

Jaulas de Faraday y el Análisis Forense en Telefonía Móvil



17.03.2011



Tel + 5255 / 5370 4334
Fax: +5255 / 5370 4107

E-mail: admin@jaulafaraday.com 1
www.jaulafaraday.com

Contenido

1	Introducción.....	3
2	El proceso Forense.....	4
3	Tipos de Evidencia.....	6
4	Problemas Actuales.....	8
5	Desarrollos Actuales.....	12
6	Conclusiones.....	14



1 Introducción

Los teléfonos móviles juegan un papel importante en la vida de hoy. Hoy en día casi si la mayoría de las viviendas particulares cuentan con un teléfono móvil, que son millones de estos. El mercado está dividido entre Nokia (34,8%), Motorola (21,1%), Samsung (11,8%), Sony Ericsson (7,4%), y LG Electronics (6,3%) Por lo que es no es ninguna sorpresa que los teléfonos móviles se encuentran con una frecuencia cada vez mayor en la escena del crimen. Los teléfonos móviles pueden desempeñar un papel primordial en la vida de una persona, no sólo como un medio de comunicación sino también como un organizador o una cámara.

Por lo que es una alta probabilidad de encontrar información útil sobre el propietario de un teléfono. En relación con un posible delito de un teléfono puede tener varias pistas a partir de contactos sobre el historial de llamadas a los mensajes SMS. Las fuerzas policiales comienzan a descubrir la utilidad de los teléfonos móviles en una investigación. En este momento que el campo de análisis forense esta siendo desarrollado y el campo se está expandiendo rápidamente.

Este artículo busca dar un esbozo de las prácticas actuales y perspectivas futuras.



2 El proceso Forense



Hay muchas directrices diferentes para el proceso forense. Este es un breve resumen de las NIST (National Institute of Standard and Technology)"Directrices sobre el análisis forense de teléfonos celulares"

Conservación y Documentación

En la recolección de pruebas es importante no alterar la escena del crimen. Uno no puede simplemente retirar el teléfono móvil de la escena del crimen. Se debe tener cuidado para salvaguardar otras formas de evidencia como huellas dactilares y rastros de ADN. Además se necesita documentar adecuadamente cada pieza de la evidencia. Esta documentación debe incluir por lo menos algunas fotos de como se encontró el teléfono móvil. También es importante tener en cuenta si el teléfono estaba encendido o no.

Adquisición

En esta fase es la recolección de datos del dispositivo. Esta recolección puede tomar varias formas. En un caso ideal los datos deben ser copiados desde el teléfono también como de la tarjeta SIM. En algunos casos dificultades técnicas pueden impedir usar esta información para una acusación. En el peor de los casos solo datos directos de la pantalla pueden ser recogidos



Examen y Análisis

Ahora los datos recogidos se analizan en busca de pistas sobre el posible delito. Estas pistas pueden adoptar diversas formas para un análisis más detallado (véase más adelante). El examen puede también hacerse a mano o con la ayuda de software. Hay diferentes herramientas de software disponibles para tales propósitos. No hay balas de plata así que se debe tener cuidado para no perder información crucial de evidencias solo por que no se tiene una herramienta que tenga las características correctas.

Reporte

El último paso es el más importante. Entre la obtención de pruebas y la presentación ante el tribunal puede pasar una cantidad significativa de tiempo. El examinador debe ser capaz de presentar sus pruebas de manera concluyente y ofrecer a la otra parte información sobre las herramientas y los métodos utilizados. La evidencia es inútil si no es admitida en el tribunal , y puede suceder que la autenticidad de las pruebas sea cuestionada por su origen o su adquisición y por no estar documentada correctamente.



Tel + 5255 / 5370 4334
Fax: +5255 / 5370 4107

E-mail: admin@jaulafaraday.com 5
www.jaulafaraday.com

3 Tipos de Evidencia



Libreta de direcciones

La libreta de direcciones almacena información de diferentes contactos. Con la ayuda de la libreta de direcciones es posible hacerse una idea de la red social de la sospecha. Se puede utilizar por ejemplo para vincular a un sospechoso a la víctima.

