RESUMEN – TRABAJO DE GRADO

AUTORES	**JOHAN SMITH RUEDA RUEDA**
FACULTAD	**FACULTAD DE INGENIERÍAS**
PLAN DE ESTUDIOS	**INGENIERÍA DE SISTEMAS**
DIRECTOR	**MS.C. DEWAR RICO BAUTISTA**
TÍTULO DE LA TESIS	**ANÁLISIS DIGITAL FORENSE EN UN DISPOSITIVO MÓVIL CON SISTEMA OPERATIVO ANDROID UTILIZANDO UNA METODOLOGÍA POST-MORTEM**

RESUMEN

ESTE DOCUMENTO PRESENTA UN MODELO CUYO PROPÓSITO ES SERVIR DE GUÍA PARA REALIZAR UN DIGITAL FORENSE EN UN DISPOSITIVO MÓVIL CON SISTEMA OPERATIVO ANDROID. ESTE MODELO CONSTA DE OCHO FASES, Y TIENE EN CUENTA LAS BUENAS PRÁCTICAS Y RECOMENDACIONES REALIZADAS POR INSTITUCIONES REFERENTES A NIVEL INTERNACIONAL EN EL PROCESO FORENSE, LA RESPUESTA DE INCIDENTES Y EL MANEJO DE LA EVIDENCIA DIGITAL.

CARACTERÍSTICAS

PÁGINAS: 124	PLANOS: 0	ILUSTRACIONES: 10	CD-ROM: 1

ANÁLISIS DIGITAL FORENSE EN UN DISPOSITIVO MÓVIL CON SISTEMA OPERATIVO ANDROID UTILIZANDO UNA METODOLOGÍA POST-MORTEM

JOHAN SMITH RUEDA RUEDA

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
OCAÑA
2015

ANÁLISIS DIGITAL FORENSE EN UN DISPOSITIVO MÓVIL CON SISTEMA OPERATIVO ANDROID UTILIZANDO UNA METODOLOGÍA POST-MORTEM

JOHAN SMITH RUEDA RUEDA

Trabajo de grado presentado para optar el título de
INGENIERO DE SISTEMAS

Director
Ing. DEWAR WILMER RICO BAUTISTA
Magister en Ciencias Computacionales

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
INGENIERÍA DE SISTEMAS
OCAÑA
2015

AGRADECIMIENTOS

Primeramente agradecido con Dios por todas sus bendiciones. A mis padres Martin Geovany Rueda y Yolima Rueda por su gran esfuerzo y dedicación por darme una educación. Por su apoyo incondicional en todos mis sueños y emprendimientos. Sus consejos y palabra de ánimo. A mis hermanos Jhon Alexander y Jennifer, gracias.

También agradezco a mis abuelos y tíos, que de una forma y otra contribuyeron y me ayudaron en mi periodo de formación como ingeniero de sistemas.

A Meredith Mora, una gran amiga que me apoyo en este proceso. Porque hay contribuciones muy valiosas que no se pueden medir en términos materiales.

A mis buenos amigos y compañeros del semillero de investigación SIGLAS. Gracias por animarme a unirme a este grupo, allí comenzó todo este proceso. He aprendido mucho a su lado. Gracias por los momentos vividos y ayuda brindada.

Al ingeniero Dewar Rico Bautista, director de nuestro semillero. Gracias por su valiosa ayuda y contribución en nuestra formación. Gracias por su amistad, sus consejos y ayuda.

A mi institución, la Universidad Francisco de Paula Santander Ocaña. A los docentes que contribuyeron en mi formación.

A todos y cada uno de ustedes, a los que falte por nombrar, bendiciones y gracias totales.

Johan Smith Rueda

DEDICATORIA

Este trabajo se lo dedico a mi familia, las personas que estuvieron a mi lado en todo este proceso. A los que de una u otra forma me han apoyado, animado y ayudado. A aquellas personas que han hechos mis triunfos y frustraciones como suyas. A los que creyeron en mí, cuando a veces ni yo mismo lo hacía. Gracias totales.

Johan Smith Rueda

«*La verdadera ignorancia no es la ausencia de conocimientos, sino el hecho de rehusarse a adquirirlos*»
—Karl Popper

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

La informática forense es una rama de las ciencias forenses. Está relacionada con las actividades propias asociadas con la evidencia y procura describir e interpretar la información de los medios informáticos para relacionar hechos y establecer una hipótesis relacionada con un caso objeto de investigación. Para esto, utiliza procedimientos y herramientas para adquirir, preservar, examinar, analizar las pruebas obtenidas de los medios informáticos y a través de un proceso científico establecer la evidencia propia del caso. Por último, se presenta los respectivos informes donde se detallan las evidencias encontradas, los procedimientos realizados y las herramientas utilizadas con el mayor detalle posible.

En este trabajo se estudian algunas de las herramientas con licencia GPL para el análisis forense en un dispositivo móvil con sistema operativo Android. También se estudia algunos modelos forenses propuestos por instituciones o autores y que son aceptados a nivel internacional como guías para realizar el proceso forense.

De la revisión de la literatura se identificaron las guías que son referentes en lo relacionado con el análisis forense, el manejo de la evidencia y la cadena de custodia. Se tuvo en cuenta las buenas prácticas establecidas por las instituciones y fuerzas del orden autoras de dichas guías.

Una vez se identificaron las buenas prácticas, se caracterizaron los modelos forenses estudiados y se eligió las herramientas a usar se propuso un modelo práctico para el análisis forense digital en un dispositivo móvil con sistema operativo Android.

Este modelo práctico está compuesto por ocho fases y busca ser una guía para todas aquellas personas que se inician en el análisis forense digital y personas que deseen investigar sobre este tema.

1. ANÁLISIS DIGITAL FORENSE EN UN DISPOSITIVO MÓVIL CON SISTEMA OPERATIVO ANDROID UTILIZANDO UNA METODOLOGÍA POST-MORTEM.

1.1 PLANTEAMIENTO DEL PROBLEMA

La evolución que ha tenido dispositivos móviles en la última década ha marcado nuevas tendencias. Los teléfonos celulares ya no se limitan a realizar llamadas y el envío de SMS, sino que, las características –de hardware y software– que actualmente tienen los han convertido en unos "computadores de mano", ofreciendo la posibilidad de realizar tareas más complejas y funcionales, permitiendo así una mayor independencia de los computadores de escritorio y las *laptop*. Por otro lado, han aparecido nuevos dispositivos como las tabletas electrónicas.

Con el auge de los dispositivos móviles las actividades personales y laborales que se realizan a diario se han trasladado a dichas terminales[1]. La información que se maneja —en volumen e importancia— es cada vez mayor. Los principales fabricantes de teléfonos inteligentes están apuntando sus esfuerzos es crear terminales que cubran un segmento de mercado mayor al del usuario común; este segmento es el de los profesionales y ejecutivos. Dichas personas se mueven en un entorno competitivo donde las herramientas que usen para facilitar sus tareas son fundamentales. Los actuales dispositivos móviles permiten a los usuarios tener las funcionalidades de un computador de escritorio pero con la movilidad que estos no ofrecen. Esta razón, ha generado que el mercado de los dispositivo móviles este creciendo exponencialmente desde hace algunos años, razón suficiente y llamativa para que también se convierta en un objetivo importante para los cibercriminales[2] [3].

Las actividades criminales se han trasladado de los equipos de cómputo, servidores y otros dispositivos y han fijado sus objetivos en el naciente mercado de los dispositivos móviles, la potencia de estas terminales permiten que se lleven ataque sofisticados, que se creen diferentes versiones de malware para móviles. No sólo la información personal está en peligro también la organizacional, tendencias como la BYOD (*Bring Your Own Device*) donde los empleados tienen la posibilidad de llevar y utilizar sus dispositivos móviles para acceder los recursos de la empresa permiten que toda la información que se genera y circula por los dispositivos móviles este expuesta para ser obtenida con ayuda de técnicas y así se pueda sacar provecho de ella.

Los hechos realizados por los cibercriminales no son el único problema que enfrenta los dispositivos móviles. La informática forense, aunque lleva un poco más de dos décadas no es área de estudio tan conocida, aunque en los últimos años ha venido tomando fuerza. Pero si la informática forense se puede considerar relativamente nueva, esta área del conocimiento llevado hacia los dispositivos móviles lo es aún más. Se hace necesario el

[1] IAB SPAIN RESEARCH. VI Estudio Anual IAB Spain Mobile Marketing. Madrid, 2014.
[2] ESET. Guía de seguridad para usuarios de Smartphone. 2012.
[3] JAKOBSSON, Markus y RAMZAN, Zulfikar. Crimeware: Understanding New attacks and Defenses. Boston. Pearson Education Inc., 2008.

desarrollo de nuevas metodologías y guías que estén acordes con las características de dichas terminales.

Jeimy Cano afirma que, el proceso forense debe ir acompañado de la confiablidad de las herramientas y la formación y los conocimientos del investigador[4]. Así mismo, un acercamiento metodológico busca minimizar los errores humanos que se omisión y/o desconociendo, asegurar que la herramienta usada es confiable y garantizar que los procedimientos que se siguen son los adecuados[5].

1.2 FORMULACIÓN DEL PROBLEMA

¿Son las metodologías de análisis digital forense tradicional una guía idónea para realizar un análisis forense en un dispositivo móvil, teniendo en cuenta las características de dichas terminales?

1.3 JUSTIFICACIÓN

Android es el sistema operativo para dispositivos móviles más popular del mercado[6], en el 2014 registra una cuota de mercado del 84.62 %. El *malware* financiero es el más usado con un 59.06 %, siendo el Trojan-SMS el más popular con un 57.08 % y Trojan-Banker con el 1.98 % restante[7]. La gran cantidad de aplicaciones la incrementado su popularidad; esta popularidad no es solo para los usuarios, también, para los cibercriminales. Según Kaspersky Lab., el 99 % del malware para móviles está dirigido a este sistema operativo. Kaspersky Lab., también resalta que dos razones para dicho fenómeno son su popularidad y su funcionalidad[8].

Un informe de Symantec sobre plataformas móviles y la seguridad que estas manejan, describe algunos problemas relacionados con Android. Google Inc. no tiene un modelo de certificación riguroso para aplicaciones que se suben a su tienda, 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

[4] CANO, Jeimy. Introducción a la informática forense: Una disciplina técnico-legal. En: Revista Sistemas. 2007. p 64-73.
[5] CANO, Jeimy, *et al*. Evidencia digital en el contexto colombiano: Consideraciones técnicas y jurídicas para su manejo. [En línea] <http://52.0.140.184/typo43/index.php?id=856>
[6] Según Google Inc. (en www.android.com) para finales de 2013 el número de dispositivos supera los mil millones a nivel mundial.

[7] KASPERSKY LAB y INTERPOL. Mobile Cyber Threats. 2014.
[8] kASPERSKY LAB. Más de la mitad de usuarios de Android no protege sus equipos de amenazas informáticas. [En línea] <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>

otorgarla o no los permisos, de esta forma el riesgo es mayor[9].

Por estos motivos, los usuarios del sistema operativo Android, están más expuestos a los peligros informáticos que los usuarios de otros sistemas operativos móviles. Cuando se sospecha o se confirma que una terminal ha sido comprometida por algún tipo de ataque informático se hace necesario un análisis de dicho dispositivo para verificar y comprobar los hechos[10].

Es allí donde la informática forense juega un papel importante, ya que es la encargada de recoger, preservar y examinar la información contenida en cualquier medio informático. Para ello utiliza las metodologías y herramientas forenses y así poder formular hipótesis y establecer los hechos relevantes en la investigación[11] [12].

Pero los equipos de cómputo tradicionales tienen diferencias con los dispositivos móviles y estas diferencias hacen que sea necesario llevar un enfoque de la informática forense hacia estos terminales, para ello, se pretende evaluar si las metodología forenses que se han desarrollado anteriormente ofrecen al investigador una guía idónea que permita llevar de forma apropiada una investigación en un dispositivo móvil.

1.4 OBJETIVOS

1.4.1 General

Diseñar una guía práctica para el análisis digital forense en los medios de almacenamiento permanente dispositivos móviles con sistema operativo Android.

1.4.2 Específicos

- Caracterizar las herramientas utilizadas en el análisis digital forense con licencia GPL para elegir la suite de herramientas a usar.
- Analizar las metodologías usadas en un análisis digital forense tradicional y para los dispositivos móviles.
- Plantear una guía práctica que sirva como soporte para el análisis digital forense en un dispositivo móvil, teniendo en cuenta las características propias de dichas terminales.

[9] SYMANTEC. Análisis de Symantec de las plataformas iOS de Apple y Android de Google revela mayor seguridad en comparación con las PCs, pero aún existen algunas brechas. [En línea] <http://www.symantec.com/es/mx/about/news/release/article.jsp?prid=20110823_01>

[10] JARAMILLO CABRERA, Guillermo Elías. Técnicas de análisis forense digital aplicadas a dispositivos y sistemas móviles. En: Apuntes de Ciencia y Sociedad. 2011. p 167-171.

[11] CANO, Jeimy. *Op. Cit*.

[12] ARIAS CHAVES, Michael. Panorama general de la informática forense y de los delitos informáticos en Costa Rica. En: InterSedes: Revista de las Sedes Regionales. 2006. p. 141-154.

1.5 DELIMITACIONES

1.5.1 Operativa. De todo lo comprende el análisis digital forense, en este proyecto se enfocará en el análisis forense en los dispositivos móviles, y se estudiará las terminales que corren el sistema operativo Android. De todas las posibilidades que se puede dar al analizar un dispositivo móvil se trabajará en los medios de almacenamiento permanente. Se realizará un análisis forense de la memoria interna del terminal, la SDCard, y la tarjeta SIM.

Para este proyecto no se tendrá en cuanta en análisis de malware, ni el análisis de los APK (*Application PacKage File*), ni la recolección de datos en la nube que el usuario pueda haber utilizado desde su dispositivo móvil.

Por otro lado, las prácticas solo se realizarán con herramientas de software, no se implementará herramientas hardware forense como bloqueadores de escritura, o para esterilización de los medios donde se almacenará las imágenes forenses entre otros, sino será por medio del software disponible.

1.5.2 Conceptual. La base conceptual que trabaja en este proyecto comenzará de lo general a lo específico. En lo general se trabajará con la terminología necesaria en la informática forense, sus principios, metodologías y se irá especificando en la informática forense orientada a los dispositivos móviles, concretamente los que ejecutan el sistema operativo Android.

1.5.3 Geográfica. Este proyecto se desarrollará en el laboratorio del Semillero de Investigación GNU/Linux And Security (SIGLAS) de la Universidad Francisco de Paula Santander seccional Ocaña.

1.5.4 Temporal. Este trabajo tendrá una duración de doce (12) semanas.

2. MARCO REFERENCIAL

2.1 MARCO HISTÓRICO

Los análisis forenses datan desde los comienzos de la ciencia forense en el siglo XVIII. La informática forense (*Computer Forensic*) o el análisis digital forense en una rama de las ciencias forenses que nace en la década de 1980 en respuesta a la necesidad que tenían los peritos informáticos de encontrar una nueva fuente de evidencia.

En 1978 Florida, Estados Unidos reconoce los crímenes informáticos mediante la *Computer Crimes Act*. Esta ley se ocupa de los casos de sabotaje, copyright, modificación de datos y ataques similares.

En la década de 1980 nacen algunas herramientas que ayudaron a la informática forense. En 1981 nace *Copy II PC* de *Central Point Software* usada para la copia exacta de disquetes que generalmente estaba protegidos para evitar las copias piratas. Dicha herramienta fue integrada a *PC Tools*. En 1982, se publica *UnErase: Norton Utilities 1.0* que entre su conjunto de herramientas se encuentra UnErase, cuyo objetivo era recuperar archivos borrados accidentalmente. Otras herramientas integradas en UnErase son FileFix o TimeMark.

En 1984 el *Federal Bureau of Investigation* (FBI) formó el *Magnetic Media Program*; en 1991 sería el *Computer Analysis and Response Team* (CART).

En 1987 se crea la *Higth Tech Crime Investigation Association* (HTCIA), agrupa profesionales de agencias gubernamentales y de compañías privadas con el fin de centralizar el conocimiento y brindar cursos. Ese mismo año nace la compañía *AccessData* creadora de productos orientados a la recuperación de contraseñas y el análisis forense con herramientas como la actual *Forensic Toolkit* (FTK).

En 1988 se crea la *International Association of Computer Investigative Specialists* (IACIS), cuyo propósito en certificar a los profesionales de agencias gubernamentales en el *Certified Forensic Computer Examiner* (CFCE). Ese mismo año se creó el programa *Seized Computer Evidence Recovery Specialists* con el objetivo de formar a los profesionales de la informática forense.

El término *Computer Forensic* fue acuñado en 1992 por P. A. Collier y B. J. Spaul en el libro *A forensic methodology for countering computer crime*. Otros libros contribuyeron al desarrollo del término y la metodología como *Higth-Technology Crime: Investigating Cases Involving Computers* de Kenneth S. Rosenblatt.

En 1995 se crea la *International Organizations on Computer Evidence* (OICE) con el objetivo de ser un punto de encuentro entre especialistas para el intercambio de

información sobre el manejo de la evidencia digital, garantizando la autenticidad y seguridad de la información que constituye la prueba.

Desde 1996 la Interpol organiza la *International Forensic Science Symposium* como foro para debatir y compartir los avances que se dan en el área forense, compartiendo conocimiento y uniendo fuerzas.

En febrero de 1998 se estableció *The Scientific Working Group on Digital Evidence* (SWGDE) a través de un esfuerzo de colaboración de los directores de los laboratorios de los delitos federales. La SWGDE basado en lo realizado por la IOCE se encargó de la elaboración de directrices interdisciplinarias y estándares para la reparación, preservación y el examen de evidencia digital, incluyendo audio, imágenes y dispositivos electrónicos (Federal Bureau of Investigation, 2000).

En 1999 la SWG redacto el documento *Proposed Standards for the Exchange of Digital Evidence* y fue presentado en el *International Hi-Tech Crime and Forensics Conference* (IHCFC) celebrado del 4 al 7 de octubre de ese mismo año en Londres, Reino Unido. En dicho documento se propuso el establecimiento de normas para el intercambio de pruebas digitales entres naciones (Federal Bureau of Investigation, 2000).

En 2001 nace la *Digital Forensic Research Workshop* (DFRWS), un grupo de debate y discusión de carácter internacional para compartir información.

2.2 MARCO TEÓRICO

La informática forense como disciplina de las ciencias forense está regida por unas directrices que buscan servir de guías metodológicas en el proceso forense. Las recomendaciones de la *National Institute of Standards and Technology* en la *Guide to Integrating Forensic Techniques into Incident Response* define cuatro fases en el proceso forense: Recopilación de los datos (donde se definen las posibles fuentes de datos, se hace la adquisición de los datos y se considera la respuesta a incidentes), examen de los datos, análisis y la presentación de los informes[13].

Desde los inicios de la informática forense se han desarrollado modelos metodológicos, entre ellos tenemos: El modelo Casey (2000), el modelo Lee (2001), modelo Reith, Carr y Grunsch (2002), modelo integrado por Brian Carrier y Eugene Spafford (2003), el modelo mejorado propuesto por VenansiusBaryamureeba y FlerenceTuchabe (2004) y el modelo extendido de SéamusÓCiardhuáin (2004) (De León Huerta, 2009). El modelo más usado es el Casey, que ha sido mejorado desde su primera aparición en el 2011[14]

[13] KENT, Karen, et al. Guide to Integrating Forensic Techniques into Incident Response. Gaithersburg, MD. NIST, 2006.
[14] CASEY, Eoghan. Digital evidence and computer crime: Forensic science, computers and the internet. San Diego, California. Academic Press, 2011.

Como cada investigación es única y es imposible conocer a priori los aspectos que se deben tener en cuenta al realizar un procedimiento forense, por esta razón no se puede definir una metodología única para abordar este tipo de investigación. De allí nacen las aproximaciones metodológicas, y sus objetivos son: 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[15]. Cano 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[16].

La *International Organization on Computer Evidence* (IOCE), proporcionó unos principio internacionales para la recolección estandarizada de evidencia digital. Estos principios tienen que ver con la coherencia con todos los sistemas jurídicos, la previsión de un lenguaje común, la durabilidad, la capacidad de que la evidencia pueda ser usada por diferentes países, el infundir confianza con la integridad de las pruebas, y otros principios que tienen que ver con la evidencia digital, su adquisición, almacenamiento y las personas responsables de manejarla[17].

La evidencia digital debe cumplir con unos principios de admisibilidad. Estos principios son: La autenticidad, la confiabilidad, la suficiencia y la conformidad con las leyes reglas de la administración de la justicia. La autenticidad se puede entender como aquella característica que muestra la no alterabilidad de los medios originales y la confirmación de que los registros obtenidos correspondan a la realidad evidenciada en la fase de identificación y recolección. La confiabilidad demuestra que los elementos probatorios vienen de fuentes creíbles y verificables. Las pruebas recolectadas deben ser toda la evidencia necesaria para adelantar el caso[18].

El RFC 3227 "*Guidelines for Evidence Collection and Archiving*" es un documento que especifica las buenas prácticas que se deben tener en cuenta a la hora de recolectar y archivar la evidencia. Estas buenas prácticas tienen que ver con los principios que rigen la recolección de la evidencia, su volatilidad y las cosas que se deben evitar al momento de la recolección y otras consideraciones como la de privacidad, las legales. En cuanto al momento de archivar dicha evidencia se detalla la cadena de custodia, la documentación al respecto. Dónde y cómo se debe archivar dicha evidencia y las herramientas necesarias para llevar dicho proceso[19].

---

[15] CANO, Jeimy, *et al*. *Op. Cit*

[16] CANO, Jeimy. *Op. Cit*.

[17] FEDERAL BUREAU OF INVESTIGATION. Digital Evidence: Standards and Principles. Scientific Working Group on Digital Evidence (SWGDE) International Organization on Digital Evidence (IOCE). FBI, 2000.

[18] CANO, Jeimy. Admisibilidad de la evidencia digital: de los conceptos legales a las características técnicas. En: Boletín de los Sistemas Nacionales Estadísticos y de Información Geográfica. 2005. p 93-108.

[19] BREZINSKI, Dominique y KILLALEA, Tom. RFC 3227: Guidelines for Evidence Collection and Archiving. 2002.

2.3 MARCO CONCEPTUAL

2.3.1 Informática forense. La informática forense 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»[20].

2.3.2 Investigador forense. Profesional científico, formal en los procedimientos y en el uso de las herramientas, capacitado para extraer, preservar, evaluar la evidencia obtenida en los medios informáticos; que busca describir e interpretar dicha evidencia para establecer los hechos y formular las hipótesis relacionadas con el caso. Jeymi Cano establece un perfil que debe tener el invetigador forense[21] (Ver Figura 1).

Figura 1: *Perfil del investigador forense según Jeimy Cano*

2.3.3 Intruso o *cracker*. La NFC RFC 2828 - *Internet Security Glossary* define al intruso como una entidad que que gana o intenta obtener acceso a un sistema o los recursos del sistema sin tener autorización para hacerlo; y al cracker como alguien que trata de romper

[20] CANO, Jeimy. Computación forense. Descubriendo los rastros informáticos. México. Alfaomega, 2009.
[21] CANO, Jeimy. *Op. Cit.*

la seguridad, y tener acceso al sistema de otra persona sin ser invitado a hacerlo[22]. Aunque en la actualidad se usa más el término ciberdelicuente o cibercriminal que *cracker*.

