Type of the Paper (Article)

Análisis forense para Móviles

Danilo Andrés Medina Gómez [1], Miguel Hernández Bejarano [2],*

[1] Fundación Universitaria Los Libertadores; damedinag@libertadores.edu.co
[2] Fundación Universitaria Los Libertadores; mhernandezb@libertadores.edu.co
* Correspondence: damedinag@libertadores.edu.co

Received: 30/11/2020; Accepted: 15/11/2020; Published: 31/12/2020

Abstract: Este artículo trata de dar a conocer el análisis y la metodología que se deben realizar al momento de hacer un análisis forense a dispositivos móviles que sirva como evidencia para para un caso. También se mencionarán diferentes tipos de software forense que nos ayudan con la tarea de obtener la información de forma tal que puede ser tomada como evidencia.

Keywords: análisis forense; evidencia digital; teléfonos inteligentes; XRY

1. Introducción

En la actualidad se ha visto un gran incremento en la venta de dispositivos móviles, según estudio realizado por Cisco para el año 2015 se tenía alrededor de 5.500 millones de usuarios conectados y se estima que para el año 2020 será de 7.800 millones lo que equivale al 70% de la población mundial [1]. Como lo dice Debra Littlejohn el nacimiento de nuevas tecnologías crea un sin número de nuevas vulnerabilidades [2].

En este orden de ideas se puede evidenciar que un gran número de personas puede ser víctima de un ataque, sino que también existe una gran posibilidad de obtener información de estos dispositivos que aporten pruebas para una investigación. Así nos podemos dar cuenta de la importancia de conocer las técnicas forenses de alta calidad con el fin de obtener evidencia física de índole digital [3].

2. Marco teórico

INFORMATICA FORENSE: Según una publicación hecha por NITS (Instituto Nacional de Estándares y Tecnología), Directrices sobre informática forense para dispositivos móviles. La ciencia forense de dispositivos móviles es la ciencia de la recuperación de evidencia digital de un dispositivo móvil bajo condiciones forenses sólidas usando métodos aceptados [4].

EVIDENCIA DIGITAL: es cualquier valor probatorio de la información almacenada o transmitida en formato digital de tal manera que una parte o toda puede ser utilizada en el juicio [5].

Para que la evidencia sea aceptada y valga como soporte en un proceso judicial debe cumplir con los criterios de admisibilidad. Existen cuatro criterios que se deben cumplir para que la evidencia sea aprobada, estos son: la autenticidad, respeto por las leyes y reglas del poder judicial [6].

PROCEDIMIENTO OPERATIVO ESTANDARIZADO: Un SOP es un proceso desarrollado para efectuar una rutina con tiempo y recursos limitados. La importancia de un SOP adecuado a la estructura de un equipo profesional reside en el uso habitual de un procedimiento operativo escrito que está acoplado a un ambiente de trabajo y vinculado a la aplicación de técnicas y operación de herramientas, cuyo contenido está ordenado mediante texto, gráficos y otras especificaciones [7].

XRY: es un software diseñada únicamente para Windows que permite ejecutar una extracción forense segura de los datos digitales de una gran variedad de dispositivos móviles, como Smartphone, unidades de seguimiento y navegación gps, módems 3g, reproductores de música portátiles y procesadores Tablet de última generación como el iPad [8].

Para el autor Cano, se define unos principios los cuales se deben tener en cuenta al momento de realizar este procedimiento:

- Esterilidad de los medios informáticos
- Verificación de las copias en medios informáticos
- Documentación de los procedimientos, herramientas, resultados sobre los medios informáticos.
- Mantener la cadena de custodia
- Informe y presentación de los resultados del análisis de los medios informáticos
- Administración del caso realizado
- Auditoria de los procedimientos realizados [9]

2.1 Evidencia Digital

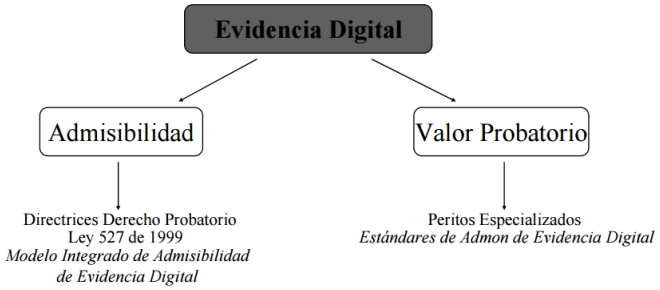

Fig. 1. Evidencia digital [10]