Historial de llamadas

El historial de llamadas ofrece una visión más profunda de las actividades del propietario. Uno puede ver las llamadas entrantes y salientes, así como su duración. Esta información puede ser utilizada para hacer algunas conclusiones indirectas.

Mensajes de Texto MSM (también correos electrónicos en teléfonos recientes)

Los mensajes SMS, así como información de correo electrónico ofrecen información concreta, en contraste con el historial de llamadas y la libreta de direcciones que sólo ofrecen información indirecta. Ellos pueden contener palabras reales escritas por el propietario o destinados para el propietario que puede servir como prueba en los tribunales.

Calendario

El calendario ofrece una visión general sobre las actividades pasadas y planeadas del propietario. Puede ser utilizado para ligar al propietario con ciertos lugares y tiempos y también posibles testigos.



Otros Medios de Comunicación

Los nuevos teléfonos móviles pueden contener también otra gran cantidad de información.

En primer lugar está la cámara. Las imágenes o películas pueden contener también elementos de prueba. No sólo en su contenido, sino también en la forma de los archivos (datos incrustados en el archivo pueden dar más información).

Es posible también que el autor tome una fotografía del crimen como trofeo. Los datos EXIF se pueden utilizar para determinar la fecha y hora exacta que fue tomada la imagen, en algunos casos incluso la ubicación. Algunos teléfonos móviles están equipados con un receptor GPS. Este receptor puede almacenar información sobre las ubicaciones y tiempos de forma independiente de las aplicaciones que se ejecuta en el teléfono móvil. Así que el propietario puede estar vinculado a la escena del crimen o posibles coartadas.



Tel + 5255 / 5370 4334
Fax: +5255 / 5370 4107

E-mail: admin@jaulafaraday.com 7
www.jaulafaraday.com

4 Problemas Actuales



Hay muchos problemas que enfrenta el análisis forense de los dispositivos móviles. En este artículo se verán aquellos que se encuentran durante el examen.

El primer problema se produce cuando el teléfono móvil se encuentra en la escena del crimen, si el teléfono está apagado todo esta bien pero si el teléfono está encendido hay un problema. Si el teléfono es dejado en la escena es posible manipular el evidencia.

Sólo algunos modelos pueden almacenar una cantidad específica de datos, por ejemplo, sólo 20 SMS. Si el criminal quiere destruir la evidencia él simplemente envía 20 Mensajes sin sentido desde otro teléfono y toda la evidencia se pierde. Escenarios similares son posibles para las llamadas entrantes, pero la amenaza mas grande es el borrado remoto.

Algunos planes de negocio en los teléfonos más complejos ofrecen borrado remoto. Estos planes de negocios son para clientes que pierden su teléfono y no quieren revelar secretos de su compañía. Un criminal puede utilizar la función para enviar una instrucción a distancia y borrar todos los datos. Por otra parte, apagar el teléfono también tiene ciertas desventajas. Si el teléfono está bloqueado por una clave PIN el investigador tiene que contactar al proveedor de servicios inalámbricos con el fin de desbloquear para obtener la información almacenada en la tarjeta SIM. En la práctica esto no es un problema importante, pero apagar el teléfono causa la pérdida de todos los datos almacenados en la memoria RAM. En algunos teléfonos, también los datos en las tarjetas SIM, como el registro de la ubicación se elimina automáticamente. Una vez más la evidencia se pierde.



La tercera opción es dejar el teléfono encendido, pero desconectarlo de la red. Este se puede hacer mediante el uso de bolsas de Faraday, que en teoría evitan cualquier fuga de radiación desde la red hacia el teléfono. Esta es sólo la teoría porque si el teléfono se deja encendido este empieza a buscar la red a través de aumentar su potencia. Esto aumenta el consumo de energía y reduce la duración de la batería. Así que de alguna manera el teléfono tiene que estar encendido. La conexión por cable reduce la efectividad de la bolsa de Faraday.

