# ANÁLISIS FORENSE DIGITAL EN DISPOSITIVOS MÓVILES

JOHAN SMITH RUEDA RUEDA
Estudiante de la Facultad de Ingenierías
Semillero de Investigación GNU/Linux And Security, SIGLAS
Investigador grupo INGAP
Universidad Francisco de Paula Santander Ocaña
jsruedar@ufpso.edu.co

DEWAR RICO BAUTISTA
Director Semillero de Investigación GNU/Linux And Security, SIGLAS
Investigador grupo INGAP1, Facultad de Ingenierías
Universidad Francisco de Paula Santander Ocaña, Colombia
dwricob@ufpso.edu.co

Fecha de recepción: 28 de agosto de 2014
Fecha de aprobación: 09 de septiembre de 2011

## RESUMEN
La informática forense es una disciplina de la ciencia forense que nace de la necesidad de adquirir una nueva fuente de evidencias. Con el auge de los dispositivos móviles, los cibercriminales han dirigidos sus ataques hacia estos dispositivos. El sistema operativo Android es el mayor objetivo de los malware para móviles. Por esta razón, se vio la necesidad de llevar el análisis forense a los terminales móviles y, a través de modelos forenses, las herramientas utilizadas para el manejo de la evidencia que sirva como soporte en un proceso judicial. Este es uno de los objetivos de las ciencias forenses.

## PALABRAS CLAVES
Android, análisis forense móvil, informática forense.

## ABSTRACT
Computer forensic is a discipline of forensic science that arises the need to acquire a new source of evidence. With the heyday of the mobile devices, cybercriminals have directed their attacks to these devices. Android OS is the main target of the malware for mobile devices. For this reason, it was seen the need for forensic analysis to the mobile terminals and through forensic models, the tools used to manage the evidence used to support a prosecution. This is one of the purpose of the forensic sciences.

## KEY WORDS
Android devices, computer forensic, mobile forensic analysis

## INTRODUCCIÓN
Los dispositivos móviles han venido en constante evolución. El desarrollo de su hardware y software ha permitido que se lleven actividades más complejas que realizar una llamada o enviar un mensaje de texto.

A estos dispositivos le hemos confiado las actividades personales y laborales. Cada día se maneja más volumen de información y de mayor importancia. Esta información es lo que convierte el mercado de los dispositivos móviles en un blanco para los cibercriminales, y tienen los mismos peligros que un computador convencional. (Eset, 2012) (Jakobsson & Ramzan, 2008)

Del mercado de los dispositivos móviles, ha estado en aumento (IAB Spain Reseaech, 2013). El sistema operativo Android es el que mayor segmento tiende del mercado (Canalys, 2013). Según Google Inc. a finales de 2013 hubo 900 millones de dispositivos que corrían su sistema operativo. (Google Inc., 2013).

Un informe presentado por Symantec sobre plataformas móviles y su seguridad, describe dos problemas fundamentales en las políticas establecidas por Google Inc. para Android (Symantec Corp., 2011).

• El primer problema es que Google no tiene un modelo de certificación riguroso de aplicaciones, lo que permite 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 otorgar o no los permisos, de esta forma el riesgo es mayor.

Claramente Android es el sistema operativo más popular del mercado. Esta popularidad es utilizada por los cibercriminales. Según Kaspersky Lab., el 99% de las muestras de malware para dispositivos móviles que han estudiado, han sido dirigidos hacia Android. Este laboratorio también aclara que hay dos razones principales por las que los cibercriminales están interesados en Android: popularidad y funcionalidad.

(Kaspersky Lab., 2013)
Otros estudios realizados por organizaciones como Cisco demuestran el alto procentaje del malware que va destinado hacia Android. (Ver figura 1).

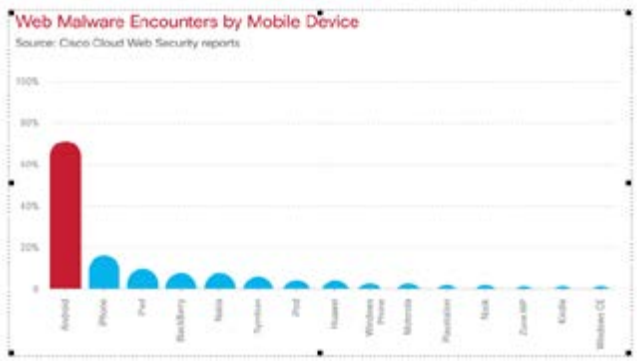


**Figura 1:** Malware encontrado en web para dispositivos móviles.

Con la marcada tendencia de llevar todas las actividades cotidianas que anteriormente se realizaban en un equipo de cómputo tradicional hacia los dispositivos móviles, la popularidad de Android, las políticas establecidas por Google crean un ambiente propicio para que se den los ataques informáticos. Cada día se verán ataque más sofisticados, ya se ven versiones para móviles de malware que han hecho de las suyas en la computación tradicional. Es allí donde la informática forense juega un papel fundamental, y procura describir e interpreta la información obtenida de los medios informáticos para establecer hecho y formular hipótesis.

# DESARROLLO

La informática forense es un área relativamente nueva. Es una rama de la ciencia forense que nace de la necesidad de encontrar una nueva fuente de evidencia. Los investigadores forenses encontraron que los dispositivos electrónicos podían brindar ese tipo de evidencia.

## Informática forense

Cano (2006) interpreta la informática forense 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 las tecnologías de los equipos de computación forense ofrece un análisis de la información residente en dichos equipos.»

El proceso forense busca 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 Chavez, 2006). Para regular la forma como se debe realizar el proceso forense, garantizando la veracidad e integridad, se creó la International Organization of Computer Evidence, OICE. (Rodríguez & Doménech, 2011) (OICE, 1999).

Cano (2006), define algunos principios que se deben tener un cuenta para realizar el procedimiento forense:

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.

## Evidencia digital

El Instituto Nacional de tecnologías de la Comunicación de España define la evidencia digital 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 Figura 2. (INTECO, s.f.)

Para que la evidencia sea aceptada y sirva 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 admisible, estos son: la autenticidad, la confiabilidad, la completitud o suficiencia, y el apego y respeto por las leyes y reglas del poder judicial. (Zuccardi & Gutiérrez, 2006) (Torres, Rueda, & Cano).


**Figura 2:** Cido de la evidencia digital Fuente: (Ghosh, 2004)

La informática forense maneja los mismos principios que las ciencias forenses, como lo es el principio de Locard: «Cualquier contacto o presencia deja algún vestigio y se lleva otros» (Alonso) (Pagès López, 2013). Ver figura 3.

Para el manejo de la evidencia electrónica la IOCE define cinco principios que rigen las acciones realizadas por los peritos informáticos: (Aguilar Espinales)

•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 debe 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 informáticos son los responsables de las acciones

que se lleven a cabo respecto a la evidencia electrónica siempre y cuando esta, esté bajo su cuidado.


**Figura 3:** Principio de Locard, versión digital.
**Fuente:** (Calzada Pradas, 2004)

## Modelos forenses

Desde sus inicios se ha desarrollado algunos modelos forenses para ayudar a desarrollar de mejor forma el proceso por el cual pasa la información, desde la extracción hasta la etapa final de la entrega del informe pericial.

Algunos de los modelos que han surgido a través de los años son: Casey (2000), el modelo publicado por el U.S Dep. of Justice (2001), el modelo Lee (2001), modelo Reith, Carr y Gunsch (2002), Modelo integrado de Brian Carrier y Eugene Spafford (2003) el modelo mejorado propuesto por VenansiusBaryamureeba y FlerenceTuchabe (2004) y el modelo extendido de SéamusÓCiardhuáin (2004). (Arquillo Cruz, 2007) (De León Huertas, 2009).

El modelo de Casey ha evolucionado desde su primera aparición en el 2000, que consta de las siguientes fases: (Casey, 2011) Ver figura 4.

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

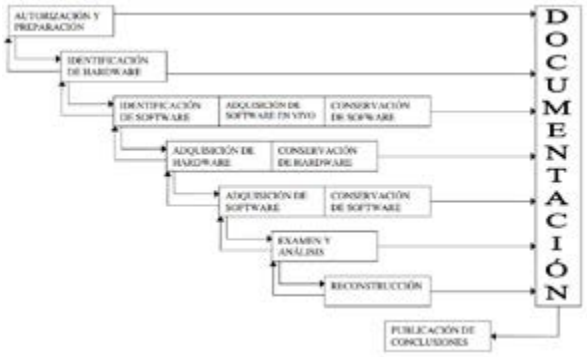


**Figura 4:** Modelo de Casey
**Fuente:** (Arquillo Cruz, 2007)

En los últimos años se ha trabajado en los dispositivos móviles, teniendo en cuenta las características propias de dichas terminales.

Goel, Tyagl, & Agarwal (2012) propusieron un modelo para desarrollar el proceso de investigación forense en los teléfonos inteligentes. Ver figura 5.

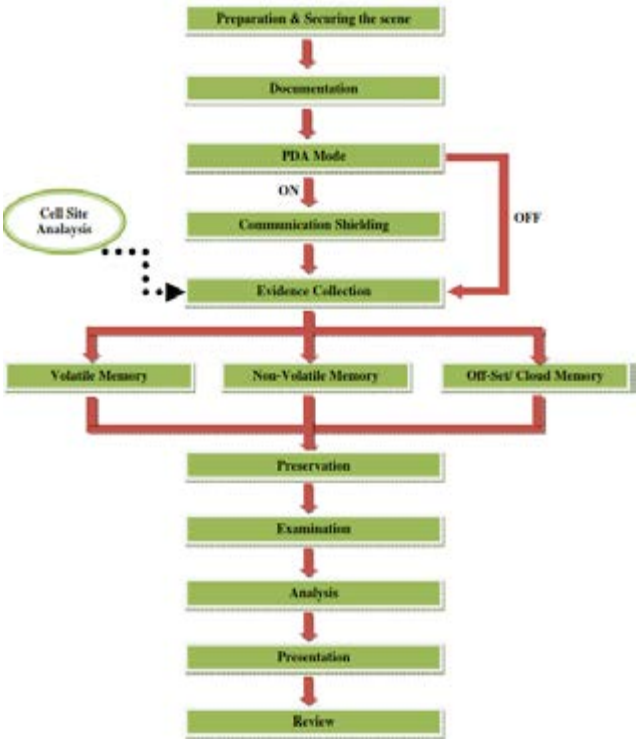


**Fig. 5:** Modelo de investigación forense para teléfonos inteligentes.

## Metodología propuesta

Para este proyecto se estableció una investigación descriptiva. Se realizará un estudio de las metodologías propuestas actualmente para el análisis forense digital, y las herramientas utilizadas para llevar cabo el procedimiento forense.

La pregunta a resolver, el cual es la base de esta investigación es: ¿Constituye las metodologías de análisis forense tradicional una forma idónea para el análisis forense móvil?

Para ellos se propone realizar un estudio de las metodologías existentes para el análisis forense digital, buscar que se ha trabajado en el área específica de los móviles en cuanto a metodologías propuestas. Por otro lado, evaluar las herramientas forenses de licencia libre, teniendo en cuenta ciertos parámetros como la robustez de la herramienta y la confiabilidad ofrecida.

Para lograr los objetivos propuestos, se estableció una metodología de cuatro fases. Las fases planteadas se presentan a continuación:

Fase 1: En esta primera fase se hizo una revisión de la literatura, consultándose material en revistas indexadas,

libros, tomando lo publicado por los expertos en la materia; con este material se realizó un estado del arte.

Fase 2: En esta segunda fase, se realizó un comparativo de algunas herramientas con licencia GPL con la cual se realizará el posterior análisis forense. Para este proceso se tuvo en cuenta la robustez del software, la confiabilidad en los resultados generados por dichas herramientas, y otras consideraciones para que el tratamiento de la evidencia tenga un grado de admisibilidad apropiada.

Fase 3: El objetivo de esta fase es resolver la siguiente pregunta: ¿Constituye las metodologías de análisis forense tradicional una forma idónea para el análisis forense móvil? Para ello se realizará un estudio de las principales metodologías forenses tradicionales y las que existen en cuanto a los dispositivos móviles. Como resultado se generará una metodología con las mejoras que se consideren pertinentes.

Fase 4: Como etapa final del proyecto, con los resultados obtenidos de las dos etapas anteriores se realizará un análisis forense en un dispositivo móvil con sistema operativo Android.

## Resultados obtenidos

Los resultados que se han obtenido es la participación como ponente en dos congresos internacionales. El 'X Congreso Internacional de Electrónica y Tecnología de Avanzada, (X CIETA)' y el 'I Congreso Internacional de Investigación en Ingeniería de Sistemas, (CIIIS 2014). También, un artículo tipo estado del arte en revisión por la Revista Colombiana de Tecnología de Avanzada.

Actualmente, se lleva un 50 % del proyecto. Con estos avances se participará en el encuentro Nacional de semilleros de investigación que se realizará en la ciudad de Tunja.

## REFERENCIAS


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

Alonso, J. (s.f.). Instituto científico de criminalística documental. Obtenido de http://www.iccd.es/descargas/EVALUACIONJAVIER.pdf

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

Arquillo Cruz, J. (Septiembre de 2007). Universidad de Jaén. Recuperado el Enero de 2014, de http://www.portantier.com/biblioteca/seguridad/analisis-forense.pdf

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

Canalys. (Mayo de 2013). Canalys. Recuperado el Octubre de 2012, de http://www.canalys.com/newsroom/smart-mobile-device-shipments-exceed-300-million-q1-2013

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

Casey, E. (2011). Digital evidence and computer crime. Forensic science, computers and the internet. Academic Press .

De León Huertas, F. J. (Diciembre de 2009). Instituto Politécnico 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.

Ghosh, A. (2004). Obtenido de http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan016411.pdf

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

Google Inc. (2013). http://www.android.com/. Obtenido de http://www.android.com/

IAB Spain Reseaech. (Septiembre de 2013). AIB Interactive Advertising Bureau. Recuperado el Noviembre de 2013, de http://www.iabspain.net/wp-content/uploads/downloads/2013/09/V_Estudio_Mobile_Marketing_version_corta.pdf

INTECO. (s.f.). Instituto Nacional de Tecnologías de la comunicación. Recuperado el Diciembre de 2013, de http://www.inteco.es/wikiAction/Seguridad/Observatorio/area_juridica_seguridad/Enciclopedia/Articulos_1/evidencia_electronica_es

Jakobsson, M., & Ramzan, Z. (2008). Crimeware. Understanding New attacks and Defenses. Boston: Pearson Education Inc.

Kaspersky Lab. (2013). Kaspersky Lab. Recuperado el 8 de Octubre de 2013, 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

OICE. (4 de Octubre de 1999). www.ioce.org. Obtenido de www.ioce.org

Pagès López, J. (2013). Temas avanzados en seguridad y sociedad de la información. IX Ciclo de conferencias UPM - TASSI. Madrid.

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

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

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

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