2.3.4 Evidencia digital. La evidencia digital son 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».

2.3.5 Principio de admisibilidad. La evidencia digital debe cumplir con unos principios para garantizar su validez probatoria. Según la legislación colombiana estos principios son: La autenticidad, la confiabilidad, la suficiencia y la conformidad con las leyes y reglas de la administración de justicia[23].

2.3.6 Técnicas anti-forenses. Jeimy Cano define la tecnica anti-forense como «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»[24].

2.3.7 Principio de Lorcard. El principio de intercambio o transferencia de Locard dice que cualquier persona u objeto que entra en la escena del crimen deja un rastro y se lleva uno consigo mismo[25].

2.3.8 Análisis post-mortem. Este análisis post-mortem se realiza utilizando un equipo dedicado específicamente para fines forenses: examinar dispositivos de almacenamiento permanente (discos duros, tarjetas SD, pendrive, etc.), datos o cualquier tipo de información recabada en un sistema que ha sufrido un incidente de seguridad[26].

2.3.9 Análisis en caliente. Este análisis realiza en un sistema que se presume ha sido afectado o esté sufriendo un incidente de seguridad. Para este tipo de análisis se utiliza un CD con herramientas de respuesta ante incidentes y análisis forense compiladas de forma que no se realicen modificaciones en el sistema. Una vez se realiza el análisis en caliente y el incidente es confirmado se realiza el análisis post-mortem[27].

---

[22] SHIREY, Robert W. RFC 2828 - Internet Security Glossary. 2002.
[23] CANO, Jeimy. Admisibilidad de la evidencia digital: de los conceptos legales a las características técnicas. En: Boletín de los Sistemas Nacionales Estadísticos y de Información Geográfica. 2005. p 93-108.
[24] CANO, Jeimy. Introducción a la informática forense: Una disciplina técnico-legal. En: Revista Sistemas. 2007. p 64-73.
[25] ZUCCARDI, Giovanni Y GUTIÉRREZ, Juan David. Informática forense. 2006.
[26] FERNÁNDEZ BLEDA, Daniel. Informática forense. Teoría y práctica. Sevilla, España. 2004.
[27] FERNÁNDEZ BLEDA, Daniel. *Op. Cit.*

2.4 MARCO LEGAL

2.4.1 Legislación internacional. A nivel internacional se ha desarrollado legislaciones que trate el área de lo que se vive en el mundo digital, en la redes de computadores. Estas legislaciones han tratado temas como los delitos informáticos y la protección de los datos personales.

2.4.1.1 Convenio sobre la ciberdelicuencia de la Unión Europea. En junio de 2001 el Consejo de Europa aprobó el 'Convenio sobre la ciberdelicuencia' en el cual se definen cuatro tipos de delitos informáticos:

- Delitos relacionados con los contenidos.
- Delitos relacionados con las infracciones a los derechos de autor.
- Delitos relacionados con la informática.
- Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos.

2.4.1.2 España. El 23 de noviembre de 1995 mediante Ley Orgánica 10/1995 fue aprobada el nuevo Código Penal español en el cual se contemplan una serie de delitos informáticos. Los principales delitos relacionados con la informática, las redes de computadores y los servicios de comunicación son los siguientes:

- Delitos contra la intimidad y el secreto de las comunicaciones (artículo 197.1).
- Estafas electrónicas (artículo 248.2).
- Infracción de los derechos de propiedad intelectual (artículo 270).
- Delitos de daños (artículo 246.2).
- Utilización de ordenadores y de terminales de telecomunicaciones sin consentimiento de su titular (artículo 256).
- Descubrimiento y relevación de secretos contenidos en documentos o soportes informáticos (artículo 278).
- Falsedad de documentos electrónicos (artículo 390).
- Fabricación o tenencia de útiles para la comisión de delitos (artículo 400).
- Distribución entre menores de edad de material pornográfico (artículo 186).
- Distribución de pornografía infantil (artículo 189).

2.4.1.3 Estados Unidos. En 1984 la ley conocida como *The Computer Fraud and Abuse Act* (CFAA) que tipifica delitos como el abuso o fraude a entidades, acceso no autorizado a sistemas y redes informáticas.

En 1986 se aprobó la *Electronic Communications Privacy Act* (ECPA), que establece la ilegalidad de interceptar las comunicaciones almacenadas o trasmitidas sin autorización, siendo las bases para la privacidad de las comunicaciones electrónicas. También se prohíbe la distribución o posesión de dispositivos de interceptación de comunicaciones telefónicas,

orales y electrónicas; pero se dan excepciones para los operadores de telecomunicaciones o los empleados del gobierno de los Estados Unidos.

Posteriormente, la *Digital Millenium Copyrigth Act* (DMCA) de 1998, es una ley federal que prohíbe la violación de las medidas tecnológicas de seguridad diseñadas para proteger contenidos y programas protegidos por los derechos de autor.

The Computer Fraud and Abuse Act, de 1994 (18 U.S.C. Sec 1030) es una nueva ley federal que modifica la CFAA y contempla nuevos delitos como la distribución de virus informáticos; la modificación, distribución, copia o trasmisión no autorizada de datos; la alteración del normal funcionamiento de los equipos o redes informáticos, etcétera.

La ley más reciente es la *Patriot Act* (Ley Patriota) de 2001, que fue aprobada a raíz de los atentados del 11 de septiembre de 2001 en Estados Unidos, tipifica como delitos de ciberterrorismo aquellos ataques informáticos que supongan pérdidas superiores a 5.000 dólares, con penas de prisión entre 5 y 20 años. Además, otorga el calificativo de 'ciberterroritas' a los *hackers* y piratas informáticos.

2.4.1.4 Alemania. La ley de mayo de 1986 contra los delitos informáticos y económicos, tipifica como delitos prácticas como:

- Espionaje de datos.
- Estafas y fraudes por medios informáticos.
- Utilización abusiva de cheques o tarjetas de crédito.
- Falsificación de datos con valor probatorio.
- Destrucción de datos.
- Sabotaje informático.
- Falsedad ideológica informática.

2.4.1.5 China. En este país se ha decidido medidas como la instalación de filtros de contenidos en los cibercafés para evitar el espionaje y las actividades disidentes en la red. El Tribunal Supremo Chino puede castigas con penas de 10 años de cárcel hasta la muerte las actividades de espionaje desde internet, sobre todo en aquellos casos que puedan afectar los secretos de alta seguridad y la seguridad estatal.

2.4.2 Legislación colombiana

2.4.2.1 Ley 527 de 1999. "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"

CAPITULO II
Aplicación de los requisitos jurídicos de los mensajes de datos

ARTÍCULO 6º. *Escrito*. Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito.

ARTÍCULO 7º. *Firma*. Reglamentado por el Decreto Nacional 2364 de 2012. Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:

a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación;
b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma.

ARTÍCULO 8º. *Original*. Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si:

a) Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;
b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que la información no sea presentada o conservada en su forma original.

ARTÍCULO 9º. *Integridad de un mensaje de datos*. Para efectos del artículo anterior, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

ARTÍCULO 10. *Admisibilidad y fuerza probatoria de los mensajes de datos*. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.

ARTÍCULO 11. *Criterio para valorar probatoriamente un mensaje de datos.* Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

ARTÍCULO 12. *Conservación de los mensajes de datos y documentos.* Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre que se cumplan las siguientes condiciones:

1. Que la información que contengan sea accesible para su posterior consulta.
2. Que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y
3. Que se conserve, de haber alguna, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.

No estará sujeta a la obligación de conservación, la información que tenga por única finalidad facilitar el envío o recepción de los mensajes de datos.

Los libros y papeles del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta.

ARTÍCULO 13. *Conservación de mensajes de datos y archivo de documentos a través de terceros*. El cumplimiento de la obligación de conservar documentos, registros o informaciones en mensajes de datos, se podrá realizar directamente o a través de terceros, siempre y cuando se cumplan las condiciones enunciadas en el artículo anterior.

2.4.2.2 Ley 1273 de 2009. "Por medio de la 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".

EL CONGRESO DE COLOMBIA

DECRETA:

Artículo 1°. Adiciónese el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

CAPITULO. I
De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: *Acceso abusivo a un sistema informático*. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: *Obstaculización ilegítima de sistema informático o red de telecomunicación.* El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: *Interceptación de datos informáticos*. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: *Daño Informático*. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: *Uso de software malicioso*. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: *Violación de datos personales*. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: *Suplantación de sitios web para capturar datos personales*. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: *Circunstancias de agravación punitiva*: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO. II
De los atentados informáticos y otras infracciones

Artículo 269I: *Hurto por medios informáticos y semejantes*. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: *Transferencia no consentida de activos*. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Artículo 2°. Adiciónese al artículo 58 del Código Penal con un numeral 17, así:

Artículo 58. *Circunstancias de mayor punibilidad*. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera:
(...)
17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.

Artículo 3°. Adiciónese al artículo 37 del Código de Procedimiento Penal con un numeral 6, así:

Artículo 37. *De los Jueces Municipales*. Los jueces penales municipales conocen:
(...)
6. De los delitos contenidos en el título VII Bis.

Artículo 4°. La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias, en especial el texto del artículo 195 del Código Penal.

2.4.2.3 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"

Artículo 8. *Criterios para establecer el grado de seguridad de las firmas electrónicas*. Para determinar si los procedimientos, métodos o dispositivos electrónicos que se utilicen como

firma electrónica son seguros, y en qué medida lo son, podrán tenerse en cuenta, entre otros, los siguientes factores:

1. El concepto técnico emitido por un perito o un órgano independiente y especializado.
2. La existencia de una auditoría especializada, periódica e independiente sobre los procedimientos, métodos o dispositivos electrónicos que una parte suministra a sus clientes o terceros como mecanismo electrónico de identificación personal.

2.4.2.4 Resolución No. 0-6394 de 2004. "Por medio de la cual se adopta el manual de procedimientos del Sistema de Cadena de Custodia para el Sistema Penal Acusatorio"

2.4.2.5 Resolución 02770 de 2005. "Por medio de la cual se modifica el manual de procedimientos del sistema de cadena de custodia para el sistema penal acusatorio, adoptado mediante Resolución 0-6394 de diciembre 22 de 2004"

2.4.2 Ley 842 de 2003. "Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones".

CAPITULO I
Disposiciones generales

Artículo 29. Postulados éticos del ejercicio profesional. El ejercicio profesional de la Ingeniería en todas sus ramas, de sus profesiones afines y sus respectivas profesiones auxiliares, debe ser guiado por criterios, conceptos y elevados fines, que propendan a enaltecerlo; por lo tanto deberá estar ajustado a las disposiciones de las siguientes normas que constituyen su Código de Ética Profesional.
Parágrafo. El Código de Ética Profesional adoptado mediante la presente ley será el marco del comportamiento profesional del ingeniero en general, de sus profesionales afines y de sus profesionales auxiliares y su violación será sancionada mediante el procedimiento establecido en el presente título.

Artículo 30. Los ingenieros, sus profesionales afines y sus profesionales auxiliares, para todos los efectos del Código de Ética Profesional y su Régimen Disciplinario contemplados en esta ley, se denominarán "Los profesionales".

CAPITULO II

Artículo 33. Deberes especiales de los profesionales para con la sociedad Son deberes especiales de los profesionales para con la sociedad:

a) Interesarse por el bien público, con el objeto de contribuir con sus conocimientos, capacidad y experiencia para servir a la humanidad.
b) Coopera para el progreso de la sociedad, aportando su colaboración intelectual y material en obras culturales, ilustración técnica, ciencia aplicada e investigación científica.

c) Aplicar el máximo de su esfuerzo en el sentido de lograr una clara expresión hacia la comunidad de los aspectos técnicos y de los asuntos relacionados con sus respectivas, profesiones y su ejercicio;

Artículo 34. Prohibiciones especiales a los profesionales respecto de la sociedad. Son prohibiciones especiales a los profesionales respecto de la sociedad:

a) Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación.
b) Imponer su firma, a título gratuito u oneroso, en planos, especificaciones, dictámenes, memorias, informes, solicitudes de licencias urbanísticas, solicitudes de licencias, informes, solicitudes de licencias urbanísticas, solicitudes de licencias de construcción y toda otra documentación relacionada con el ejercicio profesional, que no hayan sido estudiados, controlados o ejecutados personalmente.

Artículo 37. Deberes de los profesionales para con sus colegas y demás profesionales. Son deberes de los profesionales para con sus colegas y demás profesionales de la ingeniería:

a) Respetar y reconocer la propiedad intelectual de los demás profesionales sobre sus diseños y proyectos.

Artículo 38. Prohibiciones a los profesionales respecto de sus colegas y demás profesionales. Son prohibiciones a los profesionales, respecto de sus colegas y demás profesionales de la ingeniería:

a) Utilizar sin autorización de sus legítimos autores y para su aplicación en trabajos profesionales propios, los estudios, cálculos, planos, diseños y software y demás documentación perteneciente a aquellos, salvo que la tarea profesional lo requiera, caso en el cual se deberá dar aviso al autor de tal utilización.

2.4.4 Licencias para el uso de software libre

2.4.4.1 *General Public License* Version 3 (GPL V3).

Preámbulo: La Licencia Pública General de GNU es una licencia libre, bajo “copyleft”, para software y otro tipo de obras.

Las licencias para la mayoría del software y otras obras de carácter práctico están diseñadas para privarle de la libertad de compartir y modificar las obras. Por el contrario, la Licencia Pública General de GNU pretende garantizar su libertad de compartir y modificar todas las versiones de un programa –para cerciorar que permanece como software libre para todos sus usuarios. Nosotros, la Free Software Foundation, usamos la Licencia Pública General de GNU para la mayoría de nuestro software; la cual se aplica también a cualquier otra obra

publicada de esta forma por parte de sus autores. Usted también puede aplicarla a sus programas.

Cuando hablamos de software libre (free software), nos referimos a libertad, no a precio. Nuestras Licencias Públicas Generales están diseñadas para garantizar su libertad de distribuir copias de software libre (y cobrar por ellas si lo desea), recibir el código fuente o poder obtenerlo si quiere, modificar el software o usar fragmentos de él en sus nuevos programas, y que sepa que puede hacer esas cosas. (Free Software Foundation, 2007)[28]

2.4.5 Derecho de autor. Los derechos de autor en Colombia están soportado por la siguiente legislación:

2.4.5.1 Ley 23 de 1982 "Sobre derechos de autor"

Artículo 1º.- Los autores de obras literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente Ley y, en cuanto fuere compatible con ella, por el derecho común. También protege esta Ley a los intérpretes o ejecutantes, a los productores de programas y a los organismos de radiodifusión, en sus derechos conexos a los del autor.

Artículo 2º.- Los derechos de autor recaen sobre las obras científicas literarias y artísticas las cuales se comprenden todas las creaciones del espíritu en el campo científico, literario y artístico, cualquiera que sea el modo o forma de expresión y cualquiera que sea su destinación , tales como: los libros, folletos y otros escritos; las conferencias, alocuciones, sermones y otras obras de la misma naturaleza; las obras dramáticas o dramático-musicales; las obras coreográficas y las pantomimas; las composiciones musicales con letra o sin ella; las obras cinematográficas, a las cuales se asimilan las obras expresadas por procedimiento análogo a la cinematografía, inclusive los videogramas; las obras de dibujo, pintura, arquitectura, escultura, grabado, litografía; las obras fotográficas o las cuales se asimilan las expresadas por procedimiento análogo a la fotografía; las obras de arte aplicadas; las ilustraciones, mapas, planos croquis y obras plásticas relativas a la geografía, a la topografía, a la arquitectura o a las ciencias y, en fin, toda producción del dominio científico, literario o artístico que pueda reproducirse, o definirse por cualquier forma de impresión o de reproducción, por fonografía, radiotelefonía o cualquier otro medio conocido o por conocer.

2.4.5.2 Ley 44 de 1993. "Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944"

Artículo 6º.- Todo acto en virtud del cual se enajene el Derecho de Autor, o los Derechos Conexos así como cualquier otro acto o contrato vinculado con estos derechos, deberá ser

[28] Versión traducida de la "*General Public Lincense*" por estudiantes del master en sistemas telemáticos de la Universidad Rey Juan Carlos. (http://hjmacho.github.io/translation_GPLv3_to_spanish/)

inscrito en el Registro Nacional del Derecho de Autor como condición de publicidad y oponibilidad ante terceros.

2.4.5.3 Decreto 1474 de 2002. "Por el cual se promulga el "Tratado de la OMPI, Organización Mundial de la Propiedad Intelectual, sobre Derechos de Autor (WCT)", adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos noventa y seis (1996)".

3 DISEÑO METODOLÓGICO

3.1 TIPO DE INVESTIGACIÓN

La investigación que se realiza en este trabajo tendrá un enfoque descriptivo. El estudio descriptivo busca describir las propiedades, las características del objeto de análisis, buscando medir o recoger información de las variables a las que se refieren pero su objetivo no es indicar cómo se relacionan estas[29].

En este trabajo se caracterizará las herramientas con licencia GPL utilizadas en cada una de las fases del análisis forense para determinará cuáles de esas herramientas son las más idóneas para realizar el análisis forense a un dispositivo móvil con sistema operativo Android. También se caracterizara las metodologías más utilizadas en el análisis forense convencional y las que se han desarrollado específicamente para dispositivos móviles.

Con los resultados obtenidos en las anteriores caracterizaciones se desarrollará una metodología práctica que sirva como guía metódica en el proceso forense en un dispositivo móvil con sistema operativo Android.

3.2 POBLACIÓN

La población está conformada por el administrador del Semillero de Investigación GNU/Linux And Security (SIGLAS), que pertenece al Grupo de Investigación en Ingenierías Aplicadas (INGAP) de la Universidad Francisco de Paula Santander Ocaña.

3.3 MUESTRA

Al ser la población muy limitada se tomará el 100 % de la población, el administrador del Semillero de Investigación GNU/Linux And Security (SIGLAS).

3.4 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

La técnica utilizada para recoger la información en esta investigación es la observación estructurada. Esta técnica es utilizada cuando se quiere probar una hipótesis o una descripción sistemática de un fenómeno. El investigador sabe de antemano qué aspectos son relevantes y cuales no para el propósito de su investigación[30].

En el proceso de la investigación se estudiará el comportamiento técnico que tienen las herramientas forenses, sus características y funcionalidades. También, se analizará cómo se desarrolla el proceso forense en las diferentes metodologías propuestas. Una vez hecho estas observaciones, estudios, pruebas, y se organice la información entre las que aprueben o refuten la hipótesis se planteará un acercamiento metodológico teniendo en cuenta las características de los dispositivos móviles.

---

[29] HERNÁNDEZ SAMPIERI, Roberto, et al. Metodología de la investigación. México. McGraw Hill, 2010.
[30] GALLARDO, Yolanda y MORENO GARZÓN, Adonay. Módulo 3: Recolección de información. Serie Aprender a investigar. ICFES, 1999.

3.5 ACTIVIDADES DE ELABORACIÓN DEL PROYECTO

Objetivo específico	Actividades	Indicadores
Caracterizar las herramientas utilizadas en el análisis digital forense con licencia GPL para elegir la suite de herramientas a usar.	Revisión de literatura de las herramientas con licencia GPL para el proceso forense.	Lista de herramientas seleccionadas.
	Depuración previa de herramientas teniendo algunas consideraciones hechas por el autor.	
	Revisión de las herramientas que pasaron el/los filtros anteriores.	
	Selección de las herramientas	
Analizar las metodologías usadas en un análisis digital forense tradicional y para los dispositivos móviles.	Revisión de literatura de los modelos usados el proceso forense tradicional	Descripción las principales modelos más usadas en el análisis forense.
	Descripción de sus características, enfrentándolas a las necesidades de los dispositivos móviles.	Cuadro comparativo de las fases implementadas en cada modelo
Plantear una guía práctica que sirva como soporte para el análisis digital forense en un dispositivo móvil, teniendo en cuenta las características propias de dichas terminales.	Revisión de estándares, las buenas prácticas propuesta por las organizaciones y autores en cada etapa del proceso forense y en el manejo de evidencia, la cadena de custodia.	Referencias teóricas en las que se basará la guía propuesta.
	Proponer una guía práctica para el análisis forense en un dispositivo móvil.	Modelo de la guía propuesta
	Redacción informe.	Informe final, dónde se muestra el proceso realizado, los resultados obtenidos y la guía práctica propuesta con cada una de sus fases descritas.

3.6 CRONOGRAMA DE ACTIVIDADES

SEMANAS ACTIVIDADES	1	2	3	4	5	6	7	8	9	10	11	12
Revisión de literatura de las herramientas con licencia GPL para el proceso forense.												
Depuración previa de herramientas teniendo algunas consideraciones hechas por el autor.												
Revisión de las herramientas que pasaron el/los filtros anteriores.												
Selección de las herramientas												
Revisión de literatura de los modelos usados el proceso forense tradicional												
Descripción de sus características, enfrentándolas a las necesidades de los dispositivos móviles.												
Diseñar e implantar laboratorios para las pruebas controladas												
Revisión de estándares, las buenas prácticas propuesta por las organizaciones y autores en cada etapa del proceso forense y en el manejo de evidencia, la cadena de custodia.												
Proponer una guía práctica para el análisis forense en un dispositivo móvil.												
Redacción informe.												

***Tabla 1**- Cronograma de Actividades.*

4. HERRAMIENTAS DIGITALES FORENSES LICENCIA LIBRE

Existe una gran variedad de herramientas forenses que se pueden utilizar para realizar un análisis en un dispositivo móvil con sistema operativo Android, las cuales pueden ser de licencia propietaria y licencia GPL (*General Public License*).

Para la realización de esta guía se realizará un estudio de las herramientas forenses con licencia GPL. Hay que hacer una diferencia entre las herramientas y la suite de herramientas disponibles. Las primeras es una aplicación que fue programada con un propósito, y la segunda es el compendio de herramientas que tiene un fin en común.

4.1 HERRAMIENTAS FORENSES EN ANDROID

4.1.1 Herramientas para la adquisición. En un análisis post-mortem o en frío u *offline* como también se le conoce se lleva a cabo en los medios de almacenamiento permanente, como son la memoria del teléfono, las memorias externas (ya sean SD, o MMC) y las tarjetas sim. Los datos volátiles no se tienen en cuenta en este tipo de análisis, por lo tanto, la memoria RAM no se incluye en esta guía.

Las tarjetas SD o MMC se analizan como un ***sistema de archivos*** FAT tradicional. Para ellos se utiliza las herramientas para crear imágenes forenses como se haría un disco duro tradicional. Algunas herramientas son:

4.1.1.1 Comando dd: Es una herramienta sencilla y de fácil uso. Permite realizar copias bit a bit, lo que permite clonar ficheros de un dispositivo de almacenamiento (ya sea un disco o una partición) creando una imagen del mismo. El comando dd lee un bloque de datos de un tamaña determinado (512 bytes por defecto) del dispositivo de origen y lo escribe en el dispositivo de destino, y así sucesivamente hasta completar el tamaño total del disco/partición que se esté copiando; todo esto sin alterar la fuente original.

4.1.1.2 Comando dc3dd: Creada en el Centro del Ciber Crimen del Departamento de Defensa de los Estados Unidos. Es una modificación del comando dd, incluye características que facilitan la adquisición de imágenes forenses. Permite dividir la salida en distintos archivos con extensión secuencial (imagen.dd.000, imagen.dd.001, etc.) y calcula el *hash* para cada uno de los archivos comparando contra el disco de origen. Entre los algoritmos de *hash* que soporta son md5, sha1, sha256 o sha512. El *hash* se va calculando en paralelo a la realización de la imagen, una vez termina el proceso se calcula el *hash* de salida y se contrasta con el de origen.

