# Open Practice Guide for Digital Forensics on Android Devices

**Article** *in* RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao · February 2019

CITATIONS
0

READS
4,368

**3 authors:**

Johan Smith Rueda-Rueda
Autonomous University of Bucaramanga
**19** PUBLICATIONS **73** CITATIONS
SEE PROFILE

Dewar Rico-Bautista
Universidad Francisco de Paula Santander
**95** PUBLICATIONS **386** CITATIONS
SEE PROFILE

Cesar D. Guerrero
Autonomous University of Bucaramanga
**64** PUBLICATIONS **313** CITATIONS
SEE PROFILE

ISSN: 1646-9895

# risti

Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Fevereiro 19 • February 19



Nº E18

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 27/11/2018
Aceitação/Acceptance: 02/12/2018

# Guía práctica abierta para el análisis forense digital en dispositivos Android

Johan Smith Rueda-Rueda[1], Dewar Rico-Bautista[2], Cesar D. Guerrero[3]

**jrueda526@unab.edu.co, dwricob@ufpso.edu.co, cguerrer@unab.edu.co**

[1] Centro de Excelencia y Apropiación en IoT - Nodo Oriente, Grupo de Investigación en Tecnologías de Información. Universidad Autónoma de Bucaramanga, Avenida 42 No. 48 – 11, 680003, Bucaramanga, Colombia.

[2] Departamento Sistemas e Informática. Universidad Francisco de Paula Santander Ocaña, Sede Algodonal Vía Acolsure, 546551, Ocaña, Colombia.

[3] Centro de Excelencia y Apropiación en IoT - Nodo Oriente, Grupo de Investigación en Tecnologías de Información. Universidad Autónoma de Bucaramanga, Avenida 42 No. 48 – 11, 680003, Bucaramanga, Colombia.

**Pages: 442–457**

**Resumen:** Android es el sistema operativo móvil usado en la actualidad y el más atacado por los cibercriminales. El análisis forense digital es el proceso de aplicar métodos científicos para recopilar y analizar datos e información que puede ser utilizada como evidencia y puede ser aplicado a los dispositivos móviles. Varias instituciones e investigadores han propuesto modelos y lineamientos para guiar el proceso forense, pero estos son muy antiguos, o son muy técnicos o son más genéricos y no tienen en cuenta los dispositivos móviles; por esta razón, se propone una guía práctica abierta para contribuir en la apropiación del procedimiento forense en dispositivos móviles por parte de los integrantes de semilleros y grupos de investigación y profesionales que quieran iniciar el aprendizaje e investigación en esta área. Esta guía está conformada por ochos fases e integra todo el proceso forense, las buenas prácticas y el perfil de investigador forense.

**Palabras-clave**: Análisis forense digital, análisis forense móvil, dispositivos Android, guía práctica.

## *Open Practice Guide for Digital Forensics on Android Devices*

***Abstract:*** Android is the mobile operating system used today and the most attacked by cybercriminals. Digital forensics is the process of applying scientific methods to collect and analyses data and information that can be used as evidence and can be applied to mobile devices. Several institutions and researchers have proposed models and guidelines to guide the forensic process, but these are very old, are very technical or are more generic and do not consider mobile devices; For this reason, an open practical guide is proposed to contribute to the appropriation of the forensic procedure in mobile devices by the members of seedlings and research groups and professionals who want to initiate the learning and investigation in this area. This

guide is made up of eight phases and integrates the entire forensic process, good practices, and the profile of forensic investigator.

***Keywords**:* Android devices, digital for1ensics, mobile forensics, practical guide.

## 1. Introducción

Android es el sistema operativo móvil -incluyendo de escritorio o móviles- más usado en el mundo, superando al sistema operativo Windows (StatCounter, 2017). Esta popularidad ha provocado que Android sea el sistema operativo móvil más atacado y, con gran capacidad de cómputo que disponen las actuales terminarles, han contribuido a que cada día se presenten ataques más sofisticados para esta plataforma. Los cibercriminales han tenido en cuenta este nuevo objetivo y han migrado los ataques que tradicionalmente era para los equipos de escritorio y laptops hacia los dispositivos móviles, y entre las amenazas que enfrentan los usuarios se encuentra una gran variedad de malware, algunos tan particulares como el ransomware y botnets creadas con dispositivos Android.

Cuando ocurre un incidente de seguridad o se sospecha que un equipo informático ha sido comprometido, es donde la informática forense tiene su campo de aplicación, para determinar lo qué pasó, cómo ocurrió y determinar quién es el responsable. La informática forense es una disciplina de las ciencias forenses, y se define como el proceso de aplicar métodos científicos para recopilar y analizar datos e información que puede ser utilizada como evidencia (Nelson, Phillips, & Steuart, 2010). Esta disciplina trabaja con evidencia digital, y mantiene los principios de las ciencias forenses como es la rigurosidad del manejo de la evidencia, el principio de Locard y los retos a los que se enfrentan el equipo de investigadores forenses, como son las técnicas anti-forenses, que buscar impactar de manera negativa la identificación, la disponibilidad, la confiabilidad y la relevancia de la evidencia en un proceso forense (Rueda-Rueda & Rico Bautista, 2016).

