Análisis forenses a tarjetas SIM (Recuperando SMS's)

esto es un copy&paste

Una **tarjeta SIM** es una tarjeta inteligente desmontable y usada en teléfonos móvile que almacena de forma segura la clave de servicio del suscriptor usada para identificarse ante la red, de forma que sea posible cambiar la línea de un terminal a otro simplemente cambiando la tarjeta.

El uso de la tarjeta SIM es obligatorio en las redes GSM Su equivalente en las redes UMTS se denomina USIM

Las tarjetas SIM está disponibles en dos tamaños. El primero es similar al de una tarjeta de crédito (85,60 × 53,98 × 0,76 mm). El segundo y más popular es la versión pequeña (25 × 15 × 0,76 mm). Más en Wikipedia

La tarjeta también posee información independiente a la del sistema operativo del teléfono y la información que suele contener es:

- **IMSI** (Clave identificativa para cada dispositivo en el sistema), información sobre idiomas preferidos,
- **Información sobre la localización**: La SIM guarda la última área en donde el dispositivo se registró ante el sistema.
- **MSISDN** el cual puede ser usado para recuperar las llamadas originadas por el usuario a otros números de teléfono.
- **Información sobre el tráfico SMS**: Es posible leer mensajes enviados y recibidos fuera de la tarjeta SIM y saber si fue leído o no cada mensaje
- **Información sobre el proveedor**: Es posible obtener el nombre del proveedor y la red celular comúnmente usada para la comunicación, junto con las redes que están prohibidas para el dispositivo.
- **Información sobre llamadas:** Los últimos números marcados son guardados en un archivo en el sistema de ficheros de la SIM. La clave usada para cifrar la última llamada también es guardada allí.

Toda SIM a su vez contiene distintos niveles de seguridad:

- **PIN**: Al intentar acceder la información de la SIM se requiere introducir el número de identificación personal de la tarjeta. En caso de que sea introducido más de tres veces de forma errónea, esta se bloquea, siendo necesario el código PUK, suministrado por el fabricante u operadora.
- **PUK**: Este código sirve para habilitar tarjeta SIM debido ala introducción errónea del PIN. En algunos sistemas, si el PUK es introducido de manera incorrecta determinado número de veces, la información de la SIM se elimina de manera automática y de manera irrecuperable.

En un análisis forense la obtención de datos sobre una tarjeta SIM, es cada vez más compleja dado que los nuevos terminales almacenan esta información sobre la base del mismo sistema operativo (su estructura de disco y fichero) delegando a la tarjeta el almacenamiento, cuando el disco de datos del sistema operativo se llena.

No obstante existen diferentes técnicas de obtención, cobrando interés las soluciones comerciales, dado que son las más completas y funcionales.

En la siguiente lista podemos ver los diferentes productos que existen y que dan soporte al análisis de tarjetas SIM:

- Forensic Card Reader
- SIMIS
- USIM Detective
- Oxygen PM for Symbian
- PDA Seizure
- Pilot-Link
- BitPIM
- Cell Seizure
- CellDEK
- GSM .XRY
- MobilEdit!!
- PhoneBase
- Secureview
- TULP 2G

ANALIZANDO UNA TARJETA SIM

Para ello voy a emplear un lector de tarjetas SIM y software 'Open Source' como comercial.

EMPEZAMOS

Lo fundamental es disponer de un lector de tarjetas SIM compatible , en mi caso he elegido por su compatibilidad en el mercado, un dispositivo

DEKART (33 Euros + Gastos de envío) que es compatible con los drivers PC/SC.

las características son las siguientes:

- Dispositivo de lectura y escritura por USB
- Busca, edita, añade y borra entradas de la tarjeta SIM
- Permite hacer copias de seguridad
- Permite manejar los PIN's
- Exporta la libreta de direcciones a Outlook, MS Office
- Software de exploración de ficheros

En esta ocasión para obtener información de la SIM voy a utilizar MOBILedit! en su dos versiones Forensics, y este es el resultado:

Como vemos en la pantalla anterior, me permite cambiar o deshabilitar el acceso a las contraseñas o PIN's. En la siguiente pantalla puedo acceder a todas las posiciones de la tarjeta SIM

En la siguiente pantalla podemos ver los SMS's enviados y recibidos (oculto los datos de carácter personal, como es obvio). No obstante veo que algunos de los SMS's que he

borrado a conciencia no salen en la lista de 'Deleted Items', mientras que otros si.