4.1.1.3 Comando dcfldd: Aunque está basada en dd no es una actualización de esta, es una bifurcación. Con respecto a dc3dd el código y las características son distintas. Permite escribir varios *logs* en ficheros (de *hash*, de verificación y de errores). El *hash* se calcula en paralelo a la copia de los datos. La comparación de los hash de entrada contra los de salida no es realizada en forma automática. Para ello, se debe volver a ejecutar el comando dcfldd pero con otros parámetros o utilizar una herramientas como md5sum.

4.1.1.4 AFLogical OSE: Es la edición *Open Source* de la herramienta AFLogical desarrollada por ViaForensic[31]. Esta aplicación proporciona un marco de trabajo básico para la extracción de datos de los dispositivos Android mediante proveedores de contenidos y luego guarda los datos en la tarjeta SD del dispositivo incluyendo: Contactos, registro de llamadas, SMS, MMS, partes MMS, información del dispositivo.

Esta aplicación fue liberada para el uso de personal de las fuerzas de la ley, sino para los aficionados Android y para gurús forenses. Para el personal de las fuerzas de la ley está disponible la versión completa de forma gratuita pero bajo registro, en el cual se debe indicar el país y el departamento al cual pertenecen.

4.1.2 Herramientas para la examinación

4.1.2.1 Foremost. Es una aplicación de línea de comandos para el análisis forense, que permite recuperar archivos basados en sus encabezados, pies de página, y las estructuras de datos internas. Este proceso se conoce como 'tallado de datos' (*Data Carving*). El principal puede trabajar en archivos de imagen, tales como los generados por dd, Safeback, Encase, etc., o directamente en una unidad. Este breve artículo muestra cómo puede utilizar sobre todo para recuperar archivos borrados.

4.1.2.2 Photorec[32]**.** Es un software diseñado para recuperar archivos perdidos incluyendo videos, documentos y archivos de los discos duros y CD así como imágenes perdidas (por eso el nombre *PhotoRecovery*) de las memorias de las cámaras fotográficas, MP3 *players*, *PenDrives*, etc. PhotoRec ignora el sistema de archivos y hace una búsqueda profunda de los datos, funcionando incluso si su sistema de archivos está muy dañado o ha sido re-formateado. Para más seguridad, PhotoRec usa un acceso de sólo lectura para manejar el disco o la memoria de donde se recobrará los datos perdidos.

4.1.2.3 Testdisk[33]**.** Es un potente software de recuperación de datos gratuito. Fue diseñado principalmente para ayudar a recuperar particiones perdidas y/o hacer discos no booteables booteables nuevamente cuando estos síntomas son causados por software defectuoso: ciertos tipos de virus o error humano (como borrar accidentalmente una tabla de particiones).

4.1.2.4 Myrescue. Es un programa para rescatar a los datos aún legibles desde un disco duro dañado. El proyecto es similar en propósito a dd_rescue, sino que trata de salir rápidamente de las áreas dañadas de manejar primero la parte aún no dañados del disco y volver más tarde.

[31] ViaForensics pasó a llamarse NowSecure
[32] Sitio web del proyecto http://www.cgsecurity.org/wiki/PhotoRec
[33] Sitio web del proyecto http://www.cgsecurity.org/wiki/TestDisk

4.1.3 Herramientas para el análisis

4.1.3.1 The Sleuth Kit (TSK)[34]**.** Es una biblioteca y colección de herramientas de línea de comandos que permite investigar imágenes de disco. Su funcionalidad principal es la de analizar los volumen de datos y del sistema de archivos. Cuenta con un marco de plug-in le permite incorporar módulos adicionales para analizar el contenido del archivo y construir sistemas automatizados.

Permite examinar un ordenador de forma no intrusiva debido a que las herramientas no se basan en el sistema operativo para procesar los sistemas de archivos, borrado y el contenido oculto se muestra. Se ejecuta en plataformas Windows y Unix (ha sido probado en Linux, Mac OS X, CYGWIN, Open & FreeBSD y Solaris).

TSK soporta los sistemas de archivos NTFS, FAT, UFS 1, UFS 2, EXT2FS, EXT3FS, Ext4, HFS, ISO 9660, y yaffs2 (incluso cuando el sistema operativo host no o tiene un orden endian diferente).

De las técnicas de búsqueda se puede decir que:

- Lista asigna y elimina nombres ASCII y archivos Unicode.
- Muestra los detalles y contenidos de todos los atributos NTFS (incluyendo todas las secuencias de datos alternativas).
- Muestra del sistema de archivos y metadatos detalles de la estructura.
- Crear líneas de tiempo de actividad de los archivos, que se puede importar en una hoja de cálculo para crear gráficos e informes.
- Hashes de archivos de búsqueda en una base de datos de hash, como el NIST NSRL, Hash Guardián, y bases de datos personalizados que se han creado con la herramienta 'md5sum'.
- Organizar los archivos en función de su tipo (por ejemplo, se separan todos los ejecutables, archivos JPEG y documentos). Páginas de miniaturas se pueden hacer de las imágenes gráficas para el análisis rápido.

4.1.3.2 Autopsy[35]**.** Es una plataforma de análisis forense digital y la interfaz gráfica de The Sleuth Kit y otras herramientas forenses digitales. Es utilizado por las fuerzas del orden, los militares y los examinadores corporativos para investigaciones.

Fue diseñada para intuitiva, de fácil instalación una plataforma de extremo a extremo con módulos que vienen con él fuera de la caja y otros que están disponibles a partir de terceros. Autopsy tiene las siguientes características:

[34] Sitio web del proyecto TSK www.sleuthkit.org/sleuthkit/
[35] Sitio web de Autopsy http://www.sleuthkit.org/autopsy/index.php

- **Análisis de la línea de tiempo**: Muestra los eventos del sistema en una interfaz gráfica para ayudar a identificar la actividad.
- **Búsqueda por palabra**: extracción de texto y el índice de búsquedas en módulos que permiten encontrar los archivos que mencionan términos específicos y encontrar patrones de expresiones regulares.
- **Artefactos Web**: Extractos de actividad web de los navegadores comunes para ayudar a identificar la actividad del usuario.
- **Análisis del Registro**: Usa RegRipper para identificar los documentos usados recientemente y dispositivos USB.
- **Análisis de archivo LNK**: Identifica atajos y documentos accedidos
- **Análisis de correo electrónico**: Analiza MBOX mensajes de formato, tales como Thunderbird.
- **EXIF**: Extrae la ubicación geográfica y la información de la cámara de los archivos JPEG.
- **Selección tipo archivo**: Los archivos de grupo por su tipo de encontrar todas las imágenes o documentos.
- **Soporte de reproducción**: Ver vídeos e imágenes en la aplicación y no requiere de un visor externo.
- **Visor de miniaturas**: muestra en miniatura de las imágenes para ayudar al acceso rápido de las mismas.
- **Análisis del sistema de archivo robusto**: Soporte para sistemas de archivos comunes, incluyendo NTFS, FAT12 / FAT16 / FAT32 / ExFAT, HFS +, ISO9660 (CD-ROM), Ext2 / Ext3 / Ext4, yaffs2 y UFS de The Sleuth Kit.
- **Hash Set Filtrado**: Filtra archivos buenos conocidos usando NSRL y archivos malos conocida usando hashsets personalizados en HashKeeper, md5sum y formatos EnCase.
- **Etiquetas**: archivos de etiquetas con nombres de etiquetas arbitrarias, tales como "marcador" o "sospechoso", y añadir comentarios.
- **Extracción de string unicode**: Extrae las cadenas de espacio no asignado y tipos de archivos desconocidos en muchos idiomas (árabe, chino, japonés, etc.).
- Tipo de archivo de detección basada en firmas y detección de falta de coincidencia de extensión.
- Módulo de archivos interesante será archivos bandera y carpetas basándose en el nombre y la ruta.
- Soporte Android: extrae datos de SMS, registros de llamadas, contactos, Tango, palabras con los amigos, y más.

Autopsy analiza imágenes de disco, unidades locales o carpetas de archivos locales. Los formatos de disco pueden estar en formato Raw, dd o E01. El soporte para E01 es proporcionada por libewf. También cuenta con una estructura de información que permite la generación de informes.

Nota: Autopsy es una herramienta que se ejecuta en principio en la plataforma Windows, así que la versión 3.0 no está disponible para otras plataformas hasta el momento. Si se quiere ejecutar Autopsy en Linux y OS X debe usar la versión 2.0.

4.1.3.3 Digital Forensics Framework – DFF[36]. Es una plataforma informática forense de código abierto construida encima de una interfaz de programación de aplicaciones (API, *Application Programming Interface*) dedicado. Construida para un uso sencillo y la automatización. Su interfaz guía al usuario a través de los pasos principales de una investigación digital, por lo que puede ser utilizado tanto por profesionales y no expertos para llevar a cabo de forma rápida y fácilmente a las investigaciones digitales y realizar respuesta a incidentes. DFF trabaja en tres ejes:

Análisis forense digital. Es capaz de realizar un análisis de la memoria volátil y los discos de forma rápida para investigaciones en profundidad de una computadora o un teléfono inteligente. DFF utiliza tecnología de bloqueo de escritura con el fin de asegurar la evidencia y preservar la integridad de los medios de comunicación.

Investigación del fraude. El potente motor de búsqueda integrado le permite orientar rápidamente documentos, multimedia y buzones artefactos.

Detección y análisis de amenazas. DFF es capaz de agrupar diversas fuentes de información, desde la memoria volátil, discos de sistema y de almacenamiento, hasta los medios extraíbles. Esto permite tener una visión completa de las actividades del sistema y de los usuarios, también para conectarse a otra detección de amenazas y sistema de análisis.

Características:

- Bloqueador lógico de escritura.
- Compatibilidad con los formatos Raw, AFF y EWF de Encase.
- Trazabilidad (cadena de custodia).
- Cálculo de hash criptográfica.
- Detección de firmas de archivos.
- Avanzada filtrado y motor de búsqueda
- Detecta y monta particiones.
- Formato de disco virtual VMDK.
- Sistemas de archivos FAT 12/16/32, HFS HFS + HFSX (OSX y iPhone) y Ext 2/3/4 (GNU/Linux y Android).
- Extracción de metadatos EXIF.
- Análisis de Windows: analizador de archivos LNK, análisis Prefetch, análisis de registro y buzones de Microsoft Outlook PST.
- Análisis de memoria.
- Análisis de documentos.

[36] Sitio web del proyecto http://www.arxsys.fr/discover/

4.1.3.4 log2timeline[37] es una herramienta diseñada para extraer las marcas de tiempo de varios archivos encontrados en un sistema informático típico y agregarlos a la línea del tiempo.

4.2 OTRAS HERRAMIENTAS NECESARIAS PARA EL ANÁLISIS FORENSE

4.2.1 Comando ADB (*Android Debug Bridge*)[38]. Es una herramienta de línea se comandos versátil que le permite comunicarse con una instancia del emulador o dispositivo Android conectado. Es un programa cliente-servidor que incluye tres componentes:

1. Un cliente, que se ejecuta en el equipo de desarrollo. Se puede invocar un cliente desde un *shell* mediante la emisión de un comando adb. Otras herramientas de Android, como el *plugin* ADT y DDMS también crean clientes adb.
2. Un servidor, que se ejecuta como un proceso en segundo plano en el equipo de desarrollo. El servidor gestiona la comunicación entre el cliente y el demonio adb se ejecuta en un emulador o dispositivo.
3. Un demonio, que se ejecuta como un proceso en segundo plano en cada emulador o dispositivo instancia.

4.3 SUITE DE HERRAMIENTAS

Existes una variedad de suite de herramientas o distribuciones GNU/Linux que ya han recopilado las diferentes herramientas dedicadas a análisis forense y primera respuesta a incidentes. Entre las suite que veremos a continuación hay dedicadas especialmente a los dispositivos móviles y otras más generales.

4.3.1 CAINE Linux (*Computer Aided Investigative Environment*)[39]. Es una distribución GNU/Linux de origen italiana, creada por Giancarlo Giustini para el Centro de Investigación en Seguridad (CRIS). Es un entorno forense que se organizó para integrar herramientas de software existentes, módulos de software y proporcionar una interfaz gráfica amigable. En su versión 6.0 está basada en Ubuntu 14.4.1-64 bit. En cuanto a su diseño, CAINE se propone tres objetivos:

- Un entorno interoperable que apoya el investigador digital durante las cuatro fases de la investigación digitales.
- Una interfaz gráfica fácil de usar.
- Una compilación semiautomática del informe final.

[37] Sitio web del proyecto https://github.com/log2timeline/plaso
[38] Documentación sobre ADB en Android Developers http://developer.android.com/tools/help/adb.html
[39] Sitio web del proyecto CAINE http://www.caine-live.net/

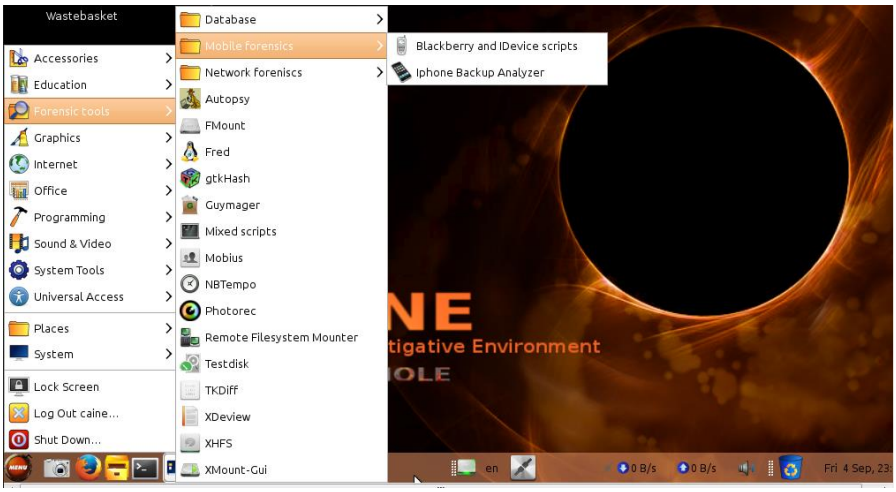


Figura 2*- Menú de herramientas de CAINE Linux. Fuente: Autor.*

4.3.2 Santoku Linux[40]. Es una distribución dedicada al análisis forense en móviles Android, Blackberry, iOS y *Windows Phone*; también permite realizar pruebas de seguridad y análisis de malware. Está basada en Lubuntu 14.04 y contiene diferentes plataformas SDK, controladores y utilidades para que las aplicaciones funcionen sin problemas; también viene con *framework* con interfaz de usuario que soportar herramientas con interfaz y con detección automática y configuración de nuevos dispositivos móviles conectados.

El proyecto Santoku es patrocinado por *NowSecure*, antes conocida como *viaForensics*.

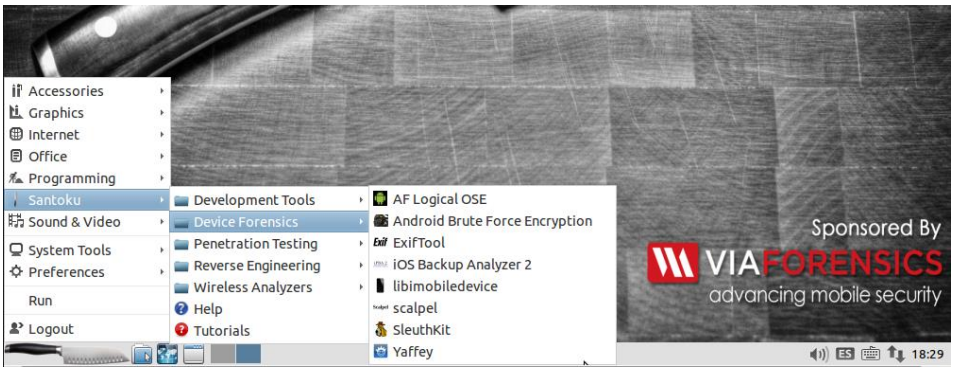


Figura 3*- Menú de herramientas de Santoku. Fuente. Autor.*

Las herramientas con que dispone Santoku se pueden clasificar en tres categorías:

En cuanto a **análisis forense** dispone de herramientas para la adquisición de las imágenes y análisis de los datos. Herramientas para imágenes de NAND, tarjetas de memoria y de la memoria RAM.

[40] Web del proyecto Santoku https://santoku-linux.com/

Para el **análisis de *malware*** cuanto con emuladores de dispositivos móviles, utilidades para simular los servicios de res para un análisis dinámico, herramientas de descompilación y desmontaje y el acceso a bases de datos de malware.

Y para las **pruebas de seguridad** cuenta con herramientas de descompilación y desmontaje, scripts para detectar problemas comunes en las aplicaciones móviles, scripts para automatizar el descifrado de archivos binarios, la implementación de aplicaciones, la enumeración de detalles de la aplicación, entre otras.

Es importante destacar que entre las herramientas para el análisis forense en dispositivos cuenta con AF Logical OSE.

4.3.3 DEFT (*Digital Evidence & Forensic Toolkit*) [41]. Es una distribución que se compone de GNU/Linux y DART (Kit de herramientas de Respuesta Digital Avanzada). Esta suite está dedicada al análisis forense digital y actividades de inteligencia.

La versión 8.2 está basada en Ubuntu 12.10 y cuenta con DART es su versión 2. DART es una suite para la gestión y respuesta ante incidentes desde sistemas operativos Windows, que incluye un lanzador de herramientas para este sistema operativo.

***Figura 4**- Menú de herramientas de DEFT. Fuente. Autor.*

Hay ciertas características a DEFT que minimizan el riesgo de alterar los datos que están siendo sometidos a análisis (Fratepietro, Rossetti, & Dal Checco, 2012). Algunas de estas características son:

1. En el arranque, se analiza el sistema no utiliza las particiones de intercambio en el sistema.

[41] Sitio web del proyecto DEFT http://www.deftlinux.net/

2. Durante el inicio del sistema no hay guiones automáticos de montaje.
3. No existen sistemas automatizados para cualquier actividad durante el análisis de las pruebas;
4. Todas las herramientas de almacenamiento y adquisición de tráfico de red en masa no alteran los datos que se adquirieron.

DEFT nos ofrece sus herramientas distribuidas entre las siguientes categorías (Guasch, 2013):

- ***Analysis*** - Herramientas de análisis de ficheros de diferentes tipos
- ***Antimalware*** - Búsqueda de *rootkits*, virus, *malware*, así como PDF con código malicioso.
- ***Data recovery*** - Software para recuperación de ficheros
- ***Hashing*** - Scripts que permiten la realización de cálculo de hashes de determinados procesos (SHA1, SHA256, MD5...)
- ***Imaging*** - Aplicaciones que podemos utilizar para realizar los clonados y adquisición de imágenes de discos duros u otras fuentes.
- ***Mobile Forensics*** - Análisis de Blackberry, Android, iPhone, así como información sobre las típicas bases de datos de dispositivos móviles en SQLite utilizadas por las aplicaciones.
- ***Network Forensics*** - Herramientas para procesamiento de información almacenada en capturas de red
- **OSINT** - Aplicaciones que facilitan la obtención de información asociada a usuarios y su actividad.
- ***Password recovery*** - Recuperación de contraseñas de BIOS, ficheros comprimidos, ofimáticos, fuerza bruta, etc.
- ***Reporting tools*** - Por último, dentro de esta sección encontraremos herramientas que nos facilitarán las tareas de generación de informes y obtención de evidencias que nos servirán para documentar el análisis forense. Captura de pantalla, recopilación de notas, registro de actividad del escritorio, etc.

En abril de 2015 se lanzó DEFT Zero[42], diseñada para ser la versión ligera de DEFT. Está centrado en la copia forense de evidencias digitales (es decir, los discos duros, dispositivos USB y unidades de red), optimizado para correr en solo 400 Mb, permitiendo que se cargue por completo en memoria RAM. Basado en Lubuntu 04.14.02 LTS y se desarrollará en paralelo con las futuras versiones completas de DEFT. Soporta versiones de 32 y 64 bits, con UEFI y arranque seguro.

[42] DEFT Zero http://www.deftlinux.net/2015/04/24/deft-zero-rc1-ready-for-download/

4.3.4 SIFT Workstation. *SANS Investigative Forensic Toolkit* (SIFT) *Workstation*[43] versión 3, 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. Está basado en Ubuntu LTS 14.04 y puede ser integrado con REMnux, un kit de herramientas para ingeniería inversa y análisis de malware.

Permite examinar de forma segura discos en crudo, múltiples sistemas de archivos y diferentes formatos de evidencia. Incluye más de 100 herramientas[44] para el análisis forense en diferentes ámbitos: discos duros, redes, analizar artefactos maliciosos, entre otros.

SIFT soporta los sistemas de archivos NTFS, ISO9660, HFS+, Raw data, espacio de intercambio (Swap), FAT 12/16/32, EXT 2/3/4, UFS ½ y vmdk. También soporta una gran variedad de formatos de imágenes forenses como Raw, AFF, AFD, AFM, AFFLib, EWF (EnCase), Split raw, affuse, Split ewf, mount_ewf.py y ewfmount.

4.4 SELECCIÓN DE HERRAMIENTAS

Anteriormente se detallaron algunas herramientas agrupadas dentro de algunas categorías establecidas por el autor. Las herramientas descritas en el aparatado 4.1 son el resultado de una selección a través de la revisión bibliográfica y ya se plasman las que necesarias para el análisis forense en un dispositivo Android, y que son las más representativas. En el caso que exista varias herramientas para la misma labor se analizó sus características principales y se eligió la más acorde.

4.4.1 Herramienta para la adquisición. Las características de evaluación son establecidas por el autor del proyecto. Para las herramientas de adquisición se estableció los siguientes parámetros:

Implementación de algoritmos de hash:

1 – No implementa algoritmos de *hash*.
2 – Sí implementa algoritmos de *hash*. La comparación de los hash de entrada contra los de salida no es realizada en forma automática.
3 – Sí implementa algoritmos de *hash*. La comparación de los hash de entrada contra los de salida se realizada en forma automática.

Información al usuario: El algoritmo muestra información del proceso de creación de la imagen al usuario.

1 – No muestra información al usuario.

[43] Sitio web del proyecto SIFT Workstation http://digital-forensics.sans.org/community/downloads
[44] Para conocer en detalle las herramientas que dispone puede ingresar a http://sift.readthedocs.org/en/latest/user/packages.html

2 – (Neutro)
3 – Sí muestra información al usuario.

Segmentación de imágenes:

1 – No permite segmentación de las imágenes.
2 – (Neutro)
3 – Permite segmentación de las imágenes.

Tiempo de ejecución

1 – Menor velocidad en creación de imágenes forenses.
2 – Intermedia velocidad en creación de imágenes forenses.
3 – Mayor velocidad en creación de imágenes forenses.

Los resultados se tabulan en la siguiente tabla:

Herramienta	Implementación de Hash	Información al usuario	Segmentación de imágenes	Tiempo de ejecución	Total
dd	1	1	1	1	4
dc3dd	3	3	3	3	12
dcfldd	2	3	3	2	10

Tabla 2- Comparación de herramientas para la adquisición de imágenes forenses Fuente. Autor.

4.4.2 Herramienta para el examen. De las herramientas descritas en el apartado 4.1.2 se seleccionaron todas las herramientas descritas: Foremost, Photorec, Testdisk y Myrescue.