Algunas instituciones referentes a nivel internacional en el análisis forense digital y la respuesta a incidentes como son el National Institute of Standards and Technology – NIST y el National Institute of Justice (NIJ) – U.S. Department of Justice han propuesto guías y lineamientos para ayudar a los investigadores forenses, brindando una serie de buenas prácticas para garantizar que los procedimientos realizados sean idóneos y sujeta a la rigurosidad requerida en todas las ciencias forenses. Un inconveniente con el que se puede encontrar una persona que quiere iniciar su aprendizaje en el área de la informática forense es que estas guías no son actualizadas, y tanto las guías propuestas por el NIST (Ayers, Brothers, & Jansen, 2014; Jansen & Ayers, 2007; Kent, Chevalier, Grance, & Dang, 2006) y el NIJ (Ashcroft, Daniels, & Hart, 2012; National Institute of Justice, 2004) tienen entre 10 y 13 años de antigüedad, y las más recientes entre 3 y 5 años. Las actualizaciones de estas guías se están quedando cortas en comparación a la rápida evolución que están teniendo los dispositivitos móviles y la informática en general. Por otra parte, existen una variedad de instituciones gubernamentales y privadas, fuerzas del orden, grupos técnicos e investigadores que brindas guías y lineamientos para describir y orientar el procedimiento forense, sus buenas prácticas y el perfil del investigador forense; estas fuentes son diversas, y pueden confundir el proceso de aprendizaje de la ciencia forense digital al ser muy técnicas y obviando procesos

o buenas prácticas porque vienen implícitas con el proceso forense. Con el propósito de contribuir en la apropiación del procedimiento forense en dispositivos móviles se propone una guía práctica abierta donde se integra el proceso forense, las buenas prácticas y las características de los dispositivos móviles Android más recientes. Esta guía va dirigida a estudiantes, profesionales, semilleros y grupos de investigación que deseen comenzar el aprendizaje y la investigación en esta área. La intención de proponer una guía abierta es que pueda ser mejorada con las experiencias y contribuciones de las personas que las usen.

El resto del artículo está dividido cinco secciones. En la sección dos se presenta la revisión de la literatura en dos ejes: las herramientas forenses y los modelos forenses. En la sección tres se presenta la guía práctica propuesta, la cual consta de ocho fases. En la sección 4 se presentan los formatos propuestos para el manejo de la prueba o evidencia. Finalmente se presenta las conclusiones y el trabajo futuro.

## 2. Revisión de la literatura

El estado se presenta en dos ejes: El primero, las herramientas forenses open source, las cuales se clasificaron en herramientas para la adquisición, herramientas para el examen, herramientas para el análisis y las suites forenses. El segundo eje, los modelos propuestos por instituciones e investigadores para el análisis digital forense tradicional.

### 2.1. Herramientas forenses

Bajo la filosofía del software libre, existen una variedad de herramientas y distribuciones especializadas -suites forenses- para realizar un análisis forense en dispositivos móviles. Las herramientas se clasificaron en tres grupos: (i) Herramientas para la adquisición, (ii) herramientas para la examinación, (iii) herramientas para el análisis y (iv) suites forenses.

**Herramientas para la adquisición.** Para la adquisición de la información del dispositivo se puede utilizar AFLogical OSE (NowSecure, 2017), la cual es la edición de código abierto del software AFLogical, desarrollado por NowSecure. Para la creación de imágenes forenses se encuentran: dd, dc3dd y dcfldd. Estas herramientas se pueden utilizar para crear las imágenes forenses en las tarjetas MicroSD de los dispositivos, al igual que en otros medios de almacenamiento, como pendrive y discos duros. Dc3dd es la herramienta más completa, ya implementa Hash, permite segmentar las imágenes forenses, muestra información al usuario sobre el proceso y tiene un mejor tiempo de ejecución (Rueda & Rico, 2016).

**Herramientas para la examinación.** Para examinar la evidencia, se puede utilizar herramientas como Foremost, Photorec, Testdisk y Myrescue. Estas herramientas tienen la finalidad de recuperación de archivos, el Datacarving y el Filecarving.

**Herramientas para el análisis.** Para el análisis de la evidencia se cuenta con herramientas como Autopsy (The Sleuth Kit, 2017a, 2017b), Digital Forensic Framework (DFF) (ArxSys, 2017) y log2timeline (Gudjonsson, 2017), la cual permite realizar la línea del tiempo de los hechos ocurridos, siendo relevante a la hora de analizar la información y determinar qué hecho pasó en que instante de tiempo.

**Suites forenses.** Entre las suites forenses disponibles, existen unas suites que cuentan con las herramientas para realizar un análisis forense en un dispositivo móvil, como lo son CAINE Linux, Santoku, DEFT y SIFT Workstation.

CAINE (Computer Aided INvestigative Environment) (CAINE Linux, 2017) es una distribución live GNU/Linux italiana creada como un proyecto de forense digital, el cual ofrece un entorno forense completo, organizado para integrar las herramientas de software existentes como módulos de software y para proporcionar una interfaz gráfica amigable. Con su diseño, CAINE pretende garantizar ser un entorno interoperable que apoya al investigador digital durante las cuatro fases de la investigación digital, y que su interfaz gráfica y herramientas sean fáciles de usar.

Santoku (Santoku Linux, 2017) es una plataforma de código abierto, de fácil uso, dedicada al análisis forense, el análisis y la seguridad en dispositivos móviles, la cual está equipada con plataformas SDK, drives, frameworks, herramientas con interfaces de usuario y configuraciones para facilitar las actividades forenses. Santoku cuenta con herramientas para la adquisición forense y el análisis de datos, herramientas para examinar malware móvil y apoyo a la evaluación de la seguridad de las aplicaciones móviles. DEFT (Digital Evidence & Forensics Toolkit) (DEFT, 2017) una distribución GNU/Linux italiana, creada por Computer Forensics y gestionado y mantenido por DEFTA, con el propósito de ejecutarse en vivo en los sistemas sin alterar o corromper los dispositivos (discos duros, pendrives, etc.) conectados a la PC donde se lleva a cabo el proceso de arranque. DEFT está emparejado con DART (Digital Advanced Response Toolkit), un sistema forense que se puede ejecutar en Windows y contiene las mejores herramientas para forense y respuesta de incidentes. DART cuenta con una interfaz gráfica de usuario con registro e inspección de integridad de los instrumentos aquí contenidos.

