Informática Forense Para Moviles

Gomez Ocampo Lizeth Marcela
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
marce_liz_1@hotmail.com

RESUMEN

Este articulo proporciona información básica sobre la conservación, adquisición, examen, análisis y presentación de informes de pruebas digitales en los teléfonos celulares, pertinentes para hacer cumplir la ley, de respuesta a incidentes, y otros tipos de investigaciones. La guía se centra principalmente en las características de los teléfonos celulares, incluidos los teléfonos inteligentes con funciones avanzadas. También trata de las disposiciones que deben tomarse en cuenta durante el curso de una investigación del incidente. La guía está pensada para atender las circunstancias comunes que pueden ser encontradas por el personal de seguridad de la organización y los investigadores policiales, con la participación digital electrónica de datos que residen en los teléfonos celulares y medios de comunicación electrónicos asociados. También se destina a complementar las directrices existentes y profundizar en las cuestiones relacionadas con los teléfonos celulares y su examen y análisis.

Palabras clave

Dispositivo móvil, comunicación, sistema global, asistencia personal.

1. INTRODUCCIÓN

Los teléfonos móviles son cada vez más y más tecnificados. Casi todos los teléfonos móviles producidos en la actualidad cuentan con cámaras integradas en ellos o con más memoria, que hace que su capacidad de almacenamiento sea mayor que nunca.

Lo que antes era un trabajo para un espía internacional, ahora es una hazaña sencilla como tomar una foto discreta, la grabación no autorizada de una conversación privada o videos furtivos, fácilmente a nuestro alcance. Para la mayoría de nosotros, el uso de la cámara en nuestros teléfonos móviles es simplemente para asegurar de que podemos capturar imágenes y recordarlas. Sin embargo, para algunos, es la manera perfecta para capturar datos de misión crítica, para robar una fórmula secreta de un competidor, o simplemente para su uso en una situación de chantaje.

2. INFORMATICA FORENSE PARA MOVILES: DEFINICIÓN

La informática forense móvil es la ciencia que se encarga de la recuperación de evidencia digital desde un teléfono móvil en condiciones forenses de sonido mediante los métodos aceptados. Los teléfonos móviles, especialmente aquellos con capacidades avanzadas, son un fenómeno relativamente reciente, no suelen estar cubiertos en lo que es la informática forense clásica. Trataremos de cerrar esa brecha, proporcionando una visión profunda en los teléfonos móviles y explicar las tecnologías que intervienen y su relación con los procedimientos forenses, además, se describen los procedimientos para la conservación, adquisición, examen, análisis y presentación de informes en la presentación de información digital en teléfonos celulares, así como disponer de herramientas de software forense que apoyar esas actividades.

Algunos puntos importantes para realizar el análisis forense a los móviles se explican en los siguientes apartados.

2.1. Las organizaciones deben garantizar que sus políticas y procedimientos de apoyar el uso razonable y adecuado de las herramientas forenses para teléfonos celulares.

Las políticas y procedimientos deben ser explicadas claramente y qué acciones deben ser tomadas por una unidad forense en diversas circunstancias comúnmente encontrados con los teléfonos celulares. También debe describir la calidad de las medidas a aplicar en la verificación del buen funcionamiento de los instrumentos utilizados en el examen forense de los teléfonos celulares y los medios de comunicación asociados. Procedimientos para el manejo de información sensible que pueda ser registrado por las herramientas forenses que también se deben abordar. La Asesoría legal deberá examinar cuidadosamente toda la política de forenses y procedimientos de alto nivel para el cumplimiento con las normas internacionales, las leyes federales, estatales y locales y los reglamentos, según proceda.

2.2. Las organizaciones deben asegurarse de que sus profesionales forenses están preparados para llevar a cabo actividades en el análisis forense de teléfonos celulares.

Los profesionales forenses, deben comprender sus funciones y responsabilidades para las técnicas forenses de teléfonos celulares y recibir capacitación y educación sobre las

herramientas forenses relacionadas, las políticas, directrices y procedimientos. Los profesionales forenses también deben consultar con los asesores legales, tanto en la preparación general para las actividades forenses, como por ejemplo determinar qué acciones deben y no deben tomarse en distintas circunstancias. Además, la administración debe ser responsable de apoyar las capacidades forenses, revisión y aprobación de la política forense, examinar y aprobar las acciones inusuales forenses que pueden ser necesarias en una situación particular.