4.4.3 Herramienta para el análisis. Si bien las herramientas que se pueden usar para el análisis son muy similares en cuanto a funcionalidad yo elegí Autopsy por ser la usada en los diferentes expertos en cuanto al software libre se refiere. Pero ya es cuestión de elegir la que se adapte al usuario y a una característica específica según la necesidad. A continuación muestro una tabla comparativa de sus características principales.

Característica	DFF	Autopsy
Análisis de archivos LNK	X	X
Análisis de registro		X
Análisis de correo electrónicos	X	X
Análisis de documentos	X	
Análisis de memoria	X	
Análisis de registro	X	X
Bloqueador lógica de escritura	X	
Búsqueda por palabra (Data carving)		X
Cálculo de hash criptográfico	X	
Detección de firmas de archivos	X	X

Detecta y monta particiones	X	
Etiquetas		X
Extracción de metadatos	X	X
Extrae artefactos web		X
Extrae string unicode		X
Filtrado avanzado	X	
Línea del tiempo		X
Selección por tipo de archivo		X
Soporta varios sistemas de archivos	X	
Soporta Android[45]		X
Soporte de reproducción		X
Trazabilidad	X	
Visor de miniaturas		X

***Tabla 3**- Comparación de características de DFF y Autopsy*. Fuente. Autor.

4.4.4 Suite de herramientas. En el apartado 4.3 se describieron algunas de las suites de herramientas forenses que disponibles en el mercado. Pero estas no son las únicas herramientas que existen, para llegar a ellas se filtrado para evaluar en mayor detalle las suite más pertinentes para realizar un proceso forense en un dispositivo Android. Entre los aspectos tenidos en cuenta para aplicar el filtro se tuvo en cuenta los siguientes:

- Son para dispositivos móviles
- Soportan el sistema operativo Android
- Están bajo licencia GPL

Para las suites de herramientas que pasaron el filtro se evaluó con una calificación de 1 a 5, siento 5 el buen cumplimiento del ítem que se evalúa. Se tuvo en cuenta las siguientes consideraciones:

- **Soporta dispositivos móviles**. La mayoría de suite están diseñadas para el análisis forense en estaciones de trabajo, redes de computadoras y para la respuesta a incidentes.
- **Soporta dispositivos Android**. Algunas herramientas aunque son para móviles están diseñadas para un sistema operativo en particular, o soporta varias plataformas pero no soporta el sistema operativo Andriod.
- **El proyecto cuanto con soporte en la actualidad**. Que el proyecto cuente con un equipo o comunidad de desarrollo que trabaje para que la suite este actualizadas, con sus parches de seguridad, las últimas versiones de las herramientas instaladas permite el funcionamiento de la misma de forma óptima y eficiente. Una suite con muchos años desde su última versión no es confiable.

[45] Esta característica está disponible en la versión 3 de Autopsy, la cual hasta el momento solo está disponible para la plataforma Windows.

- **El proyecto tiene una buena documentación**. La documentación adecuada permite aprender los procedimientos de una forma correcta, y quién mejor para documentar que el equipo que soporta dicha herramienta.
- **Soporte profesional**. El equipo profesional que está soportando la suite es una garantía que las herramientas y procedimientos realizados por la suite son correctos y acordes a las leyes, dando una mayor confiabilidad a los resultados obtenidos.

Suite de herramientas	Soporta móviles	Soporte Android	Soporte técnico	Documentación	Soporte profesional	Total
CAINE	5	1	5	3.5	3.5	18
Santoku	5	5	4.5	4.2	4	22.7
DEFT	5	5	4.5	5	4	23.5
SIFT Workstation[46]	3	1	5	5	5	20

Tabla 4 *- Comparación de suite de herramientas forenses. Fuente. Autor.*

[46] En el caso de SIFT Workstation, puede ser muy útil cuando se quiere tener una estación forense completa, se le puede instalar las diferentes herramientas necesarias para realizar un análisis forense móvil.

5. METODOLOGÍAS PARA EL ANÁLISIS FORENSE POST-MORTEM

Según las recomendaciones dadas por el *National Institute of Standards and Technology* – NIST en su *Guide to Integrating Forensic Techniques into Incident Response* (SP 800-86) independientemente si el análisis forense sea post-mortem o en vivo, o del medio al cual se le necesite realizar el procedimiento forense, las investigaciones deben realizarse mediante el proceso de cuatros fases que se muestra a continuación.

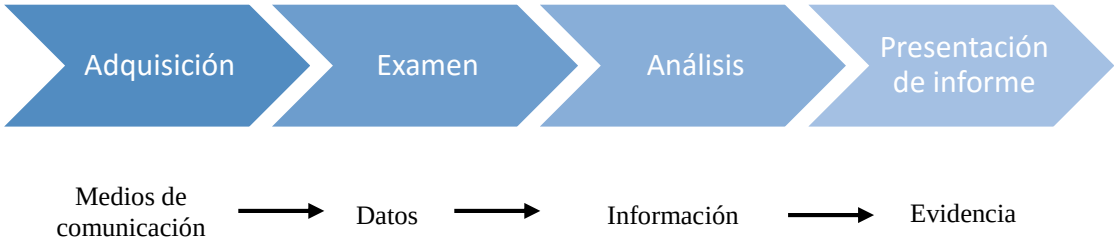


***Figura 5**: Proceso forense establecida por el NIST*

Los detalles de cada fase pueden variar dependiendo de la necesidad específica de la informática forense o de las políticas de la organización.

Adquisición: El primer paso en el proceso forense es identificar posibles fuentes de datos y adquirir los datos de ellos. Los datos relacionados con un evento específico se identifican, se etiqueta, se registra y recoge y su integridad se almacena. Se deben tener los pasos necesarios para la recopilación de datos y las medidas necesarias para apoyar los procedimientos disciplinarios legales o internas de la organización.

Examen: En esta fase se deben usar las herramientas forenses y técnicas apropiadas para los tipos de datos que se recogieron para identificar y extraer la información relevante de los datos recogidos al tiempo que se protege su integridad. Se puede usar herramientas automatizadas como procesos manuales.

Análisis: Implica analizar los resultados obtenidos en el examen para derivar información útil que responda a las preguntas que impulsaron a realizar el análisis forense. Una vez que la información relevante se ha extraídos, el analista debe estudiar y analizar los datos para sacar conclusiones de ello. El análisis debe incluir la identificación de las personas, lugares, objetos y acontecimientos, y que determinan cómo estos elementos se relacionan de manera que una conclusión se puede llegar. A menudo, este esfuerzo incluirá la correlación de datos entre múltiples fuentes. En llegado caso que se puede necesitar pruebas para acciones disciplinarias legales o internas, es indispensable que los analistas deban documentar cuidadosamente las conclusiones y todas las medidas adoptadas para llegar a ellas.

Presentación de informe: Es la fase final del proceso forense y abarba el proceso de elaboración y presentación de la información resultante de la fase de análisis. Según el

NIST en su guía SP 800-86 hay muchos factores que afectan a la presentación de informes, como por ejemplo:

- **Explicaciones alternativas:** Cuando la información sobre un evento es incompleta, puede que no sea posible llegar a una explicación definitiva de lo sucedido. Si un evento tiene dos o más plausibles explicaciones, cada uno debe ser tenido debidamente en cuenta en el proceso de presentación de informes. Los analistas deben utilizar un enfoque metódico para tratar de probar o refutar cada una posible explicación que se propone.
- **Consideración del Público**: Es importante conocer a la audiencia a la que se le presentará el informe, según quien sea querrá saber una u otra información con más detalle. Un incidente que requiere la participación de las fuerzas del orden requiere informes muy detallados de toda la información recopilada, y también puede requerir copias de todos los datos probatorios obtenidos. Un administrador del sistema puede querer ver el tráfico de red y estadísticas relacionadas con gran detalle. La alta dirección puede simplemente quieren una descripción de alto nivel de lo que pasó, como una representación visual simplificada de cómo se produjo el ataque, y lo que se debe hacer para evitar incidentes similares. Es recomendable hacer dos informes, uno para la alta gerencias y otro más técnico para el equipo de seguridad o sistemas de la compañía.
- **Información procesable**: El reporte también incluye la identificación de información procesable obtenido a partir de datos que pueden permitir a un analista para recoger nuevas fuentes de información. Por ejemplo, una lista de contactos puede ser desarrollado a partir de los datos que pueda conducir a la información adicional acerca de un incidente o delito. Además, la información puede ser obtenida que podrían prevenir futuros eventos, como una puerta trasera en un sistema que podría ser utilizado para ataques futuros, un crimen que se está planificando, un gusano programado para empezar a difundir en un momento determinado, o una vulnerabilidad que podría ser explotado.

5.1 MODELOS FORENSES

Los diferentes modelos que han surgido como guías para llevar una investigación forense digital varían una de la otra en el número de las fases que implementan, unas son más explícitas en determinada fase pero lo que sí tienen en común es las cuatro fases explicadas anteriormente.

En las últimas décadas varios autores han desarrollado modelos. Entre ellos tenemos:

- Modelo Casey, año 2000.
- Modelo del *U.S Department of Justice*, 2001.
- Modelo Lee, 2001.
- Modelo DFRWS, 2001.
- Modelo de Reith, Carr y Gunsch, 2002.

- Modelo integrado (IDIP) de Brian Carrier y Eugene Spafford, 2003.
- Modelos extendido de Séamus Ó Ciardhuáian, 2004.
- Modelo propuesto por Venansius Baryamureeba y Florence Tushabe, 2004[47].
- Modelo Casey, versión 2004.
- Modelo del *U.S Department of Justice*, 2004.

A continuación se describe brevemente algunos de los modelos forenses más reprentativos.

5.1.1 Modelo del National Institute of Justice (2001). Este modelo presentado por National Institute of Justice (NIJ)[48] y 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:

1. Identificación
2. Preservación
3. Análisis
4. Presentación.

5.1.2 DFRWS (2001). Este modelo 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[49]:

1. Identificación
2. Preservación
3. Recolección
4. Examen
5. Análisis
6. Presentación
7. Decisión

[47] Para más detalle de este modelo http://bit.ly/1jqPDTR
[48] U.S DEPARTMENT OF JUSTICE. Electronic Crime Scene Investigation: A Guide for First Responders. National Institute of Justice, 2001.
[49] DIGITAL FORENSIC RESEARCH WORKSHOP. A road Map for Digital Forensic Research: Report from the first Digital Forensic Research Workshop. Utica, New York. DFRWS, 2001. p 15-20

Identification	Preservation	Collection	Examination	Analysis	Presentation	Decision
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation	
Resolve Signture	Imaging Technologies	Approved Methods	Traceability	Traceability	Expert Testimony	
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification	
Anomalous Detection	Time Synch.	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement	
Complaints		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure	
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation	
Audit Analysis		Sampling	Hidden Data Extraction	Link		
Etc.		Data Reduction		Spacial		
		Recovery Techniques				

***Figura 6**: Modelo DFRWS*

En la parte superior del Figura 6 se encuentran las fases del modelo. El contenido de la columna debajo de cada fase métodos o técnicas que pertenecen a dichas fases. Y aunque este modelo se presenta como lineal, el proceso debe implicar retroalimentación para la investigación sea totalmente efectiva.

5.1.3 Modelo de Reith, Carr y Gunsch (2002). Este modelo es inspirado en el modelo DFRWS y se presenta como una mejora de este. Las fases de este modelo son[50]:

1. Identificación – Se reconoce un incidente y se determina su tipo.
2. Preparación – Se preparan las herramientas, técnicas a usar, órdenes de registro, autorizaciones de monitoreo y apoyo a la gestión.
3. Estrategia de enfoque - la formulación de forma dinámica de un enfoque basado en el potencial impacto en los espectadores y la tecnología en cuestión. El objetivo de la estrategia debe ser maximizar la obtención de pruebas no contaminadas, mientras que minimizar el impacto a la víctima.
4. Preservación - Aislar, asegurar y preservar el estado de bienestar físico y de las pruebas digitales.
5. Recolección - Grabar la escena física y duplicar la evidencia digital utilizando estandarizados y procedimientos aceptados.
6. Examen – Es la búsqueda sistemática en profundidad de pruebas relacionadas con el presunto delito. Este se centra en la identificación y localización de las posibles pruebas, posiblemente en lugares no convencionales. Se debe construir la documentación detallada para su análisis.
7. Análisis - Determinar el significado, la reconstrucción de fragmentos de datos y sacar conclusiones basadas en evidencias encontradas. Pueden pasar varias iteraciones de examen y análisis para apoyar una teoría del delito. La distinción de

[50] REITH, Mark, *et al*. An Examination of Digital Forensic Models. En: International Journal of Digital Evidence. Volumen 1, número 3 (2002).

análisis es que no puede requerir altos conocimientos técnicos para llevar a cabo y por lo tanto más gente puede trabajar en este caso.

8. Presentación - Resumir y proporcionar una explicación de las conclusiones. Esto debe ser escrita en términos de un laico usando terminología abstracta. Toda terminología abstraída debe hacer referencia a los detalles específicos.
9. Volviendo pruebas - La garantía de la propiedad física y digital se devuelve propietario adecuado, así como la determinación de cómo y qué se debe quitar la evidencia criminal. Una vez más no un forense explícitas paso, sin embargo, cualquier modelo que se apodera de pruebas rara vez se ocupa de este aspecto.

Retih y compañía determinaron algunos algunas fortalezas y debilidades de su modelo propuesto.

Ventajas:

- Crear un marco consistente y estandarizado para el desarrollo forense digital.
- Mecanismo para aplicar el mismo marco para futuras tecnologías digitales.
- Metodología generalizada de que los miembros judiciales puede utilizar para relacionar la tecnología para observadores no técnicos.
- Identifica la necesidad de herramientas de tecnología dependiente específicos mientras que proporciona visión de las herramientas previamente definidos de la misma categoría.
- Posibilidad de incorporación de tecnologías no digitales, electrónicas dentro de la abstracción.

Desventajas:

- Las categorías pueden ser definidos como demasiado general para el uso práctico.
- No existe un método fácil ni obvio para probar el modelo.
- Cada subcategoría añadido al modelo hará que sea más complicado de usar.

Este modelo no tiene en cuenta la cadena de custodia, y no porque no sea importante, sino que la cadena de custodia está implícito 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.

Por otra parte, con este modelo se pretende explícitamente ser un modelo abstracto aplicable a cualquier tecnología o el tipo de delito cibernético. También, que el modelo puede ser utilizado como la base para desarrollar métodos más detallados para tipos específicos de investigación, por ejemplo, tratar con discos duros fijos o incrustado memoria no volátil, mientras que la identificación de cualquier similitud posible en procedimientos o herramientas.

5.1.4 Modelo Casey (2004). Eoghan Casey presentó en el año 2000 la primera versión de su modelo para procesar y examinar evidencia digital[51]. Esta versión del modelo era muy general y podía ser aplicado en sistemas autónomos y entornos de red. Este modelo consta de cuatro fases:

1. Reconocimiento
2. La preservación, recolección y documentación
3. Clasificación, comparación, y la individualización
4. Reconstrucción

Para Casey, este no es un proceso lineal, sino que se trata de un ciclo de procesamiento de pruebas debido a que la reconstrucción puede apuntar a la evidencia adicional que hace que el ciclo comience de nuevo. El modelo se presenta primero en términos de sistemas informáticos independientes, y luego se aplica a las distintas capas de red (desde medios físicos hasta la capa de aplicaciones de usuario, e incluyendo la infraestructura de red) para describir las investigaciones en redes informáticas.

En el año 2004, Casey presentó una versión de su modelo para aplicar la ciencia forense en los computadores[52]. Esta versión viene con más fases que su antecesor. Las siete fases de este modelo son:

1. Autorización y preparación
2. Identificación
    a. Identificación de hardware
    b. Identificación de la evidencia digital
3. Documentación
4. Recolección y preservación
    a. Recolección de preservación del hardware
    b. Recolección de preservación de la evidencia digital
5. Examen y análisis
    a. Filtrado y reducción.
    b. Características individuales/clase y evaluación de la fuente
    c. Recuperación de datos y salvaguardia
6. Reconstrucción
    a. Análisis funcional
    b. Análisis relacional
    c. Análisis temporal
    d. Estenografía digital
7. Presentación de informes

[51] CASEY, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. First Edition. Academic Press, 2000. ISBN: 012162885X.
[52] CASEY, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Second Edition. Academic Press, 2004. ISBN: 0121631044.

5.1.5 Modelo del National Institute of Justice (2004). En el año 2004 el National Institute of Justice (NIJ) publicó una guía para la aplicación de la ley en el examen de la evidencia digital[53], donde la fase que se conoce como recolección en el modelo del 2001, en esta versión de dividió en dos fases: evaluación y adquisición. Las demás fases se mantienen de igual forma. El modelo es el siguiente:

1. Preparación
2. Evaluación
3. Adquisición
4. Examinación
5. Análisis
6. Presentación de informes

Evaluación de la evidencia. La evidencia digital debe ser evaluada a fondo con respecto al alcance del caso para determinar el curso de acción. También se debe evaluar el caso, y de las instalaciones de la escena del crimen, la evaluación del lugar donde se hará el procedimiento y las consideraciones legales.

Adquisición de la evidencia. La evidencia digital es frágil y puede ser alterada, dañada o destruida por un manejo o examen inadecuado. Por estas razones, se debe tomar precauciones especiales para preservar este tipo de pruebas como es la protección contra escritura. El no hacerlo puede hacerla inutilizable poder o dar lugar a una conclusión errónea.

Examen de la evidencia. Ningún caso es igual a otro, los diferentes medios de comunicación pueden requerir diferentes métodos de examen. Las personas que llevan a cabo un examen de la evidencia digital deben estar capacitados para este fin. Se debe llevar a cabo el examen de los datos que han sido adquiridos utilizando procedimientos forenses aceptados. Siempre que sea posible, el examen no debe llevarse a cabo en evidencia original.

Análisis de la evidencia. El análisis es el proceso de interpretar los datos extraídos para determinar su significado para el caso. Algunos ejemplos de los análisis que se pueden realizar son: marco temporal, los datos ocultos, de las aplicaciones y archivos, y la propiedad y posesión de los archivos. El análisis puede requerir una opinión de la solicitud de servicio, la autoridad legal para la búsqueda de la evidencia digital, pistas de investigación y/o derivaciones analíticas.

Presentación de informes. El examinador es responsable de informar de forma completa y precisa sus hallazgos y los resultados del análisis de la evidencia digital. La documentación es un proceso continuo durante todo el examen. Es importante registrar con precisión las medidas adoptadas durante el examen de la evidencia digital. Toda la documentación debe ser exacta y completa. El informe resultante debe ser escrito para el público objetivo.

[53] U.S DEPARTMENT OF JUSTICE. Forensic Examination of Digital Evidence: A Guide for Law Enforcement. National Institute of Justice, 2004.

5.1.6 Modelo extendido para las investigaciones de cibercrimen (2004). Este modelo en cascada, desarrollado por Séamus Ó Ciardhuáin y establece que las actividades para una investigación forense son las siguientes[54]:

1. Conciencia
2. Autorización
3. Planificación
4. Notificación
5. Buscar e identificar evidencias
6. Recolección de evidencia
7. Transporte de evidencia
8. Almacenamiento de la evidencia
9. Examen de la evidencia
10. Hipótesis
11. Presentación de la hipótesis
12. Comprobar/Defender la hipótesis
13. Difusión de la información

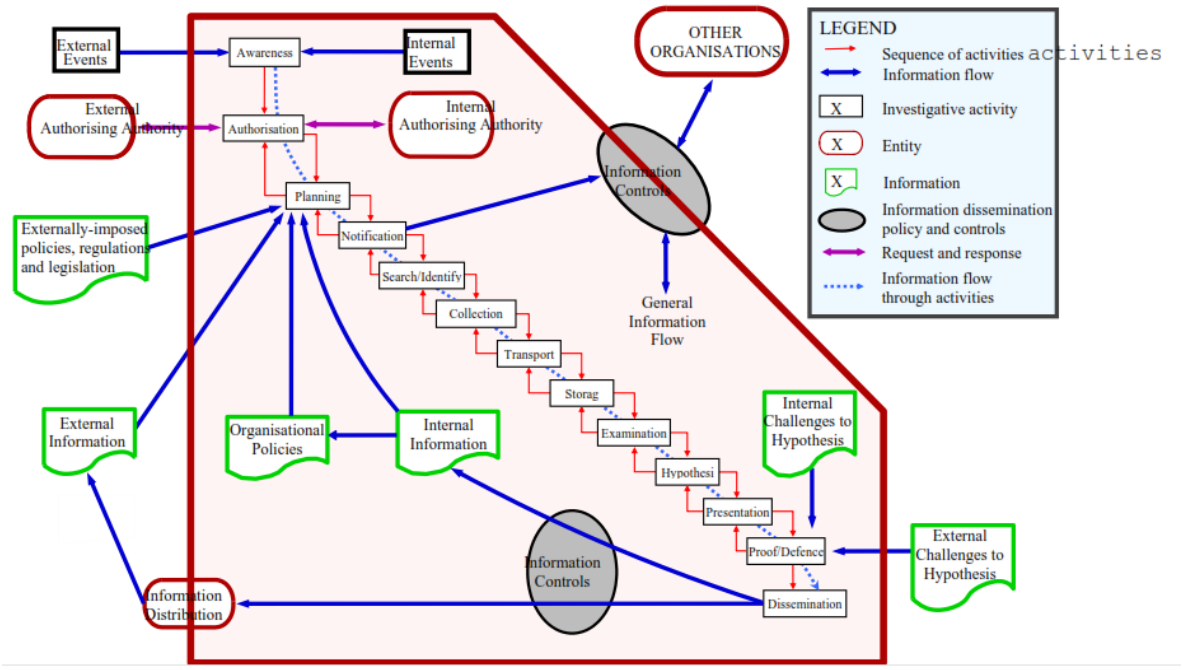


***Figura 7** - Modelo extendido para las investigaciones de cibercrimen*

Conciencia. El primer paso en la investigación es la creación de una conciencia de que se necesita investigación. Esta toma de conciencia generalmente en creado por un

[54] CIARDHUÁIN, Séamous Ó. An Extended Model of Cybercrime Investigatons. En: International journal of Digital Evidence. Volumen 3, número 1 (2002).

acontecimiento externo o interno a la organización. Esta fase permite la relación con los acontecimientos que requieren de una investigación para su aclaración. Conocer los eventos que causan la investigación pueden influir significativamente en el tipo de investigación se requiere. Es de vital importancia tener en cuenta tales diferencias para asegurar que el enfoque correcto es llevado a una investigación en un contexto particular.

Autorización. Una vez se identifica la necesidad de una investigación se debe obtener la autorización para llevarlo a cabo. El nivel de estructura formal asociado con la autorización varía considerablemente, dependiendo del tipo de investigación.

Planificación. La actividad de planificación está fuertemente influenciado por la información tanto dentro como fuera de la organización de instrucción. Desde fuera, los planes se verán influenciados por las regulaciones y leyes que establecen el marco general de la investigación y que no están bajo el control de los investigadores. También habrá información recogida por los investigadores de otras fuentes externas. Desde dentro de la organización, habrá propias estrategias de la organización, las políticas y la información sobre las investigaciones anteriores. La actividad de planificación puede dar lugar a una necesidad de dar marcha atrás y obtener una nueva autorización, por ejemplo cuando el alcance de la investigación se encuentra que es más grande que la información original mostró.