En la figura 1 vemos los conceptos que debemos tener en cuenta al momento de obtener evidencia digital

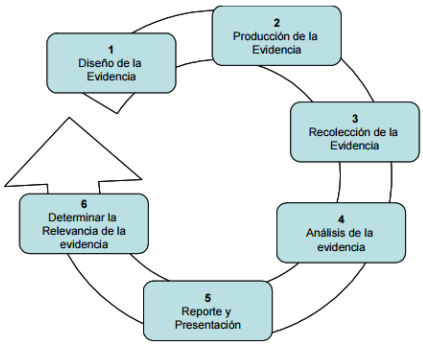

Fig. 2. Ciclo de evidencia digital [11]

A continuación, se explicará el ciclo de administración de la evidencia digital:

Diseño de la evidencia

Clasificación de la información de forma organizada para identificar la información más relevante.

Establecer tiempos de retención de documentos electrónicos, la transformación de éstos (cambios de formato) y la disposición final de los mismos

Utilización de medidas tecnológicas de seguridad informática para validar la autenticidad e integridad de los registros electrónicos. Tecnologías como token criptográficos, certificados digitales entre otras que podrían ser pretendientes para esta práctica.

La infraestructura tecnológica debe cerciorar la sincronización de las maquinas y/o dispositivos que generen la información, de tal manera que se pueda identificar con claridad de fecha y hora de los registros electrónicos.

Producción de la evidencia

Desarrollar y documentar un plan de pruebas formal para la correcta exportación de los registros.

Plantear mecanismos de seguridad basados en certificados digitales para las aplicaciones de tal forma que se pueda validar que es la aplicación la que genera los registros electrónicos.

Diseñar y mantener un control de calidad de los registros electrónicos, que permita encontrar cambios que se hayan presentado en ellos.

Recolección de evidencia

Establecer un criterio de recolección de la evidencia digital.

Documentar todas las acciones que se realizaron durante la recogida de información

Registrar en medio fotográfico o video la escena de posible ilícito, informando los elementos informáticos allí involucrados

Análisis de evidencia

Hacer copias autenticadas de los registros originales

Validar y verificar la confiabilidad y limitaciones de las herramientas de hardware y software utilizadas para adelantar los análisis de los datos.

Aplicaciones que generen registros electrónicos.

Reporte y presentación

Salvaguardar una copia de la cadena de custodia y de la notificación oficial para adelantar la investigación de los registros electrónicos

Incluir las irregularidades encontradas

Preparar una presentación de manera que las partes observe claramente el contexto del caso y las evidencias identificadas.

Detallar las conclusiones de los análisis realizados.

Contar con un formato de presentación de informe de análisis de evidencia.

Determinar la relevancia de la evidencia

Demostrar con hechos y documentación que los procedimientos aplicados para recolectar y analizar electrónicos fueron razonables y robustos.

Verificar y validar con pruebas que los resultados obtenidos luego de efectuar el análisis de los datos.

Auditar diariamente los procedimientos recolección y análisis

Fortalecer las políticas, procesos y procedimientos de seguridad de la información.

Procurar certificaciones profesionales y corporativas en temas afines con computación forense y seguridad informática.

3. Recomendaciones para hacer un analisis forense

En todo tipo de análisis forense, se deben realizar ciertos procedimientos en el manejo de la evidencia digital, que son la identificación, recolección, adquisición y preservación de la evidencia que puede ser probatorio para los siguientes dispositivos [10]:

Medios de almacenamiento digitales utilizados en ordenadores estándar como discos duros, disquetes, discos ópticos y magnetoópticos, dispositivos de datos con funciones similares,

Teléfonos móviles, asistentes personales digitales (PDA), dispositivos electrónicos personales (PED), tarjetas de memoria,

Los sistemas de navegación móvil,

Cámaras digitales fijas y de video (incluyendo CCTV)

Ordenador estándar con conexiones de red,

Redes basadas en TCP / IP y otros protocolos digitales

Dispositivos con funciones similares a las anteriores [12].

La recuperación de datos en móviles es usualmente realizada de forma lógica en lugar de una adquisición física, usando uno o más protocolos soportados por el dispositivo [13].