3. VISIÓN GENERAL DE LOS TELÉFONOS CELULARES, INCLUYENDO UNA VISIÓN GENERAL DE HARDWARE Y CAPACIDADES COMUNES DE SOFTWARE

En el mercado existen diversos dispositivos que prácticamente llevan los siguientes sistemas operativos.

Symbian es un sistema operativo que fue producto de la alianza de varias empresas de telefonía móvil. El objetivo de Symbian fue crear un sistema operativo para terminales móviles que pudiera competir con el de Palm o el Windows Mobile de Microsoft.

Palm OS es un sistema operativo hecho por PalmSource, para PDAs.

Windows Mobile es un sistema operativo basados en la API Win32 de Microsoft. Los dispositivos que llevan Windows Mobile son Pocket PC, Smartphones y Media Center. Ha sido diseñado para ser similar a las versiones de escritorio de Windows e integrables con las redes y servidores Windows 2003 y 2008

Proyectándose, lo primero es seguir las buenas prácticas de un analista forense: (1) Preservar-documentar, (2) adquirir-investigar y (3) informar.

A diferencia de las copias bit a bit que se realizan sobre los discos duros, los móviles sufren constantemente cambios en su sistema de datos y ficheros, y realizar una copia integra se presenta como una opción prácticamente imposible de realizar desde el punto de vista de la preservación de la información. Aparte de esto generalmente viene protegido por mecanismos propios del fabricante.

4. HERRAMIENTAS FORENSES

Las herramientas de software forense para teléfonos celulares es considerablemente diferente de los ordenadores personales. Mientras que las computadoras personales se han diseñado como sistema de propósito general, los teléfonos celulares están diseñados más como aparatos de efectos especiales que llevan a cabo un conjunto de tareas predefinidas. Los fabricantes de teléfonos celulares también tienden a basarse en una variedad de sistemas operativos propietarios en lugar del enfoque más estandarizado en los ordenadores personales. Debido a esto, la variedad de herramientas para dispositivos móviles es muy variado y el rango de dispositivos a través de las que operan normalmente se redujo a distintas plataformas para la línea de productos de un fabricante, una familia de sistemas operativos, o un tipo de arquitectura de hardware. Ciclos cortos de realización del producto son la norma para los teléfonos celulares, exige a los fabricantes de herramientas actualizar sus herramientas continuamente para mantener la cobertura actual.

La mayoría de herramientas de software forense para teléfonos celulares y (U) SIM adquieren los datos de forma lógica, utilizando protocolos comunes para la sincronización de dispositivos, comunicaciones, y la depuración. Algunas herramientas también pueden ser capaces de adquirir los datos físicamente para ciertas categorías de teléfonos. Los comandos AT, Sync ML, y los demás protocolos listados son de uso común en la lógica de la adquisición de teléfonos celulares. Debido a que los teléfonos pueden soportar protocolos múltiples, una herramienta puede emplear varios de ellos en la sucesión a adquirir la más amplia gama de datos disponibles. Incluso si una herramienta de usos múltiples protocolos para un teléfono particular, todos los datos disponibles no pueden ser capaces de ser recuperados.

4.1 Herramientas para el Chip(Sim)

Forensic Card Reader (FCR) es una herramienta forense de Becker & Partner que proporciona los medios para extraer los datos de SIMs. FCR no genera un archivo del caso, pero los resultados los datos adquiridos en un formato XML que puede ser visto con el editor correspondiente. FCR consiste en el software y un lector USB de tarjetas inteligentes

El kit de herramientas SIM Forense (FST) es una herramienta forense de Radio táctica que proporciona los medios para extraer y duplicar los datos de SIM / USIMs. El expediente del caso se almacena en un formato de FST de propiedad y pueden ser de salida en un archivo HTML o RTF (formato de archivo de Word). Un dongle USB que se necesita para operar el software en un ordenador de sobremesa. La terminal de adquisición de FST, una unidad independiente, duplica el contenido de la meta (U) SIM para un conjunto de datos de tarjetas de FST de almacenamiento (es decir, el Maestro de almacenamiento de datos de tarjetas de Defensa, Tarjeta de almacenamiento de datos, y procesamiento de datos Storage Card). El análisis de los datos puede llevarse a cabo utilizando los correspondientes datos de la tarjeta de almacenamiento FST con el lector de tarjetas ForensicSIM (es decir, PC / SC-lector de tarjetas compatible) conectado a un PC que ejecute la aplicación de análisis ForensicSIM. Una suma de control MD5 proporciona protección de la integridad de los datos del caso generado. FST permite la importación de los expedientes archivados y busca el archivo en la base de datos adquirida.