Notificación. Notificación en este modelo se refiere a informar al sujeto o las partes interesadas que la investigación se lleva a cabo. Esta actividad no puede ser apropiada en algunas investigaciones, por ejemplo, donde se necesita sorpresa para evitar la destrucción de pruebas.

Búsqueda e Identificación de Evidencia. Esta actividad se ocupa de la localización de la evidencia y la identificación de lo que es para la siguiente actividad. Esto puede ir desde encontrar el ordenador utilizado por un sospechoso hasta entornos más complejos como requerir trazando las computadoras a través de múltiples proveedores de Internet y posiblemente en otros países sobre la base de conocimiento de una dirección IP.

Recolección. La recolección es la actividad en la que la organización que investiga toma posesión de la prueba en una forma que pueda ser preservado y se analiza. Esta actividad es el foco de la mayoría de las discusiones en la literatura debido a su importancia para el resto de la investigación. Los errores o malas prácticas en esta etapa pueden hacer las pruebas inútiles, sobre todo en las investigaciones que están sujetos a estrictos requisitos legales.

Transporte. Tras la recolección, la evidencia debe ser transportada a un lugar adecuado para su posterior examen. Esto podría ser simplemente el traslado físico de los ordenadores incautados a un lugar seguro; sin embargo, también podría ser la transmisión de datos a través de redes. Es importante asegurarse durante el transporte que la prueba sigue siendo válida para su uso posterior, es decir, que los medios de transporte utilizados no afecta a la integridad de la evidencia.

Almacenamiento. La evidencia recogida será en la mayoría de los casos necesitan ser almacenados porque el examen no puede tener lugar inmediatamente. El almacenamiento debe tener en cuenta la necesidad de preservar la integridad que de las pruebas.

Examen. El examen de la evidencia implicará el uso de un número potencialmente grande de técnicas para encontrar e interpretar datos significativos. Puede requerir reparación de datos dañados de manera que conservan su integridad. Dependiendo de los resultados de la búsqueda / identificación y las actividades de recolección, no pueden ser muy grandes volúmenes de datos a examinar las técnicas de manera automatizada para apoyar el investigador son obligatorios.

Hipótesis. Con base en el examen de las pruebas, los investigadores deben construir una hipótesis de lo ocurrido. El grado de formalidad de esta hipótesis depende del tipo de investigación.

Entrega. La hipótesis debe ser presentada a personas distintas de los investigadores. Para una investigación policial la hipótesis se colocará ante un jurado, mientras que una investigación interna de la empresa colocará la hipótesis antes de la gestión de una decisión sobre las medidas que deban tomarse.

Comprobar/Defender. Los investigadores tendrán que demostrar la validez de su hipótesis y defenderla contra la crítica y el desafío. Desafíos exitosos probablemente resultará en dar marcha atrás a las anteriores etapas para obtener y examinar más pruebas, y construir una mejor hipótesis.

Difusión de la información. Una vez terminada la investigación de debe difundir la información de la investigación Parte de la información puede estar disponible sólo dentro de la organización donde se realizó la instrucción, mientras que otra información puede ser de más amplia difusión. La información influirá en futuras investigaciones y también puede influir en las políticas y procedimientos. La recopilación y mantenimiento de esta información es, por lo tanto, un aspecto clave de apoyo a la labor de los investigadores y es probable que sea un área fructífera para el desarrollo de aplicaciones avanzadas que incorporan técnicas tales como sistemas de minería de datos y expertos.

5.1.7 Modelo Cohen (2009). Este modelo propuesto por Fred Cohen describe el tratamiento de la evidencia digital. Cohen asume que la evidencia digital debe ser identificada, recolectada, conservada, transportada, almacenada, analizada, interpretada, atribuida, tal vez reconstruida, presentada y, de las órdenes judiciales, destruida[55].

El modelo propuesto por Cohen para el proceso de la evidencia digital en el contexto legal consta de 11 fases[56]:

1. Identificar

[55] COHEN, Fred. Challenges to Digital Forensic Evidence. Second Edition. Fred Cohen & Associates, 2008. ISBN: 1-878109-41-3.
[56] COHEN, Fred. Digital Forensic Evidence Examination. Fifth Edition. Fred Cohen & Associates, 2009. ISBN: 1-878109-48-0.

2. Recolectar
3. Preservar
4. Transportar
5. Almacenar
6. Analizar
7. Interpretar
8. Atribuir
9. Reconstruir
10. Presentar
11. Destruir

Para Cohen, el examen consta de los procesos que los examinadores utilizan para analizar, interpretar, atribuir y reconstruir los rastros.

Identificar. La evidencia debe ser identificada como tal con el fin de ser procesada y aplicada. Si las evidencias no se pueden identificar como pruebas pertinentes, nunca puede ser recogida o procesada en absoluto, y ni siquiera puede seguir existiendo en formato digital por el momento en que se descubrió que tenía relevancia.

Recolectar. Una vez se identifica la evidencia se debe recolectar de tal manera que se preserve su integridad durante todo el proceso, incluyendo la preservación de la información relacionada con la cadena de custodia en virtud de la cual fueron recogidos y conservados. Este deber se cumple normalmente mediante la recopilación y conservación de una copia de la evidencia original de modo que no necesita ser preservado el medio original real, sino más bien, puede seguir utilizándose. La recolección puede implicar muchas tecnologías y técnicas diferentes, dependiendo de la circunstancia.

Preservar. La preservación de los archivos de registro y los datos pertinentes de auditoría es particularmente importante y siempre debe ser identificado y conservado. El no hacer esto se convierte en un problema en los casos en que la pureza de la evidencia es controvertida. Por ejemplo, si una muestra contiene algún contenido corrupto, toda la exposición se convierte en sospechoso. Si los registros originales no están disponibles para la rehabilitación de las partes pertinentes de la exposición, todas las pruebas contenidas en la exposición pueden ser inadmisible.

Transportar. Cada vez más evidencia se transporta por vía electrónica de un lugar a otro, e incluso los errores más simples puede hacer que los datos que llegan a ser incorrecta o mal autenticado para los efectos legales. Se debe tener cuidado para preservar la cadena de custodia y asegurar que un testigo puede declarar con exactitud acerca de lo que tuvo lugar, el uso y la retención de notas contemporáneas, y tomando las precauciones adecuadas para asegurar que las pruebas no se expoliados y se trata adecuadamente en el camino. a evidencia es a menudo copiada y enviada electrónicamente, en discos compactos o en otros medios de comunicación, a partir de un lugar a otro. Las copias originales se mantienen normalmente en un lugar seguro con el fin de actuar como la evidencia original que se introduce en el proceso judicial.

Almacenar. Almacenamiento se debe asegurar de manera adecuada para garantizar la cadena de custodia. El papeleo asociado con todas las acciones relacionadas con la evidencia debe mantenerse para asegurar que las pruebas no ir a ninguna parte sin ser rastreado correctamente. Muchos tipos diferentes de cosas pueden salir mal en el almacenamiento, incluyendo, sin límite, el deterioro con el tiempo, los cambios ambientales resultantes de la presencia o ausencia de una condición necesaria para la preservación, el asalto ambiental directo sobre los medios de comunicación, incendios, inundaciones y otros eventos externos llegar a las pruebas, la pérdida de energía a las baterías y otros mecanismos de preservación de medios de comunicación, y el deterioro con el tiempo de otras fuentes naturales y artificiales.

Analizar. En el análisis forense, por lo general hay sólo un número finito de posibles secuencias de eventos que podrían haber producido la evidencia; sin embargo, el número real de posibles secuencias puede ser casi insondablemente grande. En esencia, casi cualquier ejecución de una instrucción por el entorno informático o genere la evidencia puede tener un impacto en la evidencia. Dado que es inviable para reconstruir cada secuencia posible, encontrar todas las secuencias que pueden haber producido las pruebas reales en un caso determinado, los analistas se centran en grandes conjuntos de secuencias de eventos y tienden a caracterizar las cosas en esos términos.

Interpretar. La presencia de este rastro en una pista de auditoría no significa lo que el analista puede suponer a primera vista. Hay muchas secuencias posibles de acontecimientos que podrían dar lugar a la presencia de una traza. El analista que trate de interpretar la evidencia debe tratar de tener en cuenta las explicaciones alternativas para pruebas para tratar de entender lo que realmente ocurrió y cómo ciertas son de las afirmaciones que hacen.

Atribuir. El análisis, interpretación y atribución de las pruebas forenses digitales también son conciliables con la evidencia no digital y externamente estipulado o hechos demostrados. Eventos de anclaje que el analista puedan acreditar que son un buen ejemplo de la interacción entre la evidencia forense digital y la realidad física. Un ejemplo de un evento de anclaje es el conocimiento del tiempo de mantenimiento de mecanismos en los sistemas que interactúan con las pruebas disponibles en el asunto en cuestión.

Reconstruir. En muchos casos, la pertinencia de las pruebas es específica de hardware y / o software. Mientras que muchos analistas hacen la suposición de que los mecanismos funcionan de acuerdo a sus especificaciones, en el campo de tecnología de la información, donde las pruebas forenses digitales originan, hay en algunas normas informativas y están generosamente violan todo el tiempo. La documentación es a menudo en desacuerdo con la realidad, las versiones de los sistemas y el cambio de software a un ritmo elevado, y los registros de lo que fue en su lugar en un momento dado son a menudo escasa o inexistente. Casos legales también a menudo vienen a juicio muchos años después de los acontecimientos reales que los llevaron a tener lugar, y la evidencia que podría haber estado presente en el momento del incidente en cuestión ya no estén disponibles en el momento en que se sabe que es de importación . En estos casos, la reconstrucción de los mecanismos

que producen las huellas importantes puede ser el único método disponible para resolver, a un nivel razonable de seguridad, lo que en realidad podría y no podría haber tenido lugar.

Presentar. La evidencia, análisis, interpretación, y la atribución, en última instancia, deben ser presentados en forma de informes periciales, declaraciones y testimonios. La presentación de la prueba y su análisis, la interpretación, y la atribución tiene muchos retos, pero presentación sólo se aborda de manera limitada en la literatura. La presentación es más un arte que una ciencia, pero hay una cantidad sustancial de la literatura científica sobre los métodos de presentación y su impacto en aquellos que observan esas presentaciones. Aspectos que van desde el orden de presentación de la información para el uso de gráficos y demostraciones todos presentan desafíos significativos y están mal definidos.

Destruir. Los tribunales suelen pedir pruebas y otra información asociada a un asunto legal que ser destruidos o devueltos después de que termine su uso en la materia. Esto se aplica a los secretos, paciente confidencial y la información del cliente relacionada, obras con derechos de autor, y de la información que las empresas normalmente disponen de pero deben conservar durante la duración del proceso legal comerciar. La retención de datos y la disposición tiene una amplia literatura que implica restricciones legales sobre y mandatos para la destrucción. También hay problemas técnicos significativos asociados con la destrucción de los datos digitales. Los procesos para la destrucción en asuntos legales rara vez alcanzan el nivel requerido para asuntos de seguridad nacional; sin embargo, los esfuerzos que intervienen en la recuperación de evidencia hacen, a veces, van los extremos.

Cohen ve el manejo de la evidencia no como un todo sino que hace parte de un contexto más general. A parte del manejo de la evidencia digital, en el proceso forense también intervienen los peritos informáticos, las herramientas y el uso de las mismas, las fallas que se comentes o por omisión, el proceso legal, la admisibilidad de la evidencia, los retos que tiene le proceso forense entre otros aspectos. La figura 8 muestra el contexto legal de la evidencia digital que plantea Fred Cohen.

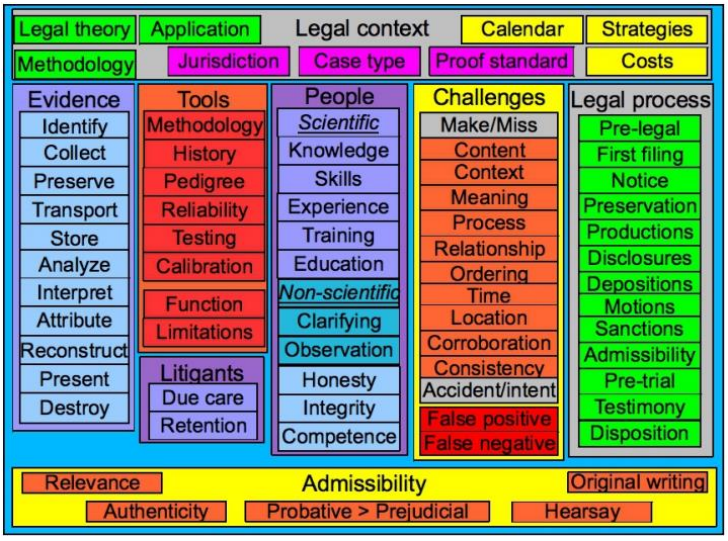


Figura 8 *- Contexto general del análisis forense digital de Cohen.*

5.2 CARACTERIZACIÓN DE LOS MODELOS

Como se mencionó anteriormente, los modelos forenses propuestos varían en sus fases pero tienen como base las cuatro fases básicas del proceso forense. En la Figura 9 se puede observar las diferentes fases implementadas y terminología utilizada por cada autor para describir el cómo debe ser un proceso forense.

En la gráfica se representa los modelos descritos anteriormente, ya que son los más representativos en el análisis forense.

5.3 DISCUSIÓN

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 habrá un modelo que contemple todas las características 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[57]. 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.

Algunos de los modelos estudiados, como es el caso de modelo del *National Institute of Justice* en su versión 2001, Casey año 2000, el DFRWS son modelos abstractos, donde se establecen unas fases de forma muy general. Indican el qué hacer pero no es muy claro en el cómo. Esto puede incurrir en que, al querer realizar un procedimiento forense se cree vacíos en el conocimiento de una persona que se esté iniciando en las ciencias forenses digitales. Puede tener un camino muy general a seguir pero no se garantiza que se estén cumpliendo con los requerimientos técnicos mínimos necesarios.

Otros modelos como el Casey del 2004, el de Reith, Carr y Gunsch empezaron a ser más claros en cuando al cómo hacerlo, eso sí, de una forma muy general. Se denotan aspectos como la documentación del proceso, asegurar y preservar la evidencia, el cuidado que se debe tener en la recolección de la misma. Pero estos modelos al considerar que las personas que realizan el procedimiento forense tienen los conocimientos necesarios para ello omiten ciertos aspectos importantísimo como es la cadena de custodia, este es el caso del modelo de Reith y compañía.

Organizaciones como *National Institute of Justice* publicaron una guía para la aplicación de la ley en el examen de la evidencia digital. Aunque este modelo maneja un número

[57] CASEY, Eoghan. Handbook of Computer Crime Investigation: Forensic Tools and Technology. First Edition. Academic Press, 2002. . ISBN: 0-12-163103-6.

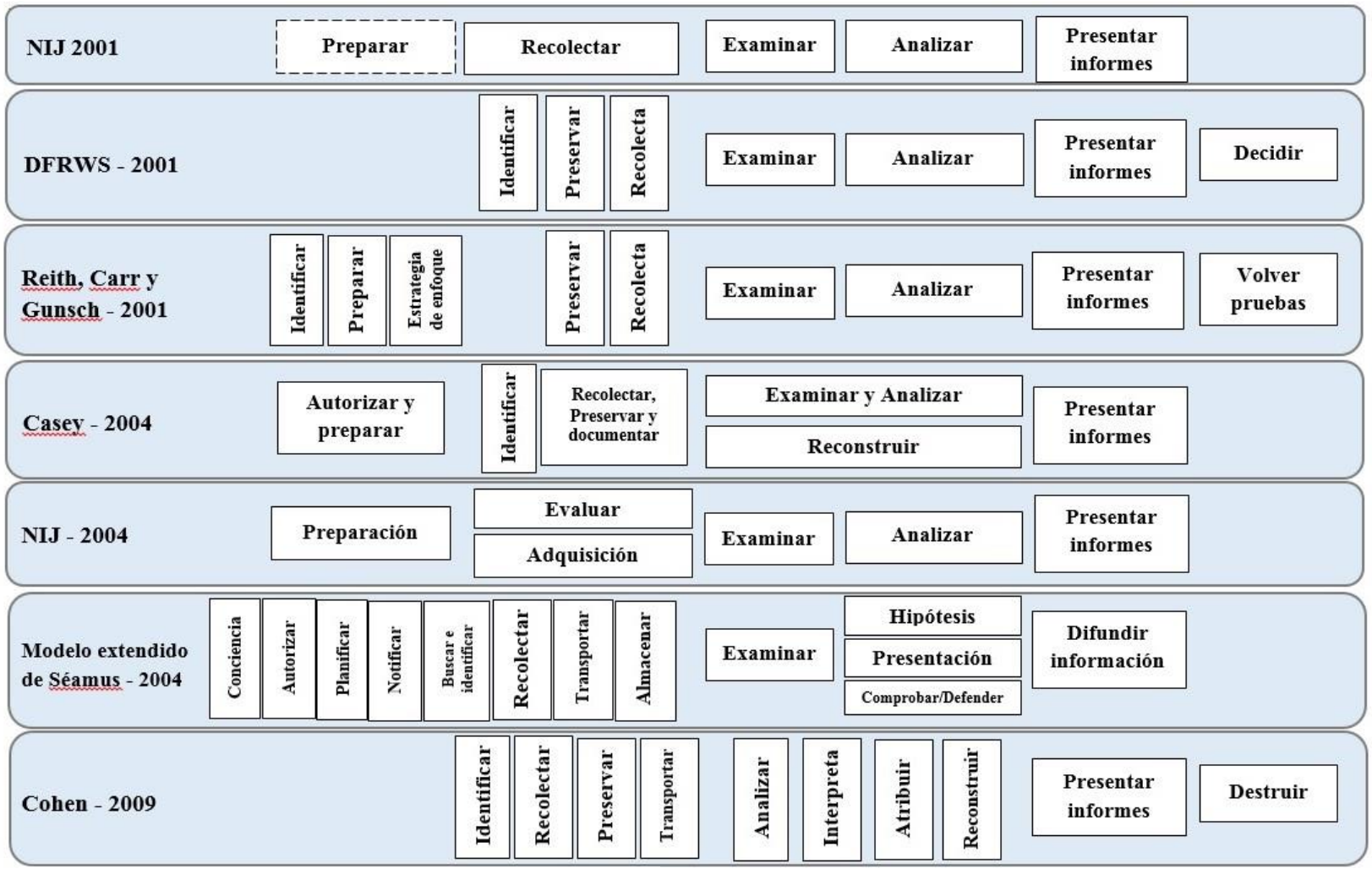


Figura 9 - Fases de los diferentes modelos forenses

reducido de fases sí maneja unos detalles más específicos en cada una de sus fases. Este modelo y con el propuesto por Séamus Ó Ciardhuáin determinan unas fases o actividades previas a la adquisición de la evidencia. Actividades como la evaluación de la evidencia, del caso y su alcance, la conciencia de qué es lo que se va a investigar, la autorización para llevarla a cabo, los aspectos legales de la misma son importantes para garantizar que le procedimiento se lleve de acuerdo a las leyes. El modelo de Cohen está más orientado al manejo de la evidencia digital y no es tan abstracto como los primeros modelos mencionados inicialmente.

Todos los modelos anteriormente mencionados pueden ser usados tantos en equipos de cómputo, medios de almacenamiento y entornos de red. En el tiempo que fueron presentados el auge de los dispositivos móviles no existía, por ende, sus características únicas no se tuvieron en cuenta. Y sí bien, las memorias usadas para el almacenamiento en estas terminales puede ser tratada como un medio de almacenamiento más tradicional, los teléfonos inteligentes poseen una arquitectura, sistema de archivos diferentes al de un equipo de escritorio o laptop. Las características con las que fueron concebidas estas tecnologías hacen que se tenga especial cuidado al someterlas a un procedimiento forense.

En conclusión, cada investigación es única, por esta razón es imposible conocer a priori los aspectos a tener en cuenta al llevar a cabo un procedimiento forense y como consecuencia no es posible definir una metodología única para abordar este tipo de investigaciones[58]. Por esta razón es importante desarrollar una guía forense aplicable a los dispositivos móviles donde se tengan en cuenta los puntos fuerte de las diferentes modelos y se tengan en cuenta las buenas prácticas y que sus actividades este apegadas a la ley.

[58] CANO, Jeimy, *et al*. Algunas consideraciones técnicas y de procedimiento para la investigación de delitos informáticos.

6. GUÍA PRÁCTICA PARA EL ANÁLISIS DIGITAL FORENSE EN DISPISITIVOS ANDROID UTILIZANDO UNA METODOLOGÍA POST-MORTEM

Está guía está conformada por ocho fases propuestas por el autor. Está guía está basada en las buenas prácticas y recomendaciones hechas por autores reconocidos en el ámbito de la informática forense a nivel nacional, latinoamericano y a nivel mundial y por instituciones y organizaciones relevantes en temas de la informática forense, la respuesta a incidentes y el manejo de la evidencia digital como los son el *National Institute of Standards and Technology* – NIST y el *National Institute of Justice – U.S. Department of Justice*.

Para detallar la guía puede revisar el *Anexo 1* de este trabajo.

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 son 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.

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 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.

Al momento de proponer un modelo que pretende ser una guía se deben tener consideraciones generales y particulares del objeto al que va orientado. Esta debe brindar el número necesario de temas que permitan el conocimiento de una forma general y que permita ser el punto de partida para un estudio más formal.

La informática forense y la seguridad informática son dos líneas de estudio muy interesantes que pueden ser abarcadas por los estudiantes de ingeniería de sistemas y carreras afinas con el área de TI. Hay muchas posibilidades de investigación a nivel de semilleros de investigación y grupos de investigación que permitan el fortalecimiento de los programas académicos y de las instituciones de educación superior.

RECOMENDACIONES

Las recomendaciones que puedo hacer para futuras investigaciones y donde este trabajo puede ser una base, es la incorporación de otros aspectos relacionados con el análisis forense. El análisis es un proceso más general y abarca otras áreas de estudio de la estudiada en este documento. A saber:

El análisis forense en vivo, que comprende la adquisición y estudio de la información obtenida de la memoria volátil del dispositivo. 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.

El estudio del malware para plataformas móviles, en especial para Android que es el sistema operativo más atacado en la actualidad que será así en los próximos años hasta que las condiciones del mercado móvil cambien.

El estudio de archivos APK (*Application PacKage File*) que pueden ser *FakeApp* para engañar a los usuarios.

El estudio de las técnicas de intrusión para los dispositivos móviles y la forma de cómo el análisis forense puede identificarlos.

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.

BIBLIOGRAFIA

ARIAS CHAVES, Michael. Panorama general de la informática forense y de los delitos informáticos en Costa Rica. En: InterSedes: Revista de las Sedes Regionales. 2006. p. 141-154.

ASSOCIATION OF CHIEF POLICE OFFICERS. Good Practice Guide for Computer-Based Electronic Evidence. Official release version.

BREZINSKI, D. y KILLALEA, T. Guidelines for Evidence Collection and Archiving. IETF, 2002. p 4.

BREZINSKI, Dominique y KILLALEA, Tom. RFC 3227: Guidelines for Evidence Collection and Archiving. 2002.

CANO, Jeimy, *et al*. Algunas consideraciones técnicas y de procedimiento para la investigación de delitos informáticos.

CANO, Jeimy, *et al*. Evidencia digital en el contexto colombiano: Consideraciones técnicas y jurídicas para su manejo. [En línea] http://52.0.140.184/typo43/index.php?id=856

CANO, Jeimy. Admisibilidad de la evidencia digital: de los conceptos legales a las características técnicas. En: Boletín de los Sistemas Nacionales Estadísticos y de Información Geográfica. 2005. p 93-108.