SIFT (SANS Investigative Forensic Toolkit) Workstation versión 3 (SANS Institute, 2017), es creado por un equipo internacional de expertos forenses encabezado por el instituto SANS (SysAdmin Audit Networking and Security Institute) para la respuesta de incidentes y análisis forense digital que se puso a disposición de toda la comunidad como un servicio público. SIFT demuestra que las capacidades avanzadas de respuesta a incidentes y las técnicas forenses digitales de inmersión profunda a las intrusiones pueden lograrse utilizando herramientas de código abierto de vanguardia que están disponibles libremente y se actualizan con frecuencia(Rico-Bautista & Alvernia-Acevedo, 2017). Teniendo en cuenta el grado en que esta suite forense soporta los dispositivos móviles Android, el soporte técnico que tiene, la documentación que se ofrece a los usuarios y el equipo técnico y profesional que está asesorando el desarrollo de estas suites, DEFT es un poco más completa que las demás (Rueda & Rico, 2016).

## 2.2. Modelos forenses

Para guiar el procedimiento forense se ha propuesto una serie de modelos, cada uno con la perspectiva que los autores tienen de la informática forense, pero teniendo en común las etapas básicas del proceso forense. Entre los modelos más conocidos se tiene: El modelo del National Institute of Justice, el modelo DFRWS, el modelo de Reith, Carr y Gunsch, el modelo Casey, la segunda edición del modelo propuesto por el National Institute of Justice, el modelo extendido para las investigaciones de cibercrimen, y el modelo de Cohen. El modelo del National Institute of Justice (National Institute of Justice, 2001),

propuesto en 2001, fue una de las grandes bases en el campo de análisis forense digital y a partir de él otros autores desarrollaron sus modelos para englobar todos los pasos de una investigación forense digital. Este modelo es muy sencillo y propone cuatro fases: Identificación, preservación, análisis y presentación.

El modelo DFRWS (DFRWS, 2001), propuesto en 2001, es el resultado de Forensics Digital Research Workshop (DFRWS), y muestra el proceso forense digital como un proceso lineal. Este modelo está compuesto por las siguientes fases: Identificación, preservación, recolección, examen, análisis, presentación y decisión. El modelo de Reith, Carr y Gunsch (Reith, Carr, & Gunsch, 2002), se propuso en 2002, y está inspirado en el modelo DFRWS, presentándose como una mejora de este. Las fases de este modelo son: Identificación, preparación, estrategia de enfoque, preservación, recolección, examen, análisis, presentación y volviendo a pruebas. Este modelo no tiene en cuenta las buenas prácticas para guardar la cadena de custodia, y no porque no sea importante, sino porque la cadena de custodia está implícita en cualquier discusión de la ciencia forense. Los autores al proponer el modelo hacen el supuesto que se mantendrá una fuerte cadena de custodia durante toda la duración de la investigación.

El modelo Casey (Casey, n.d.), presentado por Eoghan Casey en 2004, es un modelo para aplicar las ciencias forenses en los computadores (En 2001, Cohen había presentado un modelo muy general que podía ser aplicado en sistemas autónomos y entornos de red (Casey, n.d.)), el cual consta de siete fases: (i) Autorización y preparación, (ii) identificación, (ii) documentación, (iv) recolección y preservación, (v) examen y análisis, (vi) reconstrucción, y (vii) presentación de informes. La segunda edición del modelo del National Institute of Justice (National Institute of Justice, 2004), presentado en 2004, en la cual se realiza una pequeña variación con respecto a la anterior versión. La de recolección del anterior modelo se dividió en dos: evaluación y adquisición. De esta forma, el modelo quedó con seis fases: Preparación, evaluación, adquisición, examinación, análisis y presentación de informes.

El modelo extendido para las investigaciones de cibercrimen (Ciardhuáin, 2004), es un modelo en cascada, desarrollado por Séamus Ó Ciardhuáin en 2004, el cual establece que las actividades para una investigación forense son las siguientes: (i) Conciencia, (ii) autorización, (iii) planificación, (iv) notificación, (v) buscar e identificar evidencias, (vi) recolección de evidencia, (vii) transporte de evidencia, (viii) almacenamiento de la evidencia, (ix) examen de la evidencia, (x) hipótesis, (xi) presentación de la hipótesis, (xii) comprobar/defender la hipótesis, y (xiii) difusión de la información. El modelo Cohen (Cohen, 2009), propuesto por Fred Cohen en 2009, describe el tratamiento de la evidencia digital. Este modelo propuesto para el proceso de la evidencia digital en el contexto legal consta de 11 fases: (i) Identificar, (ii) recolectar, (iii) preservar, (iv) transportar, (v) almacenar, (vi) analizar, (vii) interpretar, (viii) atribuir, (ix) construir, (x) presentar, y (xi) destruir. Para Cohen el proceso forense va más allá del manejo de la evidencia, es solo una parte de un contexto más grande, el cual, también hace parte el equipo humano, las herramientas, los litigantes, el contexto y el proceso legal, el principio de admisibilidad y los retos que tiene el proceso forense.

Los modelos forenses no son absolutos, cada uno tiene sus ventajas y sus limitaciones. Teniendo en cuenta que cada caso es único, no se puede proponer un modelo que contemple todas las características y condiciones particulares de un proceso forense.