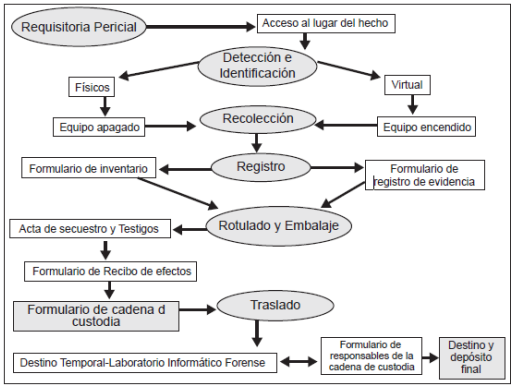

Fig. 3. Protocolo para la cadena de custodia en la pericia informático forense

Síntesis, la validez de la prueba informática depende del mantenimiento de la seguridad, de procurar el resguardo legal y del seguimiento de una metodología estricta. De este modo, en el lugar del hecho habrá de seguir una secuencia de pasos mencionadas en el siguiente procedimiento que se considerará como etapa preliminar a la elaboración del formulario de la cadena de custodia [14].

3.1 Analisis de Sim

Una tarjeta SIM es una tarjeta inteligente desmontable y usada en teléfonos móviles que almacena de forma segura la clave de servicio del suscriptor usada para identificarse ante la red [15].

La SIM, en la mayoría de los casos, se asocia a un chip o tarjeta inteligente (Smart Card) [16].

Las principales características de la sim, desde el análisis forense, son su portabilidad y memoria, capaz de almacenar datos con información del portador en un espacio de almacenamiento que esta alrededor de los 64kB [17].

Un primer acercamiento forense de la SIM debe procurar mostrar los siguientes datos:

Identificador de dónde está el dispositivo actualmente situado (o dónde estuvo antes de apagarse el celular).

IMSI (número serial que identifica al suscriptor)

CCID (número serial que identifica la SIM)

Contactos telefónicos

Mensajes de texto (o multimedia, si es el caso) Borrados
Mensajes de texto enviados y guardados en la SIM.
Números marcados (a veces este dato no se guarda en la SIM) [18].

3.2 Analisis del ME

El equipo móvil (ME) es el módulo en donde normalmente ocurre el grueso del análisis. Aunque el análisis del SIM puede dificultarse si este tiene algún Applet diferente a los proporcionados por el operador, lo normal es que no lo tenga, el análisis en la mayoría de los casos se limita a buscar en 64KB de datos. Por otro lado el ME, dependiendo de la gama, puede almacenar hasta 8 GB de información como es el caso del Smartphone [18].

Los pasos para efectuar un análisis varían dependiendo de la gama del dispositivo. Esto se debe a que los teléfonos de gama baja se limitan simplemente a guardar información básica del usuario, tal como [19]:

Fecha y hora de llamadas realizadas, recibidas y perdidas.
Fecha y hora de los Mensajes de texto recibidos, enviados y borrador.
Registro de llamadas borradas.
Contactos telefónicos
Log de las páginas Wap y Web visitadas
Imágenes y fotos.

En cambio, los teléfonos de gama alta pueden tener información comparable a la que tiene un computador. Para este tipo de dispositivos, dentro de los cuales se encuentran los Smartphone, se proponen de forma general los siguientes pasos para realizar un análisis forense:

Creación del archivo de hallazgos (documento que permite llevar un historial de todas las actividades que se llevan a cabo durante el proceso y de los hallazgos encontrados)
Imagen de datos (o backup cuando no sea es posible realizar la imagen)
Verificación de integridad de la imagen
Creación de copias de la imagen suministrada
Aseguramiento de la imagen suministrada
Revisión antivirus y verificación de la integridad de la copia de la imagen.
Identificación de las particiones actuales y anteriores (las que sea posible recuperar Esto se hace importante en los drives removibles (memorias flash removibles).
Detección de información en los espacios entre las particiones. Para no utilizar el ME de forma física, es muy útil el uso de los emuladores proporcionados por los fabricantes de teléfonos. De esta forma no se corrompe la evidencia.
Detección de las HPA - Host Protected Areas. Se deben utilizar emuladores hasta donde sea posible.
Identificación del sistema de archivos [18].