CANO, Jeimy. Computación forense. Descubriendo los rastros informáticos. México. Alfaomega, 2009.

CANO, Jeimy. Introducción a la informática forense: Una disciplina técnico-legal. En: Revista Sistemas. 2007. p 64-73.

CANO, Jeimy. Introducción a la informática forense: Una disciplina técnico-legal. En: Revista Sistemas. 2007. p 64-73.

CASEY, Eoghan. Digital evidence and computer crime: Forensic science, computers and the internet. San Diego, California. Academic Press, 2011.

CIARDHUÁIN, Séamous Ó. An Extended Model of Cybercrime Investigatons. En: International journal of Digital Evidence. Volumen 3, número 1 (2002).

COHEN, Fred. Challenges to Digital Forensic Evidence. Second Edition. Fred Cohen & Associates, 2008. ISBN: 1-878109-41-3.

COHEN, Fred. Digital Forensic Evidence Examination. Fifth Edition. Fred Cohen & Associates, 2009. ISBN: 1-878109-48-0.

DARAHUGE, María Elena y ARELLANO GONZALEZ, Luis E. Capítulo 10: Android. En: Manual de informática forense II. Primera edición. Buenos Aires: Errepar, 2012.

DARAHUGE, María Elena y ARELLANO GONZALEZ, Luis E. Manual de informática forense II. Primera edición. Buenos Aires: Errepar, 2012. p 99-100.

DARAHUGE, María Elena y ARELLANO GONZALEZ, Luis E. Manual de informática forense II. Primera edición. Buenos Aires: Errepar, 2012. p 100-101.

DARAHUGE, María Elena y ARELLANO GONZALEZ, Luis E. Manual de informática forense II. Primera edición. Buenos Aires: Errepar, 2012. p 63.

DIGITAL FORENSIC RESEARCH WORKSHOP. A road Map for Digital Forensic Research: Report from the first Digital Forensic Research Workshop. Utica, New York. DFRWS, 2001. p 15-20

ESET. Guía de seguridad para usuarios de Smartphone. 2012.

ESPINOSA, Luis R. Recolección de técnicas forenses para acceso y examinación del sistema operativo Android.

FEDERAL BUREAU OF INVESTIGATION. Digital Evidence: Standards and Principles. Scientific Working Group on Digital Evidence (SWGDE) International Organization on Digital Evidence (IOCE). FBI, 2000.

FEDERAL BUREAU OF INVESTIGATION. Digital Evidence: Standards and Principles. [En línea] <https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/>

FERNÁNDEZ BLEDA, Daniel. Informática forense. Teoría y práctica. Sevilla, España. 2004.

FISCALIA GENERAL DE LA NACION. Manual de procedimientos para la cadena de custodia ISBN 958-97542-8-7.

GALLARDO, Yolanda y MORENO GARZÓN, Adonay. Módulo 3: Recolección de información. Serie Aprender a investigar. ICFES, 1999.

HERNÁNDEZ SAMPIERI, Roberto, et al. Metodología de la investigación. México. McGraw Hill, 2010.

IAB SPAIN RESEARCH. VI Estudio Anual IAB Spain Mobile Marketing. Madrid, 2014.

JAKOBSSON, Markus y RAMZAN, Zulfikar. Crimeware: Understanding New attacks and Defenses. Boston. Pearson Education Inc., 2008.

JANSEN, Wayne y AYERS, Rick. Guidelines on Cell Phone Forensics: Recommendations of the National Institute of Standards and Technology. NIST, 2007. p 59.

JARAMILLO CABRERA, Guillermo Elías. Técnicas de análisis forense digital aplicadas a dispositivos y sistemas móviles. En: Apuntes de Ciencia y Sociedad. 2011. p 167-171.

KASPERSKY LAB y INTERPOL. Mobile Cyber Threats. 2014.

kASPERSKY LAB. Más de la mitad de usuarios de Android no protege sus equipos de amenazas informáticas. [En línea] 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, Karen, et al. Guide to Integrating Forensic Techniques into Incident Response. Gaithersburg, MD. NIST, 2006.

KRUSE II, Warren G, *et al*. Computer Forensics – Incident Response Essentials. Pearson Education, 2001.

MEROLA, Antonio. Data Carving Concepts. SANS Institute, 2008.

MOBILE PHONE FORENSICS. 47th EWPITC meeting – Final report, European Working Party on IT Crime, INTERPOL, September 7, 2006.

MOSQUERA GONZÁLEZ, José Alejandro, *et al*. Evidencia digital: contexto, situación e implicaciones nacionales. Universidad de los Andes – Facultad de Derecho, 2005.

NATIONAL INSTITUTE OF JUSTICE. Electronic Crime Scene Investigation: A guide for First Responders. U.S. Department of Justice, 2001.

NATIONAL INSTITUTE OF JUSTICE. Forensic Examination of Digital Evidence: A Guide for Law Enforcement. U.S. Department of Justice, 2004.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guide to Integrating Forensic Techniques into Incident Response – SP 800-86. NIST, 2006.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guidelines on Cell Phone Forensics (SP 800-101). NIST, 2007.

NELSON, Bill. Guide to Computer Forensics and Investigations. Fourth edition. United States of America. Course Technology, Cengage Learning, 2010. p 105.

REITH, Mark, *et al*. An Examination of Digital Forensic Models. En: International Journal of Digital Evidence. Volumen 1, número 3 (2002).

SANTIAGO CHINCHILLA, Enrique. CEH, CHFI. Curso de computación forense. Network Securiry Team.

SHIREY, Robert W. RFC 2828 - Internet Security Glossary. 2002.

SYMANTEC. Análisis de Symantec de las plataformas iOS de Apple y Android de Google revela mayor seguridad en comparación con las PCs, pero aún existen algunas brechas. [En línea] http://www.symantec.com/es/mx/about/news/release/article.jsp?prid=20110823_01

U.S DEPARTMENT OF JUSTICE. Electronic Crime Scene Investigation: A Guide for First Responders. National Institute of Justice, 2001.

WOLFE, Henry B. Evidence Analysis. En: Computers and Security. Volumen 22, numero 4. 2003. P 289-291

ZUCCARDI, Giovanni Y GUTIÉRREZ, Juan David. Informática forense. 2006.

ANEXOS

Anexo 1: Guía práctica propuesta

Esta página se dejó en blanco a propósito

GUÍA PRÁCTICA PARA EL ANÁLISIS DIGITAL FORENSE EN DISPISITIVOS ANDROID UTILIZANDO UNA METODOLOGÍA POST-MORTEM

Johan Smith Rueda R.
Semillero de Investigación GNU/Linux And Security – SIGLAS
Grupo de Investigación en Ingenierías Aplicadas para la Innovación, la Gestión y el Desarrollo – INGAP
Universidad Francisco de Paula Santander Ocaña – UFPSO

Versión 1.0
Octubre de 2015

Contenido

1. INTRODUCCIÓN

1.1 Propósito y alcance

El propósito de este documento es servir como guía en el proceso del análisis forense digital a un dispositivo móvil con sistema operativo Android, a todas aquellas personas y estudiantes que quieren iniciarse en el aprendizaje e investigación de esta área de la seguridad informática. Este documento detalla las buenas prácticas de la informática forense en general y las orientadas a dichas terminales.

El alcance de esta guía es el análisis forense a los medios de almacenamiento permanente en los dispositivos móviles con sistema operativo Android como lo es la memoria interna del terminal y la SDCard. Por otro lado, en esta guía no se implementa herramientas hardware forense como bloqueadores de escritura, o herramientas para esterilización de los medios donde se almacenará las imágenes forenses entre otros, sino que dichas actividades se realizan por medio del software disponible.

1.1. Audiencia

Este documento está dirigido a los integrantes de semilleros de investigación, de grupos de investigación, a la comunidad universitaria en general y a toda aquella persona que esté interesada en iniciarse en el estudio de la informática forense en general y el análisis forense a un dispositivo móvil con sistema operativo Android de forma particular.

1.2. Estructura del documento

Este documento presenta la siguiente estructura. En el punto 1, se hace la introducción al documento. En el punto 2 se muestra la representación gráfica del modelo propuesto que está compuesto de ocho fases las cuales se desarrollan en los puntos 3 al 10. Finalmente, en el punto 11 se presentan los anexos a esta guía, entre los cuales tenemos: Un glosario de términos, una descripción de algunas de las herramientas con licencia GPL y diferentes formatos para el manejo de las pruebas o evidencias.

2. MODELO PROPUESTO

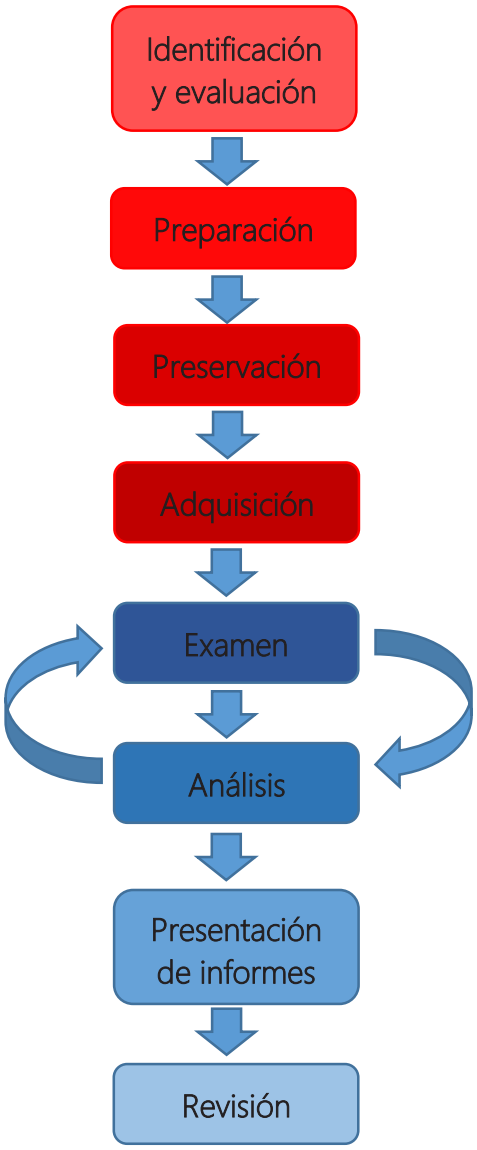


Figura 1 – Modelo propuesto. Fuente: Autor.

3. FASE DE IDENTIFICAR Y EVALUAR

En esta fase se hace el primer acercamiento con el caso a investigar. La víctima o una autoridad solicitan que se investigue una situación en particular. El investigador o el encargado de recibir ese primer contacto dentro del equipo forense debe asegurarse de obtener la mayor información posible sobre el caso es cuestión y los elementos asociados a este. En lo que respecta a esta guía, los elementos asociados de interés son los dispositivos móviles –aunque para la informática forense en el sentido general le interese todo equipo que cree, almacene y trasmita información–. La información que necesitamos conocer e identificar para ir estructurando y preparando el caso, tenemos:

- Información sobre el incidente.
- El alcance que puede tener el proceso forense.
- Escena del crimen
- Evaluar el entorno donde se realizará la extracción de las pruebas de los dispositivos móviles.
- La potencial información que pueda servir como pruebas.
- Las consideraciones legales

La información relevante que se debe conocer en primer instante es el incidente en sí, saber lo que pasó o lo que se sospecha que ha pasado. Esta información se obtiene a través de los testimonios que ha dado la victima directamente, o de las entrevistas que se realizan en la escena del crimen o a través de la documentación suministrada por una de las partes donde se plasme los acontecimientos. Esta información es importante porque marca el camino a seguir. Una vez se conozca lo que ocurrió o lo que se sospecha que ha pasado, se puede determinar el alcance que pueda tener el proceso forense, los datos o información que pueden ser relevantes como ***pruebas***[59] potenciales, y los recursos software o hardware necesarios para la investigación.

Se debe definir el objetivo o la misión de la investigación. No todas las investigaciones se realizan por la misma razón, y esto determina el alcance que pueda tener la investigación. Entre las razones por las cuales se puede realizar una investigación está la búsqueda de información sobre un tema específico, la recuperación de archivos importantes, la comprobación de si se cometió un delito informático, entre otras razones. Todo depende del por qué el cliente solicita la investigación. Definir el objetivo claro reduce el tiempo y costos del examen, ya se centra en qué buscar y donde se debería buscar, esto toma relevancia con la capacidad de almacenamiento que poseen los discos duros y demás medios de almacenamiento.

También es importante evaluar el escenario de trabajo dónde se realizará la adquisición de las pruebas. Esto depende del estado en la que se encuentre el dispositivo móvil, la escena del crimen en la situación en sí de los hechos. Para determinar el escenario en el cual se

[59] Esta guía dispone de un glosario para definir o explicar un término. Dichos términos aparecerán en *cursiva* y en **negrita** la primera vez que se mencione. El glosario se encuentra en el Anexo A.

podrá adquirir las pruebas del teléfono se debe dar respuesta al siguiente interrogante ¿se puede trasladar el dispositivo al laboratorio forense? Para dar respuesta se debe considerar si se tiene las garantías para el traslado. Sí la respuesta es sí, se procede con la siguiente fase que es la preservación. Si la respuesta en No, se va directo a la fase de adquisición de las pruebas –lo que indica que se debe llevar una estación forense a la escena del crimen–, y es esta la que se traslada al laboratorio.

Identificar la potenciales pruebas es muy importante, ya es que el punto de partida para que se desarrollen otras fases como la adquisición, el examen y su posterior ***análisis***. Si una prueba no es identificada a tiempo no podrá ser recolectada y procesada y se corre con el riesgo que en una fase posterior cuando el perito se percate de su relevancia esta información ya no exista o haya sido modificada, lo cual puede afectar la ***admisibilidad*** de la ***evidencia*** y se ponga en tela de juicio los resultados obtenidos por el perito informático. Los dispositivos Android tienen una gran cantidad de información que puede ser recolectada y analizada:

- Mensajes de texto (SMS-MMS)
- Lista de contactos
- Registro de llamadas
- Mensajes de correo electrónico
- Mensajería instantánea
- Coordenadas GPS
- Historial web
- Historial de búsquedas web
- Multimedia (Fotografía, audio y videos)
- Redes sociales
- Archivos guardados o descargados en el dispositivo
- Notas
- Agenda
- Información financiera
- Información de comercio electrónico
- Historial de compras el línea
- Archivos compartidos
- Conexiones (red de datos, Wi-Fi, Bluetooth)
- Las aplicaciones instaladas

Las consideraciones legales que se deben tener en cuenta son la autorización para llevar a cabo el proceso, por ejemplo una orden de registro o el consentimiento del propietario. La estructura formal para la autorización varía dependiendo del tipo de investigación. Por otra parte se debe revisar la normatividad de la organización, como sus políticas y estrategias[60].

[60] BREZINSKI, D. y KILLALEA, T. Guidelines for Evidence Collection and Archiving. IETF, 2002. p 4.

4 FASE DE PREPARAR

Una vez se tiene conocimiento del caso, la escena del crimen y se ha identificado las fuentes de las pruebas, se procese a preparar todo lo relacionado para realizar el procedimiento forense y el manejo de la prueba: documentación, extracción, empaquetado, almacenamiento y transporte. Esta es la etapa previa a la adquisición de las imágenes forenses.

Las herramientas y equipos necesarios son dictadas por cada aspecto del proceso. Los avances tecnológicos pueden dictar los cambios en las herramientas y equipos necesarios.

4.1 Hardware. En esta guía, los implementos hardware no son solo esos componentes físicos que integran una computadora o sistema informático; sino todos aquellos elementos tangibles que componen el laboratorio forense[61]. El hardware necesario en un laboratorio forense es:

- Diferentes interfaces para conectar los dispositivos móviles a la estación forense.
- Cargadores.
- Fuente portátil de energía suplementaria para garantizar que el dispositivo móvil no se apague el tiempo necesario para realizar la adquisición de las imágenes forenses.
- Medios de almacenamiento esterilizados para guardar las imágenes forenses, pueden ser tarjetas de memoria, *pendrive* o discos duros.
- Una caja o bolsa de Faraday.
- Guantes de látex, caso que el dispositivo móvil haga parte de una escena del crimen y se requiera extraer de este las huellas dactilares para posterior análisis.
- Bolsas antiestáticas

4.2 Software. En este apartado se puede trabajar de dos formas: 1. Utilizando una suite de herramientas forense dedicada a los dispositivos móviles o 2. Instalando las herramientas necesarias para el análisis en un dispositivo móvil en una estación forense y de respuesta a incidentes (*Ver Anexo H)*.

En ambos casos lo recomendable es tener un equipo dedicado para realizar los análisis forenses.

1. **Utilizando una suite de herramientas forense dedicada a los dispositivos móviles.** En esta caso, solo es instalar en un equipo de cómputo las distribución DEFT Linux que fue la elegida para realizar el análisis forense al dispositivo Android.

[61] En un laboratorio forense hay otra cantidad de componente hardware que no se tendrán en cuenta es la presente guía. Las razones es por su alto costo y porque para su adquisición hay requisitos como que sea un laboratorio forense o una fuerza del orden de un estado. Las personas naturales no tiene acceso libre a dichas herramientas. Pero el autor quiere dejar en claro que existen y que son necesarios para conformar un laboratorio forense. Entre esos recursos hardware tenemos *Forensic Workstation*, herramientas para la esterilización de los discos entre otras herramientas.

2. **Instalando las herramientas necesarias para el análisis en un dispositivo móvil en una estación forense y de respuesta a incidentes**. Como estación forense base se eligió SIFT Workstation V3 por ser una estación forense confiable que cuenta con el soporte de un equipo internacional de expertos forenses encabezado por el Instituto SANS. A esta estación forense se le instalará las herramientas que fueron elegidas en el apartado 4.4. Estas herramientas son:

    - Herramientas para la adquisición.
        - ☑ dc3dd
        - ☑ AFLogical OSE
    - Herramientas para la examinación.
        - ☑ Autopsy
        - ☑ Foremost
        - ☑ Testdisk
        - ☑ Myrescue
    - Herramientas para el análisis.
        - ☑ Autopsy
        - ☑ Log2timeline
    - Y en otra herramientas necesarias.
        - ☑ Comando adb

4.3 Equipo forense. El equipo forense es un equipo interdisciplinario. El personal que interviene en una investigación forense es la siguiente:

- Abogados, es el encargado de las consideraciones legales.
- Fotógrafos, se encarga de documentar visualmente la escena del crimen y los diferentes elementos en ella.
- Unidad de respuesta a incidentes, personas encargadas de llevar el procediendo de primera respuesta (*Véase Anexo 1: Glosario*)
- Analizadores de Incidentes
- Analista Forense: Entre sus funciones está la de dar una idea de los tipos de cosas que se deben buscar.
- Examinador de evidencias: Proporciona los medios para encontrar información relevante que pudiera estar en el sistema.
- Administrador de evidencias
- Testigos Expertos / peritos

El equipo forense debe estar integrado por personal con sus conocimientos certificados. Existen certificaciones a nivel internacional que acreditan esos conocimientos. También se debe conocer las herramientas y técnicas certificadas. Esto es importante para la idoneidad del profesional, uno de los puntos que se pueden poner en duda para dejar sin base a un caso. También es recomendable, refrescar periódica las habilidades a través de cursos, en la experiencia de trabajo y en fuentes académicas mantener el ritmo de la rápida evolución de las tecnologías y las responsabilidades del trabajo.

Con respecto a cómo se debe regir el equipo forense, grupos de profesionales reconocidos a nivel internacional en el ámbito de la informática forense ha establecido una serie de principio. La *Association of Chief Police Officers* (ACPO) plantea cuatro principios en su guía para en manejo de la prueba electrónica[62], a saber:

- **Principio 1**: Ninguna acción tomada por las fuerzas del orden, las personas empleadas dentro de esas agencias o sus agentes deben cambiar los datos que posteriormente pueden ser invocados en los tribunales.
- **Principio 2**: En los casos en que una persona se ve obligado a acceder a los datos originales, esa persona debe ser competente para ello y ser capaz de prestar declaración explicando la importancia y las implicaciones de sus acciones.
- **Principio 3**: Una pista de auditoría u otro registro de todos los procesos aplicados a la prueba digital deben ser creados y conservados. Una tercera parte independiente debe ser capaz de examinar los procesos y lograr el mismo resultado.
- **Principio 4**: La persona a cargo de la investigación tiene la responsabilidad general de garantizar que la ley y estos principios se cumplen.

Otra organizaciones que han descritos principio sobre el equipo forense y su forma de proceder con la prueba digital es el S*cientific Working Group on Digital Evidence* (SWGDE) y *el International Organization on Digital Evidence* (IOCE). Los principios descritos a continuación fueron presentados y aprobados en el *International Hi-Tech Crime and Forensics Conference* in Octubre de 1999. Estos son[63]:

- Al incautar la prueba digital, las medidas tomadas no deben cambiar esa prueba.
- Cuando es necesario para una persona para acceder a la prueba digital original, esa persona debe ser forense competente.
- Toda actividad relacionada con la incautación, el acceso, el almacenamiento o la transferencia de la prueba digital debe estar plenamente documentado, preservada, y está disponible para su revisión.
- Un individuo es responsable de todas las acciones tomadas con respecto a las pruebas digitales, mientras que la prueba digital es en su posesión.
- Cualquier agencia que se encarga de la incautación, acceder, almacenar o transferir prueba digital es responsable del cumplimiento de estos principios.

4.4 Suministros para el manejo de la prueba. El equipo forense debe tener a su disposición elementos que le permita etiquetar, registrar, almacenar y transportar la prueba.

- Formatos para el manejo de la prueba o evidencia (*Véase anexos de la guía*).
    - Formato de rotulado de evidencia física o material de prueba (*Anexo B*)
    - Registro del dispositivo móvil (*Anexo C*)
    - Registro de evidencia digital (*Anexo D*)
    - Registro de cadena de custodia (*Anexo E*)

[62] ASSOCIATION OF CHIEF POLICE OFFICERS. Good Practice Guide for Computer-Based Electronic Evidence. Official release version.

[63] FEDERAL BUREAU OF INVESTIGATION. Digital Evidence: Standards and Principles. [En línea] <https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/>

    - Registro de cadena de custodia digital (*Anexo F*)
    - Registro responsables de la cadena de custodia (*Anexo G*)
- Cámara fotográfica y grabadora para proporcionar recordatorios visuales y auditivos de la escena del crimen y del dispositivo[64].
- Etiquetas para cables
- Marcadores indelebles
- Etiquetas adhesivas
- Bolsas de pruebas
- Cinta de prueba
- Libreta para tomar notas rápidas y para crear croquis de la escena del crimen.
- Medios para el transporte 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 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. El *National Institute of Justice* lista algunas consideraciones generales que pueden ayudar al investigador durante todo el proceso de documentación[65]:

- Tome notas al consultar con el investigador de caso y/o el fiscal.
- Mantenga una copia de la autoridad de búsqueda con las notas del caso.
- Mantener la solicitud inicial de ayuda con el expediente del caso.
- Mantenga una copia de la cadena de custodia de documentación.
- Tome notas detalladas suficientes para permitir la duplicación completa de acciones.
- Incluir las fechas, hora, notas, descripciones y resultados de las acciones tomadas.
- Irregularidades de documentos encontrados y las medidas adoptadas en relación con las irregularidades durante el examen.
- Incluir información adicional, como la topología de la red, lista de usuarios autorizados, acuerdos de usuario y/o contraseñas.
- Documentar los cambios realizados en el sistema o red o en la dirección de la aplicación de la ley o el examinador.
- Documentar el sistema operativo y versión de software relevante y actual, parches instalados.
- Documentar la información obtenida en el lugar en relación con el almacenamiento remoto, acceso de usuarios remotos, y las copias de seguridad fuera del sitio.