Voy a tener que esforzarme por entender este caso y recuperar los SMS's

RECUPERANDO SMS'S DE LA SIM

Recuperar un SMS es algo que muchos de nosotros necesitamos hacer de vez en cuando, dado que a veces recibimos datos importantes a través de un mensaje SMS como por ejemplo una dirección, un número de teléfono, una contraseña, o un código PIN, pero si no nos damos cuenta y eliminamos el SMS esto puede llegar a ser un problema.

Por otro lado cuando analizamos un móvil sospechoso es necesario el recuperar los mensajes. Por ejemplo esto ocurre en casos de acoso o grooming

Como se borra un SMS

Con el fin de recuperar un SMS, tenemos que entender la forma en que se eliminan.

La tarjeta SIM contiene un archivo especial donde se guardan los SMS, el archivo tiene varias "franjas horarias" y en él, existe una zona para cada mensaje, siendo el número de franjas de forma finita, es decir, una tarjeta SIM puede almacenar unas 20 o 25 SMS dependiendo de la capacidad. Las tarjetas más modernas tienen más zonas.

Cuando todas las zonas están llenas, hay que borrar una zona antigua, antes de guardar un mensaje nuevo.

La estructura de una de estas franjas horarias se compone de varios campos, tales como:

- El número de teléfono del remitente
- La fecha y la hora en que se ha recibido el SMS
- El texto del mensaje en sí.

Existen otros campos que no se muestran para nosotros, uno de ellos es el estado actual de la zona, que puede ser tanto "vacío", o "en uso".

Algunos teléfonos eliminan un SMS al establecer el valor "en uso" a un nuevo valor "vacio", dejando intactos los otros campos. Cuando se recibe una nueva recepción de SMS, el teléfono tiene que verificar si existen espacios libres, y si es así será utilizado para almacenar el nuevo SMS.

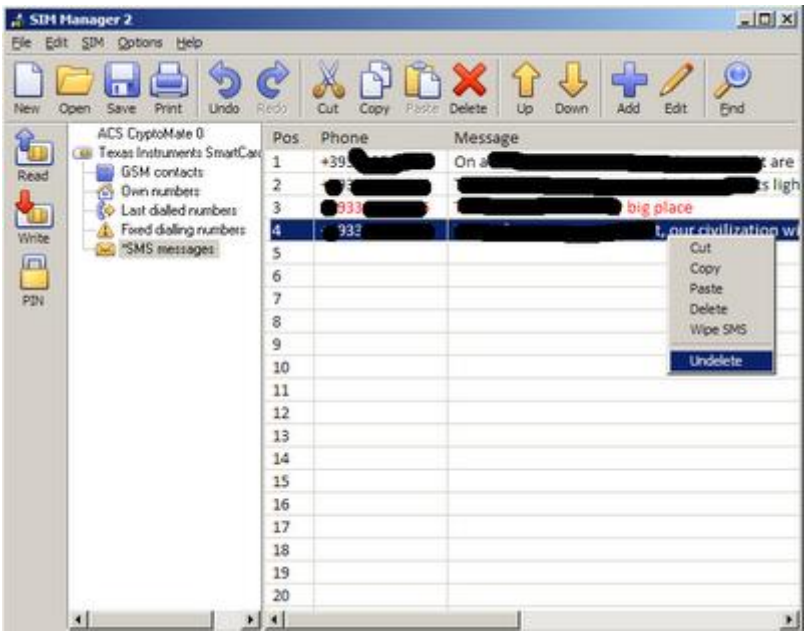
En este punto se centra nuestro interés. Los SMS pueden ser recuperados, mediante un simple cambio de "estado" de "vacío" a en "uso". Para ello podemos utilizar la herramienta *SIM Manager .* Que en mi caso con la compra del producto 'dekart' me permite descargar desde la web

NOTA: *¡¡Solo funciona correctamente con la versión en Ingles!!*

SIM Manager mostrará los mensajes que fueron marcados como eliminados en color rojo, pulsamos con el botón derecho del ratón y pulsamos recuperar. (Nunca antes fué tan sencillo recuperar un SMS).

Por contra también podemos asegurarnos que no se va a poder recuperar definitivamente con tan solo indicarle borrar.