Los diferentes países han resuelto estos problemas de varias maneras. La mejor práctica en los Estados Unidos recomienda el uso de bolsas de Faraday en el Reino Unido y Holanda, se recomienda apagar el teléfono. En los nuevos modelos hay una solución. El modo de vuelo desconecta el teléfono móvil de la red si el cliente desea utilizar otras aplicaciones mientras esta volando. Pero a fin de utilizar esta función, el investigador debe saber si un teléfono en particular tiene esta característica o no en la escena del crimen lo que obliga a estar al día con todos los modelos actuales, que no es una tarea fácil.

El siguiente problema es identificar el teléfono. Hay muchos diferentes fabricantes que ofrecen una gran cantidad de modelos diferentes, con nuevos modelos disponibles casi todos los meses. Si el teléfono se encuentra en la escena del crimen tiene que ser identificado antes de que la investigación puede comenzar para que el especialista pueda familiarizarse con el. Hay maneras diferentes de hacer esto. Por lo general, el logotipo del fabricante y el proveedor de telefonía móvil se muestran en uno de los lados. Pero esto es sólo un punto de partida. Hay algunos sitios web que tratan de ayudar. Los más notables son www.gsmarena.com y www.phonescoop.com. Ambas páginas tienen una enorme lista de teléfonos con imágenes y enlaces con el fabricante. Después de un poco de investigación el investigador puede identificar el teléfono que ha encontrado.

Ahora el problema de la conectividad y la batería se incrementan. Como se mencionó anteriormente, si el teléfono se deja encendido este tiene que ser cargado durante la investigación, ya que la batería de mayoría de los teléfonos no va a durar más que una semana. Una vez más hay muchos modelos por muchos fabricantes y todos requieren diferentes cables de alimentación. La única opción viable para el investigador es tener la mayoría de los cables a la mano o después de identificar el teléfono ir a la tienda y comprar el cargador correcto. Este escenario también se debe considerar si el investigador decide apagar el teléfono en la escena del crimen, ya que tiene que ser alimentado durante la investigación.



Después de el teléfono se enciende automáticamente intenta restablecer la conexión con la red móvil. **Esto no es un gran problema ya que el teléfono puede ser manejado en una situación muy controlada y la mayoría de los laboratorios forenses tienen áreas las cuales son protegidas por jaulas de Faraday de las interferencias externas.**

El problema más grande es conectar el teléfono a un PC con el fin de investigar. Entre más viejo es el teléfono más grande es el problema. Una vez más no hay ninguna interfase estándar y cada fabricante ha desarrollado su propio protocolo e interfase así como su software. Esto conduce a una gran cantidad de diferentes cables. Hoy es un poco más fácil porque la mayoría de los teléfonos ofrecen una conexión USB para que el cliente descargue tonos de llamada u otras aplicaciones. La misma conexión se puede utilizar para la investigación. Sin embargo, algunos fabricantes (por ejemplo, Motorola) cambia la definición de PIN con el fin de obligar a los clientes utilizar sus propios cables.

El investigador tiene varias opciones para solucionar este problema. Hay muchas soluciones de software para ayudar a la investigación forense de un teléfono móvil. Este es muy útil para los teléfonos de uso común. Para modelos raros los cables de conexión tienen que ser comprados por separado. Pero uno tiene que ser capaz de analizar también los nuevos modelos. Algunos fabricantes de software (Susteen, Parabeen) ofrecen cables para los nuevos modelos hasta por dos años después de comprar su software.

El siguiente problema es elegir el software adecuado para un teléfono en particular. Como mencionado anteriormente hay muchos programas o soluciones de hardware a escoger. Cada uno de ellos tiene ciertas ventajas o desventajas, tanto en lo que respecta a los modelos de apoyo y funciones de software. Aquí el investigador tiene que recurrir a la experiencia anterior. En un mundo ideal, con solo ver el teléfono se tendría que saber que software funciona mejor. En el mundo real el investigador se enfrenta a nuevos teléfonos.