SIMCon es una herramienta forense de InsideOut Forense que proporciona los medios para extraer los datos de SIMs y USIMs. El expediente del caso tiene un formato propietario, pero pueden ser exportados a un formato de texto ASCII estándar. Adicionales (por ejemplo, el hardware, el dongle USB, lectores de tarjetas de propiedad) no son necesarios para la adquisición. SIMCon adquiere los datos de un (U) SIM a través de un PC / SC-lector de tarjetas compatibles y utiliza un hash SHA1 para proteger la integridad de los datos del caso generado. SIMCon proporciona la posibilidad de importar archivos de casos archivados y exportar datos específicos en un informe final.

SIMIS es una herramienta forense de Crownhill EE.UU. que proporciona los medios para extraer los datos de SIMs y USIMs. El expediente del caso se genera en un archivo de formato HTML. Adicionales "SIM vertedero" característica que ofrece un caso más detallado de archivo en un formato de texto ASCII estándar. Un dongle USB que se necesita para operar el software en un ordenador de sobremesa. SIMIS adquiere información de un (U) SIM a través de un PC / SC-lector de tarjetas compatible y genera hashes MD5 y de SHA2 de los datos adquiridos. SIMIS ofrece la posibilidad de crear, señalar el informe, importar archivos de casos archivados, búsqueda de datos.

Soluciones Quantaq USIMdetective, es una herramienta de adquisición de SIM que proporciona a los examinadores la capacidad de adquirir, analizar y producir informes de cualquier tarjeta SIM o USIM utilizando un lector PC / SC compatibles. Elementos adquiridos que se pueden mostrar en un formato de texto o hexadecimal. USIMdetective utiliza una instalación de dispersión interna para garantizar la integridad del caso. Comprobación de integridad de la imagen (.iic), los archivos se crean con cada adquisición de protección contra la manipulación de datos. Hashes MD5 y SHA1 garantizan que el archivo original adquirido es compatible con el expediente reabierto. USIMdetective ofrece varios tipos de salida que van desde un informe "estandard", para una información más detallada "del archivo contenido del informe."

4.2 Capacidades

Las herramientas de software forense se esfuerzan para hacer frente a una amplia gama de dispositivos aplicables a manejar las situaciones más comunes de investigación con los requisitos de modesto nivel de habilidad y mantener el dispositivo intacto. Situaciones más difíciles, tales como la recuperación de datos eliminados, requieren más herramientas y conocimientos técnicos especializados, y a menudo el desmontaje del dispositivo. La gama de apoyo, incluidos los cables de teléfono y los controladores, documentación del producto, (U) SIM de los lectores, y las actualizaciones, puede variar significativamente entre productos. Las funciones que ofrece, tales como la búsqueda, favoritos, y las capacidades de presentación de informes también pueden variar considerablemente.

Las Herramientas forenses para teléfonos móviles están en sus primeras etapas de la madurez. Por lo general tienen limitaciones en tanto la amplitud de los dispositivos de apoyo y la profundidad de la evidencia recolectada. Errores sutiles también se pueden encontrar en su uso. Por ejemplo, un elemento de datos que se muestran en la pantalla pueden variar de la misma partida que figura en un informe generado. La práctica y la experiencia con una herramienta que normalmente pueden compensar estos problemas y los procedimientos pueden ser adaptados en consecuencia. En ocasiones, las nuevas versiones de una herramienta puede no funcionar tan bien como un ejercicio anterior. La característica más importante de una herramienta forense es su capacidad para mantener la integridad de la fuente de datos original que se adquieran y también la de los datos extraídos. El primero se realiza mediante el bloqueo o la eliminación de las solicitudes de escritura para el dispositivo que contiene los datos. Este último se realiza mediante el cálculo de un código criptográfico de los contenidos de las pruebas de los archivos creados y recurrentes, comprobar que este valor se mantiene sin cambios durante todo el ciclo de vida de dichos archivos. Preservar la integridad no sólo mantiene la credibilidad de una perspectiva jurídica, sino que también permite que cualquier investigación posterior para utilizar la misma base de referencia para replicar el análisis.