4. Metodología para el análisis forense

Para realizar un análisis forense a un dispositivo móvil, es indispensable contar con el equipo necesario, no solo para investigar sino también para proteger la lealtad de los datos a analizar, de forma tal que la información adquirida sea válida como prueba[20].

Fases del análisis forense:

- Asegurar la escena
- Identificar la evidencia
- Adquisición de la evidencias
- Análisis e investigación de la evidencia

- Informe pericia [21]

En el presente existen herramientas de *Open Source* como de uso comercial, permiten: adquirir, analizar y generar reportes de la investigación. Entre las herramientas más conocidas se puede nombrar: open source (Sistema Operativos Kali Linux, Santoku Linux que contiene herramientas para el análisis forense y auditoría digital) de uso comercial (Oxigen Forensic Kit, Andriller, Cellebrity, MSAB).

Para el artículo se estudiarán solo tres herramientas

4.1 MSAB

Esta herramienta contiene las soluciones de XRY necesarias para que los investigadores puedan tener acceso a todos los métodos posibles para recuperar datos en los diferentes dispositivos móviles. Este procedimiento está basado en aplicaciones de software, que permiten extraer la información almacenada en este tipo de dispositivos y además permiten analizar el contenido de ha sido obtenido durante la extracción [20].

El paquete MSAB incluye:

- Software de la aplicación XRY y clave de licencia
- Unidad de comunicación XRY
- Kit de cable de teléfono móvil XRY Physical
- Dispositivo SIM id-Cloner con licencia de 12 meses
- Lector de tarjeta de memoria con protección de escritura
- Accesorios y cepillo de limpieza
- Soporte telefónico gratuito, foro en Internet o por correo electrónico
- Mantenimiento y actualizaciones de software gratuitos por 12 meses

En la figura 4 encontramos al lado izquierdo del notebook el maletín con el kit de cableado, con sus accesorios y cepillo de licencia.

Fig. 4. Kit de Oficina MSAB [22]

MSAB suministra software en diferentes plataformas de hardware. Estas plataformas se dividen en dos categorías, abierto y llave en mano. Las plataformas abiertas (oficina y de campo) están diseñados para equipos tradicionales de Windows. Plataformas llave en mano (Kiosk y Tablet) son más fáciles de usar sistemas a través de interfaces de pantalla táctil [22].

4.2 Cellebrite

Cellebrite es una nueva generación de soluciones para el análisis forense a dispositivos móviles.

Cellebrite permite la extracción, decodificación, análisis y generación de informes de datos móviles. También realiza extracciones físicas y lógicas de archivos y contraseñas de todos los datos (incluido los borrados). Funciona tanto en equipos tradicionales como en Smartphone, dispositivos gps, portátiles y tabletas [23].

4.3 Oxygen Forensic Detective

Es un software forense para la extracción y análisis de datos de teléfonos celulares, Smartphone y tabletas. Usando protocolos propietarios que le permitan extraer mucho más datos garantizando su funcionamiento de footprint cero, sin dejar rastros y sin hacerle modificaciones al contenido [24].

5. Conclusiones

Este artículo menciona los protocolos y métodos que se deben tener en cuenta para poder realizar un análisis forense obteniendo información que pueda ser tenida en cuenta como prueba para un caso.

Adicionalmente se menciona varios softwares que se encuentran vigentes y actualizados para poder obtener toda la información necesaria de forma segura y documentada.

También se muestra explica de forma eficaz como se debe hacer el análisis forense en un dispositivo móvil, explicando y mostrando las diferencias entre el SIM y el ME.

References

Bibliografía

[1] Cisco, «Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020 White Paper,» 1 Febrero 2016. [En línea]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html?CAMPAIGN=Mobile+VNI+2016&COUNTRY_SITE=us&POSITION=Press+Release&REFERRING_SITE=PR&CREATIVE=PR+to+WP.

[2] D. L. Shinder, «Scene of the Cybercrimen: Computer Forensics Handbook.,» de Scene of the Cybercrimen: Computer Forensics Handbook., Technical, 2002, pp. 62 - 90.

[3] C. A. y. R. Hernández., «Analisis Forense en Dispositivos Moviles Con Symbian os,» Junio 2008. [En línea]. Available: http://artemisa.unicauca.edu.co/~rhernandez/articulos/Articulo_UPM-Criptored_Symbian_OS_Forensics_UJaveriana.pdf.