Aquí se tiene que ser muy cuidadoso para no destruir pruebas. Hay diversas recomendaciones sobre cómo proceder.

En primer lugar, el investigador debe descargar del fabricante el manual del teléfono para familiarizarse con las características y capacidades del teléfono. También ayuda a leer diversos foros en Internet que tratan de ofrece ayuda al investigador.

Tras la investigación inicial, se recomienda comprar un teléfono del mismo modelo para probar la funcionalidad del software. Además, es primordial no confiar en una única solución de software.



Tel + 5255 / 5370 4334
Fax: +5255 / 5370 4107

E-mail: admin@jaulafaraday.com 10
www.jaulafaraday.com

Mientras se testifica en los tribunales es importante que uno pueda demostrar que los mismos resultados se obtuvieron al utilizar métodos diferentes para dar mayor credibilidad a los mismos.

Dar credibilidad a los resultados no es tan fácil como parece. Todos los teléfonos móviles tienen un reloj interno que cambia los datos en la memoria, así como el desgaste de nivelación. El desgaste de nivelación es un proceso que trata de maximizar el tiempo de vida de la memoria flash en un teléfono móvil. La memoria flash sólo se puede escribir y borrar una cierta cantidad de veces. El desgaste de Nivelación utiliza software y hardware para asegurarse de que todas las partes de la memoria se utilizan de forma sistemática y por lo tanto el tiempo de vida es tan largo como sea posible. Ambos procesos hacen uso de las sumas de comprobación. En análisis forenses de discos duros las sumas de comprobación son utilizadas en los tribunales para demostrar que las pruebas no han sido manipuladas.

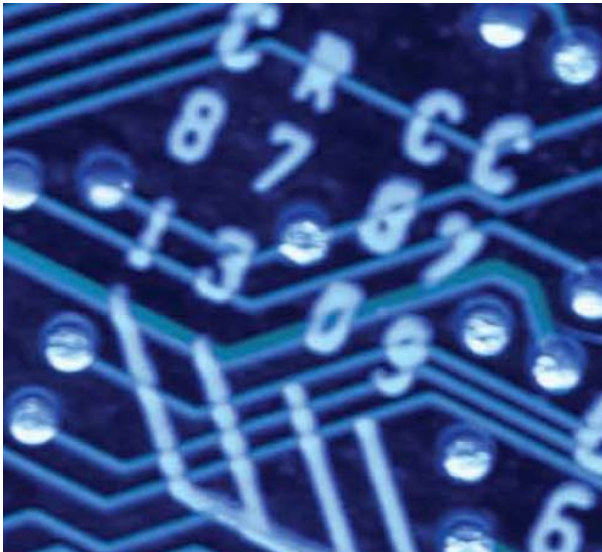
Por último pero no menos importante, es la tarjeta SIM en el teléfono móvil. Los datos pueden ser almacenados de forma independiente, en el teléfono móvil, o en la tarjeta SIM. Un hecho interesante es que la tarjeta SIM ofrece características como los últimos números marcados (la mayoría de las tarjetas SIM puede almacenar hasta cinco), pero los fabricantes suelen poner en práctica la función de la tarjeta SIM en el teléfono. Esto puede causar redundancia y puede ser útil en las investigaciones. La tarjeta SIM comenzó con espacio de almacenamiento relativamente pequeña. Hoy en día las tarjetas SIM con hasta a 4 Megabytes están comercialmente disponibles

La tarjeta SIM contiene información importante como el archivo Location Information File (LOCI). En el archivo LOCI el investigador puede encontrar información sobre las últimas células en el que el teléfono estaba activo. La información se conserva después de que el teléfono está apagado, pero solo puede contener más de una celda y el investigador puede establecer los últimos movimientos del teléfono desde este archivo. Para una discusión detallada ver [AS07]