Lo que sí se puede hacer es una aproximación metodológica que permita minimizar los errores humanos cometidos por omisión y/o desconocimiento, asegurar el uso de herramientas confiables y garantizar que los procedimientos seguidos son los adecuados y pueden reproducirse obteniendo los mismos resultados. Cada autor propuso en su modelo una representación de las diferentes etapas o pasos que conlleva, a su parecer, realizar un procedimiento forense en medio electrónico. En la Fig. 1 se muestra una vista general de las etapas de cada uno de los modelos y sus equivalencias con otros modelos presentados.

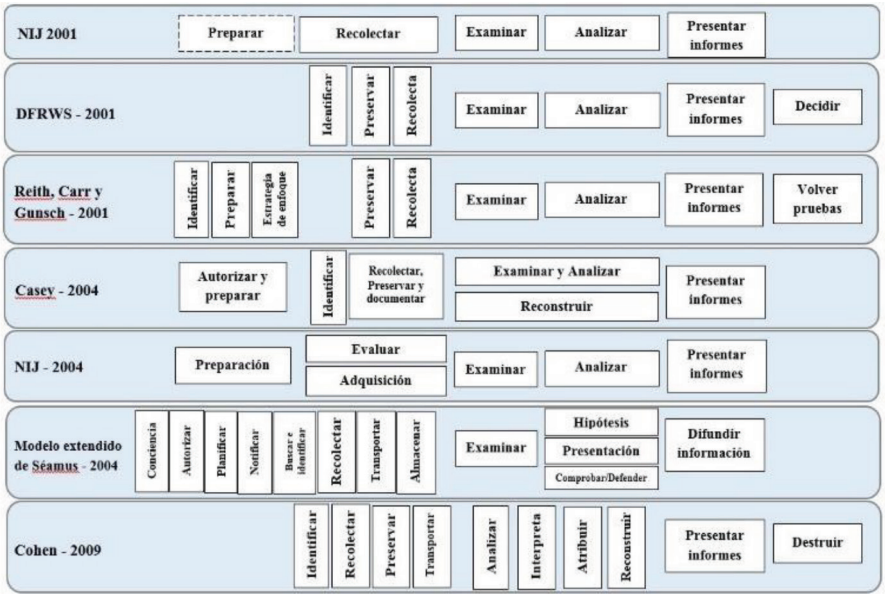



Figura 1 – Fases de los modelos estudiados.

## 3. Modelo propuesto

La guía propuesta cuenta con un modelo compuesto por ocho fases, a saber: (i) Fase de identificación y evaluación; (ii) Fase de preparación; (iii) Fase de preservación; (iv) Fase de adquisición de datos; (v) Fase de examinación; (vi) Fase de análisis; (vii) Fase de presentación de informes y (viii) Fase de revisión, como se muestra en la Figura 2.

### 3.1. Fase de identificación y evaluación

En esta fase, el investigador tiene la primera aproximación con el caso a investigar. El investigador debe asegurarse de que obtiene la mayor información posible sobre el caso y los elementos asociados con él. La información que se necesita identificar y conocer para estructurar y preparar el procedimiento forense es la siguiente: (i) información sobre el incidente; (ii) el alcance del proceso forense; (iii) información sobre la escena del crimen; (iv) evaluar el entorno en el que se realizará la extracción de datos de los dispositivos móviles; (v) identificar la información potencial que se puede usar como evidencia; y vi) consideraciones jurídicas.

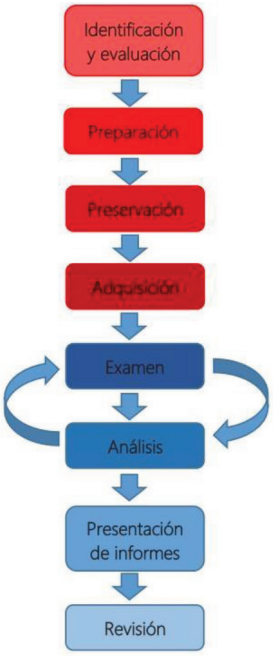



Figura 2 – Modelo propuesto.

El investigador puede obtener la información sobre el incidente a través de la documentación proporcionada, entrevistas o por medio del testimonio de la víctima. Saber lo que sucedió o lo que se sospecha que ha ocurrido es relevante porque guía al investigador para establecer el camino a seguir durante la investigación. Por lo tanto, el examinador puede determinar el objetivo y el alcance del proceso forense, los datos que pueden utilizarse como evidencia y los recursos de hardware y software necesarios para la investigación. Definir el alcance de la investigación reduce el tiempo y los costos del examen porque el investigador se centra en qué buscar y dónde buscarlo.

### 3.2. Fase de preparación

En esta fase el investigador se provee y prepara los elementos necesarios para la realización del procedimiento forense y el manejo de la prueba: documentación, extracción, empaquetado, almacenamiento y transporte. Los elementos que se deben preparar son de tipo hardware, software, los suministros para el manejo de la evidencia y los profesionales que integran el equipo forense.

**Preparación de hardware.** El hardware que se debe preparar están las interfaces para conectar el dispositivo móvil con la estación forense, los cargadores, fuentes de energía suplementaria para garantizar que el dispositivo se mantenga encendido el tiempo necesario para la extracción de las imágenes forenses, medios de almacenamiento esterilizados para almacenar dichas imágenes, cajas o bolsas de Faraday, bolsas

antiestáticas y guantes de látex en caso que se requiera extraer las huellas dactilares del dispositivo.

**Preparación de software.** En cuando al software se prepara la estación forense, que básicamente es un equipo con las herramientas o la suite de herramientas para la adquisición, examen y análisis de la información recolectada en el terminal.

