de las palabras concretas con que se lo indica. No se debe confundir este concepto (algo así como lo que entiendo de la oración), con la proposición lógica (oración con valor de verdad).

Pragmática: Relación entre los signos y las personas que los usan.

Pragmática: Es el significado de la expresión lingüística para una persona determinada. La disciplina que estudia el discurso, como acto humano, que se dirige a la producción de efectos.

Privar: según el diccionario de la Real Academia Española, significa: (Del lat. *privāre*).

tr. Despojar a alguien de algo que poseía.

tr. Destituir a alguien de un empleo, ministerio, dignidad, etc.

tr. Prohibir o vedar.

tr. Quitar o perder el sentido, como sucede con un golpe violento u olor sumamente vivo. U. m. c. prnl.

tr. Complacer o gustar extraordinariamente. A Fulano le priva este género de pasteles.

intr. Tener privanza.

intr. Dicho de una persona o de una cosa: Tener general aceptación.

prnl. Dejar voluntariamente algo de gusto, interés o conveniencia. Privarse del paseo.

prnl. C. Rica y El Salv. Quedarse profundamente dormido.

De ninguna manera se puede utilizar en castellano con el sentido de restringir o limitar. Por lo tanto la única forma de privar a un hombre de su libertad, si lo mantenemos con vida, es el coma profundo.

Lo que en realidad hacen la cárcel, la prisión, la reclusión y otras formas de contener a una persona es restringir su libertad ambulatoria. De ahí que estas penas deban ser denominadas *"penas restrictivas de la libertad ambulatoria"*. Por tratarse de un lenguaje técnico debe mantener la pureza del idioma original y puede agregar nuevos términos técnicos, pero no deformar el idioma. Recuerden que un error de muchos no convalida el error y que la opinión mayoritaria no siempre es la más adecuada a la realidad: *"millones de moscas no pueden equivocarse…"*

Signo: Es un fenómeno relacionable con otro fenómeno.

Semántica: Estudio de los signos en relación con los objetos designados. Se clasifica en:

pura o filosófica (examina las bases teóricas que soportan cualquier análisis semántico particular),

descriptiva o lingüística

especial (castellano, guaraní),

general (historia de los lenguajes).

lexicografía (significado de la palabra, en un idioma y momento dados).

Semiótica: Teoría general de los signos, conocimientos genéricos sobre el lenguaje, relaciones con otras ciencias sociales: antropología (Lévi Strauss), psicología (Lacan), literarios o la moda (Barthes).

Significación: Relación entre signo y fenómeno representado frente a nuestra mente. **Símbolo:** Requiere un vínculo arbitrariamente fijado. Los símbolos conforman el lenguaje. **Sintaxis:** Estudia los signos en sí mismos, con independencia del significado.

Universales: Lo frío, lo blanco, lo blando. La tesis esencialista nació de llevar al terreno ontológico las observaciones acerca de la estructura del lenguaje (sustantivos, adjetivos, verbos). Podría pensarse en lenguajes basados en otros elementos gramaticales. Al respecto recomiendo con especial énfasis el cuento "Tlön, Uqbar, Orbis, Tertius" de Borges, allí aparece una interesante propuesta de lenguaje basado en el participio, en un entorno idealista.

Utilidad del lenguaje: Cuando una persona dice algo a otra, intenta influir en la segunda. Los motivos para hacerlo se clasifican en:

Función descriptiva: En el sentido de informar, modificar creencias del receptor por medio de nuevos datos (*Nietzsche proclamó la muerte de Dios*).

Función directiva: Se busca provocar un cierto comportamiento o influir en su voluntad, pueden ser órdenes o pedidos (*firmes, páseme la sal*).

Función expresiva: Se utilizan para manifestar sentimientos o emociones (*pero qué gil de goma*).

Función operativa: Se usa en ceremonias o actos formales (*buenos días, los declaro marido y mujer*).

Usos mixtos: Se emplea en una forma pero se pretende otra (¿me *puede decir la hora?*).

Vaguedad: Libro es un conjunto de muchas hojas impresas, encuadernadas juntas y con cubierta (¿cuántas hojas? ¿impresas? ¿encuadernadas? ¿con tapas?).

APÉNDICE 11
RESUMEN DE LÓGICA PROPOSICIONAL

Proposición: Es una afirmación, en lenguaje descriptivo (una oración en lenguaje natural, que admita valor de verdad V/F).

Conectivas **lógicas:**

	I. Símbolo Lógico	**II. Locución en lenguaje usual**	**III. Ilustración en lenguaje usual**	**IV. Simbolización de III**
Negación	–	No…	No llueve	– p
Conjunción	.	…y…	Llueve y truena	p . q
Disyunción (inclusiva)	v	…o…	Estaba triste o preocupado (o ambas cosas)	p v q
Disyunción (exclusiva)	w	…o…	Iremos al cine o al teatro (pero no a ambos lados)	p w q
Condicional	⊃	Si… entonces…	Si llueve, entonces habrá cosecha	p ⊃ q
Bicondicional	≡	…si y sólo si…	Habrá cosecha si y sólo si llueve	p ≡ q

Negación conjunta	↓	Ni… ni…	Ni trabaja ni estudia	p ↓ q
Incompatibilidad	|	No es cierto (a la vez) que… y …	No es cierto que Juan sea secretario y sobrino del juez	p | q

Tablas de verdad:

Negación

p	−q
V	F
F	V

Conjunción

p	q	p · q
V	V	V
F	V	F
V	F	F
F	F	F

Disyunción inclusiva

p	q	p v q
V	V	V
F	V	V
V	F	V
F	F	F

Disyunción exclusiva

p	q	p w q
V	V	F
F	V	V
V	F	V
F	F	F

Condicional

p	q	p ⊃ q
V	V	V
F	V	V
V	F	F
F	F	V

Bicondicional

p	q	p ≡ q
V	V	V
F	V	F
V	F	F
F	F	V

Negación conjunta

p	q	p ↓ q
V	V	F
F	V	F
V	F	F
F	F	V

Incompatibilidad

p	q	p | q
V	V	F
F	V	V
V	F	V
F	F	V

Lógica deóntica:

Operadores deónticos:

O: Obligatorio

P: Permitido

Ph: Prohibido

Los operadores deónticos y algunas de sus interpretaciones más comunes son los siguientes (donde "*p*" representa una oración):

Op: "Es obligatorio *p*", "es indispensable *p*", "es exigible *p*", "es imperativo *p*", "es imprescindible *p*", "debe ser el caso *p*", "es forzoso *p*", "es necesario p", etc.

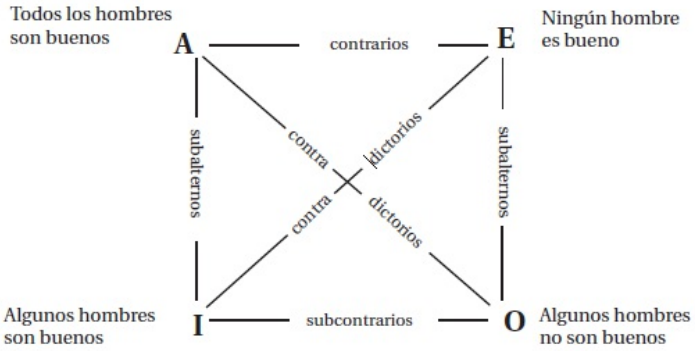
Php: "Está prohibido *p*", "es ilícito *p*", "es indebido *p*", "es injusto *p*", "es inválido *p*", "es incorrecto *p*", "es imposible *p*", etc.

Pp: "Está permitido *p*", "es lícito *p*", "es permisible *p*", "está autorizado *p*", "es válido *p*", "es justo *p*", "es correcto *p*", "puede ser *p*", "es posible *p*", etc.

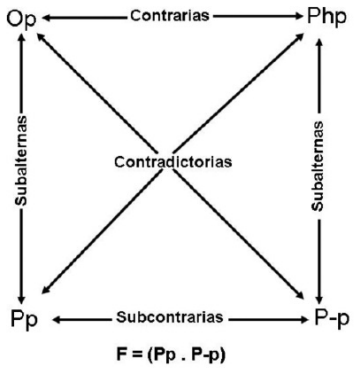
Pp: "Está permitido -*p*", "es lícito -*p*", "es permisible -*p*", "está autorizado -*p*", "es válido -*p*", "es justo -*p*", "es correcto -*p*", "puede ser -*p*", "es posible -*p*", etc.

F: "Es facultativo p", "Es indiferente *p*", "es indistinto *p*", "es adiáforo *p*", "da lo mismo *p*", "da igual *p*", etc.

A partir del cuadro de oposición clásico de los juicios:



Se genera cuadro de oposición de proposiciones deónticas:



Interdefinibilidad de operadores deónticos: Permite pasar de una norma obligatoria a sus equivalentes Permitido o Prohibido y viceversa.

Op ≡ -P-p ≡ Ph-p

O-p ≡ -Pp ≡ Php

-Op ≡ P-p ≡ -Ph-p

-O-p ≡ Pp ≡ –Php

Operador deóntico derivado: F (facultativo) F ≡ Pp . P-p

Principio de permisión: Pp v P-p

Principio de distribución deóntica: P(p v q) ≡ Pp v Pq

APÉNDICE 12
LA INSPECCIÓN JUDICIAL

Este parte del accionar pericial requiere de acciones positivas específicas por parte del tribunal interventor, que generalmente implicarán el auxilio de la fuerza pública, al respecto y por tratarse de un tema especialmente importante, se ha agregado a la presente obra un apéndice que la trata específicamente.

Recuerde que usted no tiene autoridad, ni poder delegado para realizar una inspección judicial por su cuenta. Ésta es una diligencia que debe ser ordenada por un representante del Poder Judicial, de manera explícita, escrita y detallada. Si debe actuar en el ámbito privado, a solicitud de una particular, tome los recaudos necesarios para salvaguardar su posición ante la ley. Genere un documento autorizando la inspección de los activos de la empresa y hágalo firmar por el dueño o responsables legales de ésta. No actúe sin el concurso y la certificación de un escribano. No secuestre elementos, solicite a su cliente que se los facilite y deje constancia de dicha autorización por escrito y de ser posible ante testigos (o mejor aun en presencia y con la certificación del escribano). No toque sin autorización, no participe en las discusiones entre los miembros de la empresa. Si necesita acceder a un archivo a solicitud de su cliente y en contra de la voluntad del empleado que le niega el acceso, no acceda.

Aunque la afirmación anterior parezca un contrasentido, lo cierto es que la mejor recomendación para su cliente en el momento de aceptar el trabajo consiste en sugerirle que haga una denuncia formal ante la jurisdicción que corresponda, de esta manera se salvan responsabilidades y se actúa conforme a ley. Si su cliente no lo hace y prefiere actuar por vía extrajudicial, debe asumir los riesgos y no transferírselos a usted. Lo que no está escrito es fácil de olvidar y una cosa es el accionar en el momento “en caliente”, por parte de quienes sienten vulnerados sus activos o su privacidad y otra la declaración frente a un futuro tribunal. En el segundo caso, todo el mundo trata de quitarse el lazo de encima y pasarlo a cualquiera que esté cerca. Documente, certifique, escriba y no se exceda por ningún motivo. Un profundo conocimiento de la ley de forma y fondo serán su mejor seguro de libertad, integridad y crédito profesional.

Generalidades

No existe la tarea pericial estrictamente informático forense; durante una inspección judicial, el experto se encuentra inserto dentro de un grupo de actores de distintas profesiones. De ahí que sea imprescindible un accionar interdisciplinario que converja en soluciones transdisciplinarias. La mejor opción para el perito en Informática Forense es interiorizarse en profundidad de las formas de actuar de los restantes expertos en las distintas disciplinas criminalísticas, por dos razones principales: evitar la destrucción de prueba útil para otras tareas periciales y, en caso de necesidad extrema, sustituir al experto faltante.

Recordemos que la detección, identificación, salvaguarda, protección y traslado de la prueba es tarea y responsabilidad de todos los actores involucrados y no sólo de quien debe realizar la tarea por competencia profesional. Considerando, además, que el lugar del hecho contiene todos los testigos mudos, necesarios para la investigación del delito. La misión del perito es documentar mediante acta, croquis y fotografías todo lo que en él se encuentra.

Aunque el perito que desee encarar su profesión con solvencia efectiva, eficiente y eficaz, debería formarse en profundidad en las ciencias criminalísticas, en caso de no haberlo realizado aún, es conveniente tener en cuenta algunas características principales:

En caso de lesiones, lógicamente, es primordial auxiliar a la víctima, máxime cuando ésta, por la gravedad que puedan tener las lesiones se encuentre imposibilitada de moverse por sus propios medios; pero en el caso de un occiso, no existe ninguna premura; debemos dedicarnos a preservar el lugar mientras llegan los restantes equipos técnicos y la instrucción policial (en general, dirigida por el juez de Instrucción en Capital y por el fiscal en la provincia de Buenos Aires).

Todo sirve, nada debe descartarse, aun cuando se crea que no tiene relación con el hecho ocurrido. Debe documentarse todo lo hallado, fotografiado y luego secuestrado si se considera necesario, aunque se contraponga con la hipótesis que nos hayamos formado *a priori*, es ideal evitar dichas hipótesis, analizar lo hallado y luego sacar una conclusión.

No pasar, no tocar, no mover, no encender, no abrir, no pisar y sobre todo no molestar a los demás peritos, mantener una actitud de curiosidad crítica y documentar todo.

Es de valor fundamental realizar un relevamiento previo, de ser posible. Registrar la hora exacta en que se recibe la comunicación solicitando nuestra presencia; la hora en que se llega al lugar del hecho; quién o quiénes ya se encontraban en el mismo; testigos que se hallaren, personas que nos acompañan o dirigen nuestras actividades,

sistemas de seguridad franqueados para llegar al lugar, sistemas de seguridad activos en el momento de arribar. Nada debe dejarse librado al azar. No podemos basarnos en la memoria propia ni ajena. Todo debe contarse, medirse, anotarse, registrarse, fotografiarse, en los medios disponibles (anotador de papel o electrónico); los papeles sueltos no sirven; se deterioran o se pierden y luego tenemos que describir el lugar sin la certeza imprescindible.

La mayoría de las sentencias se hacen basadas en pruebas de indicios; por ello volvemos a recalcar, todo es importante: rastros, huellas, manchas, pisadas, colillas de cigarrillos, impresiones dactilares, roturas, impactos, condiciones de los elementos evaluados, por ejemplo, equipos abiertos o cerrados, fajas de seguridad rotas, cables sueltos, equipos de conexión o distribución abiertos o cerrados, elementos próximos al área de trabajo, al parecer desconectados o sin relación con los equipos, especialmente equipos de captura de video, de comunicaciones, de impresión, de almacenamiento, de alimentación eléctrica, etc. Lo que no se documenta en la primera inspección judicial no podrá reconstruirse en una segunda, si es necesaria y se hiciere. El trabajo, en ese sentido, debe efectuarse sin prisa, pero sin pausa. Una inspección judicial mal realizada, fuera de tiempo o cuando ya se ha modificado el lugar del hecho, lleva con seguridad a un fracaso en la investigación.

Los rastros que puedan tener relación con el hecho hay que estudiarlos e interpretarlos para no caer en error. Luego documentarlos en el acta de inspección, fotografiarlos y secuestrarlos si correspondiere y fuese posible. Por ello es imprescindible que el perito informático forense tenga conocimientos apropiados de criminalística, para:

Entender las actividades de los restantes peritos y facilitar la tarea interdisciplinaria.

Evitar modificar la escena en perjuicio de otros peritos.

Preservar la prueba en ausencia de los peritos especialistas.

Colaborar en la investigación, de manera mancomunada, integrada y pro activa (ante la duda o la falta del especialista correspondiente, documente la prueba, presérvela y de ser necesario secuéstrela, aunque no pertenezca a su especialidad; siempre es preferible una prueba erróneamente secuestrada o mal conservada que ninguna prueba).

Es necesario entender que la ignorancia no justifica la inoperancia. El decir: “no sabía, no me di cuenta”, no soluciona nada. De la misma manera que el ortopedista o el pediatra no pierden su condición de médicos, el perito en Informática Forense, no puede ignorar las actividades del resto de sus colegas profesionales de la

Criminalística.

Situaciones posibles en la inspección judicial

Es necesario destacar tres situaciones diferentes en la inspección judicial, desde el punto de vista del perito informático forense:

La situación se ha desarrollado de manera confidencial. Se han iniciado las actuaciones y luego se ha decidido intervenir, detectar y secuestrar la prueba. En este caso el perito deberá realizar todas las tareas que corresponden a la etapa del relevamiento informático:

Tomar contacto con los actuados (penales, civiles, comerciales, laborales, administrativos, etcétera), extraer toda la información disponible en los mismos.

Tomar contacto con todas las personas (no involucradas como sospechosas en la investigación) que puedan aportar datos sobre el lugar, las plataformas instaladas, los sistemas operativos en uso, los mecanismos de protección instalados, la estructura de seguridad informática del lugar (física y lógica). Cuanto más sepamos *a priori* menos errores cometeremos al actuar.

De ser posible acceder a un plano del lugar a ser inspeccionado (no sólo de la habitación en cuestión, sino de todo el edificio involucrado). Lo ideal es contar además con los planos de distribución de red y de electricidad. De esta manera podrá planificarse por anticipado la ruta de acceso más segura y rápida al lugar a ser inspeccionado, realizando las acciones necesarias para la protección de la prueba e impidiendo las acciones maliciosas sobre ésta.

Recordemos que la planificación es la base del éxito. Tomar previsiones, evita pérdidas y destrucciones de información innecesarias.

Es necesario planificar el momento de acceder al lugar. De ser posible, se prefieren las horas de la madrugada (entre las tres y las cinco de la mañana), en este horario todos los recursos humanos se encuentran menos activos que en otras horas. Recordemos que algunos Códigos de Procedimientos prohíben el allanamiento nocturno, pero que se refieren a las moradas particulares y no a los lugares públicos, es necesario comprobar esta circunstancia, acorde a la jurisdicción judicial en que desarrolla sus actividades el perito. Por otra parte el juez tiene atribuciones suficientes como para habilitar horarios especiales en razón de la tarea técnica a realizar y los

sistemas de defensa a superar.

Siempre es conveniente contar con un plan alternativo, para el supuesto en que el plan principal falle (una puerta que no se abre, un acceso que ha sido eliminado o modificado, la remodelación de una oficina, sala de servidores, conexión, etc.).

Como en toda labor informática, debemos contar con resultados previsibles de máxima y mínima, que nos aseguren contar con la prueba necesaria. Si detectamos dificultades reales, para alcanzar el objetivo de mínima es necesario formular otro plan de aproximación, acceso, protección y secuestro de los datos pretendidos.

En caso de no tener acceso posible al lugar, siempre podremos recurrir a las técnicas de ingeniería social e ingeniería social inversa, como haría cualquier hacker.

Todas estas medidas deben ser informadas y autorizadas por el juez o fiscal interventor.

Nuestro encuadre legal es imprescindible, so pena de anular la prueba por razones puramente formales.

Al concurrir al lugar debe hacerlo con los elementos necesarios para realizar su tarea.

Tenga en cuenta que debe detectar, documentar, preservar y trasladar la prueba.

Respecto del punto anterior, lo ideal es el uso de una estación de trabajo informático forense portátil. (Un sistema basado en una *notebook*.) Si debe decidir entre poseer un equipo de escritorio (*desktop*) o un equipo portátil, inclínese siempre por el portátil, ya que cumple ambas funciones.

Si no dispone de estos elementos, genere su propio kit de herramientas. Recuerde que estas herramientas deben ser legales, no utilice “copias piratas”, es muy duro dar explicaciones al abogado que lo interrogue o al juez sobre la naturaleza ilegal de sus herramientas informáticas.

Debe concurrir provisto de elementos de iluminación accesoria (linternas o proyectores y pilas o baterías suficientes).

Lleve consigo una cámara digital con zoom, para poder realizar ampliaciones macrofotográficas de los elementos que necesite documentar.[2]

Además de estos elementos, debería contar con: un grabador de bolsillo con

micrófono disimulable (corbatero), un equipo portatil de GPS (o la aplicación en su celular), si no lo posee al menos una brújula (le permitirá orientar los croquis), una cinta métrica (ideal entre 5 y 10 metros), una plomada (permite medir distancias de un objeto elevado hasta el piso, simplemente ascienda hasta el objeto, deje caer la plomada hasta que contacte con el piso, baje y mida el hilo desenrollado), un cuaderno cuadriculado (para efectuar los croquis), sobres de papel de diversos tamaños, sobres plásticos de distintos tamaños (ideales, los que se venden para congelar alimentos que vienen con cierre incorporado), rótulos autoadhesivos, una lupa de tamaño cómodo para utilizar en espacios reducidos, un imán extensible (para retirar elementos metálicos del interior de los equipos), un espejo pequeño extensible a idénticos fines, marcadores al agua para destacar elementos o marcas, gasa y cinta adhesiva, para realizar pequeños envoltorios. Siempre lleve varios pares de guantes de cirugía, no trabaje sin ellos.

