Artículos de Revisión

La informática forense en dispositivos Android

The computer forensic in android device

Notas de autor

dwricob@ufpso.edu.co

Dewar Rico Bautista
Universidad Francisco de Paula Santander Ocaña , Colombia
dwricob@ufpso.edu.co

Johan Smith Rueda Rueda
Universidad Francisco de Paula Santander Ocaña, Colombia
jsruedar@ufpso.edu.co

Resumen: En este artículose estudian los principales conceptos de la informática forense. Qué es la informática forense, cuáles son sus objetivos y sus principios. También se mencionan algunas técnicas anti-forenses, el manejo de la evidencia digital, los modelos forenses y la legislación colombiana relacionada con la evidencia digital. Se hace énfasis en las buenas prácticas para la realización de un análisis forense.

Palabras clave: Análisis forense digital móvil, Dispositivos Android, Estado del arte, Informática forense.

Revista Ingenio
vol. 9, núm. 1, p. 116 - 129, 2016
Universidad Francisco de Paula Santander, Colombia
ISSN: 2011-642X
ISSN-E: 2389-864X
Periodicidad: Anual
revistaingenio@ufpso.edu.co

Recepción: 05 Abril 2016
Aprobación: 11 Mayo 2016

URL: https://portal.amelica.org/ameli/journal/814/8145122011/

Abstract: In this state of the art the main concepts of computer forensic are studied. What is the computer forensic, what are its target and principles. Some things mentioned below: anti-forensic techniques, forensic models and Colombian legislation related to digital evidence. Emphasis on good practices for conducting a forensic analysis is done.

Keywords: Android Device, Forensic Computer, Mobile Forensic Analysis, State of the Art.

1. INTRODUCCIÓN

La evolución de los dispositivos móviles ha aumentado considerablemente en los últimos años, ha pasado de ser simples celulares a computadores de mano. Por esta razón, las actividades cotidianas de las personas como revisar correos electrónicos, redes sociales, sitios de interés, incluso la banca online, han pasado a realizarse en dichos dispositivos. Éstos, se han convertido en una extensión de la vida diaria de la personas, tanto personal como laboralmente.

Con el aumento del uso del dispositivos móviles, el mercado destinado a estas terminales ha crecido fuertemente: los servicios ofrecidos, las aplicaciones cada día son más numerosas. Ya se puede estar conectado desde cualquier lugar, a la hora que se desee. Pero estos beneficios no son gratis. Esto ha traído grandes beneficios para los usuarios por la comodidad; para las empresas porque pueden ofrecer un mejor servicio, pero también, llama la atención de personas y cibercriminales que han visto un gran mercado y que en los últimos años su explotación ha estado en aumento, sacando provecho para sus intereses personales o económicos a travésde los diferentes delitos informáticos (Congreso de la República de Colombia, 2009). Los dispositivos móviles están expuestos a un sinnúmero de peligros, al igual que los computadores y otros equipos que estén conectados a la red. Pero el hecho de estar desconectado no te blinda de las amenazas informáticas (Jaramillo, 2011).

Los peligros a los que están expuesto los usuarios de un dispositivo móvil son los mismos que para cualquier usuario de otro equipo informático. Algunas de estas amenazas son: malware, spam, phishing, robo o extravío físico del dispositivo (Eset , 2012) - (Jakobsson & Ramzan, 2008).

Un informe de Symantec sobre plataformas móviles y su seguridad, describe algunos problemas relacionados con el sistema operativo Android: Google no tiene un modelo de certificación riguroso de aplicaciones, lo que permitió el creciente volumen se software malicioso. Android brinda mucho control a las aplicaciones sobre las funcionalidades del dispositivo, y deja en manos del usuario la decisión de otorgarla o no los permisos, de esta forma el riesgo es mayor (Symantec Corp., 2011).

Android sigue siendo la plataforma más popular entre los usuario y también entre los cibercriminales, siendo el principal blanco entre todas las plataformas móviles. Según *Kaspersky Security Network*, el 99% de las muestras de malware actuales analizadas por dicho laboratorio de seguridad están dirigidas a dispositivos móviles se han desarrollado para esta plataforma. También aclara que hay dos

razones principales por las que los cibercriminales están interesados en Android: su popularidad y su funcionalidad (Kaspersky Lab, 2013).

Estudios realizados recientemente en España por *IAB Spain*, da como resultados que el 100% de los encuestados usan teléfono móvil, que otros dispositivos móviles van en aumento como las tabletas (de 43 % en el 2013 a 57 % en 2014) y los *e-reader* (se ha mantenido constante en los últimos dos años con el 23%). Cada vez se ve el uso de 'smartphone', con un 87 % del uso total de móviles, los equipos móviles 3G y los básicos van disminuyendo. Una de las razones del aumento de los teléfonos inteligentes es el bajo costo de muchos modelos (IAB Spain, 2014).