[64] La grabadora y la cámara fotográfica buscan ayudar y facilitar al perito recordar con más detalle los procedimientos realizados y pueden ser de utilidad en la elaboración del informe pericial y a la hora de presentar el caso a un juzgado o parte interesada

[65] NATIONAL INSTITUTE OF JUSTICE. Forensic Examination of Digital Evidence: A Guide for Law Enforcement. U.S. Department of Justice, 2004.

5 FASE DE PRESERVAR

Uno de los retos que debe enfrentar en equipo forense es la adquisición de las pruebas. Esta actividad se complica por varios factores: el primero es que muchas organizaciones no tienen el personal disponible y capacitado para realizar los ***procedimientos de primera respuesta***, esto debido al desconocimiento, los costos o la falta de interés por los administrativos de la organización. Segundo, por el desconocimiento del personal de una organización o de las personas naturales de cómo deben actuar ante un incidente; muchos siguen usando los equipos y dispositivos comprometidos luego del incidente provocando la alteración, modificación o pérdida parcial o total de la prueba. Como tercero, que la notificación o descubrimiento del incidente suceda tiempo después de ocurrido.

Para garantizar que las pruebas sean contaminadas, estropeada o eliminada la persona de primera respuesta debe asegurar la escena del crimen y todos los elementos que estén en ella.

5.1 Asegurar, evaluar y documentar la escena. Al ocurrir un incidente de seguridad se debe asegurar la escena del crimen. La primera respuesta debe adoptar para garantizar la seguridad de todas las personas en el lugar y para proteger la integridad de todas las pruebas, ya sean electrónicas o no. Evaluar la escena y formular un plan de búsqueda, identificar las posibles pruebas y asegurar, documentar y/o fotografiar las potenciales pruebas. Para asegurar y evaluar la escena de debe tener en cuenta medidas como[66]:

- Siga la política jurisdiccional para asegurar la escena del crimen. Esto incluye garantizar que todas las personas se retiran de la zona inmediata a la evidencia, ***acordonar*** el lugar y colocando a un custodio del área física, ya sea del personal de vigilancia de la organización o del personal que lleva a cabo el ***procedimiento de primera respuesta***. No se debe alterar el estado de los dispositivos electrónicos: Si está apagado, dejarlo apagado. Si está encendido, déjelo encendido.
- Proteja los datos perecederos física y electrónicamente. Cualquier dispositivo que contenga datos perecederos se debe asegurar de inmediato, documentado, y/o fotografiado.
- Identifique las líneas telefónicas y LAN/Ethernet, documente, desconecte, y etiquete que sea posible.

Llevar a cabo las entrevistas preliminares para obtener información como usuarios, contraseñas, propietarios/usuarios de los dispositivos electrónicos que se encuentran en escena y otra información que pueda ser relevante en el caso.

Para documentar la escena se debe crear un registro histórico permanente de la escena. Anotar la ubicación y el estado de los equipos, medios de almacenamiento, otros dispositivos digitales, y las pruebas convencionales. Documentar la condición y ubicación del sistema informático, incluyendo el estado de energía del ordenador (encendido, apagado o en modo de reposo). También se debe identificar y documentar los componentes

[66] NATIONAL INSTITUTE OF JUSTICE. Electronic Crime Scene Investigation: A guide for First Responders. U.S. Department of Justice, 2001.

electrónicos relacionados que no serán recogidos y fotografiar toda la escena para crear un registro visual.

Las pruebas deben ser registradas con exactitud. Las pruebas no electrónicas manuales pueden proporcionar información útil sobre las capacidades del dispositivo, la red utilizada, información de la cuenta, y los códigos de desbloqueo para el PIN.

Se debe obtener registro fotográfico de los dispositivos digitales, incluidos los teléfonos móviles que puedan almacenar datos. Estos se deben fotografiar junto con cables periféricos, conectores de alimentación, medios extraíbles, y conexiones.

Es recomendable tener a una persona encargada de realizar las tareas de custodia de la prueba en la escena del crimen junto con la persona responsable de la documentación de las pruebas durante la recolección de la misma.

5.2 Embalaje, Transporte, Almacenamiento. Se debe iniciar la ***cadena de custodia*** de pruebas electrónicas, la documentación de su ***embalaje***, transporte y almacenamiento. Antes de ser envasado las pruebas deben documentar adecuadamente y etiquetarse. Si es un medio magnético el embalaje se realiza en un embalaje antiestático (papel o bolsas de plástico antiestático).

Durante el transporte y almacenamiento evite las fuentes magnéticas (por ejemplo, transmisores de radio, imanes de altavoz). También evite condiciones de calor excesivo, frío o humedad y los golpes y vibraciones excesivas.

En Colombia, estos procedimientos están regulados por el Manual de procedimientos para la cadena de custodia de la Fiscalía General de la Nación, el cual 'contempla las normas, el proceso y los procedimientos del sistema de cadena de custodia que permitirán alcanzar niveles de efectividad para asegurar las características originales de los elementos materia de prueba o evidencias físicas desde su recolección hasta su disposición final'[67].

5.3 Del dispositivo móvil. Anteriormente se describieron algunas consideraciones que se deben tener en cuenta de forma general para cualquier dispositivo en una escena del crimen. Aplica también para los dispositivos móviles. A continuación con tienen algunas consideraciones especialmente para estos dispositivos:

- En caso de ser necesario aplicar medidas forenses tradicionales, como identificar las huellas dactilares o las pruebas de ADN –para establecer un vínculo entre un teléfono móvil y su propietario o usuario, o por otras razones–, se debe extraer primero la prueba de dispositivo ya que los químicos usados para las pruebas físicas pueden causar alteraciones, daños o mal funcionamiento del terminal.
- En consecuencia con lo anterior, el investigador deber usar guates de látex para evitar contaminar las pruebas físicas que puedan ser útil en otro proceso de la investigación.

[67] FISCALIA GENERAL DE LA NACION. Manual de procedimientos para la cadena de custodia ISBN 958-97542-8-7.

- Se debe aislar el dispositivo apagando las interfaces inalámbricas, tales como radios Bluetooth y WiFi.
- En las entrevistas preliminares, considere solicitar al propietario o usuario del dispositivo móvil los códigos de seguridad o contraseñas necesarias para acceder a su contenido. A los sospechosos no se les deberían permitir manejar los teléfonos móviles u otros dispositivos móviles. Muchos teléfonos tienen códigos de restablecimiento maestro que borrar el contenido del teléfono a las condiciones originales de fábrica.
- Evite el apagar intencionalmente o dejar que la batería se agote ya que en el proceso se pueden perder datos o el dispositivo pida una contraseña al encender.
- La extracción de la batería también puede causar el contenido de algunos dispositivos que se pierda, tales como ciertos teléfonos inteligentes.
- En el caso que el dispositivo esté sumergido en líquidos, la batería debe ser retirada para evitar cortocircuitos. El resto del teléfono debe ser sellado en un recipiente adecuado lleno con el mismo líquido para el transporte al laboratorio, siempre y cuando el líquido no es cáustico.

Los dispositivos móviles también deben ser fotografiados. En el proceso, evite tocar o contaminar el teléfono y el entorno donde se encontró. Si la pantalla del dispositivo se encuentra en un estado visible, el contenido de la pantalla debe ser fotografiado y, si es necesario, registran manualmente, capturando el momento, el estado del servicio, nivel de batería, y otros iconos que aparecen.

El grupo forense en dispositivos móviles que es un sub-grupo del Grupo de Trabajo Europeo de Interpol sobre delitos de TI ha identificado como los principios ACPO de prueba se aplican en la incautación de los teléfonos móviles[68]. A continuación se resumen algunas de las implicaciones para la adecuada recolección. Tenemos:

- El teléfono se debe aislar de otros dispositivos utilizados para la sincronización de datos para impedir que los nuevos datos se contaminan con datos existentes.
- Si el dispositivo se encuentra conectado a un ordenador a través de un cable, tirando del enchufe de la parte posterior del equipo elimina la transferencia de datos o sobrescribe sincronización.
- El teléfono debe incautarse junto con los soportes y cables que se encuentran con él.
- No se deben quitar las tarjetas de los medios de comunicación, las SIM y otro hardware que residan en el teléfono.
- Se puede aprovechar la computadora al que se conecta al teléfono para adquirir desde el disco duro los datos sincronizados con el dispositivo y que no podrían obtenerse del teléfono.
- Cualquier hardware asociado con el dispositivo como tarjetas de memoria, SIM, adaptadores de corriente, fundas de dispositivos o periféricos deben aprovecharse

[68] MOBILE PHONE FORENSICS. 47th EWPITC meeting – Final report, European Working Party on IT Crime, INTERPOL, September 7, 2006.

junto con materiales relacionados, tales como manuales de productos, empaques y software.

Aislar el dispositivo de la redes es importante para evitar que nuevo tráfico como SMS, notificaciones de aplicaciones puedan sobrescribir los datos existentes. Existe tres métodos básicos para aislar el dispositivo de la redes. Estos son: apagar el dispositivo, mantenerlo encendido pero en una ***jaula de Faraday*** y activar el modo avión. Pero cada método tiene su inconveniente:

- Apagar el dispositivo puede activar códigos de autenticación, como por ejemplo, el pin de la SIM y/o seguridad del teléfono.
- Al mantener encendido el teléfono pero en una jaula Faraday, acelera el gasto de batería debido al aumento de consumo de energía, ya que intenta sin éxito conectarse a una red, elevando su potencia de la señal al máximo.
- Habilitar el modo avión requiere la interacción con el teléfono, lo que representa algún riesgo. Este riesgo se minimiza si el técnico está familiarizado con el dispositivo y documenta las acciones tomadas, por ejemplo, en papel o en video.

Dos profesionales argentinos, Luis E. Arellano y María E. Darahuge establecen unos procedimientos para proteger el dispositivo según el posible estado en que se encuentre el dispositivo[69]. Dicho procedimientos lo cito textualmente a continuación:

"Encendido:

1. Mantener la batería cargada y no manipularlo. Según el tipo de dispositivo, evitar tocar la pantalla.
2. Efectuar las maniobras necesarias para aislar el dispositivo de la red, cubriéndolo con varias capas de papel aluminio o colocándolo en una jaula de Faraday o configurándolo en modo avión.
   En el modo avión, el celular no puedo enviar o recibir llamadas telefónicas, mensajes de texto, mensajes con imágenes o mensajes con video; el usuario no podrá navegar por internet o utilizar los dispositivos Bluetooth. El resto de las aplicaciones siguen en funcionamiento –reproductor de música, juegos, agenda, etcétera– y pueden seguir siendo utilizados. En los dispositivos en general, se debe oprimir el botón de apagado y seleccionar el *modo avión*. Otro modo es presionar *Menú* de la pantalla inicial, luego *Configuración* o *Ajustes*, luego la opción *Redes inalámbricas* o *Wireless Network*, y luego aparece el Modo avión."

"Apagado:

1. Dejar el dispositivo apagado, encenderlo implicaría la sobrescrita de datos.
2. Se recomienda apagar el equipo por la posibilidad de que se pierdan los datos ya sea porque la batería se agotó o porque ocurrió alguna pérdida de señal de la conexión con la red telefónica. Los datos de carácter temporal se perderán con el apagado del

[69] DARAHUGE, María Elena y ARELLANO GONZALEZ, Luis E. Manual de informática forense II. Primera edición. Buenos Aires: Errepar, 2012. p 99-100.

equipo. Al encenderlo, es posible que el dispositivo tenga una clave de acceso y por consiguiente el acceso al celular será restringido.

Observación: Si el teléfono está apagado y se le conecta el cargador es como si se lo hubiera encendido. Por esta razón, se recomienda esperar hasta que se pueda iniciar el dispositivo en el modo de recuperación o en el modo a prueba de fallos (DFU, *Device Failsafe Utility*, utilidad a modo de prueba de fallos del dispositivo) para la recolección de datos y en esta situación conectarlo al cargador".

Evaluar el estado de la batería del dispositivo y se deben tomar medidas para mantener el nivel de la batería a un nivel apropiado hasta que una exitosa adquisición se lleva a cabo. Por ejemplo, si el dispositivo tiene que ser aislado en una jaula de Faraday, se requiere que sea colocado en la jaula junto con una fuente portátil de energía suplementaria.

Embalaje, Transporte, Almacenamiento

Una vez el dispositivo está listo para ser incautado, se debe sella el dispositivo 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.

Al momento de transportar el dispositivo, este debe estar firme para evitar que se mueva y que accidentalmente se pulsen las teclas, como por ejemplo, el de encendido cuando está en la bolsa de pruebas. Al aislar el dispositivo en una jaula de Faraday, este se puede colocar conectado a un cargador de corriente externa para mantener el nivel de potencia completa durante el tránsito. Otra opción es conectar el cargador al encendedor de cigarrillos para mantener la carga. En este caso, se el cargador pasa a través de un agujero en la jaula de Faraday –el agujero se debe sellar bien, para evitar que se pierda el efecto de aislamiento–. Si un adaptador de corriente se utiliza en conjunto con una bolsa de aislamiento de radiofrecuencia, el cable debe estar protegido adecuadamente para evitar que actúa como una antena y anular el efecto de la bolsa de aislamiento.

El dispositivo también se debe proteger de golpes, roturas y temperaturas extremas. Las instalaciones de almacenamiento de las pruebas deben ser un área segura con acceso controlado y proporcionar un ambiente fresco y seco.

5.4 Cadena de custodia. La cadena de custodia es el proceso de documentar el recorrido completo que hace la prueba a través del ciclo de vida del caso. 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[70]. La cadena de custodio debe responder a los siguientes interrogantes:

- ¿Quién lo recogió? (es decir, dispositivos multimedia, periféricos asociados, etc.)
- ¿Cómo y dónde? (es decir, ¿cómo fue la evidencia recopilada y dónde se encuentra?)
- ¿Quién tomó posesión de ella? (es decir, persona a cargo de las pruebas incautación)

[70] KRUSE II, Warren G, *et al*. Computer Forensics – Incident Response Essentials. Pearson Education, 2001.

- ¿Cómo fue almacenada y protegida en el almacenamiento? (es decir, los procedimientos de pruebas de custodia)
- ¿Quién lo sacó de almacenamiento y por qué? (es decir, la documentación del nombre y el propósito del individuo en curso para pruebas de comprobación de salida)

La cadena de custodia se aplica a los elementos físicos materia de prueba y en el caso de los medios informáticos, las imágenes forenses creadas a partir de estos[71], 'para garantizar la autenticidad de los mismos, acreditando su identidad y estado original, las condiciones y las personas que intervienen en la recolección, envío, manejo, análisis y conservación de estos elementos, así mismo, los cambios hechos en ellos por cada custodio. La cadena de custodia se inicia en el lugar donde se obtiene, encuentre o recaude el elemento físico de prueba y finaliza por orden de la autoridad competente'[72]. Esta documentación se debe mantener archivada en un lugar seguro para su referencia actual y en un futuro.

6 FASE DE ADQUIRIR PRUEBAS

Esta fase consiste en la búsqueda, el reconocimiento, recolección y documentación de la prueba electrónica[73]. Una vez que el dispositivo ha sido llevado al laboratorio forense, se registra su ingreso (*ver Anexo C*) y continúa con la cadena de custodia se procede con la identificación del dispositivo.

Los pasos recomendados en este proceso son:

- Identificar las fuentes de datos.
- El desarrollo de un plan para adquirir los datos[74].
- La adquisición de los datos
- La verificación de la integridad de los datos.

El plan de adquisición de datos contempla todo lo relacionado al procedimiento de recolección, desde el orden en que se deben adquirir los datos hasta las medidas que se deben tomar para minimizar el riesgo del fracaso en la investigación.

Esta guía solo contempla en ***análisis post-mortem***. Pero al realizar un ***análisis en vivo o caliente*** como también se le llama, el plan debe dar prioridad a la fuente de datos, estableciendo el orden en que los datos deben ser adquiridos en función del valor probable de los datos, la volatilidad de los datos, y la cantidad de esfuerzo requerido.

---

[71] Las imágenes forenses de deben preservar y seguir la cadena de custodia al igual que el dispositivo físico, ya que estás imágenes en una copia exacta y fidedigna del dispositivo original. Es como si se tratase con el dispositivo físico.

[72] MOSQUERA GONZÁLEZ, José Alejandro, *et al*. Evidencia digital: contexto, situación e implicaciones nacionales. Universidad de los Andes – Facultad de Derecho, 2005.

[73] ASSOCIATION OF CHIEF POLICE OFFICERS. Good Practice Guide for Computer-based Electronic Evidence. Official release version.

[74] NELSON, Bill. Guide to Computer Forensics and Investigations. Fourth edition. United States of America. Course Technology, Cengage Learning, 2010. p 105.

En un análisis post-mortem los datos que se recolectan están almacenados en medios permanentes. En el caso de crear una imagen de la tarjeta SD del dispositivo, esta se trata como cualquier otro sistema de ficheros FAT, por lo cual, herramientas de líneas de comandos como dd, dc3dd y dcfldd que se usan para realizar copias bit a bit de un disco duro o un pendrive pueden ser usadas.

Una vez los datos han sido adquiridos y se han creado las ***imágenes forenses*** se debe comprobar la integridad de los datos. Eso se realiza para verificar que la imagen corresponde a la original y la prueba no ha sido modificada en el proceso. Esta verificación se realiza mediante algoritmos criptográficos como MD5 o SHA1. Si se usa el comando dd el proceso de *hashing* o creación de huella dactilar del documento se debe realizar con otra herramienta externa. Las herramientas dc3dd y dcfldd sí integran el proceso de *hashing*.

En estas dos últimas herramientas el *hash* se va calculando en paralelo a la realización de la imagen. Una vez termina el proceso se calcula el *hash* de salida y se contrasta con el de origen. Con dc3dd esta comparación se realizada en forma automática, en cambio con dcfldd no.

Se recomienda realizar dos imágenes forenses. La primera, que será copia original, se almacena de forma segura. Y una segunda copia, es con la cual se trabaja. Esta es una buena práctica para minimizar el fracaso de la investigación. En caso que se estropee la copia con la cual se trabaja o que por otra razón sea necesario obtener una copia extra, se hará un duplicado de la copia original.

En esta fase se sigue con el manejo de la cadena de custodia para evitar las acusaciones de mal manejo o manipulación de pruebas.

Entre los elementos que se pueden recolectar de un dispositivo móvil y la tarjeta SIM, tenemos[75]:

1) Sistema operativo
2) Llamadas realizadas (fecha, hora, duración)
3) Llamadas recibidas (fecha, hora, duración)
4) Ultimo numero marcado (LDN- *Last Dialed Number*)
5) Lista de contactos
6) Mensajes de texto
7) Fotografías
8) Archivos
9) Archivos borrados
10) Espacio desperdiciado
11) Videos
12) Agencia
13) Correo electrónico

[75] DARAHUGE, María Elena y ARELLANO GONZALEZ, Luis E. Manual de informática forense II. Primera edición. Buenos Aires: Errepar, 2012. p 100-101.

14) Tonos de timbre (ring tones) personalizados, los cuales pueden ser identificados por un testigo permitiendo ubicar a alguien en un determinado lugar

15) Ubicación, establece la ubicación física de una persona o su dirección de traslado o viaje

16) Tarjeta sim (*Subscriber identity module*)- contiene un procesador con memoria no volátil-, se utiliza como dispositivo de almacenamiento de información relacionada con el subscriptor, incorporada a la red global de celulares GSM (*Global Systems for Mobile Communications*). En la tarjeta se puede obtener:

- **a)** Identificador de área local, identificada donde está ubicado actualmente el celular. Este valor permanece almacenado en el SIM luego de apagado el celular. Es útil para identificar cual fue la última ubicación donde se utilizó el celular
- **b)** Número de serie, se puede obtener sin tener el PIN (*Personal Identification Number*) e identifica al SIM mismo.
- **c)** Numero de cliente, se refiere al IMSI (*International Mobile Subscriber Identity*), que es el número de identificación del cliente que permitirá, junto con la ayuda del proveedor de servicio, identificar al cliente propietario del celular.
- **d)** Número de teléfono del celular. Se refiere al MSISDN (*Mobile Subscriber Intergrated Services Digital Network).*

17) De la información que contiene la tarjeta SIM podemos extraer:

- **a)** Mensaje de texto: existe un espacio en la tarjeta que mostrara los últimos 12 mensajes enviados. Los celulares almacenan los mensajes en memoria. La mayoría utiliza la memoria de la tarjeta SIM primero antes de usar la memoria interna.
- **b)** Mensajes borrados: similar al borrado de archivos en un disco rígido, el primer byte es configurado en cero. Esto significa que los mensajes borrados pueden recuperarse, excepto el primer byte mientras no se sobrescriba con nuevos mensajes.
- **c)** Guía de teléfonos: la mayoría de los celulares tienen la capacidad de almacenar un mínimo de 100 números marcados con su respectivo nombre asociado.

Los dispositivos móviles pueden presentar obstrucciones o no a la hora de realizar la adquisición. Un dispositivo sin obstrucciones hace referencia al dispositivo que no requiere de una contraseña u otra técnica de autenticación para obtener acceso al dispositivo y realizar una adquisición. Los dispositivos que presentan obstrucciones son aquellos que al apagarse activan una medida de autenticación. Esta puede ser una contraseña, contraseña de PIN activada, una configuración de bloqueo, las contraseñas de bloqueo de tarjetas de memoria o el cifrado de los contenidos del teléfono.

El NIST en su guía[76] divide en tres clases las maneras de recuperar datos de los dispositivos obstruidos: basados en software, basados en hardware y los métodos de investigación.

Los métodos de investigación son procedimientos que no requieren de herramientas forenses ya sean software o hardware. Entre ellos tenemos:

[76] Guidelines on Cell Phone Forensics (SP 800-101).

- **Pregúntele al sospechoso**. La contraseña, PIN, o el patrón es un mecanismo de autenticación basada en el conocimiento[77], se puede consultar esta información al sospechoso, víctima o persona que solicita en análisis durante la entrevista inicial.
- **Revisión incautado materiales**. Las contraseñas o PIN pueden ser escritas en un trozo de papel y se mantiene con o cerca del teléfono, en una computadora de escritorio utiliza para sincronizar con el teléfono o la puede tener el sospechoso, por ejemplo dentro de su billetera, y podrá recuperar a través de la inspección visual..
- **Suministrar manualmente de entrada comúnmente utilizado**. Los usuarios pueden debilitar un mecanismo por el modo en que se utiliza. Por ejemplo, si la (U) SIM de un teléfono móvil requiere un PIN de 4 dígitos, un examinador puede que desee probar una combinación PIN uso común (por ejemplo, 1-2-3-4, 0-0-0-0, etc.), como uno de los tres intentos permitidos antes de que el dispositivo está completamente bloqueado.
- **Pregúntele al proveedor de servicios**. Si un teléfono móvil GSM está protegido con un PIN en la tarjeta SIM, el identificador de la tarjeta SIM (el ICCID) se puede obtener de ella y utilizado para solicitar el PUK de su proveedor de servicio y restablecer el PIN. Algunos proveedores de servicios ofrecen la posibilidad de recuperar el PUK online, introduciendo el número de teléfono del teléfono y cierta información sobre los abonados en páginas web públicas creadas para este fin.
- **Explotar posibles configuraciones inseguras.** Algunos modelos de celulares pueden producir fácilmente el acceso debido a errores de configuración comunes de los usuarios.