Tenga en cuenta a la hora de dibujar que todos los artistas han recurrido siempre a una técnica simple cuando debieron copiar elementos de la naturaleza, ampliar o reducir dibujos: se cuadricula el dibujo, se realiza una cuadriculación a escala del elemento a copiar y luego se representa cada cuadrícula independientemente. En los locales especializados se venden pequeñas ventanas de cuadriculación con un soporte de tipo trípode pequeño, que son de suma utilidad para representar elementos distantes, no mensurables, a mano alzada y mantener las proporciones apreciadas.

El perito ha sido llamado para actuar en un lugar que desconoce y no tiene tiempo para realizar una planificación adecuada:

Aproveche el viaje hacia el lugar para relevar toda la información posible antes de efectuar el ingreso. Realice un relevamiento tanto más profundo como tiempo tenga disponible.

Pregunte sobre la naturaleza de las acciones pretendidas y autorizadas por el juez o fiscal interventor. Nuestro encuadre legal es imprescindible, so pena de anular la prueba por razones puramente formales o resultar culpables de algún delito.

Al concurrir al lugar debe hacerlo con los elementos necesarios para realizar su tarea.

Tenga en cuenta que debe detectar, documentar, preservar y trasladar la prueba.

Respecto del punto anterior, lo ideal es el uso de una estación de trabajo informático forense portátil. (Un sistema basado en una *notebook*.) Si debe decidir entre poseer un equipo de escritorio (*desktop*) o un equipo portátil, inclínese siempre por el portátil, ya que cumple ambas funciones.

Si no dispone de estos elementos, genere su propio kit de herramientas. Recuerde que estas herramientas deben ser legales, no utilice “copias piratas”, es muy duro dar explicaciones al abogado que lo interrogue o al juez sobre la naturaleza ilegal de sus herramientas informáticas.

El perito ha sido llamado para actuar en el lugar y no está autorizado a retirar elementos del mismo, pero puede realizar copias de la información que le resulte de interés. Actúe de acuerdo a lo tratado con anterioridad, pero ponga especial énfasis en los elementos de copia y resguardo de la prueba, ya que sólo podrá acceder a los originales una vez.

El perito ha sido llamado para actuar en el lugar y no está autorizado a retirar elementos de éste, es decir debe trabajar en el lugar.

Es el peor de los casos, sólo su habilidad, capacidad profesional, inteligencia práctica y aptitud investigativa podrán ayudarlo.

Son los casos más raros, pero no imposibles.

Sea minucioso, tómese todo el tiempo posible (o disponible), no se apresure, analice las pruebas en profundidad, no se deje engañar con las apariencias.

Es el ambiente ideal para montar un escenario que engañe al perito.

Siempre insista en lo parcial y acotado de su trabajo, de ser posible intente obtener una copia de la prueba analizada (siempre por medios legales).

No comprometa su opinión salvo que esté completamente seguro.

Estos casos, se producen generalmente en ambientes que contienen información altamente sensible para un determinado organismo, institución o empresa. Generalmente se trata de informes preliminares o informales, ya que esta manera de trabajar es contraria a los códigos de procedimientos. No obstante, no se puede descartar la posibilidad de que ocurra (p. ej., registros de bases de datos de organismos gubernamentales, militares, de fuerzas de seguridad, de estructuras religiosas o políticas, etc.)

Metodología de trabajo

La inspección no debe limitarse solamente al lugar en donde se encuentra almacenada la información o desde donde se accede a ésta; debe extenderse a todo su contorno y lugares aledaños. Por ejemplo, si el hecho sucedió en la sala de servidores,

la inspección debe ampliarse a todos los nodos accesibles de la empresa, esta verificación puede ser física o remota, pero debe hacerse.

Una manera interesante de hacer la observación es mediante la forma que se denomina espiral; por ejemplo, en el interior de una habitación se encuentra una computadora asegurada (ya hicimos lo necesario para que no la desconecten, apaguen o modifiquen); comenzaremos a inspeccionar caminando en forma de espiral, es decir, desde las paredes, y de esa manera nos iremos acercando hasta llegar al lugar principal, esto es, donde está la computadora a examinar. Es una técnica similar a la utilizada por otros expertos, aunque éstos en general comienzan del centro hacia fuera, en nuestro caso es preferible converger desde la periferia, porque el orden de aproximación se corresponde con la conectividad y luego el almacenamiento.

Cuando el sitio a inspeccionar es muy grande, se lo fracciona en cuadrículas; luego se revisan las cuadrículas con el método espiral más adecuado al acto (desde fuera hacia adentro en la mayoría de los casos, de adentro afuera, cuando exista un elemento principal a partir del cual investigar, por ejemplo un rack de comunicaciones, almacenamiento o procesamiento). Podemos derivar las inspecciones de los lugares anexos de menor interés a otras personas que puedan ayudarnos, pero en caso de encontrar alguna cosa interesante, no deben tocarla, se limitarán a llamarnos y mostrarnos el descubrimiento, nosotros decidiremos la acción a tomar en cada caso. La ayuda por parte de otras personas debe ser analizada con cuidado, pero si establecemos que se trata de personas confiables, no debemos olvidar que las mujeres y los niños son sumamente hábiles para detectar elementos que se nos hayan pasado por alto, nunca debemos subestimar una opinión, ni un dato por su aparente obviedad. Las diferentes distancias a que se encuentran los elementos, así como también las dimensiones de la habitación o lugar, deben ser medidas con exactitud y no calculadas a simple vista o por medio de pasos. Si es posible contar con un telémetro portátil, este elemento resultaba sumamente oneroso, sin embargo actualmente existen algunos sumamente accesibles que son empleados por arquitectos y profesionales de la arquitectura en general. El fotógrafo estará permanentemente con el perito (o el perito hará de fotógrafo. Esto es de vital importancia, toda vez que se trata de una reconstrucción permanente del lugar del hecho y de lo hallado en el mismo. En lo posible utilice cámaras digitales, lo que facilitará su posterior inserción en archivos o presentaciones resultantes de la actividad pericial.[3]

La Criminalística es en la mayoría de los casos una disciplina reconstructiva de efectos (siempre interviene *a posteriori*). Considerando el delito desde este punto de vista en particular, la mayoría de las veces la acción delictiva se comete y el autor desaparece, pero deja en el lugar del hecho rastros que pueden servir para lograr su identificación, y el cuándo, cómo y dónde ocurrió. De ahí que sea necesario

documentar, describir y conservar las huellas que pueden servir para lograr dilucidar lo ocurrido. En Informática Forense la prueba tiene dos componentes de suma importancia que la hacen diferente de las restantes pruebas indiciarias:

Principio de identidad impropio: Si generamos un archivo informático, mediante la copia bit a bit de un original, ambos elementos son idénticos e indistinguibles (el simple hecho de hablar de original y copia es contradictorio en sí mismo). Mientras que ningún perito confundiría un rastro digital con el correspondiente dactilograma utilizado en la comparación, si no recurrimos a medios externos de identificación (por ejemplo, soporte magnético de origen), no es posible dilucidar original y copia en dos archivos idénticos bit a bit. Ésta es una dificultad agregada a nuestra especialidad que no debemos perder de vista.

El sospechoso puede haber desaparecido como en cualquier otra actividad pericial, pero también puede haber permanecido y ser inalcanzable. Basta con pensar en accesos remotos, actividades ilícitas a distancia, almacenamiento remoto, etc. Es muy importante conocer las limitaciones legales de nuestro accionar, si debemos recolectar información a distancia, almacenada fuera de la jurisdicción judicial en que nos hallamos, debemos informar al juez o al fiscal, antes de actuar y dejar que ellos decidan o tomen las medidas apropiadas para realizar esta actividad (exhortos, oficios, requerimientos etc.). Nuestra actividad debe limitarse a los componentes informáticos del lugar, en los demás casos es necesario pedir autorización, informando la localización exacta de los archivos a acceder, los motivos para hacerlo y la naturaleza de las acciones a realizar sobre los mismos. No debemos modificar archivos remotos, por ningún motivo, salvo que se posea una orden judicial directa y documentada.

La ley procesal indica que las presunciones o indicios son las circunstancias o antecedentes que, teniendo relación con el delito, pueden razonablemente fundar una opinión sobre hechos determinados. Lógicamente, para que haya plena prueba por presunciones o indicios se requiere que ellos reúnan ciertas condiciones (además de ser conducentes y pertinentes):

que se relacionen con el hecho principal que motiva la investigación y que actúa como punto de partida de la misma;

que no sean equívocos, es decir que todos reunidos no puedan conducir a conclusiones diversas;

que estén directa y estrictamente relacionados, de manera que conduzcan lógica y naturalmente al hecho de que se trate;

que sean concordantes los unos con los otros, de forma que tengan íntima conexión

entre sí y se relacionen sin esfuerzo desde la hipótesis propuesta hasta la conclusión alcanzada;

que no sean contradictorios con otros elementos probatorios propios o de otras áreas de la prueba indiciaria (o con hechos ciertos y probados de las pruebas confesional o testimonial);

que se funden en sucesos reales y probados y nunca en otras presunciones o indicios;

que las operaciones realizadas sobre los indicios sean científica, tecnológica y técnicamente correctas, evaluables y repetibles;

que las conclusiones extraídas se funden en técnicas de evaluación estrictas y teóricamente fundamentadas (método científico, evaluaciones físicas y químicas);

que la estructura demostrativa que relacione los hechos, se base en la más pura lógica silogística;

que el evaluador posea la capacitación profesional necesaria para realizar la tarea. En el caso de los peritos informático forenses, es imprescindible el título de grado habilitante en el área de incumbencia específica. El simple hecho de ser ingeniero o licenciado en sistemas, no debería ser condición suficiente para actuar como perito en Informática Forense (al menos desde la ética profesional), de la misma manera que el hecho de ser ingeniero no habilita para realizar pericias en accidentología vial, ni al médico clínico para realizar necropsias;

la Informática Forense requiere conocimientos profundos de seguridad informática, sistemas operativos, redes, medios de almacenamiento primario, secundario y terciario, metodología de investigación científica y criminalística, códigos de fondo, forma y legislación vigente en materia de informática jurídica, legislación pericial y testimonial y varias áreas complementarias que no aparecen en la formación curricular académica de un licenciado o ingeniero en Informática y las carreras afines (computación, sistemas, electrónica, contador, etc.);

por ello volvemos a insistir: en la investigación de los hechos delictivos sirve todo lo que se encuentra en el lugar del suceso. Nada debe descartarse como inútil; todo debe documentarse y secuestrarse;

la ley no se determina fehacientemente en cuáles delitos debe confeccionarse el croquis y efectuarse la inspección judicial formal, pero recordemos que lo que abunda no daña. No obstante ello, debe pensarse que la inspección judicial y el croquis deben

demostrar o documentar algo.

A veces los delincuentes desconocen las características del lugar donde han almacenado la información (realizada por acceso remoto), han modificado la misma o la han dañado, pero sí recuerdan algunos puntos claves de la estructura lógica de la máquina accedida. Por ello es importante en la inspección judicial dejar constancia de la estructura lógica de los elementos informáticos accedidos (capturar pantallas del explorador). Estas estructuras *a posteriori,* si concuerdan con la declaración del imputado, pueden también servir de indicios de gran importancia.

Recuerde que siempre debe registrar la prueba antes de acceder a la misma. Es decir:

realice el *hash* del soporte accedido; por medios no invasivos;

cuando tenga dicho soporte identificado, registrado legalmente y certificado de manera adecuada, puede realizar un análisis del equipo sospechado, utilizando herramientas convencionales;

este hecho debe serle comunicado a la autoridad que interviene en el lugar (juez, fiscal o sus representantes) y actuar sólo con autorización de la misma (siempre explique detalladamente las acciones a realizar y los motivos que las provocaron, sea claro, exprésese correcta y sencillamente en lenguaje natural).

Si las diligencias fueron realizadas durante la noche y de estimarlo necesario, puede solicitar a la autoridad interventora concurrir en otro horario para comprobar algunas circunstancias que no son visibles en dicho momento (antenas externas, conexiones con otros edificios, etc.). Por eso es recomendable actuar en las horas que preceden al amanecer (entre las tres y las cinco), de esta manera al finalizar las tareas en el interior se tendrá suficiente visibilidad para comprobar los elementos externos y no tener necesidad de concurrir nuevamente.

La comprobación judicial exige la mayor celeridad posible, y es de suma importancia que las cosas permanezcan en su estado primitivo, y que ninguna alteración pueda hacerlas ver desde un punto de vista equivocado. Si es necesaria la asociación de peritos, el juez hará vigilar el sitio e impedirá todo movimiento antes de la llegada de aquéllos; otras veces procederá por sí mismo a inspeccionar los objetos que no requieren la observación del especialista, prescindiendo de aquellos que sólo pueden ser examinados útilmente por éste (pero sucede a menudo que no puede separarse la inspección judicial del examen pericial, y que, procediendo aisladamente, suele haber perjuicio en alguna de las instancias). Finalmente, es su deber oír, durante la operación, a las personas que hayan llegado en primer término, y que habiendo

desde un principio observado las cosas pueden dar a conocer el estado en que han encontrado el lugar y los cambios que haya podido sufrir.

Cuando se ha procedido a la comprobación judicial en aquella etapa del proceso, en que la información ya va dirigida contra un inculpado, puede ser necesario hacer asistir a éste a las operaciones. Debe hacerse así siempre que las explicaciones generales suministradas por él no tengan el grado de precisión necesario, y queden por practicar pormenores por él alegados, o también cuando los objetos deban ser objeto de reconocimiento por su parte.

Acta de inspección o secuestro

Lógicamente, la inspección judicial del lugar del hecho debe documentarse en un acta, es decir, con escritura de corrido y todo en letras, con la menor cantidad de números posibles. La misma debe ser firmada por todos los intervinientes, juez o fiscal, testigos, peritos, víctima/s e imputado/s si se encontraren presentes. Cuando se utilice más de una foja, las firmas irán insertas en todas ellas, es decir, en todas las utilizadas.

Ésta puede labrarse en el lugar del hecho, pudiendo ser manuscrita, pero nada impide que utilicemos los medios a nuestra disposición (*notebook* e impresora o elementos presentes en el lugar). Además de todas las circunstancias observadas en la escena, se dejará constancia de los pequeños interrogatorios que se les haya efectuado a los presentes.

El acta puede servir para dejar constancia formal de una serie de diligencias y operaciones técnicas sobre la prueba indiciaria y también para efectuar el secuestro de dicha prueba, al respecto:[4]

El acta debe identificar claramente a las personas, en lo posible con la totalidad de sus nombres y con la mayor cantidad de datos filiatorios.

Si los testigos no pueden ser hallados, su testimonio final resultará nulo.

Aunque ningún Código de Procedimientos a la sazón exige el teléfono y el e-mail, es la forma más directa en que el perito podrá contactarse con los testigos, no logrará una comunicación legalmente válida, pero al menos tendrá datos reales de las personas que estuvieron en el acto de secuestro.

2 La observación anterior es aplicable a todos sus desplazamientos en un vehículo propio o ajeno. Nunca se sabe cuándo puede ocurrir un accidente y una fotografía en el momento adecuado le puede ahorrar muchos años de litigio, sea usted o no el culpable del accidente. Recuerde que la industria del juicio en nuestro país está especialmente orientada a la accidentología vial y a las relaciones laborales. Evite quedar en el medio de estas actividades dudosamente lícitas.

3 El equipo ideal consiste en un equipo de cámaras estereométricas con reconstituidor digital. Sin embargo estos equipos poseen un costo de adquisición muy alto, que difícilmente pueda ser asumido y amortizado por el profesional independiente. Se sugiere para aquellos casos de trabajo institucional, cuyo volumen pericial lo justifique.

4 En referencia a estos actos tenga en cuenta el correcto empleo de los siguientes vocablos:

Expropiar (paras. de propio)

Desposeer legalmente (de una cosa) a su propietario por razón de interés público.

tr. Quitar una cosa a su propietario por motivos de utilidad pública y a cambio ofrecerle generalmente una indemnización: le han expropiado una finca para construir una autopista.

Confiscar

Atribuir al fisco (los bienes de una persona).

tr. Privar a alguien de sus bienes y aplicarlos a la Hacienda Pública o al Fisco.

Apropiarse las autoridades competentes de lo implicado en algún delito: *"confiscar mercadería de contrabando".*

Apropiarse de algo (por la fuerza, con o sin violencia).

Secuestrar

tr. Detener y retener por la fuerza a una o a varias personas para exigir dinero u otra contraprestación a cambio de su liberación: *"amenazaron con asesinar a los secuestrados, si no liberaban a sus compa*ñ*eros encarcelados".*

Tomar el mando de un vehículo o nave por la fuerza, reteniendo a sus pasajeros o a su tripulación, con el fin de obtener un beneficio a cambio de su rescate: *"secuestrar un avión".*

Ordenar el juez el embargo o retirada de la circulación de una cosa: *"secuestrar la*

edición de un periódico”.

Decomisar

tr. Incautarse el Estado como pena de las mercancías procedentes de comercio ilegal o los instrumentos del delito:

“se ha decomisado un kilo de heroína”.

Incautar(se) (no existe el verbo incautar): (de *in* y *cautum*, multa) Forma pronominal.

Dicho de una autoridad judicial o administrativa. Privar a alguien de sus bienes como consecuencia de la relación de éstos con un delito, falta o infracción administrativa. Cuando hay condena firma se sustituye por la pena accesoria de comiso.

Apoderarse arbitrariamente de algo. Fuente: www.rae.es.

APÉNDICE 13
MISCELÁNEAS

Listado de Claves BIOS CMOS

AWARD

ALFAROME AWARD PW J64 SER 589589

ALLy AWKWARD J256 SKY_FOX 589721

aLLy Awkward J262 SYXZ 595595

aLLY BIOSTAR j332 syxz 598598

ALLY CONCAT j322 shift + syxz

aPAf CONDO KDD TTPTHA

_award Condo Lkwpeter ZAAADA

AWARD_SW d8on LKWPETER ZBAAACA

AWARD?SW djonet PINT ZJAAADC

AWARD SW HLT pint 1322222

AMI

AMI AMI?SW

AAAMMMIII AMI_SW

BIOS LKWPETE

PASSWORD A.M.I.

HEWITT RAND CONDO

PHOENIX

Phoenix CMOS

PHOENIX BIOS

Otras

ALFAROME LKWPETER

BIOSTAR lkwpeter

biostar setup

biosstar SETUP

CMOS Syxz

cmos Wodj

Varios fabricantes

Manufacturer	Password
VOBIS & IBM	merlin
Dell	Dell
Biostar	Biostar
Compaq	Compaq
Enox	xo11nE
Epox	central
Freetech	Posterie
IWill	iwill
Jetway	spooml
Packard Bell	bell9
QDI	QDI
Siemens	SKY_FOX
TMC	BIGO
Toshiba	Toshiba

TOSHIBA

La mayoría de las *notebook* y computadoras de escritorio ignora la clave del BIOS cuando se mantiene presionada la tecla SHIFT IZQUIERDA, durante el inicio.

IBM APTIVA BIOS

Se ignora la clave del BIOS cuando se presionan los botones primario y secundario del mouse en forma reiterada durante el inicio.