En Colombia, un estudio realizado por el Ministerio de las TIC afirma que el 42 % de las personas cuenta con teléfono inteligente, y que el 34 % accede a internet desde su dispositivo móvil. En cuanto al tipo de dispositivo móvil que usan para acceder a Internet, el computador conserva el primer lugar, procedido por la tableta (MinTIC & Ipsos Napoleón Franco, 2013).

En 2015, de los usuarios de Internet en Colombia el 81 % se conecta a través de su celular, teniendo un incremento del 41 % con respecto al periodo 2012-2013. El 55 % de los usuarios usan los teléfonos inteligentes y las tabletas, el 37 % solo usa teléfonos inteligente, el 4 % tabletas solamente y el 4 % de los usuarios solo utiliza las computadoras de escritorio (HEADWAY Digital, 2015).

En cuanto a los sistemas operativos para dispositivos móviles, en el segundo trimestre del 2015, el mercado a nivel mundial está dominado por Android con el 82.8 %, seguido de los sistemas operativos de Apple con un 13.9 %, seguido por Windows Phone y Blackberry OS (IDC Analyse the Future, 2015). En Colombia se mantiene la tendencia mundial, Android tiene el 78 %, iOS con el 15 % y otros sistemas operativos tienen el 7 % (HEADWAY Digital, 2015).

El amplio crecimiento de las aplicaciones para este sistema operativo es uno de sus puntos a favor, según Google Inc. son un poco más de 1,3 millones (Google Inc. , 2015).

Con el aumento del mercado móvil, la cantidad y la importancia de la información que se confía a estos dispositivos también crecerán los ataques, intrusiones y demás peligros informáticos.

Por eso en necesario es la implementación de políticas que ayuden a mitigar estos ataques, la sensibilización a los usuarios y, en caso tal que ocurra una intrusión poder establecer los hechos relevantes en la investigación, y esclarecer los hechos. Es allí donde entra la informática forense.

2. INFORMÁTICA FORENSE

La computación o informática forense es un área que se ha venido desarrollando desde la última década del siglo XX. Esta área es el resultado de una necesidad: obtener una nueva fuente de material probatorio. Las escenas criminales no solo se limitaba a pruebas balísticas, muestras de sangre, sino que también, los elementos electrónicos podrían brindar pistas, ayudar a formalizar una hipótesis y llevar a resolver un caso judicial.

Existen muchas definiciones en el tema de la informática forense, y surgen a la par términos que la describen de una manera más general y otras más específicas. La computación forense (Computer Forensics) se puede interpretar de dos maneras: «1. Disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia, procura describir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso; o 2. Como la disciplina científica y especializada que entendiendo los elementos propios de la tecnologías de los equipos de computación forense ofrece un análisis de la información residente en dichos equipos» (Cano, 2009).

Otra definición que puede describir lo que es un análisis forense es: enfoque científico que aprovecha efectos electromagnéticos para «recolectar, analizar, verificar y validar todo tipo de información existente, o información que se considerada como borrada» usando un conjunto de herramientas y técnicas (Arias Chaves, 2006). Esta área, al tener un enfoque científico cuenta con principios que rigen la forma como se debe llevar dicho análisis, para garantizar su veracidad e integridad, ver Fig. 1. Para esta finalidad se creó la IOCE (*International Organization of Computer Evidence*) (Rodríguez & Doménech, 2011).

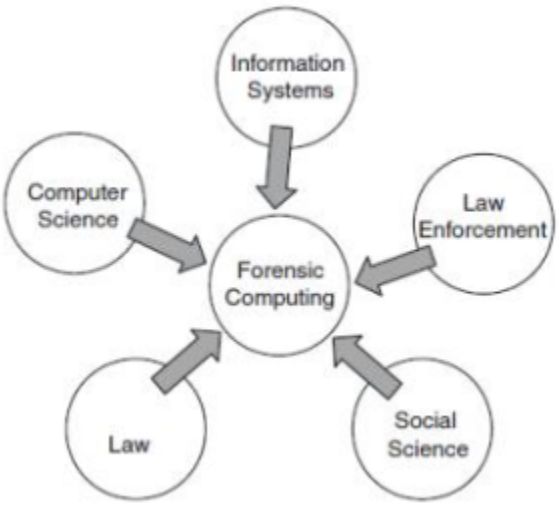

Figura 1
Dominio de la informática forense.
(Broucek & Turner, 2006)

Se puede encontrar diferentes tipos análisis forenses: análisis forense de sistemas (servidores, estaciones de trabajo), análisis forense de redes (cableadas, *wireless, Bluetooth*, etcétera) y análisis forense de sistemas embebidos (móviles, PDS, entre otros) (Rifà, Serra, & Rivas, 2009).

Independientemente del tipo de análisis, la informática forense tiene tres objetivos: 1. La compensación de los daños causados por los criminales o intrusos; 2. la persecución y procesamiento judicial de los criminales y 3, la creación y aplicación de medidas para prevenir casos criminales (Zuccardi & Gutiérrez, 2006). Y para lograr estos objetivos, la principal forma es la recolección de evidencia (Wang, Cannady, & Rosenbluth, 2005).