Otro problema es el bloqueo de SIM. La tarjeta SIM y sus datos pueden ser asegurados usando un PIN (Número de Identificación Personal). Uno sólo tiene tres intentos en la tarjeta SIM y 10 intentos para el PUK (código de desbloqueo personal). Si el teléfono se encuentra lo mejor la práctica es pedirselo de lo contrario la única solución es pregunta el PUK a el fabricante. Con el fin de conocer el código PUK se debe conocer el ICCI (Integrated Circuit Card Identifier). Este número por lo general que se encuentran impreso en la superficie de la tarjeta SIM



5 Desarrollos Actuales



Mirando hacia el futuro de la ciencia forense móvil hay muchas novedades en el horizonte. Como siempre, algunos son buenos y otros parecen tener muchos obstáculos

Los teléfonos móviles seguirán obteniendo mayor procesamiento de datos así como capacidad de almacenamiento. Por un lado esto abre la posibilidad para nuevas aplicaciones y por otro lado hay más espacio de almacenamiento para ser analizados. En teoría esto no debería causar mayores problemas porque la misma ley se aplica al software y hardware, el examinador utiliza y así él debe ser capaz de hacer frente a ella.

Pero hay problemas mayores. Algunos fabricantes de teléfonos móviles están planeando encriptar sus teléfonos móviles, así como los datos almacenados en ellos. Para ellos este paso es natural porque el sistema operativo en los teléfonos es de su propiedad intelectual . Se han gastado dinero para desarrollar y quieren ganar dinero con esto. Además, puede servir como base para sus futuras ganancias. Con Digital Right Management (DRM) y los teléfonos siendo cada vez más populares haya aumento de mercado para otras aplicaciones en desarrollo y las empresas están tratando de proteger su cuota de mercado.

Esto puede causar problemas para el investigador. Casi todas las herramientas actuales no trabajan con un sistema de encriptado de alta seguridad. Además, incluso si los datos como un SMS se recupera, será en su forma cifrada y así, sin la clave adecuada es casi inútil. El investigador tendría que depender de la cooperación de fabricante de software en casi todas las investigaciones que podrían conducir a una gran cantidad de gastos



Pero hay una evolución positiva también. Las herramientas actuales están empezando a depender en una interfaz común de la prueba Joint Test Action Group (JTAG). JTAG es / era el diseño original para probar los circuitos en los procesadores, chips de memoria y conexiones físicas.

Lo interesante de esto es que podría facilitar el acceso directo a los procesadores y los bancos de memoria sin confiar en el sistema operativo. El inconveniente para que esto funcione uno necesita saber exactamente la instrucción exacta del procesador o bancos de memoria.

Pero ya hay algunas herramientas que ya hacen uso de JTAG. Estas herramientas se llaman Flasher Boxes.

En estos momentos solo es posible leer los bancos de memoria de algunos modelos. El único problema es que en realidad es un volcado hexadecimal de raíz.

Los datos son fragmentados e incluyen bits usados por el sistema operativo. En algunos casos como el Nokia serie 30 y 40 ha sido posible reservar en el archivo de memoria permitiendo al investigador acceso a todos los datos almacenados en el teléfono.

Por otro lado si no se sabe nada los datos se parece a números al azar. Todo depende de que el investigador resuelva la utilidad de la información.



Tel + 5255 / 5370 4334
Fax: +5255 / 5370 4107

E-mail: admin@jaulafaraday.com 13
www.jaulafaraday.com

6 Conclusiones

Como se puede ver el campo del análisis forense para la telefonía móvil ofrece muchas posibilidades para el investigador pero todavía hay muchos obstáculos que superar antes de que todo su potencial sea alcanzado.

Con un mercado en constante cambio los teléfonos móviles siempre tienen nuevos retos para un investigador. Pero su utilidad para ayudar a resolver un caso no puede ser subestimada.

HHHHHHHHHHHHH



Tel + 5255 / 5370 4334
Fax: +5255 / 5370 4107

E-mail: admin@jaulafaraday.com 14
www.jaulafaraday.com