

Informática Forense

Hernán Herrera - Sebastián Gómez



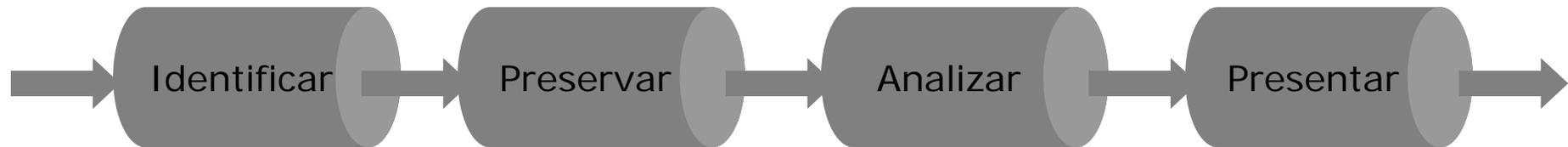
Jornadas de Seguridad Informática
Noviembre 2009

Contenidos

- **Definición de informática forense**
- **Organización interna del Laboratorio**
- **Software forense**
- **Hardware forense**
- **El paradigma de la virtualización aplicado a la informática forense**

Definición de informática forense

“Es el proceso de identificar, preservar, analizar y presentar evidencia digital, de manera que esta sea legalmente aceptable”



Identificación de la evidencia digital

En una investigación que involucra información en formato digital, se debe:

- ✓ Identificar las fuentes potenciales de evidencia digital
- ✓ Determinar qué elementos se pueden secuestrar y cuáles no
- ✓ Si se trata de un escenario complejo:
 - Tomar fotografías del entorno investigado
 - Documentar las diferentes configuraciones de los equipos, topologías de red y conexiones a Internet

Preservación de la evidencia digital

Al trabajar con evidencia digital deben extremarse los recaudos a fin de evitar la contaminación de la prueba, considerando su fragilidad y volatilidad

- ✓ **Mantenimiento de la Cadena de Custodia**
 - Registro de todas las operaciones que se realizan sobre la evidencia digital
 - Resguardo de los elementos secuestrados utilizando etiquetas de seguridad
- ✓ **Preservación de los elementos secuestrados de las altas temperaturas, campos magnéticos y golpes**
 - Los elementos de prueba originales deben ser conservados hasta la finalización del proceso judicial
- ✓ **Obtención de imágenes forenses de los elementos secuestrados**
 - Por cuestiones de tiempo y otros aspectos técnicos, esta tarea se realiza una vez que ha sido secuestrado el elemento probatorio original
 - En caso de que la creación de una imagen forense no sea posible, el acceso a los dispositivos originales se realiza mediante mecanismos de protección contra escritura
- ✓ **Autenticación de la evidencia original**
 - Generación de valores hash –MD5 o SHA-1- a partir de los datos contenidos en los diferentes dispositivos secuestrados

Análisis de la evidencia digital

Involucra aquellas tareas orientadas a localizar y extraer evidencia digital relevante para la investigación

Mediante la aplicación de diversas técnicas y herramientas forenses se intenta dar respuesta a los puntos de pericia solicitados

- ✓ **El análisis de datos requiere un trabajo interdisciplinario entre el perito y el operador judicial –juez, fiscal- que lleve la causa**

- ✓ **Tareas que se llevan a cabo dependiendo del tipo de investigación**
 - **Búsqueda de palabras claves o documentos en todo el espacio de almacenamiento del dispositivo investigado**
 - **Determinar si ciertas aplicaciones fueron utilizadas por un determinado usuario**
 - **Determinar qué tipo de actividad tenía el usuario en la Web, análisis del historial de navegación, análisis de correo electrónico, etc**