**Preparación del equipo forense.** El equipo forense es un equipo interdisciplinario, entre los que se encuentran abogados, que se encargan de las consideraciones legales; los fotógrafos, encargados de documentar visualmente la escena del crimen y los diferentes elementos en ella; la unidad de respuesta a incidentes, que son las personas capacitadas para llevar el procediendo de primera respuesta;  el analista de incidentes; el analista forense, que entre sus funciones está la de dar una idea de los tipos de cosas que se deben buscar para encontrar la evidencia; el examinador de evidencias, el cual proporciona los medios para encontrar información relevante que pudiera estar en el sistema; el administrador de evidencias y los testigos expertos/peritos. En la práctica profesional, el equipo forense debe estar integrado por personal con sus conocimientos certificados.

**Suministros para el manejo de la evidencia.** Entre los suministros para el manejo de la prueba están formatos para el manejo de la prueba o evidencia (en la sección 5 de este artículo se muestran en detalle), la cámara fotográfica y grabadora, para proporcionar recordatorios visuales y auditivos de la escena del crimen y del dispositivo; etiquetas adhesivas y etiquetas para cables, marcadores indelebles, bolsas de pruebas, cinta de pruebas, libreta para notas rápidas y crear el croquis de la escena del crimen y todo aquello que sea útil para registrar y transportar la evidencia, como cajas o recipientes, que permita que la prueba se mueva lo menos posible.

La documentación de todo lo que se hace durante el proceso forense será de vital importancia para la redacción de un buen informe en el cual se detalle todo el caso, la forma en que se procedió, los resultados encontrados y las conclusiones a la cual se llegaron.

### 3.3. Fase de preservación

Esta fase es una de las más críticas en el proceso forense, ya que es en la cual se busca proteger la integridad de todas las pruebas, ya sean electrónicas o no, que la evidencia no sea contaminada, se altere o se destruya por completo. La preservación de la evidencia se puede complicar por varios factores: (i) las organizaciones no cuentan con personal disponible y capacitado para realizar los procedimientos de primera respuesta; (ii) el desconocimiento del personal de una organización o de las personas naturales de cómo deben actuar ante un incidente; y (iii) que la notificación o descubrimiento del incidente suceden tiempo después de ocurrido el ciberdelito.

En el caso que el dispositivo móvil sea parte de una escena del crimen, esta se debe asegurar, evaluar y documentar. Como parte de la evaluación de la escena, se formula un plan de búsqueda, identificando las posibles pruebas y documentando todo tanto las pruebas como el procedimiento. Una vez el dispositivo se ha incautado, se sella en una bolsa de prueba estática y se etiqueta. La persona que se apodera del dispositivo debe firma y fechar la etiqueta para iniciar la cadena de custodia, la documentación de su

embalaje, transporte y almacenamiento, evitando las fuentes magnéticas (por ejemplo, transmisores de radio e imanes), condiciones de calor excesivo, frío o humedad, los golpes y vibraciones excesivas, procurando que esté firme para evitar que se mueva y que accidentalmente se pulsen las teclas. Aislar el dispositivo de las redes es importante para evitar que nuevo tráfico como llamadas, SMS o notificaciones de aplicaciones puedan sobrescribir los datos existentes.

La cadena de custodia es el proceso de documentar el recorrido completo que hace la prueba a través del ciclo de vida del caso, y se aplica a los elementos físicos materia de prueba y de las imágenes forenses creadas a partir del dispositivo móvil y la memoria externa. El cuidadoso mantenimiento la cadena de custodia protege la integridad de las pruebas, y hace que sea difícil para alguien argumentar que la evidencia fue manipulada en el proceso. La cadena de custodio debe responder a los siguientes interrogantes: ¿Quién lo recogió?, ¿cómo y dónde se encontró?, ¿quién tomó posesión de ella?, ¿cómo fue almacenada y protegida en el almacenamiento?, y ¿quién lo sacó de almacenamiento y por qué?

### 3.4. Fase de Adquisición

En esta fase se busca, se identifica, recolecta y documenta las pruebas electrónicas. Una vez el dispositivo móvil ingresa al laboratorio forense, se debe registrar su ingreso y se continúa con la cadena de custodia. Para este proceso se recomiendas cuatro pasos: (i) identificar la fuente de los datos, (ii) desarrollar el plan para adquirir los datos, (iii) adquisición de los datos y (iv) se verifica la integridad de los mismos.

El plan de adquisición de datos contempla todo lo relacionado con el procedimiento de recolección de los mismos; se establece el orden en que se deben adquirir los datos y las medidas que se deben tomar para minimizar el riesgo del fracaso en la investigación. De un dispositivo móvil se puede recolectar información de su memoria interna y externa y de la tarjeta SIM, entre ella tenemos información sobre el sistema operativo, llamadas realizadas y recibidas (fecha, hora, duración), último número marcado, lista de contactos, MSM, archivos multimedia (fotografías, videos, audios), los archivos almacenados y borrados, el espacio en memoria desperdiciado, datos de geolocalización, correos electrónicos, por dar algunos ejemplos.

Con respecto a las imágenes forenses, una de las buenas prácticas es crear dos imágenes: una para trabajar en el caso, y la segunda, para almacenarla como respaldo en caso de que la primera copia se estropee. Al crear una imagen forense se debe comprobar la integridad de la misma, verificando que la imagen es una copia fidedigna del elemento original. Esta verificación se realiza mediante algoritmos criptográficos como MD5 Y SHA1. En esta fase se sigue con el manejo de la cadena de custodia para evitar las acusaciones de mal manejo o manipulación de pruebas.