La siguiente captura de pantalla muestra una tarjeta SIM con 20 ranuras de SMS, 4 de los cuales contienen mensajes, pero sólo los dos primeros están en uso, los dos últimos son marcados como eliminados.



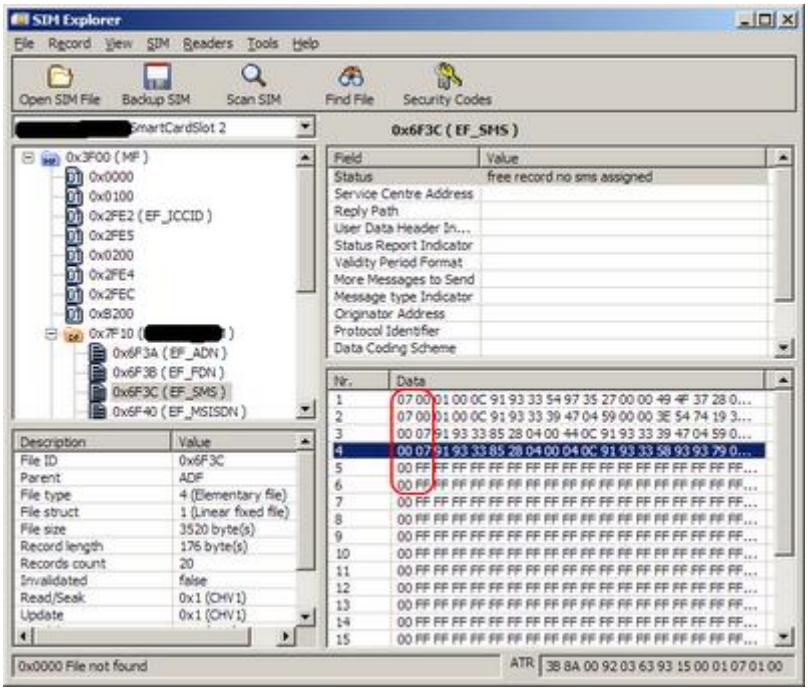
A continuación se muestra otra imagen, con una herramienta de análisis forense llamada SIM Explorer, que muestra los datos de la tarjeta SIM.

La herramienta se utiliza para reunir las pruebas electrónicas de tarjetas SIM, pero en nuestro caso vamos a utilizarlo para para echar un vistazo a las entrañas de la tarjeta y entender cómo funciona **la recuperación de la tarjeta SIM.**

Hay dos conceptos, el "00" que siginifica "Libre" y el 07 que significa "ocupado".

Como se puede apreciar, los dos primeros mensajes se mostrarán por el teléfono, los siguientes dos mensajes no van a ser mostrados por el teléfono móvil. El resto del archivo son las ranuras de expansión vacías.

Hay que tener en cuenta que no sólo tienen "00" en el inicio, y que el resto se presenta con "FF FF" - que es el valor predeterminado para un mensaje de borrado.



¿Cuando NO se puede recuperar un mensaje?

Lamentablemente a veces las cosas no son tan sencillas tal y como lo hemos descrito anteriormente.

Algunas compañías utilizan el software del móvil y marcan el SMS' como borrado de forma permanente y sin posibilidad alguna de poder recuperar. La descripción de este mecanismo es muy dificil de conseguir y estas compañias no indican el procedimiento que siguen para borrar sus mensajes, es decir no dan esta información. Bajo mi parecer creo que sobrescriben la zona un numero determinado de veces con lo que consiguen eliminarlo correctamente, pero esto que digo es tan solo una hipotesis.

Por último, hay otro detalle, como he dicho anteriormente muchos de los nuevos teléfonos tienen la forma de almacenar el SMS en su propia memoria, en lugar de en la tarjeta SIM. En ese caso, la solución descrita aquí no se aplica, ya que cada fabricante tiene una forma distinta de hacerlo según el teléfono y el sistema operativo.

También hay casos en los que el teléfono va a utilizar su propia memoria de almacenamiento de SMS, y cuando se llena, el nuevo SMS se almacenarán en la tarjeta SIM.

Otras formas de recuperar la información es utilizando hardware. Estos mecanismos mantienen la integridad de la tarjeta SIM aunque son muy elevados economicamente y solo para empresas especializadas.

Bueno para finalizar este post, aquí os dejo este modelo especifico Csurv M-TEK de la empresa 3GForensics y que podéis ver en acción en este vídeo.

FUENTE