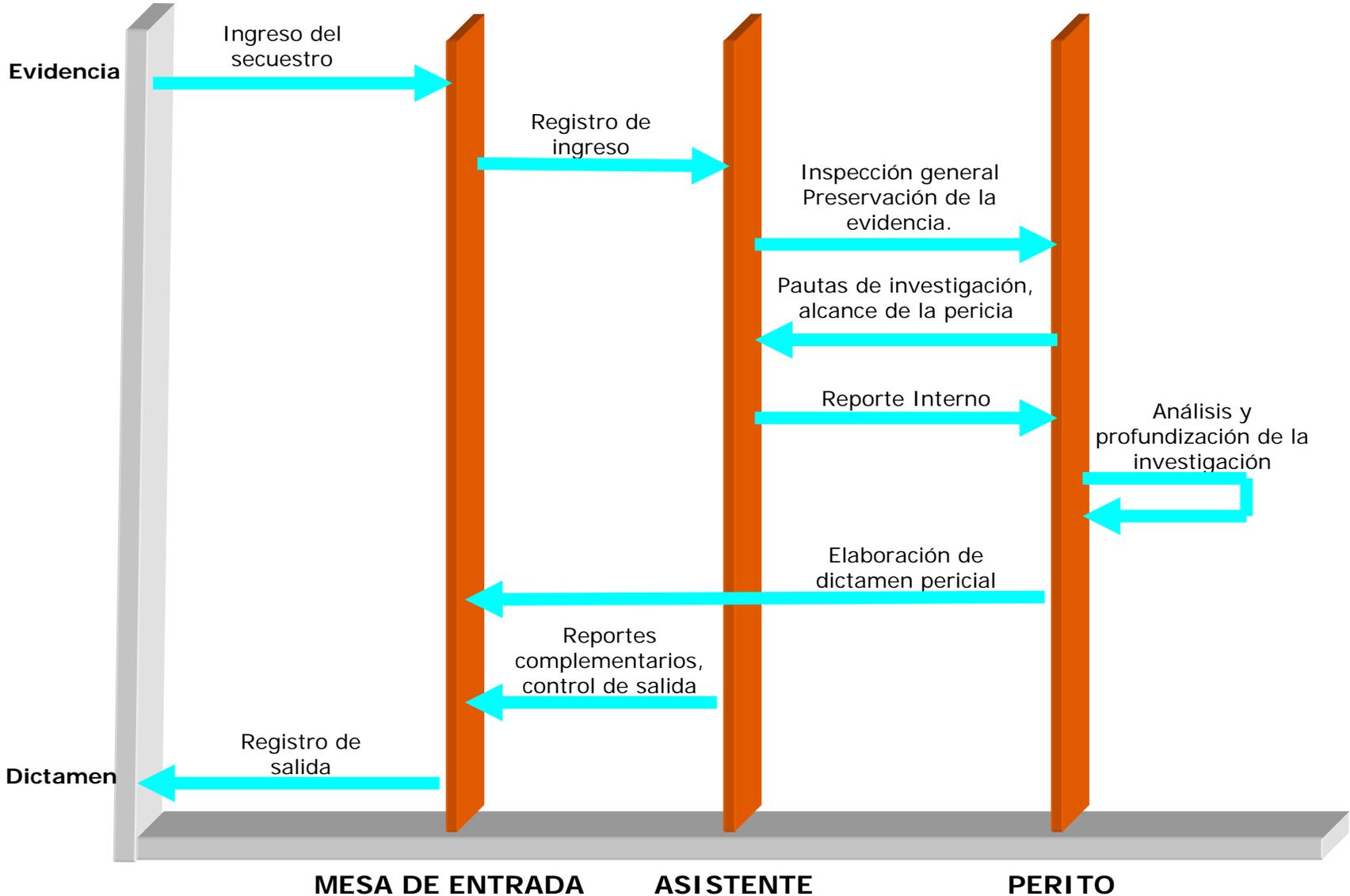
Presentación de la evidencia digital

Consiste en la elaboración del dictamen pericial con los resultados obtenidos en las etapas anteriores

- ✓ **La eficacia probatoria de los dictámenes informáticos radica fundamentalmente en la continuidad en el aseguramiento de la prueba desde el momento de su secuestro**
- ✓ **El dictamen debe ser objetivo y preciso, conteniendo suficientes elementos para repetir el proceso en caso de ser necesario (por ejemplo en un juicio oral)**