### 3.5. Fase de examinación

El objetivo de esta fase es que la evidencia sea visible, explicar su origen e importancia. El investigador debe documentar el contenido y estado de las pruebas en su totalidad. Una vez los datos se han expuesto, se procede a la reducción de los datos, separando la

información relevante de la irrelevante para el caso. En esta fase también se incluye el proceso de búsqueda que puede estar oculta.

En esta fase se asocian el investigador o analista forense con el examinar forense. El analista da una idea de los tipos de cosas que se deben buscar, mientras que el examinador forense proporciona los medios para encontrar información relevante que pudiera estar en el sistema. Es importante determinar palabras claves para ayudar a localizar información relevante para el caso dentro de toda la información recolectada, utilizando técnicas como el Data Carving. Esta lista de palabras claves debe estar compuesta por la mayor información posible sobre el caso o la persona que se investiga, como, por ejemplo: nombres y apellidos, usuarios, números de teléfono, números de identificación, fechas, otras palabras claves según sea el caso, ya sea extorsión, robo y otro delito informático.

Una vez los datos se han adquirido, en esta fase se procede a recuperar de archivos borrados, recuperar los archivos escondidos, identificación los archivos existentes que son fácilmente legibles (solo con abrirlos con el programa adecuado se pueden visualizar su contenido, sin ningún otro procedimiento adicional), identificar los archivos protegidos que tienen algún control de acceso (archivos cifrados) y se van consolidando en carpetas los archivos potencialmente analizables con el fin de reducir la búsqueda y centrarse en ciertos tipo de archivos relevantes para el caso. Una vez los archivos se han identificado, filtrado y clasificado, se puede desechar los archivos irrelevantes para el caso, centrándose en aquellos que sí lo son.

### 3.6. Fase de análisis

Con los archivos identificados y clasificados se procede el análisis de esa información. El objeto de esta fase es establecer un enlace creíble entre el atacante, la víctima y la escena del crimen a través de la evidencia digital. El examinador y analista forense trabajan para llegar a los siguientes objetivos y responder a las siguientes preguntas: Recopilar información sobre el individuo(s) que participan, el ¿quién lo hizo?; determinar la naturaleza exacta de los acontecimientos que se produjeron, el ¿qué hizo?; construir una cronología de eventos, el ¿cuándo lo hizo?; descubrir la información que explica la motivación por el delito, el ¿por qué lo hizo?; y descubrir qué herramientas o hazañas fueron utilizados, el ¿cómo lo hizo? No existe un único camino para analizar la información. El análisis depende del objetivo que se planteó en la fase de identificación y evaluación, y, a partir de este objetivo se va determinando el camino a seguir y se va refinando a medida que va avanzando el proceso forense. Una actividad importante en el análisis es establecer la línea del tiempo, para comprender el orden cronológico en que sucedieron los hechos.

### 3.7. Fase de presentación de informes

En esta fase es donde se recopila todas las notas y apuntes tomadas en las fases previas y se prepara un resumen detallado de todas las medidas adoptadas y las conclusiones que se alcanzaron en la investigación. Un buen informe depende del registro cuidadoso de todas las acciones y observaciones realizadas, que describan los resultados de las pruebas y exámenes realizados, y que expliquen las conclusiones extraídas de la evidencia. El informe puede ser impugnado por la contraparte, por esta razón, se debe documentar

la evidencia, las herramientas usadas (nombre, versión, etc.) y las metodologías usadas en el examen. La documentación apropiada permitirá recrear el proceso de principio a fin con el fin de corroborar los resultados y conclusiones presentadas en el informe. La documentación de software utilizado es importante porque si el procedimiento se recrea en un momento posterior y en el trascurso de ese periodo de tiempo haya salido una nueva versión de software, este puede que varíe en los resultados obtenidos. Esta premisa aplica para el software libre como para software comercial.

Es importante identificar el público al cual va dirigido el informe, no todos los grupos de personas tienen los mismos intereses y conocimientos técnicos. No es lo mismo redactar un informe para una fuerza del orden o como soporte en un caso judicial, el cual se requiere que todos los procedimientos, actividades realizadas estén de forma detallada, que un informe para los administrativos de la organización en el cual solo desean saber qué fue lo que sucedió, que activos se comprometieron, o para el equipo de seguridad de la organización que quieren detalles más técnicos. Se puede presentar el caso y es recomendable que se redacten varios informes dependiendo del grupo al cual va dirigido. Muchas herramientas forenses permiten la creación de forma automática, este tipo de informes pueden ser anexados a informe escrito. El informe debe ser soportado con el mayor número de evidencias, ya sean fotografiáis, capturas de video y acompañado de CD o DVD para presentar archivos cuyo formato no permite ser impreso como un video o audio.

### 3.8. Fase de revisión

Esta fase busca la mejora continua. La revisión a conciencia de las actividades realizadas en cada fase durante la investigación permitirá refinar estas acciones para una futura investigación. Se busca en enriquecer la pericia del investigador o del equipo forense, ya que no hay una sola forma de proceder en una investigación, cada caso tiene su particularidad y sus retos.

## 4. Formatos para el manejo de la prueba o evidencia

Para complementar la guía práctica, se propuso unos formatos para el manejo de la prueba o evidencia física y digital, y el registro de la cadena de custodia de las mismas, como se muestra en las Figuras 3-9. La construcción de dichos formatos es el resultado de la revisión de la literatura y el Manual de procedimientos para la cadena de custodia de la Fiscalía General de la Nación (Fiscalía General de la Nación, 2012).