Listado de Puertos utilizados por Troyanos

puerto 1 (UDP) Sockets des Troie

puerto 2 Death

puerto 15 B2

puerto 20 Senna Spy FTP server

puerto 21 Back Construction, Blade Runner, Cattivik FTP Server, CC Invader, Dark FTP, Doly Trojan, Fore, FreddyK, Invisible FTP, Juggernaut 42, Larva, MotIv FTP, Net Administrator, Ramen, RTB 666, Senna Spy FTP server, The Flu, Traitor 21, WebEx, WinCrash

puerto 22 Adore sshd, Shaft

puerto 23 ADM worm, Fire HacKer, My Very Own trojan, RTB 666, Telnet Pro, Tiny Telnet Server

TTS, Truva Atl

puerto 25 Ajan, Antigen, Barok, BSE, Email Password Sender EPS, EPS II, Gip, Gris, Happy99, Hpteam mail, Hybris, I love you, Kuang2, Magic Horse, MBT (Mail Bombing Trojan), Moscow Email trojan, Naebi, NewApt worm, ProMail trojan, Shtirlitz, Stealth, Stukach, Tapiras, Terminator, WinPC, WinSpy

puerto 30 Agent 40421

puerto 31 Agent 31, Hackers Paradise, Masters Paradise

puerto 39 SubSARI

puerto 41 Deep Throat, Foreplay

puerto 44 Arctic

puerto 48 DRAT

puerto 50 DRAT

puerto 53 ADM worm, Lion puerto 58 DMSetup

puerto 59 DMSetup

puerto 69 BackGate

puerto 79 CDK, Firehotcker

puerto 80 711 trojan (Seven Eleven), AckCmd, Back End, Back Orifice 2000 Plug-Ins, Cafeini, CGI Backdoor, Executor, God Message, God Message 4 Creator, Hooker, IISworm, MTX, NCX, Noob, Ramen, Reverse WWW Tunnel Backdoor, RingZero, RTB 666, Seeker, WAN Remote, Web Server CT, WebDownloader

puerto 81 RemoConChubo

puerto 99 Hidden

puerto, Mandragore, NCX puerto 110 ProMail trojan

puerto 113 Invisible Identd Deamon, Kazimas

puerto 119 Happy99

puerto 121 Attack Bot, God Message, JammerKillah

puerto 123 Net Controller

puerto 133 Farnaz

puerto 137 Chode

puerto 137 (UDP) Msinit, Qaz

puerto 138 Chode

puerto 139 Chode, God Message worm, Msinit, Netlog, Network, Qaz, Sadmind,

SMB Relay

puerto 142 NetTaxi

puerto 146 Infector

puerto 146 (UDP) Infector

puerto 166 NokNok

puerto 170 A-trojan

puerto 334 Backage

puerto 411 Backage

puerto 420 Breach, Incognito

puerto 421 TCP Wrappers trojan

puerto 455 Fatal Connections

puerto 456 Hackers Paradise

puerto 511 T0rn Rootkit

puerto 513 Grlogin

puerto 514 RPC Backdoor

puerto 515 lpdw0rm, Ramen

puerto 531 Net666, Rasmin

puerto 555 711 trojan (Seven Eleven), Ini-Killer, Net Administrator, Phase Zero, Phase-0, Stealth Spy

puerto 600 Sadmind puerto 605 Secret Service puerto 661 NokNok

puerto 666 Attack FTP, Back Construction, BLA trojan, Cain & Abel, lpdw0rm, NokNok, Satans Back Door SBD, ServU, Shadow Phyre, th3r1pp3rz (= Therippers)

puerto 667 SniperNet

puerto 668 th3r1pp3rz (= Therippers)

puerto 669 DP trojan

puerto 692 GayOL

puerto 777 AimSpy, Undetected

puerto 808 WinHole

puerto 911 Dark Shadow, Dark Shadow

puerto 999 Chat power, Deep Throat, Foreplay, WinSatan

puerto 1000 Connecter, Der Späher / Der Spaeher, Direct Connection

puerto 1001 Der Späher / Der Spaeher, Le Guardien, Silencer, Theef, WebEx

puerto 1005 Theef

puerto 1008 Lion puerto 1010 Doly Trojan

puerto 1011 Doly Trojan

puerto 1012 Doly Trojan

puerto 1015 Doly Trojan

puerto 1016 Doly Trojan

puerto 1020 Vampire

puerto 1024 Jade, Latinus, NetSpy, Remote Administration Tool RAT [no 2]

puerto 1025 Fraggle Rock, md5 Backdoor, NetSpy, Remote Storm

puerto 1025 (UDP) Remote Storm

puerto 1031 Xanadu

puerto 1035 Multidropper

puerto 1042 BLA trojan

puerto 1042 (UDP) BLA trojan

puerto 1045 Rasmin

puerto 1049 /sbin/initd

puerto 1050 MiniCommand

puerto 1053 The Thief

puerto 1054 AckCmd

puerto 1080 SubSeven 2.2, WinHole

puerto 1081 WinHole

puerto 1082 WinHole

puerto 1083 WinHole

puerto 1090 Xtreme

puerto 1095 Remote Administration Tool RAT

puerto 1097 Remote Administration Tool RAT

puerto 1098 Remote Administration Tool RAT

puerto 1099 Blood Fest Evolution, Remote Administration Tool RAT

puerto 1104 (UDP) RexxRave

puerto 1150 Orion

puerto 1151 Orion

puerto 1170 Psyber Stream Server PSS, Streaming Audio Server, Voice

puerto 1174 DaCryptic

puerto 1180 Unin68

puerto 1200 (UDP) NoBackO

puerto 1201 (UDP) NoBackO

puerto 1207 SoftWAR

puerto 1208 Infector

puerto 1212 Kaos

puerto 1234 SubSeven Java client, Ultors Trojan

puerto 1243 BackDoor-G, SubSeven, SubSeven Apocalypse, Tiles

puerto 1245 VooDoo Doll

puerto 1255 Scarab

puerto 1256 Project nEXT, RexxRave

puerto 1269 Matrix

puerto 1272 The Matrix

puerto 1313 NETrojan

puerto 1337 Shadyshell

puerto 1338 Millennium Worm

puerto 1349 Bo dll

puerto 1386 Dagger

puerto 1394 GoFriller

puerto 1441 Remote Storm

puerto 1492 FTP99CMP

puerto 1524 Trinoo

puerto 1568 Remote Hack

puerto 1600 Direct Connection, Shivka-Burka

puerto 1703 Exploiter

puerto 1777 Scarab

puerto 1807 SpySender

puerto 1826 Glacier

puerto 1966 Fake FTP

puerto 1967 For Your Eyes Only FYEO, WM FTP Server puerto 1969 OpC BO

puerto 1981 Bowl, Shockrave puerto 1991 PitFall

puerto 1999 Back Door, SubSeven, TransScout

puerto 2000 Der Späher / Der Spaeher, Insane Network, Last 2000, Remote Explorer 2000, Senna Spy Trojan Generator

puerto 2001 Der Späher / Der Spaeher, Trojan Cow puerto 2023 Ripper Pro

puerto 2080 WinHole

puerto 2115 Bugs

puerto 2130 (UDP) Mini Backlash

puerto 2140 The Invasor

puerto 2140 (UDP) Deep Throat, Foreplay

puerto 2155 Illusion Mailer

puerto 2255 Nirvana puerto 2283 Hvl RAT

puerto 2300 Xplorer

puerto 2311 Studio 54

puerto 2330 IRC Contact

puerto 2331 IRC Contact

puerto 2332 IRC Contact

puerto 2333 IRC Contact

puerto 2334 IRC Contact

puerto 2335 IRC Contact

puerto 2336 IRC Contact

puerto 2337 IRC Contact

puerto 2338 IRC Contact

puerto 2339 IRC Contact, Voice Spy

puerto 2339 (UDP) Voice Spy

puerto 2345 Doly Trojan

puerto 2400 puertod

puerto 2555 Lion, T0rn Rootkit

puerto 2565 Striker trojan

puerto 2583 WinCrash

puerto 2589 Dagger

puerto 2600 Digital RootBeer

puerto 2702 Black Diver

puerto 2716 The Prayer

puerto 2773 SubSeven, SubSeven 2.1 Gold

puerto 2774 SubSeven, SubSeven 2.1 Gold

puerto 2801 Phineas Phucker

puerto 2929 Konik

puerto 2989 (UDP) Remote Administration Tool RAT

puerto 3000 InetSpy, Remote Shut

puerto 3024 WinCrash

puerto 3031 Microspy

puerto 3128 Reverse WWW Tunnel Backdoor, RingZero

puerto 3129 Masters Paradise

puerto 3131 SubSARI

puerto 3150 The Invasor

puerto 3150 (UDP) Deep Throat, Foreplay, Mini Backlash

puerto 3456 Terror trojan

puerto 3459 Eclipse 2000, Sanctuary

puerto 3700 puertoal of Doom

puerto 3777 PsychWard

puerto 3791 Total Solar Eclypse

puerto 3801 Total Solar Eclypse

puerto 4000 Connect-Back Backdoor, SkyDance

puerto 4092 WinCrash

puerto 4201 War trojan

puerto 4242 Virtual Hacking Machine VHM

puerto 4321 BoBo

puerto 4444 CrackDown, Prosiak, Swift Remote

puerto 4488 Event Horizon

puerto 4523 Celine

puerto 4545 Internal Revise

puerto 4567 File Nail

puerto 4590 ICQ Trojan

puerto 4653 Cero

puerto 4666 Mneah

puerto 4950 ICQ Trogen (Lm)

puerto 5000 Back Door Setup, BioNet Lite, Blazer5, Bubbel, ICKiller, Ra1d, Sockets des Troie

puerto 5001 Back Door Setup, Sockets des Troie

puerto 5002 cd00r, Linux Rootkit IV (4), Shaft

puerto 5005 Aladino

puerto 5010 Solo

puerto 5011 One of the Last Trojans OOTLT, One of the Last Trojans OOTLT, modified puerto 5025 WM Remote KeyLogger

puerto 5031 Net Metropolitan

puerto 5032 Net Metropolitan

puerto 5321 Firehotcker

puerto 5333 Backage, NetDemon

puerto 5343 WC Remote Administration Tool wCrat

puerto 5400 Back Construction, Blade Runner

puerto 5401 Back Construction, Blade Runner, Mneah

puerto 5402 Back Construction, Blade Runner, Mneah

puerto 5512 Illusion Mailer

puerto 5534 The Flu

puerto 5550 Xtcp

puerto 5555 ServeMe

puerto 5556 BO Facil

puerto 5557 BO Facil

puerto 5569 Robo-Hack

puerto 5637 PC Crasher

puerto 5638 PC Crasher

puerto 5742 WinCrash

puerto 5760

puertomap Remote Root Linux Exploit

puerto 5802 Y3K RAT

puerto 5873 SubSeven 2.2 puerto 5880 Y3K RAT puerto 5882 Y3K RAT

puerto 5882 (UDP) Y3K RAT

puerto 5888 Y3K RAT

puerto 5888 (UDP) Y3K RAT

puerto 5889 Y3K RAT

puerto 6000 The Thing

puerto 6006 Bad Blood

puerto 6272 Secret Service

puerto 6400 The Thing

puerto 6661 TEMan, Weia-Meia

puerto 6666 Dark Connection Inside, NetBus worm

puerto 6667 Dark FTP, EGO, Maniac rootkit, Moses, ScheduleAgent, SubSeven, Subseven 2.1.4 DefCon 8, The Thing (modified), Trinity, WinSatan

puerto 6669 Host Control, Vampire

puerto 6670 BackWeb Server, Deep Throat, Foreplay, WinNuke eXtreame

puerto 6711 BackDoor-G, SubSARI, SubSeven, VP Killer puerto 6712 Funny trojan, SubSeven

puerto 6713 SubSeven

puerto 6723 Mstream

puerto 6767 UandMe

puerto 6771 Deep Throat, Foreplay

puerto 6776 2000 Cracks, BackDoor-G, SubSeven, VP Killer puerto 6838 (UDP) Mstream

puerto 6883 Delta Source DarkStar (??) puerto 6912 Shit Heep

puerto 6939 Indoctrination

puerto 6969 2000 Cracks, Danton, GateCrasher, IRC 3, Net Controller, Priority puerto 6970 GateCrasher

puerto 7000 Exploit Translation Server, Kazimas, Remote Grab, SubSeven, SubSeven 2.1 Gold puerto 7001 Freak88, Freak2k, NetSnooper Gold

puerto 7158 Lohoboyshik

puerto 7215 SubSeven, SubSeven 2.1 Gold

puerto 7300 NetMonitor

puerto 7301 NetMonitor

puerto 7306 NetMonitor

puerto 7307 NetMonitor, Remote Process Monitor

puerto 7308 NetMonitor, X Spy

puerto 7424 Host Control

puerto 7424 (UDP) Host Control

puerto 7597 Qaz

puerto 7626 Binghe, Glacier, Hyne

puerto 7718 Glacier

puerto 7777 God Message, The Thing (modified), Tini

puerto 7789 Back Door Setup, ICKiller, Mozilla

puerto 7826 Oblivion

puerto 7891 The ReVeNgEr puerto 7983 Mstream

puerto 8080 Brown Orifice, Generic backdoor, RemoConChubo, Reverse WWW Tunnel Backdoor, RingZero

puerto 8685 Unin68

puerto 8787 Back Orifice 2000 puerto 8812 FraggleRock Lite puerto 8988 BacHack

puerto 8989 Rcon, Recon, Xcon

puerto 9000 Netministrator

puerto 9325 (UDP) Mstream

puerto 9400 InCommand

puerto 9870 Remote Computer Control Center

puerto 9872 puertoal of Doom

puerto 9873 puertoal of Doom

puerto 9874 puertoal of Doom

puerto 9875 puertoal of Doom

puerto 9876 Cyber Attacker, Rux

puerto 9878 TransScout

puerto 9989 Ini-Killer

puerto 9999 The Prayer

puerto 10000 OpwinTRojan

puerto 10005 OpwinTRojan

puerto 10008 Cheese worm, Lion

puerto 10067 (UDP) -

puertoal of Doom

puerto 10085 Syphillis

puerto 10086 Syphillis

puerto 10100 Control Total, GiFt trojan

puerto 10101 BrainSpy, Silencer

puerto 10167 (UDP) -puertoal of Doom

puerto 10520 Acid Shivers

puerto 10528 Host Control

puerto 10607 Coma

puerto 10666 (UDP) Ambush

puerto 11000 Senna Spy Trojan Generator

puerto 11050 Host Control

puerto 11051 Host Control

puerto 11223 Progenic trojan, Secret Agent

puerto 11831 Latinus

puerto 12076 Gjamer

puerto 12223 Hack´99 KeyLogger

puerto 12310 PreCursor

puerto 12345 Adore sshd, Ashley, cron / crontab, Fat Bitch trojan, GabanBus, icmp_client.c, icmp_pipe.c, Mypic, NetBus, NetBus Toy, NetBus worm, Pie Bill Gates, ValvNet, Whack Job, X-bill

puerto 12346 Fat Bitch trojan, GabanBus, NetBus, X-bill

puerto 12348 BioNet

puerto 12349 BioNet, Webhead

puerto 12361 Whack-a-mole

puerto 12362 Whack-a-mole

puerto 12363 Whack-a-mole

puerto 12623 (UDP) DUN Control

puerto 12624 ButtMan

puerto 12631 Whack Job

puerto 12754 Mstream

puerto 13000 Senna Spy Trojan Generator, Senna Spy Trojan Generator

puerto 13010 BitchController, Hacker Brasil HBR

puerto 13013 PsychWard

puerto 13014 PsychWard

puerto 13223 Hack´99 KeyLogger

puerto 13473 Chupacabra

puerto 14500 PC Invader

puerto 14501 PC Invader

puerto 14502 PC Invader

puerto 14503 PC Invader

puerto 15000 NetDemon

puerto 15092 Host Control

puerto 15104 Mstream

puerto 15382 SubZero

puerto 15858 CDK

puerto 16484 Mosucker

puerto 16660 Stacheldraht

puerto 16772 ICQ Revenge

puerto 16959 SubSeven, Subseven 2.1.4 DefCon 8

puerto 16969 Priority

puerto 17166 Mosaic

puerto 17300 Kuang2 the virus

puerto 17449 Kid Terror

puerto 17499 CrazzyNet

puerto 17500 CrazzyNet

puerto 17569 Infector

puerto 17593 AudioDoor

puerto 17777 Nephron

puerto 18667 Knark

puerto 18753 (UDP) Shaft

puerto 19864 ICQ Revenge puerto 20000 Millenium

puerto 20001 Insect, Millenium, Millenium (Lm) puerto 20002 AcidkoR

puerto 20005 Mosucker puerto 20023 VP Killer

puerto 20034 NetBus 2.0 Pro, NetBus 2.0 Pro Hidden, NetRex, Whack Job

puerto 20203 Chupacabra

puerto 20331 BLA trojan puerto 20432 Shaft

puerto 20433 (UDP) Shaft

puerto 21544 GirlFriend, Kid Terror, Matrix

puerto 21554 Exploiter, FreddyK, Kid Terror, Schwindler, Winsp00fer

puerto 21579 Breach

puerto 21957 Latinus

puerto 22222 Donald Dick, Prosiak, Ruler, RUX The TIc.K

puerto 23005 NetTrash, Olive, Oxon

puerto 23006 NetTrash

puerto 23023 Logged

puerto 23032 Amanda

puerto 23321 Konik

puerto 23432 Asylum

puerto 23456 Evil FTP, Ugly FTP, Whack Job

puerto 23476 Donald Dick

puerto 23476 (UDP) Donald Dick

puerto 23477 Donald Dick

puerto 23777 InetSpy

puerto 24000 Infector

puerto 24289 Latinus

puerto 25123 Goy'Z TroJan

puerto 25555 FreddyK

puerto 25685 MoonPie

puerto 25686 MoonPie

puerto 25982 MoonPie

puerto 26274 (UDP) Delta Source

puerto 26681 Voice Spy

puerto 27160 MoonPie

puerto 27374 Bad Blood, EGO, Fake SubSeven, Lion, Ramen, Seeker, SubSeven, SubSeven 2.1 Gold, Subseven 2.1.4 DefCon 8, SubSeven 2.2, SubSeven Muie, The Saint, Ttfloader, Webhead

puerto 27444 (UDP) Trinoo

puerto 27573 SubSeven

puerto 27665 Trinoo

puerto 28431 Hack´a´Tack

puerto 28678 Exploiter

puerto 29104 NetTrojan

puerto 29292 BackGate

puerto 29369 ovasOn

puerto 29559 Latinus

puerto 29891 The Unexplained

puerto 30000 Infector

puerto 30001 ErrOr32

puerto 30003 Lamers Death

puerto 30005 Backdoor JZ

puerto 30029 AOL trojan

puerto 30100 NetSphere

puerto 30101 NetSphere

puerto 30102 NetSphere

puerto 30103 NetSphere

puerto 30103 (UDP) NetSphere

puerto 30133 NetSphere

puerto 30303 Sockets des Troie

puerto 30700 Mantis

puerto 30947 Intruse

puerto 30999 Kuang2

puerto 31221 Knark

puerto 31335 Trinoo

puerto 31336 Bo Whack, Butt Funnel

puerto 31337 ADM worm, Back Fire, Back Orifice 1.20 patches, Back Orifice (Lm), Back Orifice russian, Baron Night, Beeone, bindshell, BO client, BO Facil, BO spy, BO2, cron / crontab,

Freak88, Freak2k, Gummo, icmp_pipe.c, Linux Rootkit IV (4), Sm4ck, Sockdmini

puerto 31337 (UDP) Back Orifice, Deep BO

puerto 31338 Back Orifice, Butt Funnel, NetSpy (DK)

puerto 31338 (UDP) Deep BO, NetSpy (DK)

puerto 31339 NetSpy (DK), NetSpy (DK)

puerto 31557 Xanadu

puerto 31666 BOWhack

puerto 31745 BuschTrommel

puerto 31785 Hack”a´Tack

puerto 31787 Hack´a´Tack

puerto 31788 Hack´a´Tack

puerto 31789 (UDP) Hack´a´Tack

puerto 31790 Hack´a´Tack

puerto 31791 (UDP) Hack´a´Tack

puerto 31792 Hack´a´Tack

puerto 32001 Donald Dick

puerto 32100 Peanut Brittle, Project nEXT

puerto 32418 Acid Battery

puerto 32791 Acropolis

puerto 33270 Trinity

puerto 33333 Blakharaz, Prosiak

puerto 33567 Lion, T0rn Rootkit

puerto 33568 Lion, T0rn Rootkit

puerto 33577 Son of PsychWard

puerto 33777 Son of PsychWard

puerto 33911 Spirit 2000, Spirit 2001

puerto 34324 Big Gluck, TN

puerto 34444 Donald Dick

puerto 34555 (UDP) Trinoo (for Windows)

puerto 35555 (UDP) Trinoo (for Windows)

puerto 37237 Mantis

puerto 37266 The Killer Trojan

puerto 37651 Yet Another Trojan YAT

puerto 38741 CyberSpy

puerto 39507 Busters

puerto 40412 The Spy

puerto 40421 Agent 40421, Masters Paradise

puerto 40422 Masters Paradise

puerto 40423 Masters Paradise

puerto 40425 Masters Paradise

puerto 40426 Masters Paradise

puerto 41337 Storm

puerto 41666 Remote Boot Tool RBT, Remote Boot Tool RBT

puerto 44444 Prosiak

puerto 44575 Exploiter

puerto 44767 (UDP) School Bus

puerto 45559 Maniac rootkit

puerto 45673 Acropolis

puerto 47017 T0rn Rootkit

puerto 47262 (UDP) Delta Source

puerto 48004 Fraggle Rock

puerto 48006 Fraggle Rock

puerto 49000 Fraggle Rock

puerto 49301 OnLine KeyLogger

puerto 50000 SubSARI

puerto 50130 Enterprise

puerto 50505 Sockets des Troie

puerto 50766 Fore, Schwindler

puerto 51966 Cafeini

puerto 52317 Acid Battery 2000

puerto 53001 Remote Windows Shutdown RWS

puerto 54283 SubSeven, SubSeven 2.1 Gold

puerto 54320 Back Orifice 2000

puerto 54321 Back Orifice 2000, School Bus

puerto 55165 File Manager trojan, File Manager trojan, WM Trojan Generator

puerto 55166 WM Trojan Generator

puerto 57341 NetRaider

puerto 58339 Butt Funnel

puerto 60000 Deep Throat, Foreplay, Sockets des Troie

puerto 60001 Trinity

puerto 60008 Lion, T0rn Rootkit

puerto 60068 Xzip 6000068

puerto 60411 Connection

puerto 61348 Bunker-Hill

puerto 61466 TeleCommando

puerto 61603 Bunker-Hill

puerto 63485 Bunker-Hill

puerto 64101 Taskman

puerto 65000 Devil, Sockets des Troie, Stacheldraht

puerto 65390 Eclypse

puerto 65421 Jade

puerto 65432 The Traitor (= th3tr41t0r)

puerto 65432 (UDP) The Traitor (= th3tr41t0r)

puerto 65530 Windows Mite

puerto 65534 /sbin/initd

puerto 65535 Adore worm, RC1 trojan, Sins

APÉNDICE 14
LA YAPA

En algún momento un manual debe cerrarse, es una simple cuestión temporal, de lo contrario, se seguirá construyendo *ad infinitum* y no verá la luz jamás, por eso con autorización de nuestra querida Editorial Errepar, publicamos el último artículo, con ligeras modificaciones, al 3 de junio de 2011.