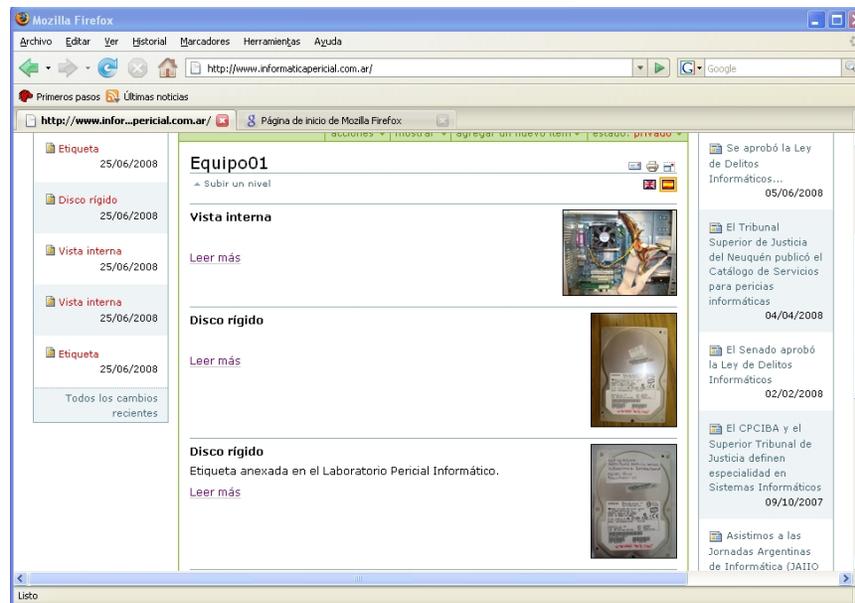
Organización interna del Laboratorio

Workflow del Laboratorio Pericial Informático

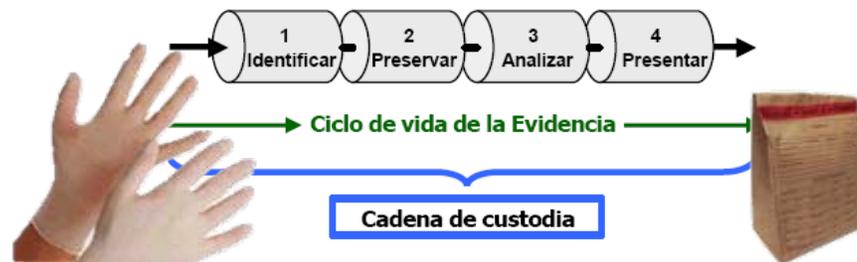


Ingreso del secuestro

- Registro de fotografías digitales en el CMS



- Verificación de la cadena de custodia



Preservación



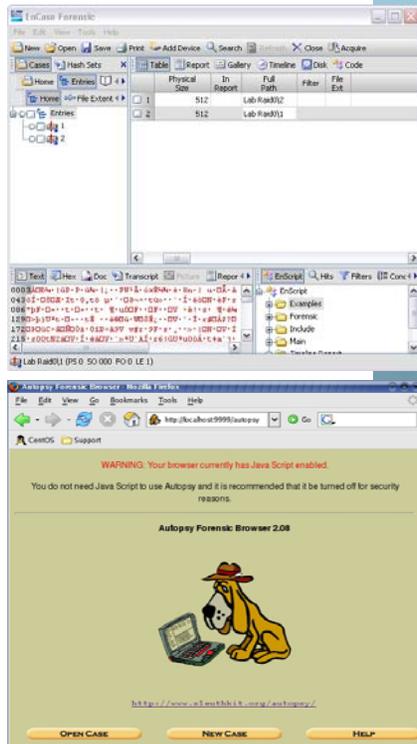
Equipos Informáticos



Telefonía Celular



Análisis



Utilización de software forense



Puesto de trabajo forense

Laboratorio Pericial Informático

Reporte Interno

Figura 1 de 10

Revisión: 2010/02
 Autor: GONZALO MELÉN FELIZ, SANTIAGO GARCÍA SOTIL, ESTEFAN DE GRADO DE TRIVITTOLI

Objetivo del Informe

Características de la evidencia:

Sección	Características	Formato	Resolución	Color	Tamaño	Tipos	CCITT	CCITT	CCITT
1
2
3
4
5

Tercer Sección

1. Registro de la evidencia base/Análisis y registro
2. Análisis de evidencia base
3. Descripción de evidencia base/Análisis y registro de evidencia base

Confección de reporte interno



Registro de casuística en el CMS

Presentación y envío



Uso de
etiquetas de
seguridad



Evidencia Procesada



Registro
fotográfico



Dictamen

Software forense

Generación de una imagen forense para practicar la pericia informática

The screenshot shows the EnCase Forensic interface with an 'Options' dialog box open. The dialog is used to configure the creation of a forensic image. Key elements include:

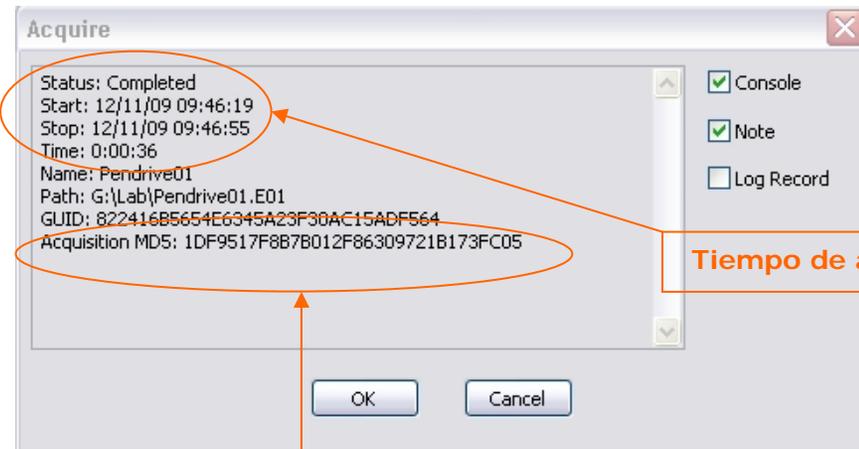
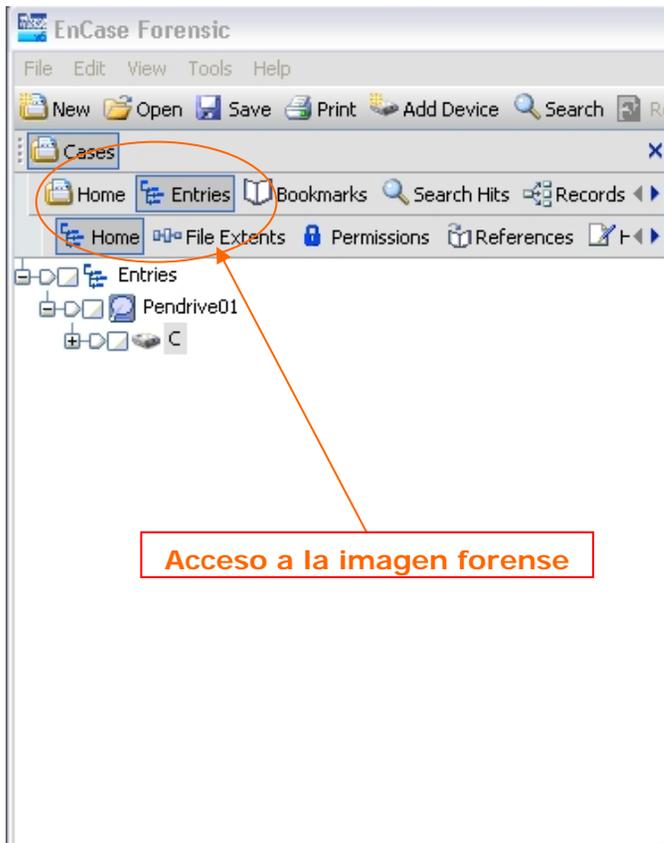
- Name:** Pendrive01
- Evidence Number:** 01
- Notes:** Dispositivo: Pendrive 01
- File Segment Size (MB):** 640
- Start Sector:** 0
- Stop Sector:** 499198
- Block size (Sectors):** 64
- Error granularity (Sectors):** 64
- Compression:** Good (Slower, Smaller) (selected)
- Acquisition MDS:** Checked
- Acquisition SHA1:** Unchecked
- Output Path:** G:\Lab\Pendrive01.E01

Three callout boxes provide additional context:

- Archivo que contendrá la evidencia:** Points to the Output Path field.
- Tipo de valor hash que se utilizará para autenticar la evidencia:** Points to the Acquisition MDS checkbox.
- Tipo de compresión utilizada:** Points to the 'Good (Slower, Smaller)' radio button.