[4] N. I. o. S. a. Technology, «Guidelines on Mobile Device Forensics,» Mayo 2014. [En línea]. Available: http://csrc.nist.gov/publications/PubsSPs.html#800-101.

[5] I. F. Colombiana, «Informatica Forense Colombiana,» 30 Diciembre 2015. [En línea]. Available: http://www.informaticaforense.com.co/index.php/la-evidencia-digital.

[6] j. S. R. R. y. D. R. Bautista, «Analisis Forense digital en Dispositivos moviles,» Ufpso, vol. 1, nº 4, p. 4, 2014.

[7] L. S. Gomez, «Análisis forense de dispositivos de telefonía celular,» Simposio Argentino de Informatica y Derecho, [En línea]. Available: http://sedici.unlp.edu.ar/bitstream/handle/10915/55345/Documento_completo.pdf-PDFA.pdf?sequence=1. [Último acceso: 26 10 2016].

[8] MSAB, «MSAB,» Septiembre 2015. [En línea]. Available: https://www.msab.com/download/product_sheets/spanish_product_sheets/What%20is%20XRY%20ES.pdf.

[9] J. J. Cano, «Introduccion a la Informatica Forense,» Sistems 91, nº 2, pp. 64-73.

[10] J. J. Cano, «Administracion de la Evidencia Digital,» GECTI, p. 7, 2006.

[11] A. Ghosh, «Guidelines for the Management of IT Evidence,» p. 27, 2004.

[12] ISO, «ISO/IEC 27037:2012 Information technology Security techniques Guidelines for identification, collection, acquisition and preservation of digital evidence,» 15 Octubre 2012. [En línea]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=44381.

[13] C. A. y. R. Hernández, «Análisis forense en dispositivos móviles con Symbian OS,» [En línea]. Available: http://www. criptored. upm. es/guiateoria/gt_m142e1. htm.. [Último acceso: 2016].

[14] L. E. A. y. C. M. Castañesa, «La Cadena de Custodia Informatico - Forense,» Activa, pp. 67-81, 2012.

[15] P. S. Cordero, «Analisis Forense a Tarjetas SIM,» 2011. [En línea]. Available: http://conexioninversa.blogspot.com.co/2009/07/analisis-forenses-tarjetas-sim.html.

[16] A. S. P. G. Fabio Casadei, «Forensics and SIM cards: an Overview,» 2006. [En línea]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.160.4644&rep=rep1&type=pdf.

[17] R. P. A. Wayne Jansen, «Forensic Software Tools for Cell Phone Subscriber Identity Modules,» 20 Abril 2006. [En línea]. Available: https://www.nist.gov/node/624931.

[18] C. A. y. R. Hernández, «Analisis Forense en Dispositivos Moviles Con Symbian os,» Junio 2008. [En línea]. Available: http://artemisa.unicauca.edu.co/~rhernandez/articulos/Articulo_UPM-Criptored_Symbian_OS_Forensics_UJaveriana.pdf.

[19] G. D. Presman, «Introduccion al Analisis Forense de Dispositivos Moviles,» 21 Julio 2010. [En línea]. Available: http://www.presman.com.ar/admin/archivospublicaciones/archivos/Analisis%20forense%20de%20celulares_20100721064941.pdf.

[20] o. internacional, «ondatashop,» 2016. [En línea]. Available: http://www.ondata.es/recuperar/analisis-forense-moviles.htm. [Último acceso: 18 10 2016].

[21] M. A. A. murillo, «Analisis Forense de Dispositivos Moviles iOS y Android,» 04 Enero 2016. [En línea]. Available: openaccess.uoc.edu/webapps/o2/bitstream/10609/.../malvarezmuTFG0116memoria.pdf.

[22] MSAB, «plataforma MSAB,» 2016. [En línea]. Available: https://www.msab.com/products/msab-platforms/#tablet. [Último acceso: 20 10 2016].

[23] Cellebryte, «Cellebrite delivering mobile expertise,» 2016. [En línea]. Available: http://www.cellebrite.com/es/Mobile-Forensics/Solutions. [Último acceso: 25 10 2016].

[24] O. Forensics, «Oxygen Forensic® Detective Características,» Octubre 2016. [En línea]. Available: http://www.oxygen-forensic.com/es/products/oxygen-forensic-detective.