Ayer nos sorprendió la noticia de la aprobación de la ley 26.685, denominada genéricamente como "Ley del documento electrónico", cuyos primeros artículos reproducimos:

"Artículo 1º. Autorízace la utilización de expedientes electrónicos, documentos electrónicos, firmas electrónicas, firmas digitales, comunicaciones electrónicas y domicilios electrónicos constituidos, en todos los procesos judiciales y administrativos que se tramitan ante el Poder Judicial de la Nación, con idéntica eficacia jurídica y valor probatorio que sus equivalentes convencionales.

"Artículo 2º. La Corte Suprema de Justicia de la Nación y el Consejo de la Magistratura de la Nación, de manera conjunta, reglamentarán su utilización y dispondrán su gradual implementación."

Nos surgen algunas dudas: ¿estos nuevos documentos son instrumentos privados o públicos, dependiendo del tipo de firma que los suscribe? Por ejemplo, si tiene firma digital y su correspondiente certificado digital, ¿es entonces instrumento público?, pero si tiene sólo firma electrónica ¿sería ¿instrumento privado? y ¿si no cuenta con ninguna de las dos, entonces sería un simple documento privado, con relativa validez probatoria? Estas preguntas por el momento nos superan. La Ley de Firma Digital no parece producir modificaciones de peso, en particular con la prueba de contratos a partir del intercambio de mensajes de correo electrónico, sin firma alguna. En el mejor de los casos con un texto que los suscribe, pero que no es nada más y nada menos que la simple habilitación de la opción firma que brindan algunas aplicaciones de correo electrónico y que no tienen certificación alguna. Éstas y otras preguntas intentaremos analizarlas en alguna de las actualizaciones que brindaremos en breve, pero por el momento sólo podemos decir:

Errores inauditos, ¿*In audita altera pars?*

La gestión de la prueba documental informática se halla limitada por algunos

elementos esenciales que no pueden ser soslayados por quien la solicita y por los encargados de llevar a cabo la tarea pretendida. Al respecto es necesario considerar el fuero en que se está realizando la labor técnica:

En el Fuero Penal, la decisión de recolectar una prueba documental informática estará fundada en un documento emanado del fiscal o del juez que intervienen en la causa; para que esta recolección se realice en condiciones óptimas de validación, certificación y traslado, es necesario que cuente con los siguientes elementos esenciales:

Órdenes de secuestro y allanamiento, confeccionadas en forma legal.

Descripción detallada y explícita de las tareas a realizar. Entre ellas el secuestro de elementos físicos, la inspección de programas y determinación de sus relaciones lógicas, el criterio de selección de la información a recolectar. Pero sobre todo los límites de dicha recolección para asegurar el derecho a la privacidad de las partes de la causa y de terceras personas. Esta última consideración raras veces aparece en la orden de secuestro emitida por la autoridad judicial correspondiente.

Presencia de un funcionario judicial que convalide el acto y pueda tomar decisiones al respecto ante las posibles dudas surgidas entre los funcionarios de las Fuerzas de Seguridad, que brindan asistencia policial a la tarea y/o los técnicos que la realizan. Esto debe incluir la presencia de testigos imparciales y culturalmente capacitados para entender lo que se le pide que observe (al menos la secuencia de acciones a registrar en el acta que describe los hechos y actos jurídicos realizados).

Presencia de personal técnico capacitado para que realice la tarea. Este tema es ineludible y sumamente polémico. Para dilucidarlo voy a recurrir a la analogía: nadie aceptaría la revisión de un cadáver por otro funcionario que no fuere el médico legista. Esta característica de médico legista brinda seguridad jurídica respecto de la necropsia realizada por el profesional, el informe que la describe y la validez legal de éste. A partir de ese aserto es suficiente con afirmar y aceptar que: *"La Informática Forense es a la Informática lo que la Medicina Legal es a la Medicina".* Los requisitos académicos y profesionales establecidos para la Medicina Legal y para la Informática Forense deberían ser similares, desde sus respectivos campos de acción. En particular los títulos que certifican la idoneidad del profesional. Un médico legista es un médico que luego de recibido ha realizado una carrera de posgrado de médico legista, de por lo menos dos años de duración. No es concebible que la tarea pericial informático forense la realice un funcionario policial, que en la mayoría de los casos sólo cuenta con un título secundario y alguna instrucción somera impartida por la Fuerza a la que pertenece. *Este accionar es violatorio de los principios de debido*

proceso y legítima defensa, porque permite la manipulación de prueba que puede ser decisoria para la causa, por parte de personal cuya idoneidad profesional es al menos dudosa.

En el Fuero Civil y Comercial, la gestión de la prueba documental informática depende directamente de la acción de las partes y por lo tanto requiere de otro tipo de recaudos y otra sucesión de actos, entre ellos:

Luego de la entrevista previa entre el cliente y el abogado que le brindará soporte técnico legal (patrocionio o representación), este último, ante la necesidad de recolectar prueba documental informática con fines probatorios, debería requerir de inmediato la participación de un consultor técnico especializado (experto en Informática Forense). La razón de esta reunión transdisciplinaria reside en la necesidad cierta de recolectar alguna prueba que pueda estar en poder de la parte consultante, de la futura contraparte o de terceros, que puede ser información privada o pública, que tal vez sea necesario certificar por medio de pruebas de informes (en particular a los proveedores de servicios –ISP–) y en caso de negativa, revisadas, analizadas y resueltas por medios periciales (puntos de pericia previsibles). Seguidamente, describiremos el caso más complejo, a partir del cual es posible insertar otros casos con menos requisitos.

Establecida la necesidad de recolectar información privada en poder de la contraparte o de terceros, se hace necesario solicitar esa medida como prueba anticipada, ya que el riesgo de pérdida por borrado doloso de los datos, al tener noticias de la futura demanda, es algo posible y sumamente probable como estrategia de defensa del demandable.

Para solicitar esa medida preliminar es necesario fundamentarla, evitando el rechazo *in limine* por parte del Juzgado que debe resolver el incidente previo ante la falta de justificación cierta, evidente y comprobable de dicha medida. Esto significa que es necesario comprobar el peligro en la demora y la posibilidad de desaparición de la prueba pretendida ante acciones positivas por parte del futuro demandado. Una de las formas de comprobarlo es presentar documentos digitales que brinden credibilidad a la pretensión. Esos documentos digitales están conformados por la información en poder de la parte consultante.

Actuando en consonancia, la primera acción a realizar es la recolección, certificación, preservación y resguardo de la información en poder del consultante. Esta acción requiere de la intervención del consultante, el abogado patrocinante, el consultor técnico y un escribano público. Consiste en las tareas ya descriptas en otros artículos anteriores,[5] las que finalizan generalmente con el resguardo de los datos en

un disco óptico no regrabable, con su correspondiente digesto (*hash*), acta de recolección protocolizada por el escribano y dentro de un sobre, lacrado y certificado por el escribano. Este digesto debe colocarse a su vez en el acta realizada por el escribano, en el exterior del sobre lacrado y en la cadena de custodia que se inicia en ese momento. Es también conveniente realizar varias copias de los sobres y sus discos ópticos contenidos, ya que por error en la manipulación de éstos puede producirse la ruptura de la cadena de custodia, anulando la prueba recolectada. Esta circunstancia es frecuente al entregar la prueba en el Juzgado, donde sin tomar recaudo legal alguno el funcionario a cargo de la barandilla, simplemente rompe el sobre, extrae el contenido y se niega a firmar la cadena de custodia. El tener otros facsímiles para presentar alternativamente es una muestra de buenas costumbres por parte del abogado patrocinante. En la práctica se realizan copias para: el escribano, la parte consultante y por lo menos cuatro para el abogado (al solicitar la prueba anticipada deberá presentar una copia en el tribunal designado y seguramente necesitará otras dos al presentar la demanda, para el Juzgado y para la contraparte), todas con sus correspondientes cadenas de custodia, iniciadas, firmadas y certificadas por el escribano interventor, con su correspondiente constancia en el acta protocolizada.

Es necesario destacar que la documental informática puede constituirse en elemento probatorio de muchos hechos jurídicos. Por esta razón, es necesario analizar su pertinencia probatoria. Por ejemplo, ante el constante aumento de los contratos a distancia, utilizando la modalidad de intercambio de mensajes de correo electrónico (vulgarmente denominado contrato por e-mail), se genera el problema de su validez como instrumento privado. Evidentemente no lo es por carecer de firma comprobable[6] (son muy escasos los mensajes que se intercambian utilizando firma electrónica y prácticamente inexistentes aquellos que cuentan con firma digital). Esta circunstancia no lo invalida totalmente, ya que puede ser aceptado como una prueba por escrito,[7] de ahí la necesidad imperiosa de preservarlo mediante los recaudos antes establecidos, para que pueda ser considerado válido por el tribunal interventor. Teniendo siempre en cuenta que aunque por sí solo no tenga la entidad de instrumento privado, concatenado causalmente y relacionado con la correspondiente prueba de informes, con la prueba pericial y con toda otra prueba indiciaria aportable, puede conformar una estructura probatoria sólida, coherente, creíble y comprobable.

La solicitud de prueba anticipada se respalda mediante la argumentación que corresponda (para justificar el peligro en la demora y el riesgo de pérdida de prueba) y con la documental informática resguardada según el procedimiento anterior. Es decir, se acompaña de la misma manera en que se agrega cualquier otro documento en soporte de papel. La documental informática es sólo una especie de la documental clásica (bibliográfica, foliográfica o pictográfica), que difiere de aquélla únicamente

en el soporte (digitalizado por medios ópticos o magnéticos). Los resguardos de esta prueba anticipada son similares a los referidos a la primera recolección frente al escribano, si bien la realizará un experto designado por el tribunal de entre los que obran en la lista. Es importante al solicitar la prueba especificar claramente el perfil del profesional que debería realizarla, en razón de las múltiples listas de peritos similares, de ahí que el abogado deba interiorizarse de las incumbencias profesionales de cada uno. También es de rigor la concurrencia del abogado al acto, ya que como tiene experiencia en el tema (por lo menos a partir de la acción primigenia de resguardo de datos de su cliente) puede hacer observaciones y exigir el cumplimento de todas y cada unas de las tareas necesarias para asegurar la prueba (digesto, acta, cadena de custodia, etc.).

Al confeccionar la demanda es necesario considerar de manera relacional, integrada y transdisciplinaria, la estrategia procesal a utilizar en el caso particular considerado. Respecto de la documental informática, recolectada por medio de la acción directa sobre la información obrante en poder de la futura actora y a partir de la implementación de la prueba anticipada, en general la misma debe ser convalidada por medio de prueba de informes. Esta prueba, por ejemplo, en el caso de los mensajes de correo electrónico resguardados, consistirá en el pedido de informes al proveedor del servicio de mensajería y correo (ISP), para que convalide el origen, destino, hora GMT de cada mensaje recolectado y de ser posible su contenido. Este último punto dependerá de los resguardos que mantenga el ISP y de la antigüedad del mensaje considerado, cuanto más reciente mayores serán las posibilidades de alcanzar éxito en esta gestión, de ahí que en temas informáticos forenses la celeridad constituye la norma.

Por supuesto es muy posible que la contraparte niegue el contenido de la documental informática presentada. Por esta razón es imprescindible preparar los puntos de pericia necesarios para respaldarla oportunamente. La mejor forma de realizar esa tarea y limitar la misma a los puntos pertinentes y conducentes, que brinden soporte a la estrategia procesal planificada, es efectuarla en conjunto entre el consultor técnico seleccionado (experto en Informática Forense) y el abogado patrocinante.

En lo que se refiere al Fuero Contencioso Administrativo, éste guarda relación directa con el Procedimiento Penal, con algunos visos del procedimiento Civil y Comercial, por esta razón es necesario analizar cada caso en particular y actuar en consecuencia, adaptando cada accionar a las necesidades del administrado o de la administración representados. En particular, pero no exclusivamente, ante la comprobación de pagos impositivos, declaraciones juradas y otras acciones que pueden ser realizadas mediante medios digitales (electrónicos, magnéticos u ópticos).

Respecto del Fuero Laboral, el accionar es muy similar al Fuero Civil y Comercial, pero teniendo especialmente en cuenta el principio de *in dubio pro operario* al momento de analizar las relaciones contractuales que rigen para este último. En particular, los convenios de confidencialidad y los reglamentos internos que organizan y norman el uso de la tecnología informática propietaria de la empresa empleadora. El experto deberá analizar en profundidad, a la hora de recolectar datos solicitados por la empresa, para no vulnerar la privacidad del trabajador, por ejemplo, los datos obrantes en la base de datos de personal de la empresa son de propiedad de la misma, pero contienen datos sensibles que seguramente están protegidos por la ley 25.326. De la misma manera la cuenta de correo electrónico personal del empleado es de su propiedad exclusiva y no puede ser accedida a pedido del empleador sin la correspondiente orden judicial. Aunque a veces es consultada por el empleado desde su lugar de trabajo, quedando indicios ciertos y factibles de recolección en las computadoras donde se produce la consulta y/o en los servidores que las administran, a pesar de la prohibición explícita y firmada ante el empleador, esto no autoriza su acceso sin autorización de su legítimo propietario (el empleado a quien pertenece). Es quizás el caso más delicado y requiere del accionar integrado y transdisciplinario estricto entre el operador del derecho y el experto que realiza la tarea.

Los errores cometidos en la planificación, desarrollo, implementación y certificación descriptas en los puntos anteriores, generan dificultades muchas veces insalvables, las que pueden llevar a la anulación y descarte de la prueba producida. En tal sentido es interesante analizar los siguientes fallos:

Cámara Nacional de Apelaciones en lo Criminal y Correccional, Sala V/07/29.c., 39.803, "V.

C. W. E. s/infr. ley 11.723", Procesamiento 49/169, Buenos Aires, 22 de septiembre de 2010. En este caso se desestima el acta de secuestro por fallas en la individualización de los elementos secuestrados:

"La presente instrucción adolece de un vicio insalvable que impide su subsistencia como actuación válida, por su incidencia negativa en el derecho de defensa del imputado. En efecto, la reconstrucción de la materialidad del suceso y la subsiguiente responsabilidad se han estructurado en base al acta de secuestro documentada a fs. 35/37, que, no obstante cumplir con algunas de las formalidades legalmente previstas, carece de la debida individualización del material incautado."

"Esa falencia se reiteró en los actos siguientes, destinados a determinar positiva o negativamente la ilegalidad de ese material."

"En efecto, ni en el acta de apertura para el inicio pericial, ni en el curso del

examen de la especialidad se procedió a su íntegr*a individualización (fs. 61 y 68/71).”*

“El mentado informe concluyó que la totalidad de los soportes ópticos *tipo DVD-R eran apócrifos; sin embargo, no se dio cumplimiento al punto 1 de la respectiva orden pericial (fs. 41), tendiente a identificar la totalidad de los discos compactos secuestrados…”*

“…al momento de recibírsele declaración indagatoria al imputado (fs. 316/320), oportunidad en que éste *introdujo una duda directamente vinculada con el defecto que se viene señalando, dijo entonces que no podía asegurar que las películas que se encontraban en el Juzgado fueran las mismas que se secuestraran en el allanamiento.”*

“Esa duda y las consecuencias que de ella emergen constituyen la médula de la apelación por la que en este momento intervenimos.”

“Las particularidades del caso y la falencia especificada afectaron el derecho de defensa del imputado…, cabe remarcar que el defecto señalado en párrafos anteriores impide asegurar fehacientemente que la cadena de custodia de los elementos inicialmente secuestrados no haya sido vulnerada.”

“Atento a lo expuesto, decretaremos la nulidad del acta de secuestro de fs. 35/37 y de los actos consecuentes: el informe pericial fs. 69/71, la declaración indagatoria de fs. 316/320, el auto que dispuso la falta de mérito de fs. 323/327/vta., y, finalmente, la resolución recurrida (artículo 168 del Código Procesal Penal de la Nación).”

Aunque las razones aducidas en el caso considerado aparecen como sólidas y convincentes, es conveniente que el lector analice esta resolución en relación con la que sigue, ya que podrá comprobar por sí mismo notorias diferencias en el criterio procesal, aplicado en cada caso. Éste es el tipo de inconvenientes en la gestión de la prueba documental informática que el operador del derecho debe prevenir y evitar a toda costa. Sólo la labor técnica transdisciplinaria (operador del derecho – consultor técnico) e integrada, permitirá arribar a buen puerto en la gestión de la documental informática y sus pruebas relacionadas.

Expte. N° 14.349/2010, “C. S. D. G. c/CPACF” (Expte. 24.233/09), Cámara Nacional de Apelaciones en la Contencioso Administrativo Federal, Sala V, 10/2/2011.

En este fallo el tribunal admite como prueba válida la impresión de un mensaje de correo electrónico, sin el resguardo técnico informático forense de dicho mensaje:

"Por otra parte, si bien el recurrente pone en duda que el mensaje (cuya existencia también niega) haya sido enviado por él, ya que pudo haber sido enviado por otra persona con acceso a la cuenta, es importante observar que no niega la existencia de la cuenta: [...], desde la que se envió el mensaje cuestionado. En tal contexto, el hecho de que el nombre de usuario de la cuenta coincidiera con las iniciales de su nombre y apellidos, así como la 'firma' que aparece al final del mensaje (indicando su nombre completo, nombre del estudio jurídico, domicilio y teléfonos; v. fs. 9), abonan la tesis del a quo, en cuanto a que el envío se produjo desde esa cuenta."

Esto es equivalente a considerar que el texto que aparece como opción en los aplicativos de correo electrónico, denominada "firma" por la aplicación, pero sin condición alguna que la asimile a la firma ológrafa, a la digital o a la electrónica, ya que es sólo texto introducido por el usuario y que pueden ser perfectamente simuladas por cualquiera, debería ser calificado como firma válida. Esto transformaría a los mensajes de correo electrónico que tienen un texto dudosamente autenticatorio respecto de la identidad de su autor en un instrumento privado, algo que no tiene asidero técnico o legal alguno.

"En ese entendimiento, no aparece debidamente refutada la afirmación del tribunal actuante en cuanto a que 'corre por su exclusiva responsabilidad [del imputado] permitir el acceso al mismo a pocos colaboradores de su confianza' (considerando 6). Aun cuando la dirección electrónica de origen fuera una cuenta 'masiva', el recurrente reconoce que estaba afectada al uso de sus tareas profesionales, ya que desde allí se evacuaban consultas."

"... Aun cuando el recurrente afirma que personas allegadas profesionalmente a él *y con acceso a la cuenta de correo electrónico pudieron enviar el mensaje, la presunción de inocencia se debilita en la medida en que* éste *tenía responsabilidad exclusiva en la decisión de quiénes podían hacer uso de esa cuenta y enviar mensajes desde ella."*

El tribunal ignora la posibilidad del acceso a la cuenta por parte de terceros, utilizando herramientas de violación de la seguridad informática (hacking, cracking, etc.) y otorga a una cuenta de correo electrónico una característica de credibilidad, confiabilidad y autenticidad que no están respaldadas por criterio científico, tecnológico o técnico alguno y de hecho, esta seguridad es violada a diario, de lo contrario no serían posibles los delitos informáticos propios e impropios.[8]

"En efecto, atento a los elementos de juicio que revelan las condiciones de tiempo, lugar y modo en que se emitió el mensaje cuestionado, era una carga procesal del recurrente desvirtuar los elementos de juicio que, inequívocamente, conducen a

considerarlo autor de la conducta susceptible de reproche ético*."*

Aunque parece de sentido común que no es el administrado quien debe probar su inocencia, sino la Administración quien tendría que probar su culpabilidad, por esas peculiaridades del Derecho Administrativo (evidentes en el *solve et repete*, el deber de colaboración y la implícita presunción de culpabilidad) se invierte la carga de la prueba.

Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal, Sala I, "Vázquez, Manuel y Otros s/ Rechazo del Planteo de Nulidad", 5 de mayo de 2011.

En este fallo la Cámara Nacional en lo Criminal y Correccional Federal ordenó que se realicen nuevas pruebas sobre las computadoras secuestradas en el marco de la investigación en desarrollo por presunto enriquecimiento ilícito, con el fin de establecer los motivos de disparidad entre las conclusiones a las que arribaron los peritos de la Policía Federal Argentina y los de la Universidad de Buenos Aires.

Se trata de un fallo paradigmático y ejemplificador, donde la potestad aparentemente ilimitada en el decisorio del *a quo*, es encausada y analizada desde la más pura racionalidad y teniendo en cuenta la naturaleza de la ciencia, tecnología y técnicas que brindan soporte a la Informática Forense.

"En su escrito impugnativo, los defensores de Manuel y Julián Vázquez insistieron en señalar que la cadena de seguridad de los ordenadores peritados había sido violada, y que ello era 'responsabilidad de quienes hicieron el allanamiento, ya que por desidia o ignorancia efectuaron deficientemente el sellado de las máquinas, o fue mal hecho, ya que… los puertos podían ser usados sin necesidad de romper faja alguna'. Destacaron las declaraciones testimoniales de los peritos –'ratificando que la cadena de seguridad de los ordenadores se encontraban violada'– y se preguntaron cómo era posible que la División Apoyo Tecnológico Judicial de la Policía Federal Argentina, pese a poseer la misma tecnología, no encontrara los archivos descubiertos por los expertos de la UBA."

"Por otro lado, destacaron que el a quo no los notificó de los resultados de la pericia efectuada por la UBA, sino que tomaron conocimiento de ello a través de la prensa, por lo que debieron concurrir al tribunal a peticionar copias de las actuaciones correspondientes. Hicieron saber que, a partir de allí, se denunció penalmente la filtración de información."

A pesar de los evidentes e insalvables errores procedimentales ocurridos en esta causa, los que son de conocimiento público, es preciso destacar que muchas veces las Fuerzas de Seguridad deben cumplir su tarea, sin contar con los recursos apropiados

(carencias instrumentales, de programas específicos y en especial de personal capacitado). Por otra parte, en lo referido a la Universidad, es frecuente que en la misma se recurra a supuestos "gurúes" de la Informática Forense, cuyo único título académico informático consiste en la credulidad de sus seguidores. Es así que se designan como peritos a: matemáticos, contadores, administradores de empresas o informáticos sin especialización alguna. Esta característica es propia del ambiente universitario, donde se acostumbra a dar por sentado que todo el que opina es un catedrático de peso y su análisis es creíble por la misma razón, sin analizar el currículum de quien expone y sin siquiera establecer la correspondencia de su título de grado con el tema que analiza.

Por otra parte, la prensa (eterno adversario de la ciencia), intenta adecuar la información a su propia visión personal de los hechos, lo que contribuye a complicar y desacreditar a las instituciones participantes. Son innegables los errores cometidos, pero no son propios de una sola institución, sino del sistema en general, pocos son los que conocen realmente de Informática Forense, menos aún los que tienen los títulos que se requiere, pero muchos los que opinan sobre el tema y son convalidados únicamente gracias al poder discrecional del juez para admitir y convalidar peritos, sea cuales fueran sus capacidades e incumbencia profesionales (bajo la triste y obsoleta figura del "idóneo").

"II. Observado el tenor de los planteos originarios, el confronte con las constancias actuariales nos permite advertir una seria falencia en el decisorio del juez de grado a la hora de responderlos. Básicamente, bajo pretexto de un relevamiento superficial de los cuestionamientos, como si fueran meros quebrantamientos formales, el magistrado ha esquivado la dimensión sustancial del sistema de garantías que es el verdadero eje de la crítica" (Binder, Alberto*, El incumplimiento de las formas procesales. Elementos para una crítica a la teoría unitaria de las nulidades en el proceso penal*, Buenos Aires, Ed. Ad Hoc, 2000, pág. 84).

Es destacable este párrafo del fallo, ya que implica la obligación por parte del juez de escuchar a las partes en relación con los cuestionamientos referidos a la posibilidad de introducción de prueba espuria durante el resguardo de la misma en sede policial o judicial. En efecto, el criterio anterior establecía una especie de regla de honestidad implícita en los Juzgados, que eximía de responsabilidades y cuidados a los mismos respecto de los elementos probatorios almacenados. Es común observar el trato desprejuiciado, indolente y desprevenido, respecto de los elementos que se entregan en custodia, desde el momento en que son dejados en barandilla (rotura de lacres, sellos, fajas de clausura, incumplimiento de cadena de custodia, etc.) hasta el almacenamiento (apilados en cualquier lugar, sometidos a condiciones extremas de temperatura, presión por estiba inadecuada, campos electromagnéticos de todo tipo y

accesibles por cualquier persona que ingrese al recinto del Juzgado). Por una vez surge la duda respecto de la idoneidad implícita en los Juzgados para proteger la prueba retenida en custodia y bajo su responsabilidad.

"En relación al peritaje elaborado por los expertos de la UBA, el Dr. Oyarbide recordó que la defensa de Manuel y Julián Vázquez había designado perito de parte y que no era posible que se plantee una nulidad luego de haberse consentido el acto por conocerlo y dejarlo avanzar. Un argumento del mismo tenor fue dirigido a la defensa de Ricardo Jaime."

"Finalmente, sostuvo que la cadena de custodia no fue violada –'en ningún momento los elementos han estado fuera del ámbito *de control jurisdiccional'– y aseguró,* ergo*, que el contenido de las máquinas permaneció inalterado."*

"Si bien incumbe a los jueces determinar cuáles son los extremos comprendidos en el litigio, sin que estén obligados a seguir a las partes en todas sus alegaciones, sí deben dar tratamiento a los puntos propuestos que sean conducentes para la solución del juicio (Fallos 233:147). Según se advierte, este tratamiento no ha sido el debido en este caso pues se ha abusado de afirmaciones dogmáticas, rituales, sacrificando 'la justicia sustancial a formas vacías' (Carrió, Genaro y Alejandro, El recurso extraordinario por sentencia arbitraria*, Buenos Aires, Abeledo Perrot, 1987, pág. 194). Al mismo tiempo, más allá de la discrecionalidad del juez como director de la encuesta, ha prescindido de realizar prueba decisiva, conforme más adelante se verá."*

En efecto, cuando se habla de cadena de custodia, referida a la prueba indiciaria informática, la misma debe ser estricta, documentada y suscripta por todos los que han intervenido en el proceso de recolección, traslado y resguardo, esto incluye a los miembos del tribunal que reciben y entregan los elementos probatorios. La práctica pericial nos indica que este último hecho, constituye la excepción, y no la norma, en el accionar judicial.

"III. La verdadera discusión que encierra esta incidencia se vincula con la posibilidad de utilizar prueba obtenida por medios ilícitos o prohibidos.

"Más allá de la autenticidad o no de los intercambios epistolares, las partes introducen la posibilidad de que los documentos electrónicos hayan sido colocados clandestinamente en las computadoras mientras ellas se encontraban secuestradas a disposición del Juzgado."

"La CN, como derivación del derecho a la intimidad, declara inviolables la correspondencia epistolar y los papeles privados (art. 14). Esta protección, sin

embargo, encuentra limitaciones en la ley reglamentaria (art. 28) y serán los jueces quienes en cada caso autorizarán las injerencias en el ámbito *de la intimidad de las personas cuando ellas se encuentren justificadas. Así fue como se llevó adelante el allanamiento y el secuestro de las computadoras de las oficinas de Manuel y Julián Vázquez, diligencias legalmente ordenadas por el Dr. Norberto Oyarbide a fs. 937/938."*

"Mas si esas computadoras fueron contaminadas con información introducida luego del secuestro se abren, al menos, dos posibilidades: una, que esos datos no sean auténticos; y la otra, que aun siéndolo no estuviesen albergados originariamente en ese soporte cuya inspección ordenara el juez."

Por lo tanto, el juez debe asegurar la protección estricta de los archivos informáticos secuestrados, durante toda su gestión, incluyendo el almacenamiento de los mismos dentro del local del Juzgado. Debiendo cumplir todas las normas de seguridad informática e informática forense establecidas al respecto, las que no sólo son dejadas de lado en la mayoría de los casos, sino simple y llanamente desconocidas por los miembros de los tribunales actuantes.

"De darse tanto uno como otro supuesto los archivos encontrados por los expertos de la UBA debieran ser excluidos de la prueba. La sospecha introducida por las defensas pretende en última instancia que *así sea y encuentra, en respaldo de su postura, la llamada 'regla de exclusión', receptada localmente a partir del caso 'Charles Hermanos' (Fallos 46:36) y consolidada de allí en adelante en numerosas ocasiones (Fallos 303: 1938; 306:1752; Peralta Cano; 333:1674). La regla no se conforma con proscribir la prueba falsa sino que está dirigida a excluir la prueba obtenida ilegalmente, sin importar su autenticidad ni la sospecha de culpabilidad (Carrió, Alejandro D.,* Garantías constitucionales en el proceso penal*, Buenos Aires, Hammurabi, 2003, pág. 230), pues, frente a la investigación de la verdad como meta del procedimiento penal, hace valer la dignidad del ser humano y cierto* ámbito *de privacidad que le garantiza el Estado de derecho (Maier, Julio B. J.,* Derecho Procesal Penal. I. Fundamentos*, Buenos Aires, Ed. Del Puerto, 1999, págs. 663/664 y sgtes.)."*

"En síntesis, la eventual violación de la cadena de custodia impide asegurar que los elementos secuestrados por orden del juez hayan contenido originariamente los archivos encontrados en el estudio de la UBA, lo que, en otras palabras, implica admitir que existen dudas no sólo acerca de su autenticidad sino también del modo en que ingresaron a la encuesta. Estos interrogantes plantean, como posibilidad, que en autos se haya producido una actuación ilegítima –incluso de quienes participan o auxilian a la instrucción– o bien un hecho ilícito–en perjuicio de derechos

constitucionales– del que la administración de justicia no puede pretender ser beneficiaria (Fallos 303:1938; 306:1752).”

“V.En otro orden, teniendo en consideración las manifestaciones vertidas por los defensores de Manuel Vázquez al momento de informar oralmente ante esta Alzada en relación con el estado público que han tomado los correos electrónicos que fueron extraídos de las computadoras –cuyas impresiones pudieron observarse en algunos diarios del país–, y con el objeto de asegurar, del modo más amplio posible, la efectiva vigencia de la presunción de inocencia de la que goza todo imputado, se torna necesario instar al magistrado de primera instancia a extremar las medidas necesarias a fin de evitar que, en el futuro, vuelva a presentarse una situación similar a aquélla.”

“En virtud de los argumentos desarrollados en los párrafos que anteceden, el tribunal Resuelve: Declarar la nulidad del auto de fecha 23 de diciembre de 2010 –fs. 78/89–, debiendo el a quo proceder de acuerdo a lo expresado en los considerandos (arts. 123 y 166 del CPPN).”

Estamos ante una resolución contundente y contexte con los hechos acaecidos; sería de esperar que se constituya en referente y ejemplo para otros Juzgados, intentando armonizar las acciones imprescindibles para el resguardo y protección de la documental informática, en condiciones técnicas y procedimentales ajustadas a la disciplina informático forense.

SÍNTESIS: Se hace evidente a partir de la lectura comparativa de los fallos propuestos la existencia de al menos dos criterios judiciales, con mayor o menor soporte jurídico: algunos jueces aceptan los protocolos y reglas técnicas informático forenses y otros las niegan. A partir de la lectura integradora de los fallos propuestos se evidencia la necesidad de establecer parámetros específicos en la gestión de la prueba indiciaria informática, los que deben formalizarse mediante normas especiales consensuadas entre los operadores del derecho y los profesionales de la Informática Forense. Es nuestra opinión, que dicha lectura confirma la necesidad de ajustar la gestión de la prueba documental informática a las consideraciones vertidas en la primera parte del artículo.

5 Recolección de información pública y privada en poder de nuestro consultante y de información pública obrante en Internet. No se puede recolectar en esta etapa información privada de terceros o de la contraparte, para hacerlo es preciso contar con orden judicial específica.

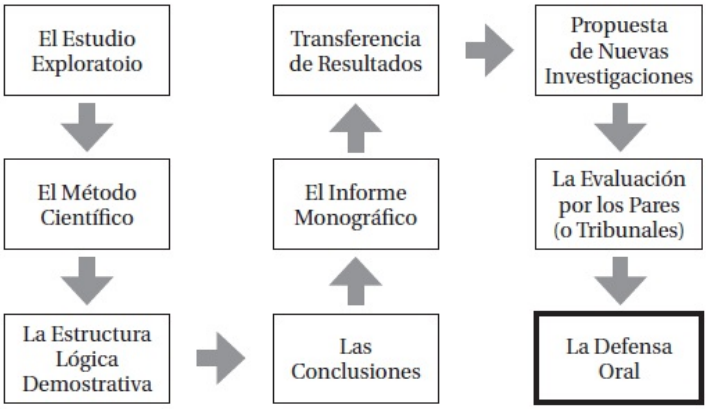
6 Código Civil. “Art. 1012. La firma de las partes es una condición esencial para la existencia de todo acto bajo forma privada. Ella no puede ser reemplazada por signos ni por las iniciales de los nombres o apellidos”.

7 Código Civil. “Art. 1190. Los contratos se prueban por el modo que dispongan los Códigos de Procedimientos de las Provincias Federadas: Por instrumentos públicos. Por instrumentos particulares firmados o no firmados. Por confesión de partes, judicial o extrajudicial. Por juramento judicial. Por presunciones legales o judiciales. Por testigos.”

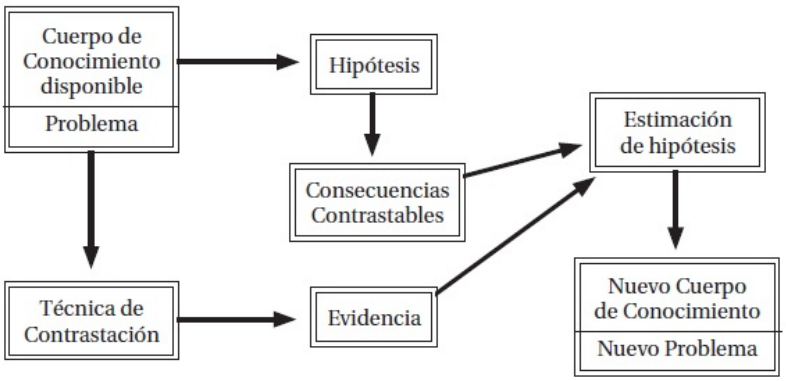
8 Delito informático propio es el que afecta a la información como bien jurídico protegido (por ejemplo, sustitución de identidad), delito informático impropio es el delito ya tipificado (robo, hurto, defraudación, extorsión, etc.) cometidos utilizando herramientas informáticas.

ANEXO 1
DIAGRAMAS CONCEPTUALES

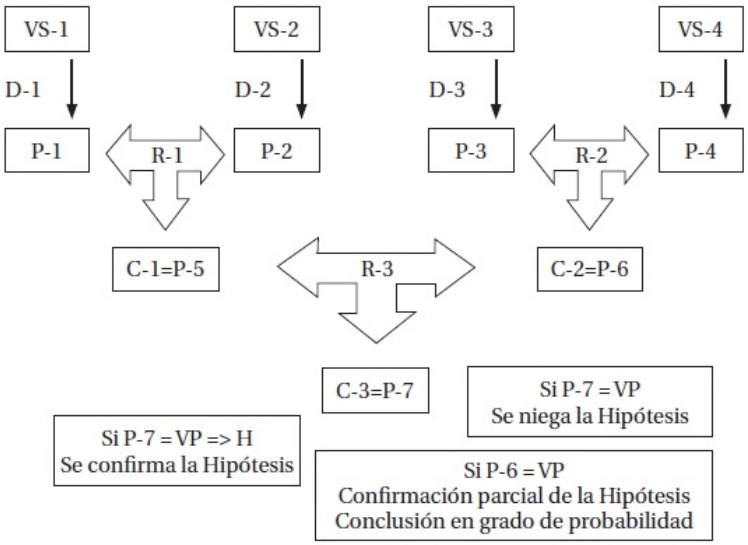
Marco científico investigativo



Esquema de investigación

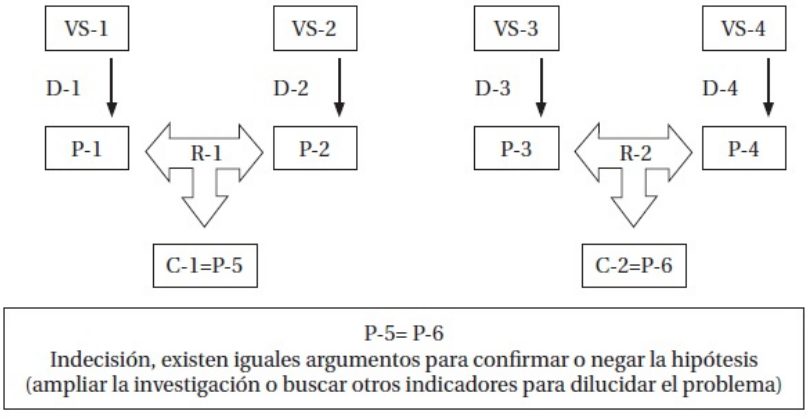


Modelo de estructura demostrativa



Referencias: VS= Variable Secundaria, D= Demostración (teórica, documental o experimental), P= Premisa, R= Razonamiento (silogismo válido), VP= Variable Principal, C= Conclusión.

Gráfico del caso particular de conclusiones contradictorias

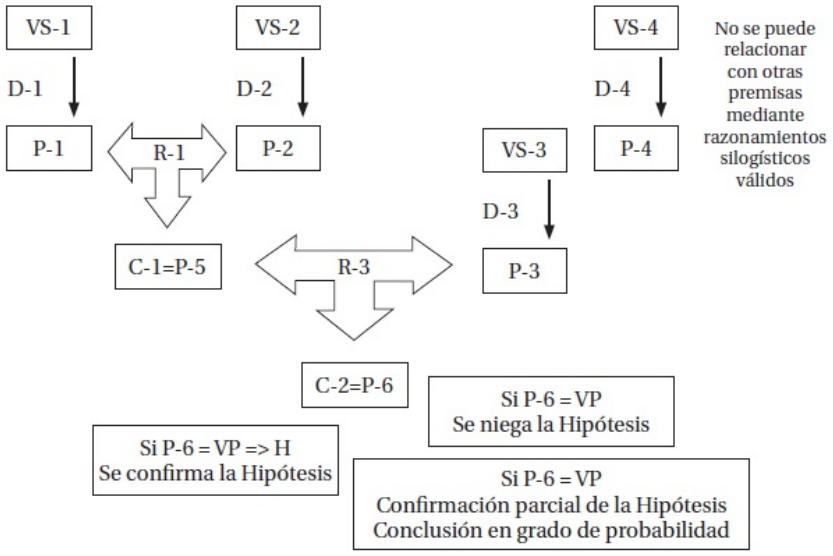


Referencias: VS= Variable Secundaria, D= Demostración (teórica, documental o

experimental), P= Premisa, R= Razonamiento (silogismo válido), VP= Variable Principal, C= Conclusión.