## 5. Conclusiones

Dentro de las herramientas que manejan la filosofía del software libre encontramos una gama de posibilidades que nos posibilitan realizar un análisis forense en un entorno académico. Estás herramientas de fácil adquisición por su disponibilidad para su descarga y uso, su bajo costo es fundamentales en un entorno académico donde los recursos son limitados, donde el proceso se centra en la investigación y aprendizaje.

Las guías con las que se dispone a nivel internacional se están quedando cortas debido al ritmo de avance que tienen los dispositivos móviles y la falta de actualización de las mismas por parte de las instituciones que las soportan.

**ROTULO DE EVIDENCIA FÍSICA O MATERIAL DE PRUEBA**
Versión 1.0

| Código del caso | Fecha y hora de la recolección |
|---|---|
| | D D M M A A - H H M M |

**Nombre del caso**

**Lugar del hallazgo**

Descripción: _____

**Evidencia física o material de prueba**

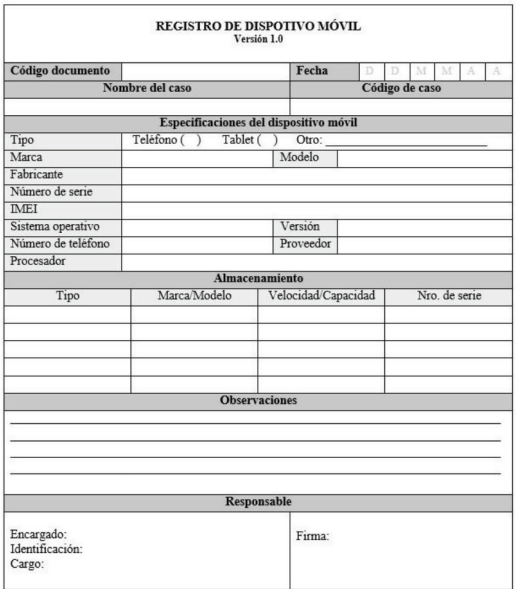
Descripción: _____

**Observaciones**

**Responsable**

| | |
|---|---|
| Encargado:<br>Identificación:<br>Cargo: | Firma: |

Figura 3 – Formato de rotulado de la evidencia física o material de prueba.



**REGISTRO DE DISPOTIVO MÓVIL**
Versión 1.0

| Código documento | | Fecha | D D M M A A |
|---|---|---|---|
| Nombre del caso | | Código de caso | |

**Especificaciones del dispositivo móvil**

| | | | |
|---|---|---|---|
| Tipo | Teléfono ( ) Tablet ( ) Otro: _____ | | |
| Marca | | Modelo | |
| Fabricante | | | |
| Número de serie | | | |
| IMEI | | | |
| Sistema operativo | | Versión | |
| Número de teléfono | | Proveedor | |
| Procesador | | | |

**Almacenamiento**

| Tipo | Marca/Modelo | Velocidad/Capacidad | Nro. de serie |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Observaciones**

**Responsable**

| | |
|---|---|
| Encargado:<br>Identificación:<br>Cargo: | Firma: |

Figura 4 – Registro del dispositivo móvil.

Los modelos forenses estudiados están más orientados al proceso forense en general, a los equipos de cómputo tradicionales y a las redes de comunicación. No se encuentra muchos modelos que estén orientados a los dispositivos móviles. Muchas de estos modelos hacen suposiciones, como, por ejemplo, que el lector conoce el proceso de

**REGISTRO DE EVIDENCIA DIGITAL**
**Versión 1.0**

| | | | |
|---|---|---|---|
| **Código documento** | | **Fecha** | D D M M A A |
| **Nombre del caso** | | **Código de caso** | |
| | | | |
| **Dispositivo de origen** | | | |
| Tipo | Teléfono ( ) Tablet ( ) Otro: _____ | | |
| Marca | | Modelo | |
| Sistema operativo | | Versión | |
| Tipo de memoria | | Capacidad | |
| | | | |
| **Medio de almacenamiento de la prueba** | | | |
| Nro. de serie | Tipo | Capacidad | Ubicación del medio de almacenamiento |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| **Observaciones** | | | |
| | | | |
| **Responsable** | | | |
| Encargado:<br>Identificación:<br>Cargo: | | Firma: | |

Figura 5 – Registro de la evidencia digital.

**REGISTRO CADENA DE CUSTODIA**
**Versión 1.0**

| | | | | | | |
|---|---|---|---|---|---|---|
| Código del caso | | | Nombre del caso | | | |
| 1. Descripción del elemento material de prueba o evidencia física | | | | | | |
| | | | | | | |
| 2. Documentación del elemento material de prueba o evidencia física | | | | | | |
| H | R | E | Nombres y apellidos | Cédula de ciudadanía | Entidad | Cargo | Firma |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

**Convenciones:**

H = Marcar con una X si corresponde a quien HALLÓ el elemento material de prueba o evidencia física
R = Marcar con una X si corresponde a quien RECOLECTÓ el elemento material de prueba o evidencia física
E = Marcar con una X si corresponde a quien EMBALÓ el elemento material de prueba o evidencia física

Se puede marcar una o varias opciones para un mismo nombre, según sea el caso

Figura 6 – Registro de la cadena de custodia.

la cadena de custodia. Lo que dificulta la apropiación de estos criterios por parte de aquellas personas que quieren iniciar en el aprendizaje de esta rama del conocimiento.

Como trabajo futuro, se pretende incorporar el análisis forense en vivo, para la adquisición y estudio de la información obtenida de la memoria volátil del dispositivo.