5. CONSERVACIÓN

La preservación de pruebas es el proceso de incautación de los bienes sospechosos, sin alterar o cambiar el contenido de los datos que residen en los dispositivos y medios extraíbles. Es el primer paso en la recuperación de evidencia digital. A continuación se proporciona una orientación más específica acerca de los teléfonos celulares. La preservación implica la búsqueda, el reconocimiento, la documentación, y la recogida de pruebas electrónicas. Con el fin de recurrir a las pruebas con éxito, ya sea en un tribunal de justicia o de un procedimiento menos formal, que debe ser preservado. La falta de preservar las pruebas en su estado original podría poner en peligro una investigación completa, que puede perder el caso valiosa información relacionada. La guía (según entidades expertas en estos procesos), ofrece los principios, políticas y procedimientos a seguir cuando se encuentran con una escena de pruebas digitales. El lector se dirige a ese informe para obtener información adicional. El siguiente es un resumen de los puntos clave para observar. Aseguramiento y Evaluación de la escena. Garantizar la seguridad de todos los individuos en la escena. Proteger la integridad de las pruebas tradicionales y/o las de

tipo electrónicas que son las más frecuentes. Evalar la escena y formular un plan de búsqueda. Identificar pruebas potenciales para tomarlas como evidencias. Todas las posibles pruebas deben ser garantizadas, documentadas y/o fotografiadas necesariamente. *Realizar entrevistas,* si el caso lo amerita. *Documentando lo refente* la escena. *Crear un registro histórico* permanente de la escena. *Registrar con precisión* la ubicación y condición de las computadoras, medios de almacenamiento y otros dispositivos digitales, y las pruebas convencionales. *Documentar la condición y la ubicación* del sistema informático, incluyendo el estado de energía del ordenador (encendido, apagado o en modo de espera). *Identificar documentos relacionados* con los componentes electrónicos que no serán recogidas. *Fotografiar toda la escena* para crear un registro visual como señaló el primero en responder.

6. PROTECCIÓN Y EVALUACIÓN DE LA ESCENA

Asegurar que las autorizaciones adecuadas (por ejemplo, una orden de registro o el consentimiento del propietario) están en su lugar, es primordial para el comienzo de una investigación. Cuando se busca un sitio, el equipo debe proceder con cautela. Procedimientos incorrectos o la manipulación indebida de un teléfono móvil durante la convulsión puede causar la pérdida de la evidencia digital. Por otra parte, las medidas tradicionales de forenses, tales como huellas dactilares o la prueba de ADN, puede ser necesario aplicar para establecer un vínculo entre un teléfono móvil y su propietario o usuario, o por otras razones. Si el dispositivo no se maneja correctamente, las pruebas físicas pueden ser fácilmente contaminados e inutilizados. El estado de alerta a las características del dispositivo y cuestiones (por ejemplo, la volatilidad de la memoria) y familiaridad con los accesorios correspondientes (por ejemplo, medios de comunicación, cables, soportes, y adaptadores de corriente) son esenciales. Para los teléfonos celulares, fuentes de datos incluyen el dispositivo, (U) SIM, y medios de comunicación. Periféricos asociados, cables, bases, adaptadores y otros accesorios son también de interés. En los alrededores y las habitaciones, excepto en donde se encuentra un dispositivo, debe ser registrada para garantizar lo relacionado con las pruebas que no sea pasado por alto. Para evitar interacciones no deseadas con los dispositivos encontrados en la escena, se debe considerar apagar las interfaces inalámbricas, como Bluetooth y radios WiFi, con relación al equipo llevado a la zona de búsqueda. Equipos asociados con el teléfono celular, tales como los medios extraíbles, (U) SIM, o incluso computadoras personales, posiblemente, sincronizada con él, pueden resultar más útil que el propio teléfono. Los medios extraíbles varían desde el tamaño de una uña a la de un sello de correos, y puede ser fácilmente oculta y difícil de encontrar. Muy a menudo, las tarjetas de memoria extraíbles son identificables por su forma característica y la presencia de clavos, pines recipientes, o los contactos situados en su cuerpo, utilizados para establecer una interfaz eléctrica con el dispositivo.

6. CONCLUSIONES

Debido a que en la actualidad el uso de teléfonos celulares es muy común como también el uso inadecuado, han surgido muchas formas de analizar, evidenciar ciertos crímenes los cuales facilitan la investigación de ciertos crímenes y faltas a la propiedad privada, etc. Por esta razón se ha descrito anteriormente como un experto debe proceder para la recolección de pruebas de un dispositivo móvil, además de la elección de las herramientas forense que puedan realizar un tratamiento cuidadoso en cuanto a estos se refiere. Además de cumplir con políticas que si bien son aplicables generalmente para equipos convencionales de computación, también se aplican en este ámbito.

8. REFERENCIAS

[1] http://www.soyforense.com/page/11/

[2] http://conexioninversa.blogspot.com/2009/04/analisis-forense-dispositivos-moviles.html

[3] http://csrc.nist.gov/publications/nistir/nistir-7387.pdf