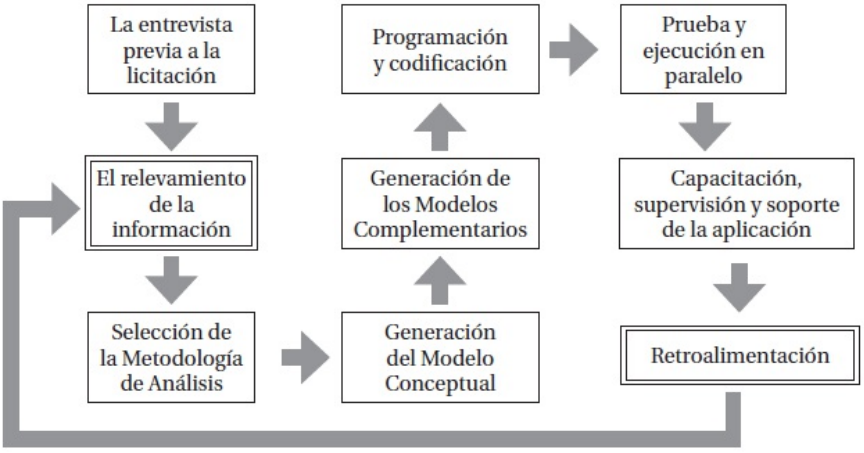
Caso especial de variable secundaria (indicador) innecesario

(VS-4, debe ser eliminada para evitar confusiones)

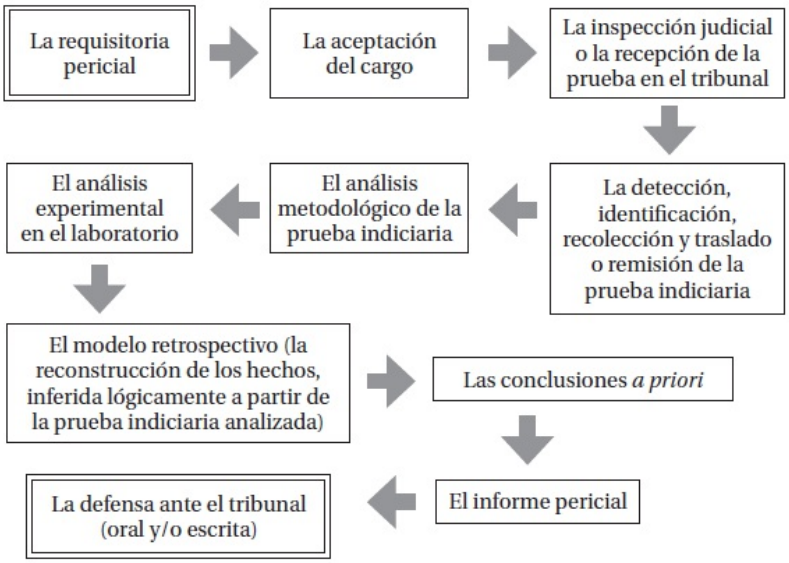


Referencias: VS= Variable Secundaria, D= Demostración (teórica, documental o experimental), P= Premisa, R= Razonamiento (silogismo válido), VP= Variable Principal, C= Conclusión.

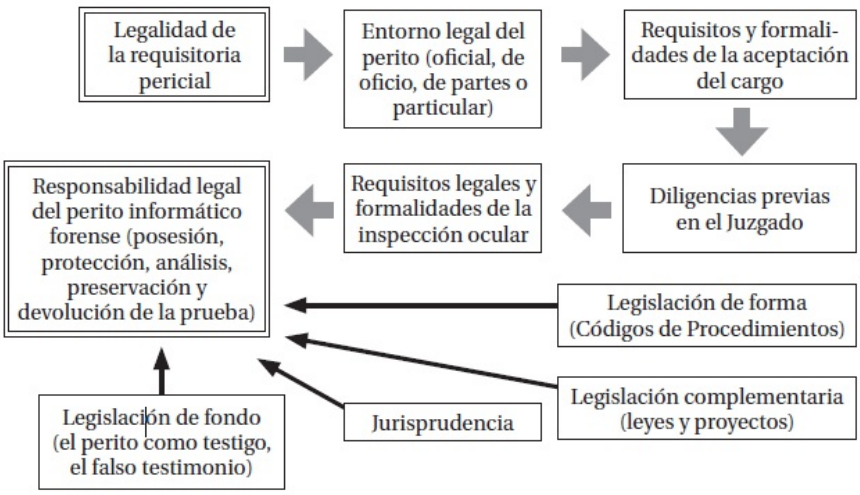
Marco, metodológico sistémico



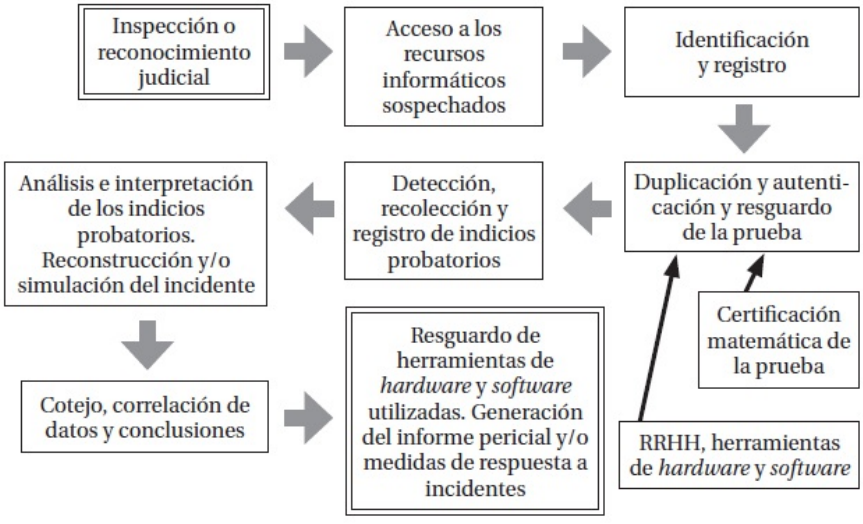
Marco metodológico criminalístico



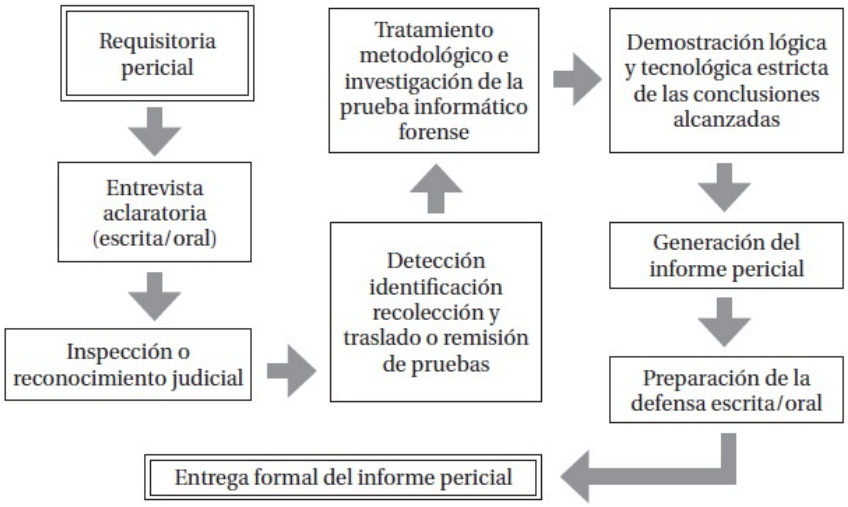
Marco legal



Marco tecnológico pericial



Metodología pericial informático forense


Requisitoria pericial
Entrevista aclaratoria (escrita/oral)
Inspección o reconocimiento judicial
Detección identificación recolección y traslado o remisión de pruebas
Tratamiento metodológico e investigación de la prueba informático forense
Demostración lógica y tecnológica estricta de las conclusiones alcanzadas
Generación del informe pericial
Preparación de la defensa escrita/oral
Entrega formal del informe pericial

ANEXO 2
MODELO DE INFORME PERICIAL

AL SR. JUEZ NACIONAL DE PRIMERA INSTANCIA EN LO CIVIL Y COMERCIAL FEDERAL DR. JORGE LAGUNA. SECRETARÍA NRO. 17 – DR. FIDEL PINTOS

S / D

El que suscribe Lic/perito/Ing Nombre y Apellido; matrícula profesional Nro:…; Nro de CUIT/CUIL:…; de nacionalidad argentina; de estado civil…; de profesión ……; con domicilio particular en ……; constituyendo domicilio legal en ….; teléfono particular número: 1234-5678, fax número: 9101-1121; correo electrónico: perito@consultora.com.ar; designado perito en Informática Forense, en los autos caratulados Sánchez, Jorge c/Milton Santos da Cunha Oliveira Palha s/incumplimiento de contrato, identificado con el número de expediente 13331/2010, tramitado ante el JUZGADO NACIONAL DE PRIMERA INSTANCIA EN LO CIVIL Y COMERCIAL FEDERAL Nro. 13 del DR. JORGE LAGUNA. SECRETARÍA NRO 17 – DR. FIDEL PINTOS, acorde

a lo determinado en los artículos 457 y subsiguientes del Código Procesal Civil y Comercial de la Nación. Reconociendo el conocimiento, alcance y penas establecidas en los artículos 275 y 276 del Código Penal de la Nación, en concordancia con el artículo 449 y las salvedades del artículo 444 del Código Procesal Civil y Comercial de la Nación se constituye ante S SA, a efectos de informarle los resultados periciales alcanzados luego de las operaciones técnicas, realizadas sobre los elementos peritados (examinados, peritados, *sub peritia)*.

OBJETO DE LA PERICIA:

La presente pericia tiene por objeto determinar *"...si los archivos dubitados se encontraban almacenados en: . . ."* (textual) , obrando requisitoria pericial a foja 75 del cuerpo principal de los autos citados.

ELEMENTOS OFRECIDOS:

En relación con la requisitoria pericial, de conformidad con el artículo 260 del Código Procesal Penal de la Nación y en las condiciones señaladas en el artículo 261 del precitado Cuerpo Legal, se recibieron los siguientes elementos *sub peritia*:

1. Documentos recibidos en custodia: Especialmente el expediente principal entregado al perito (artículo 127 del Código Procesal Civil y Comercial de la Nación) y en caso de existir, los cuadernos de prueba.

2. Elementos dubitados: Disco – Computadora – Unidad de almacenamiento – Documento Impreso – Software – Hardware – Recursos Humanos o Expertos consultados – Laboratorio consultado – Ver ampliación en el detalle técnico.

3. Elementos de comparación: Herramientas que no forman parte de la prueba dubitada (descripción estricta de las mismas, incluyendo versión y procedencia, en caso de *software* libre indicar que se trata de Licencias GNU, en caso contrario incluir el número de licencia del producto y sus especificaciones técnicas en un anexo)– Informe realizado por otro técnico, laboratorio, empresa, etc. Reconstrucción del hecho en entornos simulados como máquinas virtuales (VPC – VMWare).

OPERACIONES REALIZADAS:

(Consta de dos partes principales:

La primera secuencial, acorde al orden cronológico de las actividades en su totalidad, desde la recepción del material o la inspección ocular, hasta las últimas operaciones de registro probatorio. Sólo se describe la tarea con carácter informativo y se la referencia al detalle técnico de un anexo respectivo. Desde lo metodológico es la conversión metodológica estricta de una proposición –proveniente de la variable definida–, en su correspondiente premisa, mediante una serie de operaciones científicamente válidadas, tecnológicamente fundamentadas y técnicamente correctas, que puedan ser repetidas en cualquier momento posterior por otros expertos en el área. En caso de necesidad o riesgo evidente de destrucción total o parcial de la prueba indiciaria, como resultado de las tareas de análisis pericial efectuadas sobre la información *sub peritia*, debe solicitarse la autorización escrita del Juzgado interventor antes de proceder.

Una segunda parte que se conforma fuera de la pericia construyendo un árbol demostrativo silogístico estricto, que define, estructura y organiza la justificación de las conclusiones. A partir de dicho árbol probatorio –véase metología lógica demostrativa– se construye la redacción argumentativa, acorde a las capacidades del

perito, asimismo se debe utilizar para conformar un discurso técnico claro, conciso, breve, tecnológicamente fundamentado, acorde al nivel del destinatario y especialmente ameno, véanse técnicas de redacción y oratoria).

A efectos de cumplimentar la requisitoria pericial encomendada se procedió a realizar las siguientes operaciones periciales:

TAREAS POR ORDEN CRONOLÓGICO

Tarea 1 – Ver Anexo I

Tarea 2 Ver Anexo II

…Tarea n – Ver Anexo m

ARGUMENTACIÓN DEMOSTRATIVA

Reorganización de las tareas, incorporándolas a una estructura demostrativa estricta, en forma de árbol binario, que permita su análisis lógico estricto y su discusión silogística formal. Este árbol puede agregarse como anexo, pero en general no es conveniente porque sólo contribuye a esclarecer la demostración a las personas con una buena formación en lógica, lo que no es común, ni corriente entre la mayoría de los profesionales. No obstante este árbol constituirá la base de nuestro discurso argumentativo. Con esta estructura, sobre la base de su soporte y con el agragado de nuestras capacidades de redacción, se construirá el argumento que justifique las conclusiones alcanzadas.

Es imprescindible considerar, además, que no podemos escapar al método científico en general y al método criminalístico en particular, el análisis desde lo general a lo particular debe conformar la estructura principal (el *"backbone"*) subyacente al árbol binario demostrativo.

Recomendaciones: Una vez finalizada la demostración argumentativa estricta, puede suceder que aparezcan situaciones particulares que impliquen nuevas estructuras o pruebas que puedan ayudar a la causa, pero que no han sido incluidas en la requisitoria pericial. En este punto surge una clara dualidad, el perito no puede expedirse más allá de la requisitoria pericial (so pena de ser considerado tendencioso o parcial), pero no puede dejar de decir lo que vio, porque el falso testimonio establecido en el artículo 275 del CPN no sólo consiste en afirmar una falsedad, sino también en ocultar una verdad conocida.

Por lo tanto, no corresponde incluir estas apreciaciones en las conclusiones, que únicamente deben referirse a la requisitoria pericial, sin embargo nada impide incluirlas en este momento, explicitándolas y sugiriendo a S. Sa., que en caso de considerarlo necesario ordene la ejecución de una ampliación de pericia posterior. De esta manera se salvan ambas situaciones y se eluden responsabilidades innecesarias. Es conveniente "sugerir" asimismo los términos estrictos de dicha requisitoria, para evitar nuevas idas y vueltas por falta de claridad o definición en las mismas.

Ejemplo: Luego de examinados los archivos detectados, ha sido posible determinar que los obrantes en el disco rígido correspondiente al servidor principal de la red (identificado como Servidor A, en el apartado II del presente informe) de la empresa R, son idénticos a los que obran la terminal J (identificada…) de la Sucursal T. No obstante esta característica es señalada a título informativo a S. Sa. y en concordancia con el artículo 275 del CPN. Si S. Sa., estima conveniente analizar esta circunstancia es posible hacerlo mediante una ampliación del presente informe pericial orientada a: *"establecer si los archivos obrantes en el Servidor Principal de la red de la empresa R, son los mismos que obran en la terminal J de la Sucursal T".*

Sobre la base de los estudios, experiencias y demostraciones realizadas, es posible arribar al punto siguiente:

CONCLUSIONES:

Afirmación, negación o explicitación de imposibilidad de expedirse (por falta de elementos, por falta de tecnología o por razones demostrativas insuficientes) respecto de la requisitoria pericial analizada de forma estricta, acotada y restringida.

Con el objeto de informar a S. Sa., sobre las tareas realizadas y el tiempo demandado por las

mismas, hago saber la siguiente distribución horaria:

Nº	**Tarea**	**Actividad**	**Horas**	**OBS**
01	Gestión de expediente	Administrativa	5	Sede judicial
02	Inspección judicial	Técnica/Pericial	8	Local empresa
03	Reconocimiento judicial	Técnica/Pericial	8	Gerencia

04	Análisis de laboratorio	Técnica/Pericial	13
05	Confección del informe pericial	Administrativa	5
TOTAL			39

Se hace constar que la hora técnico pericial vigente en el mercado para un profesional universitario con título de grado, se estima en CIENTO CINCUENTA PESOS ($150), respecto de las horas de gestión administrativas, se estiman en un tercio del costo anterior ($50), lo que en el presente caso prevé un valor total estimado de $4850.

El suscripto ruega a S. Sa. tener en cuenta estos valores al momento de determinar los honorarios profesionales que le pudieran corresponder, considerando la complejidad del trabajo realizado y la capacitación profesional que el mismo requiere por parte de quien realiza la misma pericia.

Sirva la presente de formal y atenta nota de cierre y elevación del informe pericial, constituyendo formal recibo de entrega y recepción de conformidad de los elementos detallados, a sus efectos legales.

Se adjunta en devolución1 al presente informe pericial compuesto de cinco (5) fojas útiles, (en 173 renglones) y, de 8 Anexos (en un total de treinta y dos fojas útiles), el material descripto en el apartado II [9].

Por lo expuesto a S. Sa., solicito: tenga por presentado este informe, por cumplida la tarea pericial encomendada y regule mis honorarios profesionales acorde a la magnitud de los estudios experiencias y demostraciones técnicas efectuadas.

PROVEER DE CONFORMIDAD. SERÁ JUSTICIA.

Firma del perito auxiliar

(si lo hubo) Aclaración Título y cargo

Nro. de CUIL O CUIT

Firma del perito principal Aclaración

Título y cargo

Nro. de CUIL O CUIT

9 Siempre es conveniente que el informe pericial se presente en papel oficio (de tipo tribunales) escrito por ambos lados y conste de un número par de páginas. De esta manera el sello de recepción queda en la misma hoja que la diligencia de cierre y convalida el recibo, deslindando al perito de responsabilidades sobre la integridad o destino *a posteriori* de la prueba analizada.

ANEXO 3
MODELOS DE NOTAS

Excusación con **causa**

Sr. Juez:

El que suscribe Prof. Ing. Luis Enrique Arellano González, designado perito informático único en los autos: *"..."*, con domicilio constituido en … 250, piso 1, Ciudad Autónoma de Buenos Aires, TE: 4736-9551, Correo Electrónico: larellanogonzalez@yahoo.com.ar se presenta ante S. Sa. y solicita, se lo exima[10] de producir el informe pericial solicitado y se lo excluya como perito en la referida causa en razón de:

Por razones personales y laborales, ya no reside más en la Ciudad Autónoma de Buenos Aires, lo que le impide el cumplimiento de la tarea pericial en forma eficiente, efectiva y eficaz, provocando retrasos procesales injustificados en el desarrollo del expediente.

Por la razón anterior no ha renovado su inscripción en lista de peritos del presente año, ni en la correspondiente acreditación pericial frente al COPITEC y cabe la posibilidad cierta de que abandone el país por un tiempo prolongado, en relación con una beca de estudios profesionales a realizar en la CEE.

Se dé traslado a las partes.[11]

Proveer de conformidad. SERÁ JUSTICIA

Prof. Ing. Luis Enrique Arellano González

–MP 5101 (COPITEC)–

Informando percepción de adelanto para gastos

Sr. Juez

La que suscribe Prof. Ing. María. Elena Darahuge, perito en informática designada en los autos: "… S/Daños y Perjuicios", con domicilio constituido en … 250, piso 12, Ciudad Autónoma de Buenos Aires, TE: 4736-9551, Correo Electrónico: darahuge@yahoo.com.ar se presenta ante

Sa. y solicita, se tenga por percibido el adelanto para gastos solicitado, el que fue abonado en su totalidad por el actor.

Proveer de conformidad. SERÁ JUSTICIA

Prof. Ing. María Elena Darahuge

–MP 5100 (COPITEC)–

Excusación invocando razones de recusación

Sr. Juez

El que suscribe ..., perito mecánico designado en los autos: ".... c/ ...", con domicilio constituido en ...., localidad…, TE:…, Correo Electrónico: …se presenta ante S. Sa. y solicita:

Se lo excuse de proseguir actuando como perito en la causa referida, atento a lo determinado en el artículo 463, en relación con el artículo 17 del Código Procesal Civil y Comercial de la Provincia de Buenos Aires, que regulan las causas de recusación de peritos, analógicamente solicita su excusación y se considere revocada la aceptación del cargo oportunamente efectuada.

Funda esta solicitud en razones de salud que lo afectan de manera particular y le impiden realizar un viaje de esta extensión y motivos económicos que le imposibilitan solventar los gastos relacionados con los traslados requeridos para efectuar la tarea pericial encomendada.

Proveer de conformidad. SERÁ JUSTICIA

Solicitando autorización para ingresar al lugar de ejecución de las tareas periciales

Sr. Juez

El que suscribe Prof. Ing. Luis Enrique Arellano González, designado perito informático único en los autos: "…", con domicilio constituido en … 250, piso 1, Ciudad Autónoma de Buenos Aires, TE: 4736-9551, Correo Electrónico: larellanogonzalez@yahoo.com.ar se presenta ante Sa. y solicita:

Se libre oficio a la empresa M S. A. (calle … 1360, CABA) para que facilite el ingreso del suscripto al sistema informático de la misma, con el objeto de resolver los puntos periciales solicitados, fijando fecha y hora para dicha diligencia.

Se de traslado a las partes para que hagan efectiva la precitada diligencia procesal, en cumplimiento del artículo 471 *in fine,* del Código Procesal Civil y Comercial de la Nación. Se hace constar que esta notificación debe ser realizada por la parte interesada, ya que el perito no es parte en la causa y su accionar en particular debe revestirse de la imparcialidad que su labor implica. Realizar diligencias procesales, no estrictamente técnicas y propias de una de las partes afectaría la aplicación del artículo 384 del referido cuerpo legal, perjudicando a la otra.