En el proceso del análisis forense, en las metodologías que se utilizan, se tienen en cuenta unas directrices que han sido el resultado de estudios para garantizar que el proceso sea de calidad y cumpla con un alto grado de integridad, veracidad e idoneidad. Para apoyar lo anteriormente mencionado y, salvaguardando el objetivo principal de la informática forense, que es el de brindar pruebas ante un juzgado se ha creado una principios generales que pueden ser aplicadas en cualquier proceso de informática forense. En la referencia (Cano, 2006) define estos principios como:

1.Esterilidad de los medios informáticos de trabajo

2.Verificación de las copias en medios informáticos

3.Documentación de los procedimientos, herramientas y resultados sobre los medios informáticos analizados.

4.Mantenimiento de la cadena de custodia de las evidencia digitales

5.Informe y presentación de resultados de los análisis de los medios informáticos.

6.Administración del caso realizado

7.Auditoría de los procedimientos realizados en la investigación.

Siguiendo con la referencia (Cano, 2006), va más allá de describir dichos principios. Afirma que, la informática forense sin las herramientas es un contexto teórico de procedimientos y formalidades legales. El proceso forense debe ir acompañado de dos elementos: las herramientas, se debe validar la confiabilidad de los resultados generados por las mismas y, como segundo, la formación y el conocimiento del investigador que las utiliza.

Unas de las situaciones que complica en análisis forense en la heterogeneidad de las características de los dispositivos móviles, ya que sus fabricantes (de hardware y software) determinan sus propias características como sistema operativo, diseños de memoria y estructura de almacenamiento que van variando de una marca a otra, y de un modelo a otro (Agualimpia & Rodrigo) - (Santes, 2009). Pero, así los cambios en los dispositivos y en las versiones de Android son muy variados, la plataforma tiene características únicas (Jaramillo, 2011).

Otras características que varía en la diversidad de cables, interfaces y factores de forma. Este variabilidad ha generado que sea difícil manejar una forma general de hacer el análisis, hoy en día, existen paquetes de herramientas con variedad de cables, y otra clase se hardware y diferentes software para realizar dichos análisis (Vidas, Zhang, & Christin,2011).

2.1. Técnicas anti-forenses

Otro factor que incide en la informática forense, y hacen de esta un área de mucho cuidado son una serie de técnicas que buscan obstruir la labor de los peritos informáticos, las técnicas anti-forenses. Para definir qué es una técnica anti-forense, en la referencia (Cano, 2007) se propone la siguiente definición: «Cualquier intento exitoso efectuado por un individuo o proceso que impacte de manera negativa la identificación, la disponibilidad, la confiabilidad y la relevancia de la evidencia digital en un proceso forense» se podría resumir en la siguiente frase: «Haz que sea difícil para ellos encontrarte e imposible demostrar que te encontraron» (Berintato, 2007).

Tradicionalmente las técnicas anti-forenses se han clasificado en dos tipos: técnicas anti-forenses transitorias y las técnicas anti-forenses definitivas. En la técnica anti-forense transitoria, se busca dificultar el análisis con una herramienta o procedimiento específico, pero no lo hace imposible de analizar. Algunos ejemplos son: *fuzzing*,

abuso de los sistemas de ficheros con el fin de crear mal funcionamiento o para explotar vulnerabilidades de las herramientas usadas por el analista. La técnica anti-forense definitiva va más allá, busca arruinar las pruebas por lo que es imposible adquirirlas. Algunos ejemplos son: cifrado y borrado seguro (Maggi, Zanero,& Iozzo, 2008)

Ryan Harris, citado en (Botero, 2009), propone la siguiente clasificación de las técnicas anti-forenses:

- Desctrucción de la evidencia
- Ocultar la evidencia
- Eliminación de las fuentes de evidencia
- Falsificación de la evidencia

Algunas de las técnicas que pueden ser usadas en cada fase la clasificación planteada por Harris: Destrucción de la evidencia: eliminar o limpiar; Ocultar la evidencia: FIST (*Filesystem Insertion & Subversion Technique*), *salck space*, estenografía, cifrados y comprimidos y ADS (*Alternate Data Streams*); Eliminación de las fuentes de evidencia: sam juicer, syscall proxying, rexec, XSH (*the exploit shell*), Ftrans, booteable live CD & USB; Falsificación de la evidencia: cambiar marcas de tiempo, *file carving*, colisiones hash, rooted box (Cifuentes, 2010)(Garfinkel, 2007)(Jahankhani, Anastasios, & Revett, 2007)

Algunos de los objetivos que se busca alcanzar con el uso de técnicas anti-forenses son: limitar la detención de un evento que ya ha ocurrido, distorsionar información residente en el sitio, incrementar tiempo requerido para investigar el caso, generar dudas en informe forense, engañar y limitar la operación de herramientas forenses, eliminar rastros que pudieron haber quedado luego de los hechos realizados (Álvarez & Guamán, 2008).