Software forense

Generación de una imagen forense para practicar la pericia informática



Acceso a la imagen forense

Tiempo de adquisición

Valor hash del dispositivo

Software forense

Búsqueda de palabras claves

Paso 1: Definir la palabra clave

New Keyword

Search expression Code Page Keyword tester

Search expression
ubuntu

Name
ubuntu

Search Options

- ANSI Latin - 1
- UTF8
- UTF7
- Unicode
- Unicode Big-endian
- GREP
- Case Sensitive
- Whole Word

GREP Symbols

- \wFFFF Unicode character
- \xFF Hex character
- . Any character
- # Any number [0-9]
- ? Repeat zero or one time
- + Repeat at least once
- [A-Z] A through Z
- * Repeat zero+ times
- [XYZ] Either X, Y, or Z
- [^XYZ] Neither X nor Y nor Z
- \[Literal character
- (ab) Group ab together for ?, +, *, |
- {m,n} Repeat m to n times
- a|b Either a or b

Unicode View

[0055 0075][0042 0062][0055 0075][004E 006E][0054 0074][0055 0075]

Aceptar Cancelar

Paso 2: Determinar las opciones de búsqueda

Search

Selected items only 1297 Entries, 1 Record

Keyword Search Options

- Search entries and records for keywords
- Selected keywords only 1 keywords
- Search entry slack
- Use initialized size
- Undelete entries before searching
- Search only slack area of entries in Hash Library

Hash Options

- Compute hash value
- Recompute hash values

Email Search Options

- Search for email
- Recovered deleted
- Outlook (PST)
- Outlook Express (DBX)
- Exchange (EDB)
- Lotus (NSF)
- AOL
- MBOX

Additional Options

- Verify file signatures
- Identify codepages
- Search for internet history
- Comprehensive search

Start Cancel

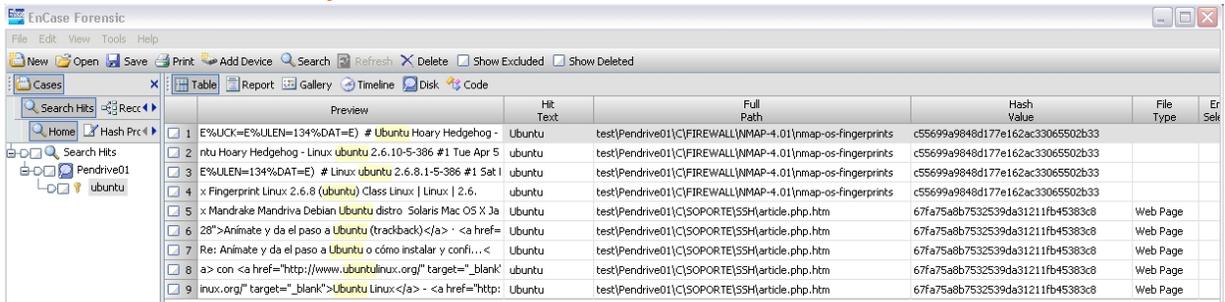
Análisis Hash Set
(National Software Reference Library)