**REGISTRO CADENA DE CUSTODIA DE PRUEBAS DIGITALES**
**Versión 1.0**

| Fecha | | | | | | | Hora militar | Nombre y apellidos de quien recibe el elemento material de prueba o evidencia física | Cédula de ciudadanía | Entidad | Calidad en la que actúa (examinador, custodio, perito, transportador) | Traspaso o traslado (Entrega almacén, Almacenamiento, Análisis, Presentación, Audiencia, Consulta, Disposición final) | Observación al estado en que se recibe el embalaje o contenedor del elemento materia de prueba o evidencia física | Firma |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D | D | M | M | A | A | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |

Figura 7 – Registro de la cadena de custodia digital.

**REGISTRO RESPONSABLES DE CADENA DE CUSTODIA**
**Versión 1.0**

| **Código del caso** | **Evidencia** | Física ( ) Digital ( ) |
|---|---|---|
| | **Código documento** | |
| **Nombre del caso** | | |

| **Responsable** | | **Fecha y hora** |
|---|---|---|
| Entregado por | Firma | D D M M A A - H H M M |
| Recibido por | Firma | D D M M A A - H H M M |
| **Responsable** | | **Fecha y hora** |
| Entregado por | Firma | D D M M A A - H H M M |
| Recibido por | Firma | D D M M A A - H H M M |
| **Responsable** | | **Fecha y hora** |
| Entregado por | Firma | D D M M A A - H H M M |
| Recibido por | Firma | D D M M A A - H H M M |
| **Responsable** | | **Fecha y hora** |
| Entregado por | Firma | D D M M A A - H H M M |
| Recibido por | Firma | D D M M A A - H H M M |
| **Responsable** | | **Fecha y hora** |
| Entregado por | Firma | D D M M A A - H H M M |
| Recibido por | Firma | D D M M A A - H H M M |

Figura 8 – Registro de la cadena de custodia digital

También, tener en cuenta la información que el usuario almacena en la nube que puede ser relevante y una fuente de evidencias en la investigación forense.

Otros puntos a trabajar el estudio del malware para plataformas móviles, en especial para Android, el estudio de archivos APK (Application PacKage File) y el estudio de técnicas de intrusión para los dispositivos móviles y la forma de cómo el análisis forense

puede identificarlos. Por último, el estudio de las técnicas anti-forenses, que son usadas por el intruso para borrar, destruir o modificar los rastros dejados para dificultar la labor del investigador forense.

## Agradecimientos

Los autores desean agradecer la colaboración de todos los socios dentro del proyecto Centro de Excelencia y Apropiación en Internet de las Cosas (CEA-IoT). Los autores también desean agradecer a todas las instituciones que apoyaron este trabajo: el Ministerio de Tecnología de la Información y Comunicaciones – MinTIC de Colombia y al Departamento Administrativo de Ciencia, Tecnología e Innovación – Colciencias, a través del Fondo Nacional de Financiamiento para la Ciencia, Tecnología y la Innovación Francisco José de Caldas (ID Proyecto: FP44842-502-2015).

## Referencias

ArxSys. (2017). Digital Forensics Framework.

Ashcroft, J., Daniels, D. J., & Hart, S. V. (2012). *Forensic Examination of Digital Evidence: A Guide for Law Enfocement*.

Ayers, R., Brothers, S., & Jansen, W. (2014). *Guidelines on Mobile Device Forensics - Revision 1*.

CAINE Linux. (2017). CAINE - Computer Forensics Linux Live Distro.

Casey, E. (n.d.). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Academic Press.

Ciardhuáin, S. Ó. (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence*, *3*(1), 1–22.

Cohen, F. (2009). *Digital Forensic Evidence Examination*. *Fifth Edition*. Fred Cohen & Associates.

DEFT. (2017). DEFT Linux - Computer Forensics live CD.

DFRWS. (2001). *A Road Map for Digital Forensic Research: : Report from the first Digital Forensic Research Workshop*.

Fiscalía General de la Nación. (2012). *Manual de procedimientos para la cadena de custodia de la Fiscalía General de la Nación*.

Gudjonsson, K. (2017). log2timeline.

Jansen, W., & Ayers, R. (2007). *Guidelines on Cell Phone Forensics - SP800-101*.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response - SP 800-86*.

National Institute of Justice. (2001). *Electronic Crime Scene Investigation. A Guide for First Responders*.

National Institute of Justice. (2004). *Electronic Crime Escene Investigation: A Guide for First Responders. Second Edition*.

Nelson, B., Phillips, A., & Steuart, C. (2010). *Guide to Computer Forensics and Investigations* (Fourth Edi). Information Security Professionals.

NowSecure. (2017). AFLogical OSE: Open source Android Forensics app and framework.

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, *1*(3), 1–12.

Rico-Bautista, D., & Alvernia-Acevedo, S. A. (2017). Análisis de una red en un entorno IPv6: una mirada desde las intrusiones de red y el modelo TCP/IP. *Revista Colombiana Tecnologías de Avanzada*, *1*(29), 81–91. https://doi.org/https://doi.org/10.24054/16927257.v29.n29.2017.2490

Rueda-Rueda, J. S., & Rico Bautista, D. (2016). Informática forense en dispositivos Android. *Revista Ingenio*, *9*(1).

Rueda, R. J. S., & Rico, B. D. W. (2016). Defining of a practical model for digital forensic analysis on Android device using a methodology post-mortem. In *Telematics and Information Systems (EATIS), 2016 8th Euro American Conference on* (pp. 1–5). Cartagena de Indias, Colombia.

SANS Institute. (2017). SANS SIFT Kit/Workstation: Investigative Forensic Toolkit.

Santoku Linux. (2017). Santoku Linux.

StatCounter. (2017). Android overtakes Windows for first time | StatCounter Global Stats.

The Sleuth Kit. (2017a). Autopsy.

The Sleuth Kit. (2017b). The Sleuth Kit (TSK).

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies