Pericias informáticas sobre telefonía celular

Laboratorio Pericial Informático

PROTOCOLO

Autor: Dr. Leopoldo Sebastián GOMEZ, Abogado y Licenciado en Ciencias de la Computación, Perito Informático Oficial

Contenidos

1. Pericias sobre telefonía celular como parte de la especialidad de informática forense

Las pericias sobre telefonía celular forman parte de la actividad pericial informática en lo que refiere a extracción de evidencia digital, tal lo indicado en el apartado 2.a) "Descripción general de servicios de informática forense" del *Protocolo de Actuación para Pericias Informáticas*[1]*. Este tipo de pericias sobre telefonía celular debe ser practicada por un profesional de grado en Ciencias Informáticas.*

En lo atinente a la aplicación de metodología[2] *de informática forense, la actividad pericial informática sobre telefonía celular no difiere de cualquier otra fuente de evidencia digital y se deben respetar las cuatro fases principales, a saber: Identificación de las fuentes de evidencia digital, Preservación de la evidencia digital, Análisis forense y Presentación de los resultados* de la pericia informática.

El origen de las *pericias sobre telefonía celular (Mobile Forensics)* como parte de la especialidad de informática forense se remonta al año 1984, año en el que Federal Bureau of Investigation (FBI) y otras agencias de investigación y apoyo a la Justicia comenzaron a desarrollar programas de especialización para facilitar el análisis de evidencia digital. Actualmente, *la especialidad de informática forense se extiende a todas las áreas donde exista evidencia digital para ser presentada en carácter de prueba científica en el marco de un proceso judicial*.

A fin de reflejar cuestiones atinentes al estado del arte en esta temática, se señalan algunas particularidades propias de la especialidad pericial informática sobre teléfonos celulares:

---

[1] Cfr. "Protocolo de Actuación para Pericias Informáticas", Poder Judicial del Neuquén, aprobado por Acuerdo N°4908, protocolizado y publicado el Boletín Oficial, Neuquén, 2012.

[2] Cfr. "El tratamiento de la evidencia digital", GOMEZ, L., Simposio de Informática y Derecho, Jornadas Argentinas de Informática, Córdoba, 2004.

- En el mercado existe una inmensa variedad de modelos de teléfonos celulares, con sistemas operativos propietarios, sistemas de archivos embebidos, así como también con disponibilidad de aplicaciones, servicios y periféricos. Se requiere conocimiento especializado en informática forense para poder contar el un mayor número de opciones de análisis sobre dichos dispositivos.
- La creciente cantidad de modelos de teléfonos celulares requiere que un perito informático cuente con la mayor cantidad posible de técnicas y herramientas forenses posible y las aplique en función de su experticia.
- Los teléfonos celulares están diseñados para comunicarse con la red de telefonía celular y con otras redes de datos mediante networking vía Bluetooth, Infrarrojo y/o Wi-Fi. La mejor forma de preservar los datos del teléfono celular es aislarlo de las redes cercanas, pero en algunos casos esto podría no ser posible.
- Los teléfonos celulares pueden contar con diversas funcionalidades de almacenamiento de información digital e incluso sincronizar información con repositorios de datos online. Por ello, resulta necesario aplicar más de una herramienta forense para extraer datos de un teléfono celular y sus dispositivos de almacenamiento asociados.
- Existen situaciones en las que las herramientas forenses utilizadas para extraer la información digital de dichos dispositivos podrían tener incompatibilidades o bien emitir reportes con información errónea. Es por ello que siempre que sea posible, resulta esencial verificar la precisión de los datos extraídos desde dichos dispositivos utilizando o complementando las técnicas con más de una herramienta forense.
- Pese a que la cantidad de datos almacenados por los teléfonos celulares es pequeña si se la compara con la capacidad de almacenamiento de información digital que tienen las computadoras, el volumen de información digital contenido en estos dispositivos continúa en aumento.
- Los tipos de datos contenidos en los teléfonos celulares y la forma en que éstos son utilizados está en evolución constante. La popularidad de los llamados teléfonos inteligentes (smart phones) hacen que ya no sea suficiente la extracción de agendas de contactos, históricos de llamadas, mensajes de texto, fotografías digitales, entradas de agenda personal, notas y otros archivos multimedia. Muchas aplicaciones instaladas en dichos dispositivos deben ser analizadas, ya que pueden contener información sensible como contraseñas, datos de geolocalización o históricos de navegación en Internet.
- Las formas de extraer datos desde los teléfonos celulares podrían variar dependiendo de las técnicas que se utilicen para ello. Dependiendo de la finalidad y profundidad con la que se requiera determinada información en el marco de una investigación judicial podrían requerirse solamente algunos datos del teléfono celular o bien una extracción completa del sistema de archivos embebido y/o de la memoria física del teléfono.

El teléfono celular es una fuente de evidencia digital sobre la que aplican procedimientos operativos estándares (SOPs), al igual que en otras actividades periciales de informática forense. Los buenos SOPs no deben contener o mencionar el nombre del hardware/software, ya que ello requiere de la experticia del perito informático a la hora de seleccionar la herramienta de informática forense que le ofrece los mejores resultados para el caso.

2. Procedimiento para pericias informáticas sobre telefonía celular

1. Verificar que el requerimiento judicial cumpla las pautas establecidas en el apartado d) del Protocolo de Actuación para Pericias Informáticas ("*Del requerimiento judicial*")
2. Priorizar el caso conforme los criterios detallados en el apartado e) del Protocolo de Actuación para Pericias Informáticas ("*De la priorización de casos urgentes*")
3. Dar ingreso al material probatorio siguiendo los lineamientos del apartado f) del Protocolo de Actuación para Pericias Informáticas ("*Del traslado y recepción del material secuestrado*")
4. Determinar si el teléfono celular está encendido o apagado
    a. Si está apagado, debe quedar apagado
    b. Si está encendido debe ser aislado de la red de telefonía celular lo antes posible con la opción que se estime apropiada:
        i) Configurando el modo "Avión" en el teléfono celular, si lo permite
        ii) Colocándolo en una caja de Faraday
        iii) Encendiendo un inhibidor de señal en cercanía del teléfono celular
        iv) Envolviéndolo con tres o más capas de papel de aluminio
        v) Apagando el teléfono y retirando la batería
5. Obtener información sobre el modelo del teléfono celular y planificar la estrategia para la extracción de evidencia digital
    a. Identificar la tecnología general del teléfono celular
    b. Localizar cables, drivers y determinar el software o hardware forense a utilizar para la pericia informática. La selección de herramientas forenses para una pericia informática sobre telefonía celular depende de diversos factores, como el nivel de detalle requerido en los puntos de pericia, el modelo de teléfono celular en cuestión y la presencia de otras funcionalidades de almacenamiento externo del dispositivo
    c. Determinar funcionalidades del teléfono celular y posibles datos almacenados en el mismo
    d. Si el teléfono celular no tiene puerto de datos, no se cuenta con el cable de datos, o no existe software o hardware forense disponible para dicho modelo, se registra esta situación
6. Consultar las especificaciones técnicas del teléfono celular y sus capacidades de almacenamiento de datos. Se recomienda los sitios web www.phonescoop.com o www.mobileforensicscentral.com
7. Preservar y analizar las fuentes de evidencia digital siguiendo las pautas prescriptas en el Protocolo de Actuación para Pericias Informáticas ("*Del análisis forense*")
    a. Tarjeta de Memoria Externa
        i. Realizar una imagen forense con la herramienta de informática forense apropiada
        ii. Extraer la evidencia digital que resulte relevante conforme los puntos de pericia que hayan sido indicados
    b. Tarjeta SIM
        i. Generar una SIM clonada o leer la información digital de dicho dispositivo utilizando un lector de SIM protegido contra escritura
        ii. Si el SIM está bloqueado por PIN, se deja constancia o se utiliza el PUK en caso de estar disponible
        iii. Si el SIM no está bloqueado, se extrae la información digital relevante al caso
    c. Equipo de telefonía celular
        i. Aislar el dispositivo de la red de telefonía celular previamente a la extracción de información digital y si es posible, durante todo el proceso.

ii. Realizar una extracción física de la memoria del teléfono celular o bien una extracción lógica utilizando todas las herramientas forenses apropiadas, tanto de hardware como de software

iii. Verificar los resultados obtenidos

1. Que los datos de salida tengan el formato adecuado al tipo de dato asociado
2. Que las fechas y horas sean consistentes
3. Que todos los datos requeridos pudieron ser extraídos
    a. Mediante comparación con datos obtenidos desde el teléfono celular
    b. Utilizando más de una herramienta forense y comparando resultados
    c. Validando mediante valores hash distintos artefactos digitales del teléfono celular

8. Documentar los resultados en un reporte informático forense
9. Elaborar el dictamen para dar respuesta a los puntos de pericia informática haciendo referencia a la evidencia digital detallada en el reporte informático forense, siguiendo las pautas establecidas en el apartado h) del Protocolo de Actuación para Pericias Informáticas ("*De la presentación del dictamen*")
10. Remitir el dictamen junto a los elementos probatorios siguiendo los lineamientos de apartado i) del Protocolo de Actuación para Pericias Informáticas ("*De la remisión del material secuestrado*")

Sin perjuicio de los pasos indicados en la guía de procedimiento para pericias informáticas sobre telefonía celular, el perito informático debe aplicar los conocimientos especializados sobre la materia y tener presente los aportes de otras guías de mejores prácticas y de procedimiento a nivel internacional. Se detallan algunos de los documentos de referencia que se utilizan en el Laboratorio Pericial Informático para las pericias informáticas sobre telefonía celular.

1. NIST(2007), Guidelines on Cell Phone Forensics, http://csrc.nist.gov/
2. ACPO & 7Safe (2008), Guide for Mobile phone seizure and examination. Good Practice Guide for Computer-Based Electronic Evidence, http://www.7safe.com/
3. SWGDE (2013), SWGDE Best Practices for Mobile Phone Forensics, , https://www.swgde.org/
4. Ayers, R., Dankar, A. & Mislan, R. (2009). Hashing Techniques for Mobile Device Forensics. *Small Scale Digital Device Forensics Journal* , 1-6.
5. Brothers, S. (2011). How Cell Phone "Forensic" Tools Actually Work - Cell Phone Tool Leveling System. *DoD Cybercrime Conference. 2011.* Atlanta, GA
6. Kessler, G. (2010). Cell Phone Analysis: Technology, Tools, and Processes. *Mobile Forensics World.* Chicago: Purdue University.
7. Mislan, R.P., Casey, E., & Kessler, G.C. (2010). The Growing Need for On-Scene Triage of Mobile Devices. *Digital Investigation*, *6*(3-4), 112-124
8. Murphy, C. (2009). The Fraternal Clone Method for CDMA Cell Phones. *Small Scale Digital Device Forensics Journal* , 4-5.
9. Murphy, C. (2010), *Digital Forensics Magazine*, http://digitalforensicsmagazine.com/blogs/?p=80
10. Punja, S & Mislan, R. (2008). Mobile Device Analysis. *Small Scale Digital Device Forensics Journal, Vol. 2, No. 1* , 2-4.

3. Uso de UFED como una de las herramienta de informática forense aplicable en el marco del procedimiento para pericias informáticas sobre telefonía celular

La herramienta de informática forense UFED puede ser utilizada sobre dispositivos de telefonía celular para dar respuesta a los servicios ofrecidos a los operadores judiciales de "Pericia sobre telefonía celular". Dicha actividad se encuentra indicada en el apartado denominado "Catálogo de Servicios" del "Protocolo de Actuación para Pericias Informáticas".

IMPORTANTE: Esta herramienta de informática forense se aplica a criterio facultativo del Perito Informático en el punto 7) del "Procedimiento para pericias informáticas sobre telefonía celular". Si se requiere, puede utilizarse en dicho paso el manual de usuario de la herramienta de informática forense UFED.

UFED tiene como punto favorable una gran cobertura de modelos telefónicos, pero como toda herramienta de informática forense tiene limitaciones y no excluye la aplicación de otras técnicas especializadas y herramientas de informática forense durante la realización de una pericia informática sobre dispositivos de telefonía celular.

El hardware de informática forense UFED tiene posibilidades de realizar extracciones lógicas y físicas. Con la primera modalidad de trabajo es factible recuperar evidencia digital desde el sistema de archivos embebido que es administrado por el sistema operativo del dispositivo. La segunda opción permite realizar una extracción completa de información digital almacenada en la memoria del dispositivo y en la tarjeta SIM, permitiendo obtener datos eliminados y otra información digital interna del teléfono celular.

Este dispositivo permite desbloquear algunos modelos de teléfonos celulares que hayan sido protegidos con una contraseña, pero no tiene capacidad de desbloquear las protecciones de la tarjeta SIM mediante el uso de PIN (Personal Identification Number). En estos casos se puede intentar hacer una clonación de la tarjeta SIM para acceder a la evidencia digital contenida en la memoria interna del dispositivo, pero si no es posible conocer a priori el PIN o el PUK (Personal Unlocking Key) se pierde la posibilidad de extraer la información digital del SIM.