Análisis de firmas

Software forense

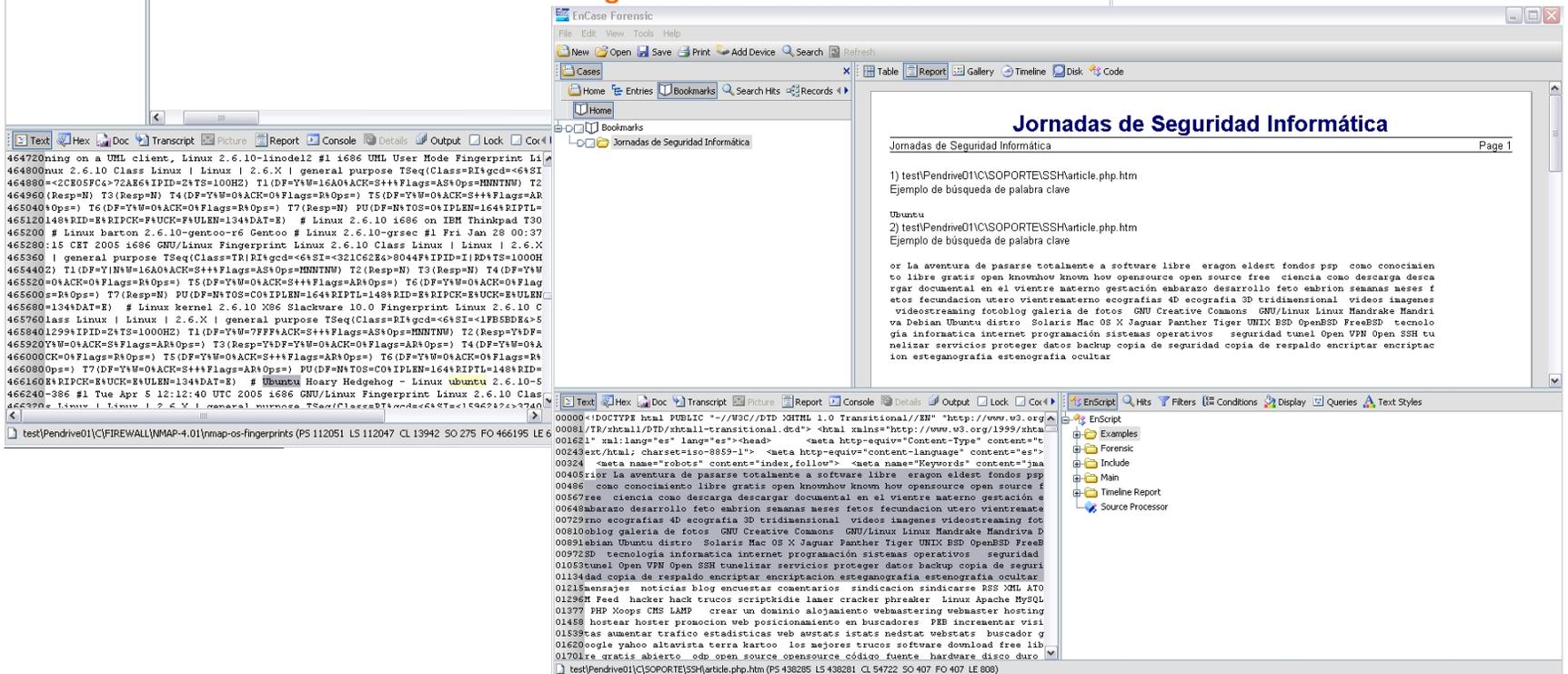
Registro de la evidencia digital relevante para la investigación

Resultado de la búsqueda



Preview	HR Text	Full Path	Hash Value	File Type	Er Sel
1 E%UCK=E%ULEN=134%DAT=E) # Ubuntu Hoary Hedgehog -	Ubuntu	test\Pendrive01\C\FIREWALL\NMAP-4.01\nmap-os-fingerprints	c55699a9848d177e162ac33065502b33		
2 ntu Hoary Hedgehog - Linux ubuntu 2.6.10-5-386 #1 Tue Apr 5	ubuntu	test\Pendrive01\C\FIREWALL\NMAP-4.01\nmap-os-fingerprints	c55699a9848d177e162ac33065502b33		
3 E%ULEN=134%DAT=E) # Linux ubuntu 2.6.8.1-5-386 #1 Sat 1	ubuntu	test\Pendrive01\C\FIREWALL\NMAP-4.01\nmap-os-fingerprints	c55699a9848d177e162ac33065502b33		
4 x Fingerprint Linux 2.6.8 (ubuntu) Class Linux Linux 2.6.	ubuntu	test\Pendrive01\C\FIREWALL\NMAP-4.01\nmap-os-fingerprints	c55699a9848d177e162ac33065502b33		
5 x Mandrake Mandriva Debian Ubuntu distro Solaris Mac OS X Ja	Ubuntu	test\Pendrive01\C\SOPORTE\SSH\article.php.htm	67fa75a8b7532539da31211fb45383c8	Web Page	
6 28">Animáte y da el paso a Ubuntu (trackback · <a href=	Ubuntu	test\Pendrive01\C\SOPORTE\SSH\article.php.htm	67fa75a8b7532539da31211fb45383c8	Web Page	
7 Re: Animáte y da el paso a Ubuntu o cómo instalar y confi.<	Ubuntu	test\Pendrive01\C\SOPORTE\SSH\article.php.htm	67fa75a8b7532539da31211fb45383c8	Web Page	
8 a> con <a href="http://www.ubuntulinux.org/" target="_blank	ubuntu	test\Pendrive01\C\SOPORTE\SSH\article.php.htm	67fa75a8b7532539da31211fb45383c8	Web Page	
9 inux.org/" target="_blank">Ubuntu Linux · <a href="http:	Ubuntu	test\Pendrive01\C\SOPORTE\SSH\article.php.htm	67fa75a8b7532539da31211fb45383c8	Web Page	