A posteriori, se autorice al suscripto a retirar el expediente del tribunal interventor, por el plazo de 10 días hábiles, a efectos de realizar el informe pericial solicitado.

Se libre giro a nombre del suscripto, en relación con el depósito efectuado el 14 de febrero de 2007, realizado en autos.

Proveer de conformidad. SERÁ JUSTICIA

Prof. Ing. Luis Enrique Arellano González

–MP 5101 (COPITEC)–

Solicitando fecha para realizar reconocimiento judicial

Sr. Juez

La que suscribe Prof. Ing. María Elena Darahuge, perito en informática designada en los autos: "…S/Cese de oposición al Registro de Marca", con domicilio constituido en … 250, piso 12, Ciudad Autónoma de Buenos Aires, TE: 4736-9551, Correo Electrónico: darahuge@yahoo. com.ar se presenta ante S. Sa., a efectos de informarle que:

Acorde a la resolución recaída en autos, ordenando se denuncie en autos fecha, hora y lugar en que se llevará a cabo el reconocimiento judicial solicitado, procedió a coordinar una fecha de realización para dicha diligencia con la abogada patrocinante de la demandada, estableciendo la misma para el día 3 de octubre de 2007, a las 15.00 horas, en el estudio de la mencionada profesional, sito en … 611, piso 5º, Dto. C de esta Ciudad Autónoma de Buenos Aires.

Asimismo solicita de S. Sa.:

Se la autorice a retirar el expediente principal y los cuadernos de pruebas asociados, con tres días de anticipación a la fecha declarada en el párrafo anterior para obtener fotocopias de los documentos cuestionados y a evaluar durante el reconocimiento.

Se dé traslado a las partes.

Proveer de conformidad. SERÁ JUSTICIA

Prof. Ing. María Elena Darahuge

–MP 5100 (COPITEC)–

Solicitando adelanto para gastos, suspensión de plazos, autorización de procuración en el expediente

Sr. Juez

La que suscribe Prof. Ing. María. Elena Darahuge, perito en informática designada

en los autos: "… S/Daños y Perjuicios", con domicilio constituido en … 250, piso 12, Ciudad Autónoma de Buenos Aires, TE: 4736-9551, Correo Electrónico: darahuge@yahoo.com.ar se presenta ante S. Sa. y solicita:

Atento a la magnitud de las tareas a realizar y la documentación *sub peritia*, la suscripta deberá incurrir en diversos gastos de fotocopias, reiterados traslados a la empresa a peritar y al Juzgado, e insumos informáticos para soporte de información, resguardo e impresión de pantallas relacionadas. Por lo que solicita, en virtud de lo establecido en el artículo 463 del Código Procesal Civil y Comercial de la Nación, se le otorgue un anticipo de gastos de $250, y que se notifique a las partes a estos efectos.

Se prorroguen los plazos procesales, hasta la resolución del adelanto para gastos producido.

Se autorice al Prof. Ing. Luis Enrique Arellano González, DNI 10.599.848, con domicilio constituido en … 250, piso 12, Ciudad Autónoma de Buenos Aires, TE: 4736-9551, Correo Electrónico: larellanogonzalez@yahoo.com.ar, a concursar el presente trámite, así como retirar copias de escritos, efectuar desgloses, diligencias cédulas, oficios, mandamientos, testimonios y a realizar cuanto trámite fuera menester.

Se dé traslado a las partes.

Proveer de conformidad. SERÁ JUSTICIA

Prof. Ing. María Elena Darahuge

–MP 5100 (COPITEC)–

Solicitando aclaratoria de puntos de pericia y suspensión de plazos

Sr. Juez

La que suscribe Prof. Ing. María Elena Darahuge, perito en informática designada en los autos: "… S/Daños y Perjuicios", con domicilio constituido en … 250, piso 12, Ciudad Autónoma de Buenos Aires, TE: 4736-9551, Correo Electrónico: darahuge@yahoo.com.ar se presenta ante

Sa. y solicita:

Que por vía de aclaratoria se deje establecida la requisitoria pericial encomendada en los puntos de pericia obrantes en el folio 32 del Cuaderno de Prueba de la Actora, en razón de que los referidos puntos son tan generales y ambiguos que imposibilitan la realización de una pericia informático forense orientada a resolverlos. Dichos puntos rezan:

Realice las periciales informáticas de rigor.

Toda otra tarea pericial que sea útil *a la pretensión de la actora.*

Se hace constar que los puntos periciales deben ser claros, conducentes y pertinentes a la función probatoria que pretenden y específicos respecto de la competencia del experto invocado.

Se prorroguen los plazos procesales, hasta la resolución de la aclaratoria solicitada.

Se dé traslado a las partes.

Proveer de conformidad. SERÁ JUSTICIA

Prof. Ing. María Elena Darahuge

–MP 5100 (COPITEC)–

10 Los artículos 465 y 466 del CPCCN norman la recusación del perito, curiosamente no tienen su equivalente respecto de la excusación del perito. Esta laguna legal, sin embargo, tiene algunos casos claramente reconocibles y que permiten analógicamente el empleo de este tipo de notas. Es el caso en que por error (más frecuente de lo esperado), un perito sea llamado para resolver puntos de pericia que no hacen a su competencia, por ejemplo: *"se desinsacule perito informático forense para que realice una auditoría contable de los activos patrimoniales de la empresa…",* ejemplo éste que le ha ocurrido al autor. Por supuesto implica la inmediata excusación por incompetencia, lo que es admitido e inmediato y se desinsacula perito contable. Si esta excusa es válida, entonces es posible excusarse, también las causas de excusación de los jueces y testigos, son para los peritos.

11 Siempre se debe "dar traslado a las partes", para que se notifiquen por ministerio de ley (en el Juzgado), nunca pedir que se notifiquen, porque esto implica notificar por cédula y el Juzgado da por sentado que las cédulas las hará el perito. El perito no es parte y por lo tanto no debe notificar a nadie.

ANEXO 4
FORMULARIOS

Lista de control de hardware en la inspección y reconocimiento judicial

Id	Tipo	Nro. de Serie/Marca/Modelo Capacidad/Velocidad	Estado	Observaciones
1	Monitor			
2	Teclado			
3	Mouse			
4	Gabinete			
5	Impresora			
6	Unidad de Zip			
7	Unidad de Jazz			
8	Pen Drive			
9	Cámara			
10	Parlantes			
11	Discos Externos			
12	Disco Rígido			
13	Diskettes			
14	CD-ROM			
15	DVD			
16	Hub			
17	Switch			
18	Router			
19	Computadora portátil			
20	Modem			
21	Placa de red			
22	Celular			
23	Teléfono			
24	UPS			
25	Ipod			
26	Otros no especificados			

Formulario de registro de evidencia

Organismo	Formulario de registro de evidencia de la computadora	IF-Nro.

Caso Nro.	Juzgado	Lugar y fecha

Especificaciones de la computadora	
Marca	
Modelo	
Nro. de Serie	
Garantía	
Placa Madre Marca/Modelo	
Microprocesador Marca/Modelo/Velocidad	
Memoria Ram	
Memoria Caché	

Almacenamiento secundario, fijo y/o removible				
Cantidad	Tipo Disketera-CD-ROM-DVD-Disco Rígido-IDE-SCSI-USB-Zip-Jazz-PenDrive	Marca/Modelo	Velocidad/ Capacidad	Nro. de Serie

Accesorios y periféricos				
Cantidad	Tipo Placa de red, módem, cámara, tarjeta de acceso, impresora, etc.	Marca/Modelo	Velocidad/ Capacidad	Nro. de Serie

Observaciones

Perito informático forense	Lugar	Fecha
Apellido: Nombre: Legajo Nro.: DNI:		
	Firma Aclaración:	

Rótulos para las evidencias

Nro.	
Caso	
Fecha	
Tipo	
Observaciones	
Firma	

Formulario – Recibo de efectos

Fecha	**Organismo**	**Caso Nro.**
Requiere consentimiento **SÍ NO**	**Firma del responsable del consentimiento**	**Rótulo**
Descripción del elemento		
Modelo		
P/N		
S/N		
Entrega conforme		**Firma**
Recibe conforme		**Firma**

Formulario para la Cadena de Custodia

Cadena de Custodia de la Evidencia					
Nro.	Ubicación actual	Fecha	Razón de traslado	Sitio a donde se traslada	Observaciones
Lugar de depósito final de la evidencia:					Fecha:

Lista de control de respuesta a incidentes

Fecha y hora:	**Nro. de incidente**
Lugar:	
Perito informático forense:	

Datos del responsable del reporte del incidente	
Nombre y Apellido:	**DNI/Legajo:**
Dirección:	**Localidad:**
Provincia:	**País:**
Área/Departamento/Oficina:	
Particular/Empresa/Organismo:	
Teléfono:	
Fax:	
Celular:	
Pager:	
Dirección de Correo Electrónico:	
Fecha y hora aproximada del incidente:	
Descripción del incidente:	

Recolección de datos del incidente		
Tipo de red		
LAN	**MAN**	**WAN**
Topología física de la red		
Estrella	**Anillo**	**Bus**
Malla	**Otra**	
Tecnología de acceso al medio		
Ethernet	**Token Ring**	**FDDI**
Otra		
Tipo de cableado		
Estructurado	**Fibra óptica**	**Coaxial**
Inalámbrica	**Satelital**	**Microondas**
Servicios de la red		
Intranet	**DMZ**	**Internet**
VPN		
Tipo de Sistema Operativo		
Nombre de o los equipos		
Dirección MAC del equipo		
Dirección IP del equipo		

Lista de control de análisis de discos

Lista de control de análisis de discos			
Rutina	**SÍ**	**NO**	**OBSERVACIONES**
Actividades Preliminares			
1. Efectuar imagen del disco o medio de almacenamiento bit a bit			
2. Generar la autenticación matemática de los datos a través del algoritmo de *hash*			
3. Registrar la fecha y hora del sistema			
4. Generar una lista de palabras claves a buscar			
Actividades en la imagen del disco			
5. Trabajar sobre la imagen del disco, efectuar autenticación matemática en cada uno de los datos analizados a través del algoritmo de *hash*.			
6. En el disco analizar:			
a. Tipo de sistema operativo			
b. Versión del sistema operativo			
c. Número de particiones			
d. Tipo de particiones			
e. Esquema de la tabla de particiones			
f. Registrar nombre de archivos, fecha y hora			
i. Correlacionar con 3.			
g. Evaluar el espacio descuidado o desperdiciado.			
i. Incluido el MBR			
ii. Incluida la tabla de particiones			
iii. Incluida la partición de inicio del sistema y los archivos de comandos			
h. Evaluar el espacio no asignado			
i. Evaluar el espacio de intercambio			
j. Recuperar archivos eliminados			
k. Buscar archivos ocultos con las palabras claves en el:			
i. espacio desperdiciado			
ii. espacio no asignado			
iii. espacio de intercambio			
iv. MBR y tabla de particiones			
l. Listar todas las aplicaciones existentes en el sistema			
i. Examinar programas ejecutables sospechosos			

Lista de control de análisis de discos			
Rutina	**SÍ**	**NO**	**OBSERVACIONES**
m. Identificar extensiones de archivos sospechosas			
i. Examinar las extensiones de los archivos y la coherencia con las aplicaciones que los ejecutan o generan			
n. Examinar archivos en busca de datos ocultos (esteganografía) ya sean de tipo gráficos, imágenes, de texto, comprimidos o de cualquier otro tipo de extensión			
o. Examinar los archivos protegidos con claves, descifrando la clave previamente			
p. Examinar el contenido de los archivos de cada usuario en el directorio raíz y si existen, en los subdirectorios			
q. Evaluar el comportamiento del sistema operativo:			
i. Integridad de los comandos			
ii. Integridad de los módulos			
r. Evaluar el funcionamiento de los programas de aplicaciones			
s. Registrar los hallazgos			
i. Capturar pantallas			
t. Generar la autenticación matemática de los datos a través del algoritmo de *hash* al finalizar el análisis			
i. Comparar resultados obtenidos de 2 y 6.p			
u. Conservar copias del *software* utilizado			

BIBLIOGRAFÍA

Libros

Jurídica

Constitución Nacional

Código Civil de la Nación Argentina

Código Penal de la Nación Argentina

Código Procesal Civil

Código Procesal Penal

Ley de firma digital: 25.506

Ley de Protección de Datos Personales: 25.326

Ley de Propiedad Intelectual: 11.723

Ley de delitos informáticos: 26.388

Informática Forense

Armisted, Leigh. Information, Operations.Warfare and the hard reality of soft power. Brassey's Inc. Washington, EE.UU., 2004.

Barrett, Diane – Kipper, Greg. Virtualization and Forensics. Libro electrónico. Elsevier, Ma, EE.UU., 2010.

Bejtlich, Richard. Extrusion Detection. Addison Wesley, 2006.

Broen, Christopher. Computer Evidence Collection & Preservation. Charles River Media.

Massachusetts, EE.UU., 2006.

Cano, Donaliza – Lugo, Danilo. Auditoría Financiera Forense. 3ra. ed., ECOE Ediciones, Bogo- tá DC., 2009.

Carrier, Brian. File System Forensic Analysis. Addison Wesley. EE.UU., 2005.

Carvey, Harlan. Windows Forensics and Incident Recovery. Addison Wesley, EE.UU., 2005.

Denning, Dorothy. Information Warfare and Security. Addison Wesley. Nueva York. EE.UU., 2006.

Eilam, Eldad. Reversing – Secrets of Reverse Engineering. Wiley. EE.UU., 2005.

Farmer, Dan – Venema, Wietse. Forensic Discovery. Addison Wesley Profesional. EE.UU., 2005.

Garrison, Clint. Digital forensics for network, internet and cloud computing. Libro electrónico.

Elsevier, Ma, EE.UU., 2010.

Harris, Shon; Harper, Allen; Eagle, Chris; Ness, Jonathan; Lester, Michael. Gray Hat Hacking, The Ethical Hacker's Handbook. McGraw-Hill/Osborne. California, EE.UU., 2005.

Jones, Robert. Internet Forenscis. O'Reilly. California. EE.UU., 2006.

Kruse II, Warren. Heiser, Jay. Computer Forensic: Incident Response Essentials. 1ra. ed., Addi- son Wesley Professional. EE.UU., 2001.

Mateos, Marino – Sigüenza, Juan. Tecnologías Biométricas aplicadas a la seguridad. Alfaomega RA-MA. México, 2005.

Middleton, Bruce. Cyber Crime Investigator's Field. Auerbach, EE.UU., 2002.

Narthcutf, Stephen; Novak, Judy. Detección de Intrusos. Guía Avanzada. 2da. ed. Prentice Hall.

Madrid, 2001.

Prosise, Chris. Mandia, Kevin and Pepe, Matt. Incident Response & Computer Forensic.

2da. ed., McGraw-Hill Osborne, California, 2003.

Scambray, Joel – Stuart, McClure - Kurtz, George. Hacking Exposed. 2da. ed. Osborne.

EE.UU., 2001.

Schneier, Bruce. Applied Cryptography. 2da. ed., Wiley. EE.UU., 1996.

Schwartau, Winn. Information Warfare. 2da. ed., Tunder´s Mouth Press. New York, EE.UU., 1996.

Schweitzer, Douglas. Incident Response, Computer Forensic Tool. Wiley Publishing. EE.UU., 2003.

Smith, Fred Chris; Gurley Bace, Rebecca. A guide to Forensic Testimony. The art and practice of presenting testimony as an experte technical eitness. Addison Wesley. Boston, EE.UU., 2003.

Solomon, Michael G y otros. Computer Forensics Jump Stara. Sybex. EE.UU., 2005.

Stallings, William, Network and Internetwork Security, Ed. Prentice Hall, New Jersey, EE.UU., 1995.

Vacca, John. Computer Forensic: Computer Crime Scene Investigation. Ed, Charles River Media, Networking Series. EE.UU., 2002.

Whitaker, Andrew; Newman, Daniel. Penetration Testing and Network Defense. Cisco Press.

Indianápolis, EE.UU., 2006.

Sistemas operativos – Protocolos y redes - Seguridad informática

Arena, Héctor. Linux Avanzado. 1ra. ed. Ed. MP Ediciones. Buenos Aires, 2000.

Bryant, Richard. Unix Security for the Organization. 1ra. ed., EE.UU, Ed. SAMS, 1994.

Carretero Pérez y otros. Sistemas Operativos – Una visión aplicada. McGraw Hill,

2001.

Comer, Douglas. E. Redes Globales de información con Internet y TCP/IP. 3ra. ed., Ed Prentice Hall, México, 1996.

Del Peso Navarro, Emilio – Ramos González, Miguel Ángel. Confidencialidad y seguridad de la información. Díaz de Santos, Madrid, 1994.

Medina, Manel. Seguridad Informática en Nuevas Instalaciones. ECI 2000. Dpto. Computa- ción Facultad de Ciencias Exactas, Apunte. Buenos Aires, 2000.

Melgabab, George. "Introducción a Unix". 1ra. ed., Prentice Hall. México. 1998.

Morant Ramon, J. L. Seguridad y Protección de la Información. Ed. Centro de Estudios Ramon Areces, Madrid, 1994.

Moritsugu Esteves. Serie Práctica Unix. Prentice Hall, España, 2000.

Peláez, Raúl. Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados.

1ra. ed., Licencia GNU. Junio 2002.

Rusinovich, Mark. E – Solomon, David. Microsoft Windows Internals. 4ta. ed. Microsoft.

Washington. 2005.

Schmidt, Jeff. Seguridad en Microsoft Windows 2000. Prentice Hall. Madrid, 2000.

Stallings, W. Comunicaciones y redes de computadoras. 7ma. ed., Pearson Educación, 2004.

Stallings, William. Network and Internetwork Security, New Jersey, Prentice Hall, 1995.

Stevens, W. Richard. TCP/IP Illustrated, Vol. 1. Ed. Addison-Wesley, EE.UU., 1994.

Streib, M. Drew – Turner, Michael. Serie Práctica LINUX. 1ra. ed., España. Ed. Prentice Hall, 2000.

Syan, K. – Hare, C. Firewall y la Seguridad en Internet. 2da. ed., México. Ed

Prentice Hall Hispanoamericana, 1997.

Syan, K. – Hare, C. Internet y Seguridad en redes. 1ra. ed., México. Ed Prentice Hall Hispano- americana, 1995.

Tanenbaum, A. Redes de computadoras. 4ta. ed., Pearson Educación, 2003.

Tare, S. R. Procesamiento de datos en Unix. 1ra. ed., España, Ed. McGraw-Hill, 1990.

Vacca, John. Los secretos de la seguridad en Internet. Anaya. Madrid, 1997.

Wayar, L. Linux Manual de referencia. 1ra. ed., Buenos Aires. Ed. PCForum, 1999.

Wyatt Allen, L. Windows NT. Manual de referencia. 1ra. ed., España. Ed. McGraw-Hill, 1994.

Investigación

Alchourrón, Carlos, Bulygin Eugenio. Introducción a la metodología de las ciencias jurídicas y sociales. Editorial Astrea. Buenos Aires, 2006.

American Psychological Association. Manual de estilo de publicaciones. Editorial Manual Moderno. Colombia, 1998.

Campbell, Stephen. Equívocos y falacias en la interpretación de estadísticas. Universidad de Denver. Noriega Editores. México, 1994.

Copi, Irving. Introduccion a la lógica. Eudeba. Buenos Aires, 1994.

Echave, Delia Teresa, Urquijo María Eugenia, Guibourg Ricardo. Lógica Proposición y Nor- ma. Editorial Astrea. Buenos Aires. 2008.

Ghersi, Carlos Alberto. Metodología de la investigación en ciencias jurídicas. Ediciones Gowa. Buenos Aires, 2007.

Guarinoni, Ricardo. Derecho, lenguaje y lógica. Editorial Lexis Nexis. Buenos Aires, 2006.

Guibourg, Ricardo. La construcción del pensamiento, Decisiones metodológicas. Ediciones Colihue. Buenos Aires, 2006.

Guibourg, Ricardo. Pensar en las normas. Eudeba. Buenos Aires, 1999.

Herrera, Enrique. Práctica metodológica de la investigación jurídica. Editorial Astrea. Bue- nos Aires, 2006.

Klimovsky, Gregorio. Las desventuras del conocimiento científico. Una introducción a la epis- temología. A-Z Editora. Buenos Aires, 2005.

Kunz, Ana, Carcinaux Nancy. Investigar en derecho. Departamento de publicaciones de la Facultad de Derecho. Universidad de Buenos Aires, 2004.

Muñoz Razo, Carlos. Cómo elaborar y asesorar una investigación de Tesis. Editorial Prentice Hall. México, 1998.