2.2.Evidencia digital

La evidencia digital o electrónica es definida por el Instituto Nacional de tecnologías de la Comunicación de España como todos aquellos datos que «de manera digital se encuentran almacenados o fueron transmitidos mediante equipos informáticos y que son recolectados mediante herramientas técnicas especializadas empleadas por un perito en una investigación informática». Cuya funcionalidad es «servir como prueba física (por encontrarse dentro de un soporte) de carácter intangible (no modificables) en las investigaciones informáticas», Ver Fig. 2.

Figura 2
Ciclo de la evidencia digital.
(Ghosh, 2004)

Existen 4 criterios que determinan la admisibilidad de la evidencia: la autenticidad, la confiabilidad, la completitudo suficiencia, y el apego y respeto por las leyes y reglas del poder judicial (Zuccardi & Gutiérrez, 2006) -(Torres D. R.). El perito informático debe tener el mayor cuidado en la recolección, el análisis, el tratamiento de la evidencia digital, siguiendo la cadena de custodia ya que es fundamental en la ciencia forense; un error en el manejo de la evidencia puede poner en duda toda la interpretación realizada, y como consecuencia su poca credibilidad en un proceso judicial.

Unos de los principios que se tienen en cuenta en la ciencia forense, es el principio de Locard: «Cualquier contacto o presencia deja algún vestigio y se lleva otros», ver Fig. 3. Este principio tiene validez en el ámbito informático y las evidencias electrónicas (Pagès López, 2013).

Figura 3

Principio de Locard, versión digital.

(Calzada Pradas, 2004)

Por esta razón, uno de los muchos cuidados o buenas prácticas que se debe tener en cuenta en el proceso del manejo de pruebas es la etapa de recolección de la evidencia. Por ejemplo, se recomienda aislar el teléfono móvil de la red o vigilar no contaminar o perder registros importantes para su posterior análisis (Curran et al., 2010).

Con respecto a la evidencia electrónica la IOCE define 5 principios que rigen las acciones realizadas por los peritos informáticos: (Aguilar, 2013).

•Al manejar evidencia electrónica se debe aplicar todos los principios procedimentales y forenses generales.

•El proceso para obtener la evidencia no debe modificarla.

•Quienes accedan a la evidencia digital original deben ser especialistas, entrenados y calificados para dicho propósito.

•Toda actividad referente a la adquisición, acceso, almacenamiento o transferencia de la evidencia electrónica, debe ser totalmente documentada, almacenada y debe estar disponible para su revisión.

•Los peritos informáticosson los responsables de las acciones que se lleven a cabo respecto a la evidencia electrónica siempre y cuando esta, esté bajo su cuidado.

También la IOCE menciona una lista de cualidades que se debe en poner en práctica en el peritaje, estos son: objetividad, autenticidad, conservación, legalidad, idoneidad, inalterabilidad y documentación (Aguilar, 2013).

En la legislación colombiana, le evidencia digital es aceptada. Leyes como la ley 527 de 1999 «por medio de la cual se define y reglamenta

el acceso y uso delos mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones» (Congreso de la República de Colombia, 1999), y el decreto 2364 de 2012 «por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones» (Congreso de la República de Colombia, 2012), dan soporte legal a la evidencia digital. Otra base legal es la resolución No. 0-6394 que adopta el "Manual de procedimiento del sistema de cadena de custodia" para el sistema penal acusatorio (Fiscalia General de la Nación, 2004).

Uno de los obstáculos para la aceptación de la evidencia digital en Colombia es la carencia de normas especializadas destinadas a salvaguardar la cadena de custodia y admisibilidad de la evidencia digital (Álvarez, Marín, & Victoria, 2012).

Aunque en Colombia la evidencia electrónica es aceptada, el delito informático no estaba explícito en el código penal (Torres D. A., 2006), la legislación colombiana dio un paso importante con la Ley 1273 de 2009 «por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado –denominado "De la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones» (Congreso de la República de Colombia, 2009) - (Santos & Flórez, 2012).

Hablando un poco más de la práctica, la potencial evidencia que se puede encontrar en un dispositivo móvil es: el historial de llamadas, la lista de contactos, mensajes de texto y correos electrónicos, multimedia (imágenes, videos, audio), historial de navegación, registro de chat, cuentas de redes sociales, notas y calendarios, las conexiones (red móvil, wi-fi, Bluetooh), la información con respecto a la localización y el software de dicho dispositivo (Abdulla, Jones, & Anthony, 2011).

Es importante determinar cómo se ha a recolectar la evidencia, ya que si se hace correctamente, es mucho más fácil aprehender al atacante, y hay mayor probabilidad que la evidencia sea admisible en el caso de un proceso judicial (Brezinski & Killalea, 2002).

La evidencia de sebe tomar en orden de volatilidad, de la más volátil a la menos volátil, en ese orden de ideas sería:

- Registros, caché
- Tabla de enrutamiento, Caché ARP, tabla de procesos, estadísticas del kernel, memoria
- Sistemade archivo temporales
- Disco
- Registro de datos y la monitorización remota que sea relevante para el sistema en cuestión

•Configuración física, topología de redLos medios de comunicación de archivos

2.3. Modelos forenses

Desde sus inicios hasta convertirse en una ciencia, la informática forense sido descrita por una serie de modelos que buscan guiar este proceso. Estos modelos son similares, varían en cuanto a algunas fases, unos más detallados que otros.

Algunos de estos modelos son: modelo Casey, año 2000, ver Fig. 4, el modelo publicado por el U.S Dep. of Justice, año 2001; el modelo Lee, año 2001; modelo Reith, Carr y Gunsch, año 2002; el modelo integrado de Brian Carrier y Eugene Spafford, año 2003; el modelo mejorado propuesto por VenansiusBaryamureeba y FlerenceTuchabe, año 2004 y el modelo extendido de SéamusÓCiardhuáin, año 2004 (Arquillo, 2007) (De León, 2009).

El modelo de Caseyha evolucionado desde su primera aparición en el 2000, que consta de las siguientes fases (Casey, 2011):

- •Autorización y preparación
- •Identificación
- •Documentación, Adquisición y Conservación
- •Extracción de información y Análisis
- •Reconstrucción
- •Publicación de conclusiones

En el 2006, el *National Institute of Standards and Technology* dio algunas recomendaciones en la una guía para la integración de técnicas forenses en respuestas a incidentes. En esta guía un describe un procesode cuatro fases: Recopilación de datos, Examinación, Análisis y presentación de informes (Kent , Chevalier , Grance , & Dang , 2006). Este es un modelo estándar. El detalle de cada fase puede variar dependiendo de la situaciónespecífica, de las políticas organizacionales, de gobierno, entre otros (León, Echeverría, & Santander).

Es importante mencionar que los modelos anteriormente mencionados son guías, y se debe estudiar cuál es el más adecuado en el entorno que se va a trabajar. Cada investigación es única, siendo imposible conocer a priorilos aspectos que se deben tener en cuenta al realizar un procedimiento forense, y por ende, no es posible definir una metodología única para abordar este tipo deinvestigación. Las aproximaciones metodológicas que puedan resultar para realizar el proceso forense buscan minimizar los errores humanos que se pueden cometer por omisión y/o desconociendo, asegurar que la herramienta usada es confiable y garantizar que los procedimientos que se siguen son los adecuados (Torres D. R.).

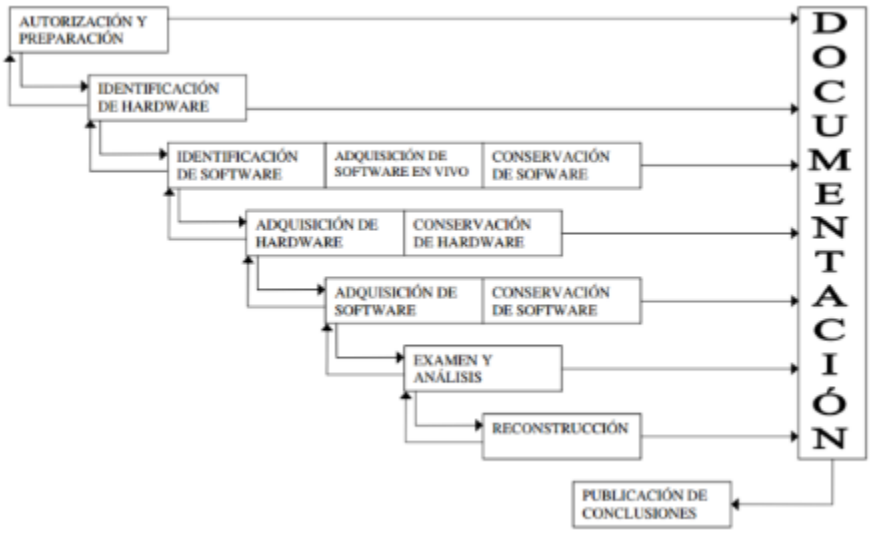

Figura 4
Modelo de Casey
(Arquillo, 2007)

Los análisis forenses sufren variaciones dependiendo a que sistema de cómputo se realice. Existe una clara diferencia entre computadores, laptop, etcétera (informática forense convencional) y los dispositivos móviles, estas diferencias como: arquitectura, funcionamiento del sistema, capacidad de memoria o de almacenamiento.

En ambos técnicas (convencional y dispositivos móviles) se puede realizar análisis en vivo o caliente y análisis post-mortem. La diferencia radica en que, en un análisis en vivo los dispositivos móviles permanecen activos contantemente, lo que produce que su contenido se actualice periódicamente. El reloj del dispositivo altera su contenido en memoria constantemente, imposibilitando una copia completa bit a bit de un teléfono inteligente (Ayers , Jansen , Cilleros, & Daniellou, 2005). También puede haber variaciones en el análisis post-mortem (Guidelines on Mobile Device Forensics, 2014).

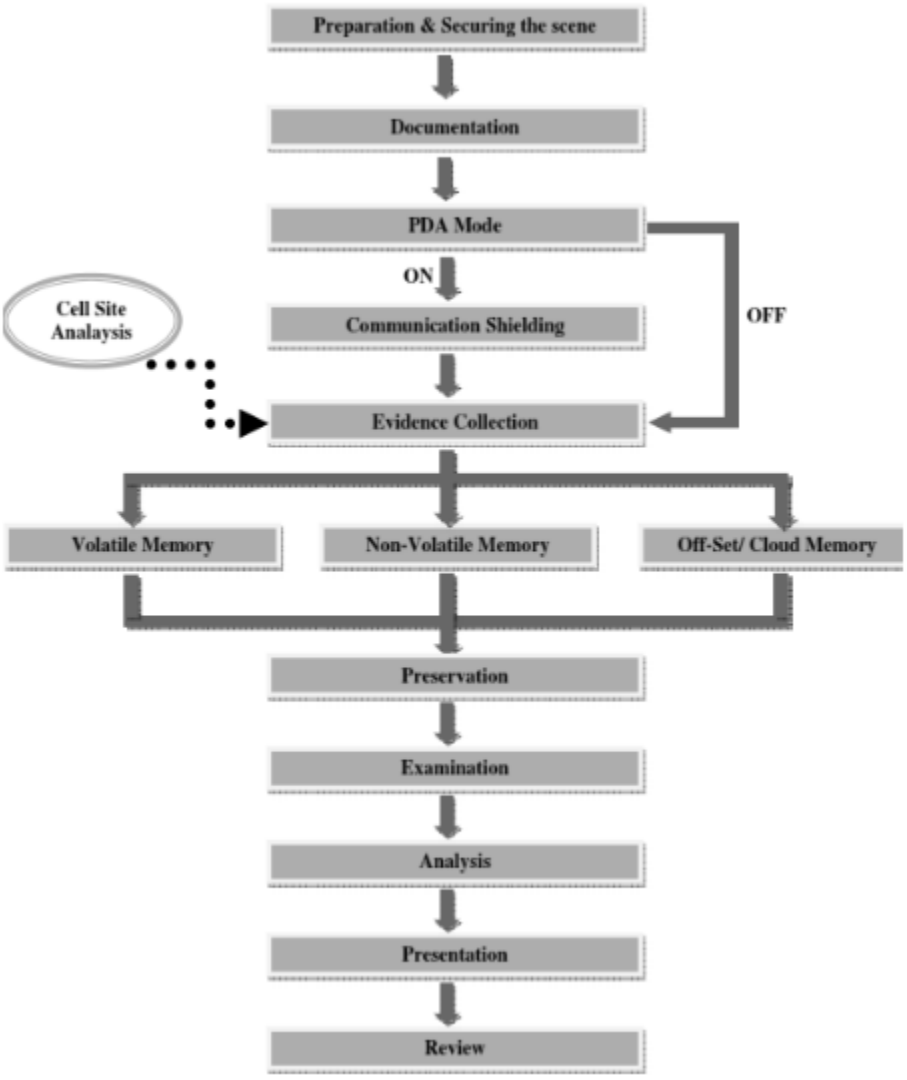

Figura 5

Modelo de investigación forense para teléfonos inteligentes.
(Goel, 2012)

Anteriormente, se mencionan algunos modelos usados en el análisis forense convencional. En la referencia (Goel, 2012) se propone un modelo para el proceso de investigación forense en teléfonos inteligentes, que consta de 14 fases, ver Fig. 5:

1.Preparación
2.Asegurar la escena
3.Documentación de la escena
4.Modo PDA
5.Bloquear comunicación externa
6.Recolección de evidencia volátil
7.Recolección de evidencia no volátil

8.Buscar evidencia almacenada fuera del dispositivo, información en la nube.

9.Análisis de la posición del teléfono (pasada y presente)

10.Preservación de la evidencia

11.Examinación de la evidencia

12.Análisis de la evidencia

13.Presentación de los resultados del análisis de la evidencia.

14.Revisión

3.DISCUSIÓN

La informática forense es un área de mucha importancia y a su vez de mayor cuidado. Para cumplir sus objetivos interactúa con evidencia, que puede ser presentada ante un juzgado para como soporte probatorio, o también, a cualquier empresa que solicite sus servicios para resolver un problema interno. Alrededor de la evidencia interactúan dos elementos importantes: Las herramientas y el perito informático.

Los autores mencionados anteriormente coinciden en lo importante que es salvaguardar las leyes, garantizar el principio de admisibilidad, guardar y seguir la cadena de custodia. También, que el conocimiento técnico, y el cómo se realiza el procedimiento forense es imprescindible. Cómo se recolecta la evidencia, cómo se preserva, su análisis y la forma en que se presentan el informe forense es fundamental, ya que garantiza en un porcentaje mucho mayor el éxito y su solidez ante las entidades correspondientes.

Estos temas se pueden trabajar a nivel académico, usando herramientas con licencias GPL, pero en un entorno laboral se deben contar con las herramientas *hardware* y *software* certificados por las autoridades pertinentes. El perito informático también debe certificar sus conocimientos, no basta con ser bueno en las ciencias computacionales. Cualquier duda o error en estos dos puntos puede poner en duda el soporte entregado por el perito informático y por ende que el caso se caiga.

4. CONCLUSIONES

La informática forense digital móvil es un área interesante y de mucha relevancia en el contexto actual. Con el crecimiento de los peligros informáticos a la par del mercado móvil, se abre un importante camino investigativo y profesional.

Android, por su popularidad tanto para clientes y cibercriminales, a la par de las políticas actuales manejadas por Google Inc. es unos de los sistemas operativos móviles más interesante para trabajar.

Con la evolución de los dispositivos móviles, la recolección de evidencia se hace más compleja, cada vez habrá más información por analizar, más complejidad en los dispositivos irá creciendo. Está evolución, conlleva a que cada día se confíe más información a dichos dispositivos, lo que crea un mayor interés por dichas terminales.

5.REFERENCIAS

Guidelines on Mobile Device Forensics.(2014). National Institute of Standards and Technology.

Abdulla, K., Jones, A., & Anthony, T. (2011). Guidelines for the digital forensic processing of smartphones. Edith Cowan University -Research Online.

Agualimpia, C., & Rodrigo, H. (s.f.). Universidad del Cauca.Obtenido de http://artemisa.unicauca.edu.co/~rhernandez/articulos/Articulo_UPM-Criptored_Symbian_OS_Forensics_UJaveriana.pdf

Aguilar, K. J. (2013). Principios jurídicos aplicables para la valoración de evidencia electrónica en el campo del despido laboral. H-TICs, I(1)., 1(1).

Álvarez, A., Marín, O., & Victoria, J. (2012). Framework para la computación forense en Colombia. Ing. USBMed, 3(2).

Álvarez, M. D., & Guamán, V. A. (Febrero de 2008). Universidad Politécnica Salesiana.Obtenido de http://dspace.ups.edu.ec/handle/123456789/546

Arias Chaves, M. (2006). Panorama general de la informática forense y de los delitos informáticos en Costa RIca. InterSedes: Revista de las sedes regionales, VII(12), 141-154.

Arquillo, J. (Septiembre de 2007). Universidad de Jaén.Obtenido de http://www.portantier.com/biblioteca/seguridad/analisis-forense.pdf

Ayers , R., Jansen , W., Cilleros, N., & Daniellou, R. (2005). Cell Phone Forensic Tools: An Overview and Analysis .Gaithersburg, MD: National Institute of Standards and Technology .

Berintato, S. (8 de Junio de 2007). The Rise of Anti-Forensic. (CSO) Obtenido de http://www.csoonline.com/article/2122329/investigations-forensics/the-rise-of-anti-forensics.html

Botero, A. C. (2009). Criptored. Obtenido de http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia3-Sesion6(3).pdf

Brezinski, D., & Killalea, T. (Febrero de 2002). Guidelines for Evidence Collection and Archiving. Network Working Group . Obtenido de http://www.rfc-editor.org/rfc/rfc3227.txt

Broucek, V., & Turner, P. (2006). Winning the battles, losing the war? Rethinking methodology for forensic computing research. Journal in Computer Virology, 3-12.

Calzada Pradas, R. (2004). Análisis forense de sistemas. II Foro de Seguridad RedIRIS

Cano, J. (2006). Introducción a la infomática forense. Sistemas, 64-73.

Cano, J. (9 de Septiembre de 2007). alfa-redi. (Derecho y Nuevas Tecnologías) Obtenido de http://www.alfa-redi.org/node/8946

Cano, J. (2009). Computación forense -Descubriendo los rastros informáticos.Almaomega

Casey , E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet(3rd ed.). Academic Press.

Cifuentes, J. (2010). Trabajos de grado Ingenieria de Sistemas. (Pontificia Universidad Javeriana) Obtenido de http://pegasus.javeriana.edu.co/~CIS0930SD01/files/AntiForenseZFS.pdf

Congreso de la República de Colombia. (18 de Agosto de 1999). Archivo General de la Nación Colombia.Obtenido de http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_527_DE_1999.pdf

Congreso de la República de Colombia. (5 de Enero de 2009). En TIC confío.Obtenido de http://www.enticconfio.gov.co/images/stories/normatividad/Ley_1273_de_2009%20.pdf

Congreso de la República de Colombia. (5 de Enero de 2009). Ministerio de las TIC.Obtenido de http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Congreso de la República de Colombia. (22 de Noviembre de 2012). Archivo General de la Nación Colombia.Obtenido de http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/DECRETO_2364_DE_2012.pdf

Curran, K., Robinson, A., Peacocke, S., & Cassidy, S. (2010). Mobile Phone Forensic Analysis. International Journal of Digital Crime and Forensics, 2(2).

De León, F. J. (Diciembre de 2009). Instituto Polotécnico Nacional.Obtenido de http://tesis.bnct.ipn.mx:8080/jspui/bitstream/123456789/7879/1/2386_tesis_Diciembre_2010_933405487.pdf

Eset . (2012). Guía de seguridad para usuarios de smartphone.