Registro de los resultados



Jornadas de Seguridad Informática Page 1

- test\Pendrive01\C\SOPORTE\SSH\article.php.htm
Ejemplo de búsqueda de palabra clave
- Ubuntu
test\Pendrive01\C\SOPORTE\SSH\article.php.htm
Ejemplo de búsqueda de palabra clave

or la aventura de pasarse totalmente a software libre eragon eldest fondos psp como conociamen to libre gratis open knowhow knowm how opensource open source free ciencia como descarga desca rgar documental en el vientre materno gestación embarazo desarrollo foto embrión semanas meses f etos fecundación utero vientrematerno ecografías 4D ecografía 3D tridimensional videos imagenes videostreaming fotoblog galería de fotos GNU Creative Commons GNU/Linux Linux Mandrake Mandri va Debian Ubuntu distro Solaris Mac OS X Jaguar Panther Tiger UNIX BSD OpenBSD FreeBSD tecnolo gía informática internet programación sistemas operativos seguridad tunnel Open VPN Open SSH tu nelizsar servicios proteger datos backup copia de seguridad copia de respaldo encriptar encriptac ion esteganografía esteganografía ocular

```
0000<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/00081/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html xmlns="http://www.w3.org/1999/xhtml001621" xal:lang="es" lang="es"><head> <meta http-equiv="Content-Type" content="c00243ext/html; charset=iso-8859-1"> <meta http-equiv="content-language" content="es">00324 <meta name="robots" content="index,follow"> <meta name="Keywords" content="mas00408rior la aventura de pasarse totalmente a software libre eragon eldest fondos psp00486 coao conocimiento libre gratis open knowhow knowm how opensource open source f00567ree ciencia como descarga descargar documental en el vientre materno gestación e00648marazo desarrollo foto embrión semanas meses fetos fecundación utero vientremate00729mo ecografías 4D ecografía 3D tridimensional videos imagenes videostreaming fot00810blog galería de fotos GNU Creative Commons GNU/Linux Linux Mandrake Mandri va D00891ebian Ubuntu distro Solaris Mac OS X Jaguar Panther Tiger UNIX BSD OpenBSD FreeB00972SD tecnología informática internet programación sistemas operativos seguridad01052tunnel Open VPN Open SSH tunnelizar servicios proteger datos backup copia de segur01134dad copia de respaldo encriptar encriptación esteganografía esteganografía ocular0121mensajes noticias blog encuestas comentarios sindicacion sindicarse RSS XML ATO01296M Feed hacker hack trucos scriptkiddie laner cracker phreaker Linux Apache MySQL013777 PHP Xoops CMS LAMP crear un dominio alojamiento webmastering webmaster hosting01458 hostear hoster promocion web posicionamiento en buscadores WEB incrementar visi01537tas aumentar trafico estadísticas web guestats istats nedstats buscador q01620oogle yahoo altavista terra kartoo los mejores trucos software download free lib01701re gratis abierto odp open source opensource código fuente hardware disco duro
```

Hardware Forense



Write Blocker - USB



Write Blocker – Discos Rígidos



Telefonía Celular - Kit de adquisición



Toolkit de allanamiento

Hardware Forense



Destructora de CD



Etiquetas de seguridad



Rotuladora



Herramientas para apertura de equipamiento

Hardware Foreense

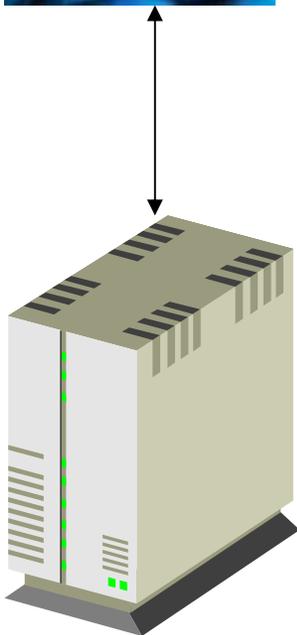


Servidores Blade



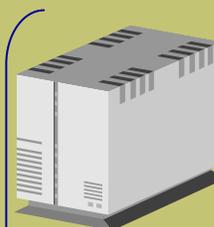
El paradigma de la virtualización

Perito Informático



Aplicaciones

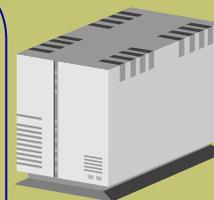
- Encase
- FTK Imager
- Otras herramientas forenses
- Aplicaciones de ofimática