Nudler, Telma, Nudler Oscar. Elementos de lógica simbólica. Editorial Kapelusz, 1973.

Salkind, Neil. Métodos de investigación. 3ra. ed., Editorial Prentice Hall. México, 1997.

Scarano, Eduardo. Manual de redacción de escritos de investigación. Ediciones Macchi.

Buenos Aires, 2004.

Sampieri, Roberto – Collado, Carlos – Baptista Lucio, María. Metodología de la investigación.

5ta ed., McGraw-Hill, México, 2010.

Sokal, Alan. Más allá de las imposturas intelectuales. Editorial Paidós. Barcelona, España, 2010.

Wayne, Daniel. Estadística con aplicaciones a las ciencias sociales y a la educación. Editorial McGraw-Hill. México, 1988.

RFC – Request for Comment

1. Brezinski, D. Killalea, T. Request for Comments: 3227 - Category: Best Current Practice. Gui- delines for Evidence Collection and Archiving, February 2002.

Normas

1. Normas ISO IEC 17799, 27001, 27002.

Internet

Fraudes, delitos informáticos y crimen en el ciberespacio

NSRL, biblioteca de referencia nacional de software, http://www.nsrl.nist.gov/

http://delitosinformaticos.com/estafas/, el sitio está en castellano y tiene un listado muy completo de casos y recomendaciones

http://www.fraud.org/news.htm, sólo se encuentra en inglés con noticias también de frau- des informáticos

http://www.fbi.gov/majcases/fraud/fraudschemes.htm, sitio en inglés del FBI

http://www.fbi.gov/majcases/fraud/internetschemes.htm

http://www.cybercrime.gov/cccases.html

http://www.fraud.org/internet/2001stats10mnt.htm

http://www.terrorism.com/iwdb/incidents.asp

http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html

Seguridad informática

Ad-Aware, www.lavasoftusa.com

ATTRITION, www.attrition.org

bastille-linux.sourceforge.net

Firma Digital, http://www.pki.gov.ar

Hispasec, www.hispasec.com

Información en varios idiomas sobre virus. spam, ataques http://www.viruslist.com/sp/news

KRIPTÓPOLIS, www.kriptopolis.com

NSA, www.nsa.gov

packet storm, packetstorm.securify.com

SecurityFocus, www.securityfocus.com

Securityportal, www.securityportal.com

SecurityTeam, www.securityteam.com

Spybot-SD, www.spybot.info

www.hp.com/security/products/linux

www.sans.org

Sitios de CERT - CERTs (Computer Emergency Response Team o Equipo de Respuesta a Emer- gencias de Cómputo) o IRT (Incident Response Team) o Equipo de Respuesta a Incidentes

España: http://escert.upc.es/

IRIS-CERT (Ámbito Académico), http://www.rediris.es/cert/

México, http://www.mxcert.org.mx/

Área de Seguridad en Cómputo UNAM http://www.asc.unam.mx

EE.UU., CERT/CC: (Centro coordinación CERTs), http://www.cert.org/

FIRST – Forum of Incident and Response Teams, http://www.first.org/

CERTs Europeos: http://www.cert.dfn.de/eng/csir/europe/certs.html

RFC y estándares

IETF (Internet Engineering Task Force) www.ietf.org/rfc.html

RFC traducidos al castellano, www.rfc-es.org

NIST, http://csrc.nist.gov/

IEEE, standards.ieee.org

ISO (Europa)

NIST, National Institute of Standards and Technology (EE.UU.,), www.nist.gov

Grados de protección IPANSI/IEC 60529-2004, www.nema.org/stds/

Auditoría

Informar vulnerabilidades - ICA – ica.nist.gov

COBIT (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas), https://www.isaca.org/Pages/default.aspx

Cooperative Association for Internet Data Analysis (CAIDA), http://www.caida.org/home/

TCSEC – Trusted Computer Systems Evaluation Criteria – Department of Defense - Orange Book. http://www.iwar.org.uk/comsec/resources/standards/rainbow/5200.28-

STD.html

ITSEC - Information Technology Security Evaluation Criteria (Europa), www.cesg.gov.uk

CTCPEC - Canadian Trusted Computer Product Evaluation Criteria, http://csrc.nist.gov/ publications/nistbul/itl98-11.txt

Códigos de ética

(ISC)2 www.isc2.org/cgi/content.cgi?category=12

The Internet Activities Board (IAB), Ethics and Internet (RFC 1087) - www.faqs.org/rfcs/ rfc1087.html

Jurídica

Consejo de la Magistratura. http://cmcaba.jusbaires.gov.ar/

Convenios Colectivos de Trabajo. Se pueden consultar en línea o bajar el texto completo: http://www.trabajo.gov.ar/left/biblioteca/index.html. Http://www.trabajo.gov.ar/legisla- cion/convenioscolectivos/index.html

Corte Suprema de Justicia de la Nación. http://www.csjn.gov.ar/

Derecho administrativo. http://www.planetaius.com.ar/foroderecho/sitemap/f-18.html

Derecho Comercial. Revista Electrónica de Derecho Comercial. http://www.derecho-co- mercial.com/

Derecho informático. http://www.ciberderecho.com.ar http://ar.groups.yahoo.com/ group/ciberderecho/

Diario Judicial. http://www.diariojudicial.com/

Justicia de transición en Argentina. Universidad de Minessota. Jurisprudencia. http:// www1.umn.edu/humanrts/research/argentina/justicia.html

Leyes CABA. http://www.cedom.gov.ar/

Leyes Nación. http://infoleg.mecon.gov.ar/

Leyes Provincia de Buenos Aires. http://www.gob.gba.gov.ar/dijl/buscador.php?id=01

Fallos. http://www.lanuevoderecho.com.ar/Recursos/Fallosoa.htm, http://www.iurede- recho.com/ Derecho de familia: http://www.estudio-petersen.com.ar/Fallos/Fallos.htm Derecho informático: http://www.dpi.bioetica.org/jurisdpi/herrera1.htm Jurisprudencia nacional: http://www.legislaw.com.ar/juris/tnacio.htm

Protección de Datos Personales. Http://www.protecciondedatos.com.ar/

Para descargar leyes on-line. http://infoleg.mecon.gov.ar/

Poder Judicial de la Nación. http://www.pjn.gov.ar/

Positivismo criminológico. http://www.ub.es/penal/historia/positivismo.html

Revista de Derecho Penal en línea. http://www.derechopenalonline.com/

Revista de Derecho y Nuevas Tecnologías. http://www.palazzi.com.ar/

Revista Electrónica de Derecho Comercial. http://www.derecho-comercial.com/

Revista Electrónica de Derecho informático. http://vlex.com/source/redi-29

Revista Latinoamericana de propiedad intelectual. http://rlapi.com.ar/

Suprema Corte de la Provincia de Buenos Aires: http://www.scba.gov.ar/portada/

Colegio de abogados

Colegio de Abogados de la Ciudad de Buenos Aires. http://www.colabogados.org.ar/

Colegio Público de Abogados de la Capital Federal. http://www.cpacf.org.ar/

Colegios de abogados. http://www.portaldeabogados.com.ar/colegios/index.htm

Criminalística

Ciencias Criminalísticas. Foro de Discusión, abarca todas las especialidades criminalísticas. http://www.criminalistica.net/forense/index.php

http://www.darahuge-arellano.com.ar

http://consultoracriminalisticapericial.blogspot.com/

Grupos de discusión

Grupos de discusión sobre Criminalística. http://www.forenseschile.tk http://es.groups. yahoo.com/group/criminalistica/

Grupo de discusión sobre Informática Forense. http://br.groups.yahoo.com/group/Peri- ciaforense/

De interés general

Biblioteca Digital Mundial: Página WEB de la Unesco. http://www.wdl.org/es/

Diccionario de la Real Academia Española. http://www.rae.es/

Libros Nuevos. http://www.amazon.com/gp/homepage.html/

Libros Nuevos y Usados. http://www.alibris.com/

Manuales en línea. http://www.solomanuales.org/

Material didáctico. http://www.slideshare.net/

Índice

ACTUALIZACIÓN ON-LINE 7
LOS AUTORES 9
PRÓLOGO 10
PREFACIO 12
Orientación para la lectura del manual 18
CAPÍTULO 2 LA PROBLEMÁTICA DE LA INFORMÁTICA FORENSE 19
El surgimiento de la Informática Forense, su inserción social, judicial y tecnológica 22
Concepto de Informática Forense 24
CAPÍTULO 3 IMPLANTACIÓN PERICIAL CRIMINALÍSTICA 26
Características destacables en la disciplina: 27
Clasificación por su relación con el lugar del hecho: 28
Causas de alteración del lugar del hecho: 29
CAPÍTULO 4 IMPLANTACIÓN INFORMÁTICA 36
CAPÍTULO 5 IMPLANTACIÓN JUDICIAL 42
El delito informático propio e impropio 43
La reconstrucción metodológica del hecho 45
El lugar del hecho virtual propio e impropio 47
Elemento probatorio pertinente y conducente 54
Prueba pericial informático forense 54
Relaciones con otras disciplinas 55
CAPÍTULO 6 INFORMÁTICA FORENSE LA PRUEBA DOCUMENTAL INFORMÁTICA 62
Principios y relaciones periciales informático forenses 62
La prueba documental informática 63
Definición y relaciones 64
Inteligencia estratégica 64
La entrevista 65
CAPÍTULO 7 INSERCIÓN LEGAL DEL PERITO EN INFORMÁTICA FORENSE LA INSPECCIÓN JUDICIAL 76

Generalidades 76
Legalidad de la requisitoria pericial 79
Formalidades de la aceptación del cargo 80
Diligencias previas en el Juzgado 81
Requisitos legales y formales de la inspección judicial 82
Legislación de fondo, el perito como testigo y el falso testimonio 88
Legislación de forma 91
Legislación complementaria, leyes y proyectos 91
Jurisprudencia 92
CAPÍTULO 8 ACTIVIDADES PERICIALES COMPLEMENTARIAS 95
La aceptación del cargo 95
El informe pericial informático forense impreso y virtual 98
El párrafo de presentación 99
El objeto de la pericia y los puntos de pericia (tarea transdisciplinaria) 100
Los elementos ofrecidos (equipos, programas, indicios y rastros) 104
Las operaciones realizadas 106
Las conclusiones 107
CAPÍTULO 9 LA IMPUGNACIÓN 113
Revisión legal 113
La relación del perito con las partes y con los abogados de las mismas 114
Control, revisión y exigencia de legalidad en las herramientas utilizadas 118
Revisión científica, tecnológica y técnica 119
Revisión lógica 121
Revisión formal 122
CAPÍTULO 10 VALOR PROBATORIO DE LA PRUEBA INDICIARIA INFORMÁTICO FORENSE 128
Prueba documental informática (recaudos procesales) 128
Inserción de la prueba documental informática 129
El acceso y resguardo de la documental informática 134
La certificación de la documental informática 135
Recolección estratégica de la documental informática 137
Prueba pericial 138
En el delito informático propio e impropio 138
CAPÍTULO 11 UN EJEMPLO DE DELITO INFORMÁTICO 143

PROPIO (EL PHISHING) 143
Herramienta de análisis del lugar del hecho real 150
Herramienta de análisis del lugar del hecho virtual 151
CAPÍTULO 12 GUÍA PARA EJECUTAR LA RECOLECCIÓN DE LA DOCUMENTAL INFORMÁTICA 154
CAPÍTULO 13 MARCO TECNOLÓGICO PERICIAL (LA PERICIA INFORMÁTICO FORENSE EN LA PRÁCTICA) 158
Listas de Control del Equipo del perito informático forense 159
Herramientas de hardware y software del perito informático forense 164
Elementos de hardware del laboratorio del perito informático forense 164
Equipo fijo de Laboratorio Estación de trabajo 165
Herramientas de software para Informática Forense 171
Herramientas de funciones específicas: 183
Borrado seguro, limpieza y desinfección: 184
Duplicación de discos 185
Características: 186
Duplicación en forma remota 186
Manejo de Particiones 187
Recuperación de archivos eliminados 187
En Windows 188
Recuperación de archivos con claves 189
En Linux / Unix 190
Clasificación e identificación de las pericias informático forenses 191
Nomenclatura 192
Ejemplos 193
Etapas del Marco Tecnológico Pericial 193
Tarea a realizar en el Laboratorio 194
Procedimiento para la limpieza y desinfección de los dispositivos de escritura 195
– Etapa: Acceso a los recursos dubitados 198
– Etapa: Identificación y registro 198
– Etapa: Autenticación, duplicación y resguardo de la prueba 199
– Etapa: Detección, recolección y registro de indicios probatorios 205
Alternativa I, para el acceso con el equipo encendido 205
En sistemas operativos Microsoft Windows 216

Envío de la evidencia a través de una conexión remota 216
Ejecución de un intérprete de comandos legítimo 217
Registro de la fecha y hora 217
Descarga de la memoria RAM 218
Verificación de los usuarios conectados al sistema y de los usuarios con acceso remoto 218
Verificación de las fechas y hora de acceso, creación o modificación de todos los archivos 220
Verificación de los puertos abiertos 182
Verificación de los procesos activos 224
Verificación de las conexiones actuales y recientes 226
Revisión de los registros de eventos o sucesos del sistema operativo 182
Verificación de la base de datos del Registro del sistema operativo 229
En el modelo de seguridad de Windows se encuentran: 182
Examinar los archivos de configuración del sistema operativo 233
Verificación y obtención de las claves de los usuarios del sistema 233
Verificación de archivos relevantes 234
Herramientas 234
Descarga de los archivos temporales 234
Verificación de los enlaces a archivos rotos 235
Verificación de los archivos de navegación por Internet 235
Los archivos fat.db, netscape.hst e index.dat son binarios y requieren un visor específico: 237
Verificación y descarga de los archivos de correo electrónico 237
Cliente de correo Outlook Express 237
Cliente de correo Microsoft Outlook 238
Cliente de correo Netscape Messenger 239
Generación de un script o secuencia de comandos 239
Respuesta a incidentes 240
Alternativa II, con el equipo apagado 242
Procedimiento 243
Análisis e interpretación de los indicios probatorios. Reconstrucción y / o simulación del incidente 246
Procedimiento para el análisis e interpretación de los indicios probatorios Procedimiento 246
Elementos a examinar en el disco duro: (Anexo Lista de control de Análisis

Discos rígidos de computadoras portátiles 252
Aspectos a considerar de los sistemas de archivos de los sistemas operativos 252
Estructura del inodo 255
Niveles de almacenamiento en el sistema de archivos 259
Análisis de particiones de los discos duros 265
Herramientas 266
En Windows XP 182
Visualización de diferentes tipos de archivos 274
Búsqueda de texto y palabras claves 275
Análisis del espacio no utilizado o no asignado 276
Eliminación o borrado de información en el disco rígido 278
Eliminación segura de los datos 282
Análisis de datos ocultos 285
Tipo: Enmascaramiento 290
Archivos protegidos con claves 294
Tipo: ocultamiento de información 294
Herramientas 295
Espacio no asignado, desperdiciado y libre 296
Tipo: Alteración del entorno 301
Herramientas 301
Código malicioso o Malware 302
Métodos de invasión o ataque 302
Modos de control de la invasión o ataque 302
Modo de distribución o impregnación 302
Objetivos del código hostil 304
Análisis del correo electrónico 308
Aspectos importantes a considerar en el análisis del encabezado del mensaje 317
Visualización de encabezados en diferentes clientes de correo electrónico 319
Verificación de los archivos de impresión 320
Análisis de código malicioso 320
VI Cotejo, correlación de datos y conclusiones 328
APÉNDICE 1 ESTUDIO DE UN CASO REPRESENTATIVO 335
APÉNDICE 2 PROCEDIMIENTO ANTE LA REQUISITORIA PERICIAL 344
APÉNDICE 3 EL MÉTODO SISTÉMICO (RESUMEN) 351

PERICIAL
APÉNDICE 3 EL MÉTODO SISTÉMICO (RESUMEN) 351
Visión sistémica de la investigación 352
Entrevista previa o licitación 354
Relevamiento de la información 357
Selección de la metodología de análisis 358
Generación del modelo conceptual 359
Generación de los modelos complementarios 359
Programación y codificación 360
Prueba y ejecución en paralelo 361
Capacitación, supervisión y soporte de la aplicación 362
Retroalimentación 363
Síntesis 364
APÉNDICE 4 INFORMACIÓN COMPLEMENTARIA 367
Requisitoria pericial 367
Título VII - Participación criminal 370
Dibujo pericial complementario 374
Fotografías durante la inspección judicial 384
APÉNDICE 5 MANUAL DE AUTOPSY 385
Introducción 385
Emulador Cygwin 386
Instalación de Cygwin: 386
Ejecución de Cygwin y acceso al intérprete de comandos (shell): 391
Instalación de Sleuth Kit: 391
Instalación de Autopsy: 393
Descripción general de Autopsy 394
Ejecución de Autopsy en Cygwin 396
Creación de un caso en Autopsy 397
Análisis de archivos File Analysis. 385
Keyword Search – Búsqueda de palabras claves: 385
Opción File Type – Tipo de Archivo: 409
Image Details Detalles de la imagen: 411
Metadata Analysis – Análisis de Metadatos o Descriptores de archivos: 412
Aclaraciones acerca de NTFS y FAT: 413
Data Unit Analisis – Análisis de la Unidad de Datos: 414

Aclaraciones sobre el sistema de archive FAT 416
Timeline Mode – Modo Línea de Tiempo: 416
Verificación de Integridad – Integrity Check: 420
Event Sequencer Secuencia de sucesos 385
Visualización de la secuencia de eventos o sucesos: 421
Configuración en Autopsy 424
Referencias 424
Anexo I Herramientas de Sleuth Kit 425
Anexo II Comando: sorter 426
APÉNDICE 6 RELACIONES CON LA PRUEBA INDICIARIA NO INFORMÁTICA 427
Expertos en Balística 427
Huellas plantares (Retrato del paso) y de vehículos 430
Huellas dactilares 430
Manchas de sangre 431
Manchas varias (material fecal, meconio, calostro, semen, orina), pelos, fibras naturales o artificiales 432
Documentos 432
Suposiciones a priori 432
APÉNDICE 7 LA ESTRUCTURA LÓGICA DEMOSTRATIVA EN LA LABOR PERICIAL 433
Demostración lógica y tecnológica de las conclusiones alcanzadas 433
APÉNDICE 8 LA REDACCIÓN FINAL 439
Generación del informe pericial 441
Preparación de la defensa escrita/oral 441
Reglas para las citas 445
La posredacción 446
Respecto de la presentación 446
Respecto de la forma de presentación 446
Entrega formal del informe pericial 448
APÉNDICE 9 LA DEFENSA ORAL 452
La defensa ante el tribunal 452
Reglas de argumentación generales 460
Reglas para evaluar argumentaciones de los interlocutores 462
Reglas para construir nuestras propias argumentaciones 463

Las respuestas estrictas 468
Consideraciones prácticas para la argumentación oral 468
APÉNDICE 10 GLOSARIO COMPLEMENTARIO BÁSICO 470
APÉNDICE 11 RESUMEN DE LÓGICA PROPOSICIONAL 476
APÉNDICE 12 LA INSPECCIÓN JUDICIAL 480
Generalidades 480
Situaciones posibles en la inspección judicial 483
Metodología de trabajo 486
Acta de inspección o secuestro 491
APÉNDICE 13 MISCELÁNEAS 494
AWARD 494
AMI 494
PHOENIX 495
Otras 495
Varios fabricantes 495
TOSHIBA 496
IBM APTIVA BIOS 497
Listado de Puertos utilizados por Troyanos 497
APÉNDICE 14 LA YAPA 521
ANEXO 1 DIAGRAMAS CONCEPTUALES 535
Marco científico investigativo 535
Esquema de investigación 535
ANEXO 2 MODELO DE INFORME PERICIAL 541
ANEXO 3 MODELOS DE NOTAS 547
ANEXO 4 FORMULARIOS 553
Lista de control de hardware en la inspección y reconocimiento judicial 553
Formulario de registro de evidencia 553
Rótulos para las evidencias 554
Formulario – Recibo de efectos 555
Formulario para la Cadena de Custodia 556
Lista de control de análisis de discos 558
BIBLIOGRAFÍA 560
Libros 560
Jurídica 560

BIBLIOGRAFÍA 560
Libros 560
Jurídica 560
Informática Forense 560
Sistemas operativos – Protocolos y redes - Seguridad informática 562
Investigación 564
RFC – Request for Comment 565
Normas 566
Internet 566
Fraudes, delitos informáticos y crimen en el ciberespacio 566
Seguridad informática 566
RFC y estándares 568
Auditoría 568
Códigos de ética 569
Jurídica 569
Colegio de abogados 570
Criminalística 571
Grupos de discusión 571
De interés general 571