Fiscalia General de la Nación. (22 de Diciembre de 2004). Alcaldía de Bogotá.Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=15634

Garfinkel, S. (2007). Cite Seer X. (The Pennsylvania State University) Obtenido de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.109.5063&rep=rep1&type=pdf

Ghosh, A. (2004). Guidelines for the Management of IT Evidence.Hong Kong, China: APEC Telecommunications and Information Working Group.

Goel, A. T. (2012). Smartphone Forensic Investigation Process Model. International Journal of Computer Science & Security, VI(5), 322-341.

Google Inc. . (2015). Android.com. Obtenido de http://www.android.com/

HEADWAY Digital. (2015). Tendencias del consumo en móviles Colombia.

IAB Spain. (2014). VI Estudio Andual Mobile Marketing.

IDC Analyse the Future. (2015). Smartphone OS Market Share, 2015 Q2.Framingham, MA: IDC. Obtenido de http://www.idc.com/prodserv/smartphone-os-market-share.jsp

Jahankhani, H., Anastasios, B., & Revett, K. (2007). Digital Anti Forensics: Tools and Approaches. The 6th European Conference on Information Warfare and Security.Shrivenham, UK

Jakobsson, M., & Ramzan, Z. (2008). Crimeware. Understanding New attacks and Defenses(First ed.). Addison-Wesley Professional.

Jaramillo, G. E. (2011). Técnicas de análisis forense digital aplicadas a dispositivos y sistemas móviles. Apuntes de Ciencia & Sociedad, 167-171.

Kaspersky Lab. (2013). Kaspersky Lab Latinoamérica. (Octubre) Obtenido de http://latam.kaspersky.com/mx/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/m%C3%A1s-de-la-mitad-de-usuarios-de-android-no-pro

Kent , K., Chevalier , S., Grance , T., & Dang , H. (2006). Guide to Integrating Forensic Techniques into Incident Response .Gaithersburg, MD : National Institute of Standards and Technology -NIST.

León, A., Echeverría, T., & Santander, M. (s.f.). Guía metodológica para la investigación forense en el navegador web Google Chrome. Kosmos -Universidad Pontificia Bolivariana, 246-255.

Maggi, F., Zanero, S., & Iozzo, V. (2008). Seeing the invisible: Forensic Uses of Anomaly Detection and Machine Learning. Newsletter, 42, 51-58.

MinTIC & Ipsos Napoleón Franco. (2013). Ministerio TIC . Obtenido de http://www.mintic.gov.co/portal/604/w3-article-6048.html

Pagès López, J. (2013). Temas Avanzados en Seguridad y Sociedad de la Información. IX Ciclo de conferencias UPM -TASSI.Madrid, España.

Rifà, H., Serra, J., & Rivas, J. (2009). Análsisis forense de sistemas informáticos.Barcelona: Universitat Oberta de Catalunya.

Rodríguez, F., & Doménech, A. (2011). La informática forense: el rastro digital del crimen. Quadernos de Criminología. Revista de Criminología y Ciencias Forenses(14), 14-21.

Santes, L. (Marzo de 2009). Instituto Politécnico Nacional -México.Obtenido de http://tesis.ipn.mx:8080/dspace/bitstream/123456789/3730/1/PROPUESTAMETODFORENSE.pdf

Santos, L. M., & Flórez, A. S. (2012). Metodología para el análisis forense en Linux. Revista Colombiana de Tecnologías de Avanzada, 2(20), 90-96

Symantec Corp. (23 de Agosto de 2011). Symantec . Obtenido de http://www.symantec.com/es/mx/about/news/release/article.jsp?prid=20110823_01

Torres, D. A. (17 de Noviembre de 2006). Asociación Colombiana de Ingeniería de Sistemas -ACIS.Obtenido de http://www.acis.org.co/index.php?id=856

Torres, D. R. (s.f.). PennState. Department of Computer Science and Engineering.Obtenido de http://www.cse.psu.edu/~ruedarod/papers/recsi04.pdf

Vidas, T., Zhang, C., & Christin, N. (2011). Toward a general collection methodology for Android devices. Digital Inventigation, S14-S24.

Wang, Y., Cannady, J., & Rosenbluth, J. (2005). Foundations of computer forensics: A technology for the fight against computer crime. Computer Law & Security Review, 21, 119-127.

Zuccardi, G., & Gutiérrez, J. D. (Noviembre de 2006). Trabajos de grado de Ingenieria de Sistemas. Pontificia Universidad Javeriana.Obtenido de http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf

Notas de autor

dwricob@ufpso.edu.co

Dewar Rico Bautista, Johan Smith Rueda Rueda
La informática forense en dispositivos Android
The computer forensic in android device

Revista Ingenio
vol. 9, núm. 1, p. 116 - 129, 2016
Universidad Francisco de Paula Santander, Colombia
revistaingenio@ufpso.edu.co

ISSN: 2011-642X
ISSN-E: 2389-864X

Universidad Francisco de Paula Santander Ocaña