- Autopsy
- AIR

Máquina Virtual Linux

- VMware Server



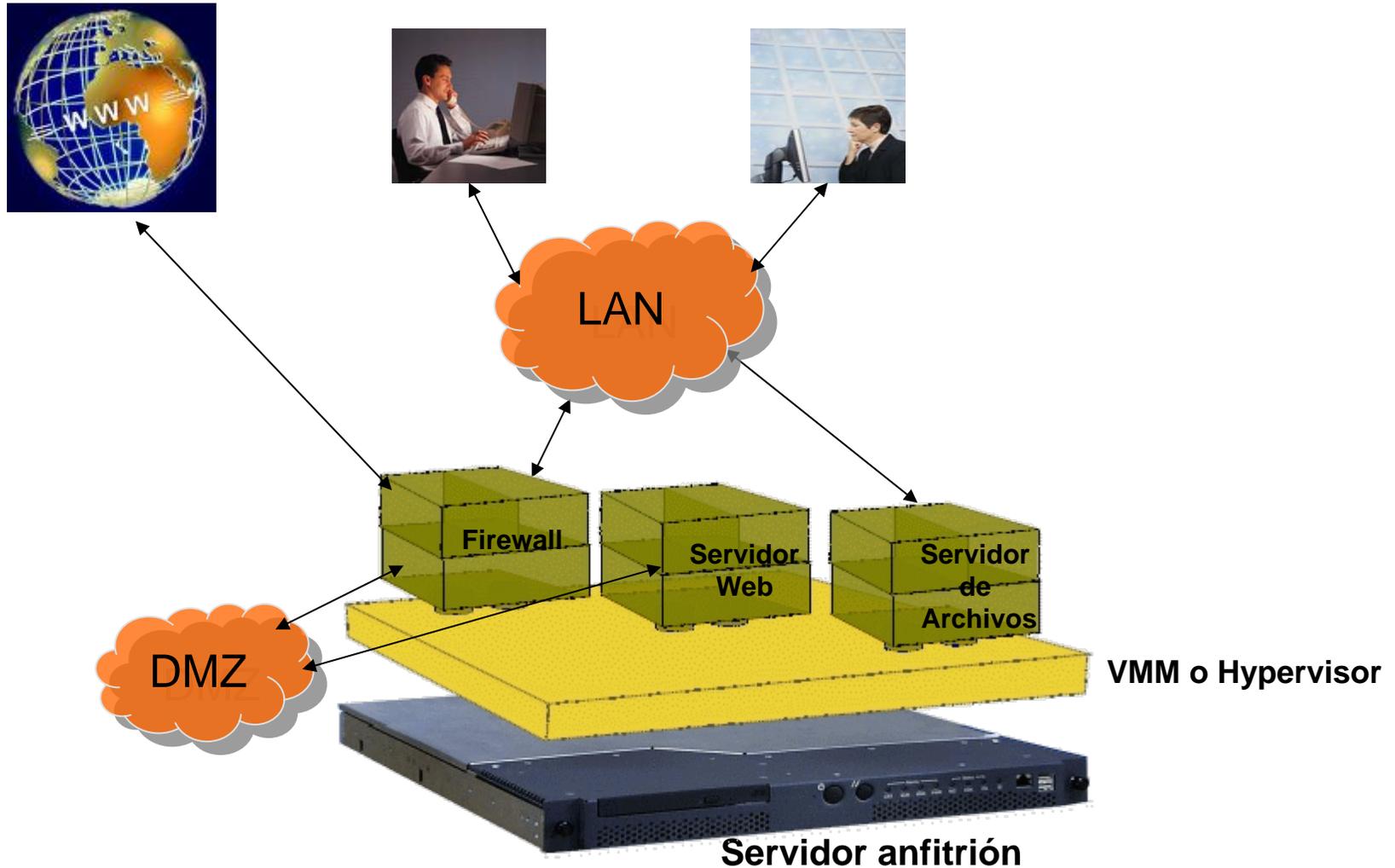
- Evidencia Digital



Máquina Virtual S.O. ...

Ventajas: Mayor disponibilidad de aplicaciones forenses para la investigación, facilidades para la inspección de evidencia digital

Virtualización de la infraestructura de servicios



Ventajas: Optimización de recursos tecnológicos, reducción de espacio físico, simplicidad de administración, mejor tolerancia a fallos

Muchas gracias por la atención

Para mayor información consulte

www.informaticapericial.com.ar