Los métodos basados en software implican técnicas de software que se utilizan para romper o evitar los mecanismos de autenticación. Entre estos métodos tenemos el obtener acceso a través de una puerta trasera o explotar las vulnerabilidades del sistema conocidos.

Entre los restos que presenta un analizador forense en un dispositivo Android está el modelo de seguridad que implementa este sistema operativo: el *kernel* de Linux, que implementa un modelo de permisos basados en usuario y aislamiento entre procesos; el *sandbox* de aplicaciones, el cual asigna un usuario único para cada aplicación, de esta forma, los recursos de cada aplicación quedan aislados y solo pueden ser accedidos por la dicha aplicación; el *rooting*, que es la única manera que un usuario o aplicación pueda acceder la información de otra es que posea los privilegios de *root*. El otro reto son las técnicas de autenticación[78].

Entre las técnicas de autenticación tenemos: el patrón, PIN, contraseña y algunos teléfonos modernos traen el desbloqueo facial y por medio de la combinación de rostro y voz.

[77] Los mecanismos de autenticación en general pueden ser de tres tipos: Los basados en lo que la persona sabe (contraseña, PIN, patrón), los basados en algo que la persona tiene (una tarjeta, un toquen) y los basados en algo que la persona es (biometría como huella dactilar, reconocimiento facial o de voz, etc.)

[78] ESPINOSA, Luis R. Recolección de técnicas forenses para acceso y examinación del sistema operativo Android.

7 FASE DE EXAMINAR

En el proceso de examinar se ayuda a que la evidencia sea visible, a explicar su origen e importancia. Para ello, se 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. En esta fase también se incluye el proceso de búsqueda que puede estar oculta[79].

El proceso de examen comienza con una copia de la prueba adquirida desde el dispositivo. Anteriormente, se realizaron una copia original, que es la que se guarda de forma segura y la copia duplicada, con la cual es la que se trabaja.

La realización del examen es una asociación del investigador o analista forense con el examinar forense. El analista da una idea de los tipos de cosas buscadas, mientras que el examinador forense proporciona los medios para encontrar información relevante que pudiera estar en el sistema[80].

El conocimiento adquirido mediante el estudio del caso también proporciona ideas sobre el tipo de datos para apuntar y palabras clave o frases específicas que utilizan en la búsqueda de los datos adquiridos.

Determinar las palabras claves es muy importante para ayudar a localizar información relevante dentro de toda la información recolectada. Esta lista de palabras claves se usa para 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.

Dependiendo del tipo de caso, la estrategia varía. Por ejemplo, si el caso es sobre pornografía infantil se puede comenzar por navegar por todas las imágenes gráficas en el sistema; si el caso es un delito relacionado con internet podría empezar a navegar por los archivos de la historia de Internet[81].

Al examinar no solo se encuentra datos potencialmente incriminatorios, también se puede encontrar otra información útil para el caso, como:

- Los tonos de llamada puedan ser relevantes, ya que las personas tienen la posibilidad de personalizarlo para distinguir su teléfono de los demás. Un tono de llamada puede ser reconocido por un testigo para identificar a una persona en cierto lugar.

---

[79] ASSOCIATION OF CHIEF POLICE OFFICERS. Good Practice Guide for Computer-based Electronic Evidence. Official release version.

[80] WOLFE, Henry B. Evidence Analysis. En: Computers and Security. Volumen 22, numero 4. 2003. P 289-291

[81] WOLFE, Henry B. Evidence Analysis. En: Computers and Security. Volumen 22, numero 4. 2003. P 289-291

- La información de la red esotérica encontrada en al SIM puede resultar útil en una investigación.

Los teléfonos celulares de última generación vienen con cada vez con mayor capacidad de almacenamiento interno y externo. Claro está, que este volumen de información comparada con un disco duro es mínima. Pero una de las técnicas usadas al momento de examinar la información es empezar a filtrar la información para así centrarse en los archivos potencialmente incriminatorios los cuales serán analizados en la siguiente fase.

Una vez se ha montado la imagen se puede empezar observar los archivos tal cual están en el dispositivo. Una vez se haga eso se puede realizar acciones como si se tratase de un dispositivo real ya se al crear una imagen se crea una copia exacta y fidedigna del medio original. En esta copia no solo se copian los sectores ocupados y los sectores libres, sino también los sectores marcados por el sistema operativo como dañados y se puede acceder a esa porción del fragmento que no ha sido ocupada completamente por el archivo pero que el sistema operativo marca ese fragmento como completamente utilizado (*Slack space*).

Una vez tengamos la imagen se puede empezar a:

- Recuperar los archivos borrados.
- Recuperar los archivos escondidos.
- Identificar los archivos existentes que son fácilmente legibles, o sea, lo que con solo abrirlos con el programa adecuado se pueden visualizar sin ningún otro procedimiento adicional.
- Identificar los archivos protegidos que tienen algún control de acceso (archivos cifrados).
- Consolidar los archivos potencialmente analizables, con el fin de reducir la búsqueda y centrarse en ciertos tipos de archivos.

Estos archivos se van almacenando en una carpeta dependiendo el tipo. Entonces abra una carpeta para ‘archivos borrados’, otra para ‘archivos cifrados’ y de esa forma con los demás.

Ya teniendo esta cantidad de archivos identificados se procede a realizar una primera clasificación de archivos. Esta primera clasificación se realiza de la siguiente manera:

- Archivos ‘buenos’ conocidos. Aquellos que su extensión corresponden con su contenido (por ejemplo, un .docx corresponde con un documento Word 2013; un .jpg con una imagen y un .rar con un archivo comprimido).
- Archivos ‘buenos’ modificados. Aquellos cuya versión original ha sido modificada.
- Archivos ‘malos’. Aquellos que representan algún tipo de riesgo para el sistema (*malware* como troyanos y gusanos, *backdoors,* etc).
- Archivos de extensión modificada. La extensión no corresponde con su contenido. Esto se usa para oculta algún archivo haciéndolo para por otro que no es y al intentar abrirlo el sistema lance un error.

Ya con los archivos identificados, filtrados y clasificados se pudo desechar los archivos irrelevantes para el caso de aquellos que sí lo son. Ahora sí se puede pasar a la siguiente fase, el análisis.

8 FASE DE ANALIZAR

El rol de la evidencia digital es establecer un enlace creíble entre el atacante, la víctima y la escena del crimen. Esta fase está mue ligada con la fase de examinar, y es posible que estando en el análisis se determine la posibilidad de volver a examinar nuevos archivos que no se tuvieron en cuenta en la fase anterior. El examinador y el analista forense deben trabajar para llegar al logro de los siguientes objetivos:

- Recopilar información sobre el individuo(s) que participan. [¿Quién?]
- Determinar la naturaleza exacta de los acontecimientos que se produjeron. [¿Qué?]
- Construir una cronología de eventos. [¿Cuándo?]
- Descubrir la información que explica la motivación por el delito. [¿Por qué?]
- Descubre qué herramientas o hazañas fueron utilizados. [¿Cómo?]

En el *Guidelines on Cell Phone Forensics* proporciona una referencia cruzada de las fuentes de pruebas genéricas que se encuentran comúnmente en los teléfonos móviles y su posible contribución a la satisfacción de los objetivos antes mencionados[82].

	Quién	Qué	Dónde	Cuándo	Por qué	Cómo
Suscriptor/Dispositivo	X					
Registro de llamadas	X			X		
Directorio	X					
Calendario	X	X	X	X	X	X
Mensajes	X	X	X	X	X	X
Localización			X	X		
URL web/Contenido	X	X	X	X	X	X
Imágenes/Video	X	X	X	X		X
Otro contenido del archivo	X	X	X	X	X	X

Tabla: Referencia cruzada de fuentes y objetivos[82]

En la anterior fase se identificó, filtró y clasificó los archivos. Ahora se procede a analizar los archivos que están comprometidos con el caso.

Como no existe un único camino para analizar la información, sino que esta depende del objetivo que se planteó en la fase de identificación y evaluación no se puede dar unas pautas específicas de qué analizar y cómo analizarlo. Esto se va determinando desde el principio y se va refinando a medida que va avanzando el proceso forense. Pero sí se puede dar algunas pautas generales de lo que se puede analizar en un dispositivo Android y el investigador será el encargado de elegir qué analizar dependiendo del caso que trabaje.

[82] JANSEN, Wayne y AYERS, Rick. Guidelines on Cell Phone Forensics: Recommendations of the National Institute of Standards and Technology. NIST, 2007. p 59.

De un dispositivo Android se puede analizar lo siguiente[83]:

- Registro de eventos o sucesos del núcleo. Como Android está basado en el *kernel* de Linux se puede usar un comando Linux para tal fin. Para ello se procede de la siguiente manera:
    - En la estación de trabajo forense se conecta el dispositivo con USB Debbuging habilitado y se ejecuta el comando dmseg[84]. Este comando no requiere de permisos administrativos.
      El resultado extraído muestra información acerca de la fecha y hora; del hardware, de las actividades del dispositivo en el inicio del sistema y del núcleo del sistema operativo.
    - Analizar la información en línea de los mensaje de depuración del sistema y de las aplicaciones con el comando logcat.
    - Analizar la información en línea de las conexiones del teléfono móvil con el sistema GSM, utilizando el comando logcat. La información puede ser de interés ya que muestra los datos sobre:
        - Fecha y hora de los eventos en formato Unix Epoch
        - Comando AT utilizados por el celular para comunicarse
        - Mensajes MSM: receptor, tamaño, fecha y hora.
        - Dirección IP del celular
        - Red y datos de la ubicación
        - Información del proveedor de servicio
    - Analizar la información en línea de los eventos utilizando el comando logcat
    - Analizar la información de los servicios, memoria, indicadores de procesos (PID), bases de datos, cuentas de acceso a redes sociales, correos electrónicos, fecha y hora y otros elementos del sistema con el comando dumpsys.
    - Analizar la información del estado del sistema con el comando dumpsys.
    - Analizar la información del estado del sistema con el comando bugreport que efectúa combinación de los comando logcat, dumpsys y dumpstate en un solo comando.
- Análisis del sistema de archivos YAFFS2
- Análisis de fragmentos (*Carving*) del sistema de archivos
- Análisis del sistema de archivos con el comando strings
- Análisis del sistema de archivos con el visor en hexadecimal
- Análisis del contenido de los directorios del sistema de archivos de Andriod

Si desea más información sobre lo anteriormente anunciado puede estudiar el capítulo 10 del Manual de informática forense II escrito por María E. Darahuge y Luis E. Arellano.

---

[83] DARAHUGE, María Elena y ARELLANO GONZALEZ, Luis E. Capítulo 10: Android. En: Manual de informática forense II. Primera edición. Buenos Aires: Errepar, 2012.

[84] dmesg (*diagnostic message*, mensajes de diagnóstico) es un comando presente en los sistemas operativos Unix que lista el buffer de mensajes del núcleo. Este buffer contiene una gran variedad de mensajes importantes generados durante el arranque del sistema y durante la depuración de aplicaciones.

Una actividad importante en el análisis es establecer la línea del tiempo, para comprender el orden cronológico en que sucedieron los hechos.

9 FASE DE PRESENTAR INFORMES

Presentar los informes es el proceso de preparar un resumen detallado de todas las medidas adoptadas y las conclusiones alcanzadas 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 explicar las conclusiones extraídas de la evidencia.

Es importante que antes de realizar el informe identifique al público al cual va dirigido, todos los grupos de personas no 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 donde 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.

Al informe debe estar soportado en el mayor número de evidencias, ya sean fotografías, capturas de video, y también se pueden entregar evidencia en soportes como CD o DVD en cual su formato no permite ser presentados en formato impreso como lo son los audios y videos.

De una forma general, el informe puede incluir la siguiente información[85]:

- Identidad de la agencia que presenta el informe.
- Identificador del caso o número de presentación.
- Investigador del caso.
- Identidad del remitente.
- Fecha de recibo.
- Fecha del informe.
- Lista descriptiva de artículos presentado para su examen, incluyendo el número de serie, marca, y el modelo.
- Identidad y firma del examinador.
- Breve descripción de las medidas adoptadas durante el examen, tales como búsquedas de cadenas, gráficos búsquedas de imágenes, y la recuperación de archivos borrados y demás medidas adoptadas.
- Resultados / conclusiones.

[85] NATIONAL INSTITUTE OF JUSTICE. Forensic Examination of Digital Evidence: A Guide for Law Enforcement. U.S. Department of Justice, 2004

El informe puede ser impugnado por la contraparte. Por esto se debe documentar la evidencia, las herramientas usadas (nombre, versión, etc.), 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.

10 FASE DE REVISAR

En la cultura japonesa hay una filosofía llamada Kaizen (‘cambio a mejor’ o ‘mejora’) y su principio es que hoy se puede ser mejor que ayer y mañana mejor que hoy. Una revisión a conciencia por parte del equipo forense de todos y cada uno de las fases desarrolladas durante la investigación permite refinar las actividades realizadas durante la preparación, adquisición, examen y análisis para una futura investigación.

No hay una sola forma de proceder en una investigación, cada caso tiene su particularidad y sus retos. Por ello, es importante que una vez se termine la investigación se analice las eventualidades de cada fase para enriquecer la pericia del investigador o del equipo forense en general.

La experiencia es una parte importante en la integridad del proceso forense. Con las herramientas adecuadas, los procedimientos técnicos garantizados y los conocimientos técnicos certificados se puede realizar un procedimiento forense acorde a los requerimientos legales, pero es la pericia de investigador que hace la diferencia a la hora de enfrentar un caso en particular teniendo como soporte la experiencia previa en otras investigaciones.

Anexo A: Glosario

Acordonamiento Acción de aislar el lugar de los hechos considerando sus características mediante la utilización de barricadas, cintas, personas y vehículos, entre otros.

Admisibilidad

Análisis Estudio técnico - científico al lugar de los hechos y a los elementos materia de prueba y evidencia física.

Análisis post-mortem Este análisis post-mortem se realiza utilizando un equipo dedicado específicamente para fines forenses: examinar dispositivos de almacenamiento permanente (discos duros, tarjetas SD, pendrive, etc.), datos o cualquier tipo de información recabada en un sistema que ha sufrido un incidente de seguridad.

Análisis en caliente Este análisis realiza en un sistema que se presume ha sido afectado o esté sufriendo un incidente de seguridad. Para este tipo de análisis se utiliza un CD con herramientas de respuesta ante incidentes y análisis forense compiladas de forma que no se realicen modificaciones en el sistema. Una vez se realiza el análisis en caliente y el incidente es confirmado se realiza el análisis post-mortem.

Cadena de custodia La cadena de custodia informático forense es un procedimiento controlado y supervisable, que se aplica a los indicios materiales o virtuales relacionados con un hecho delictivo o no, desde su localización hasta su valoración por los encargados de administrar justicia, y que tiene como fin asegurar la confiabilidad de la prueba documental recolecta en un determinado lugar del hecho real o virtual desde su identificación hasta su disposición definitiva por orden judicial[86].

Data Carving (Tallado de datos) Es el proceso de extraer un conjunto de datos de un conjunto de datos más grande. Las técnicas de tallado de datos se producen con frecuencia durante una investigación digital cuando se analiza el espacio del sistema de archivos no asignado para extraer los archivos. Los archivos son "tallados" del espacio no asignado utilizando valores de cabecera y pie de página específicos del tipo de archivo[87].

Embalaje Es el procedimiento técnico , utilizado para preservar y proteger en forma adecuada los elementos materia de prueba y evidencia física hallados y recolectados en el lugar de los hechos, lugares relacionados y en las diferentes actuaciones de policía judicial , con el fin de ser enviados a los respectivos laboratorios o bodegas de evidencia.

Evidencia El diccionario panhispánico de dudas define la evidencia como la ‘certeza clara y manifiesta de la verdad o realidad de algo’[88]. La evidencia demuestra de forma clara y contundente un hecho, por ello, la importancia de no romper con el principio de admisibilidad (*Ver Principio de admisibilidad*). El rol de la evidencia digital es establecer

[86] DARAHUGE, María Elena y ARELLANO GONZALEZ, Luis E. Manual de informática forense II. Primera edición. Buenos Aires: Errepar, 2012. p 63.
[87] MEROLA, Antonio. Data Carving Concepts. SANS Institute, 2008.
[88] Definición de Evidencia http://lema.rae.es/dpd/?key=evidencia

un enlace creíble entre el atacante, la víctima y la escena del crimen[89]. La evidencia no se puede confundir o usar como sinónimo de *prueba* o *indicio* (*Ver Prueba*).

Según el RFC 3227, la evidencia digital debe ser:

- Admisible: Se debe cumplir con ciertas normas legales que se le han se puede poner ante un tribunal (*Ver Admisibilidad*).
- Auténtico: Debe ser posible vincular positivamente material probatoria al incidente.
- Completa: Se debe contar toda la historia y no sólo una perspectiva en particular.
- Confiable: No debe haber nada acerca de cómo la evidencia fue recogida y posteriormente manejada que arroja dudas sobre su autenticidad y veracidad.
- Creíble: Debe ser fácilmente creíble y comprensible por un tribunal.

Faraday, Jaula o bolsa de La Jaula de Faraday es una estructura que permite reproducir el efecto homónimo descubierto por Michael Faraday durante sus estudios del Electromagnetismo. Dicho efecto provoca que el campo magnético en el interior de un conductor en equilibrio sea nulo, quedando neutralizado el efecto de los campos electromagnéticos.

Formato AFF (*Advanced Forensic Format*) es un formato de adquisición de datos desarrollado por Simson L. Garfinkel y Basis Technology.

Hash Es un valor hexadecimal unicode que identifica a un archivo o dispositivo.

Imagen forense Una imagen de archivos forenses es la forma técnica e idónea de copiar los datos de un medio informático con el propósito de preservar la evidencia y su posterior examinación. Dicho proceso se conoce como copia *bit-stream* (usualmente es conocido como adquisición o creación de la imagen), el cual consiste en copiar bit a bit los datos de un medio de almacenamiento original. Dicha copia es almacenada en un archivo conocido como imagen *bit-stream*. Entre los formatos para imágenes forenses tenemos como Raw, AFF, AFD, AFM, AFFLib, EWF (EnCase).

Sistema de archivos Define la forma en que los archivos se nombran, almacenar, organizar y acceder a los volúmenes lógicos (Un volumen lógico es una partición o una colección de particiones que actúen como una sola entidad que se ha formateado con un sistema de archivos). Existen muchos sistemas de ficheros diferentes, cada uno proporciona características únicas y estructuras de datos. Sin embargo, todos los sistemas de archivos comparten algunos rasgos comunes. En primer lugar, utilizan los conceptos de directorios y archivos para organizar y almacenar datos. En segundo lugar, los sistemas de archivos utilizan alguna estructura de datos para que apunte a la ubicación de los archivos de los medios de comunicación. Algunos de los sistemas de archivos más conocidos son: FAT 12/16/32, NTFS y los Ext2/3/4.

[89] SANTIAGO CHINCHILLA, Enrique. CEH, CHFI. Curso de computación forense. Network Securiry Team.

Primera respuesta, Procedimiento. El procedimiento de primera respuesta es realizada por el *First Responder,* que es la persona tiende acceso a la escena del crimen un momento después del incidente, y es el encargado de proteger, preservar y controlar el acceso a la evidencia antes que llegue el personal forense. Este procedimiento incluye identificar y proteger la escena del crimen, preservar la evidencia más frágil y temporal, recolectar información sobre el incidente, documentar los hallazgos y en algunos casos empacar y transportar la evidencia[90].

Principio de Locard El principio de intercambio o transferencia de Locard dice que cualquier persona u objeto que entra en la escena del crimen deja un rastro y se lleva uno consigo mismo.

Prueba Es la 'forma, argumento, instrumento y otro medio con que se pretende mostrar y hacer patente la verdad o falsedad de algo'. No debe confundirse con *Evidencia* (*Ver Evidencia, también, prueba pericial*).

Prueba digital Pruebas que consiste en la información almacenada o transmitida en forma electrónica

Prueba pericial Medio de prueba legal que consiste en los análisis científicos que realizan los expertos en las diferentes ciencias, disciplinas y artes que aplican a la investigación criminal.

[90] SANTIAGO CHINCHILLA, Enrique. CEH, CHFI. Curso de computación forense. Network Securiry Team.

Anexo B: Formato de rotulado de evidencia física o material de prueba

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: Identificación: Cargo:	Firma:

Anexo C: Registro del dispositivo móvil

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: Identificación: Cargo:	Firma:

Anexo D: Registro de evidencia digital[91]

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							

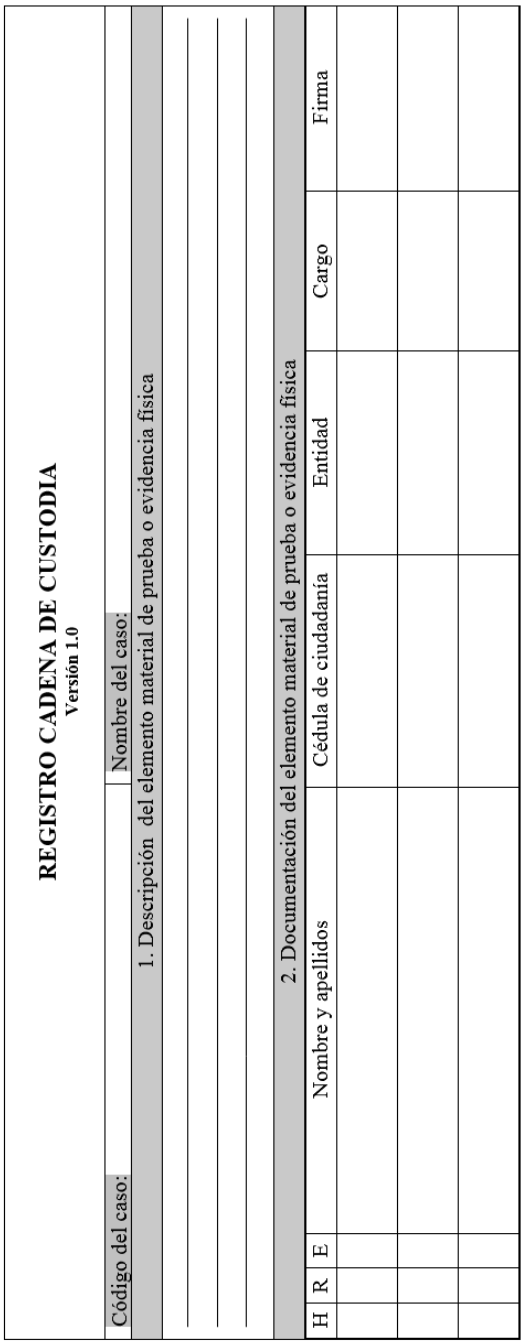
Medio de almacenamiento de la prueba			
Nro. de serie	Tipo	Capacidad	Ubicación del medio de almacenamiento

Observaciones
_____ _____ _____ _____

Responsable	
Encargado: Identificación: Cargo:	Firma:

[91] La evidencia digital hace referencia a las imágenes forenses creadas del dispositivo físico. Esta debe llevar un proceso de cadena de custodia independiente.

Anexo E: Registro de cadena de custodia[92]



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	Nombre y apellidos	Cédula de ciudadanía	Entidad	Cargo	Firma

Convenciones:

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

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

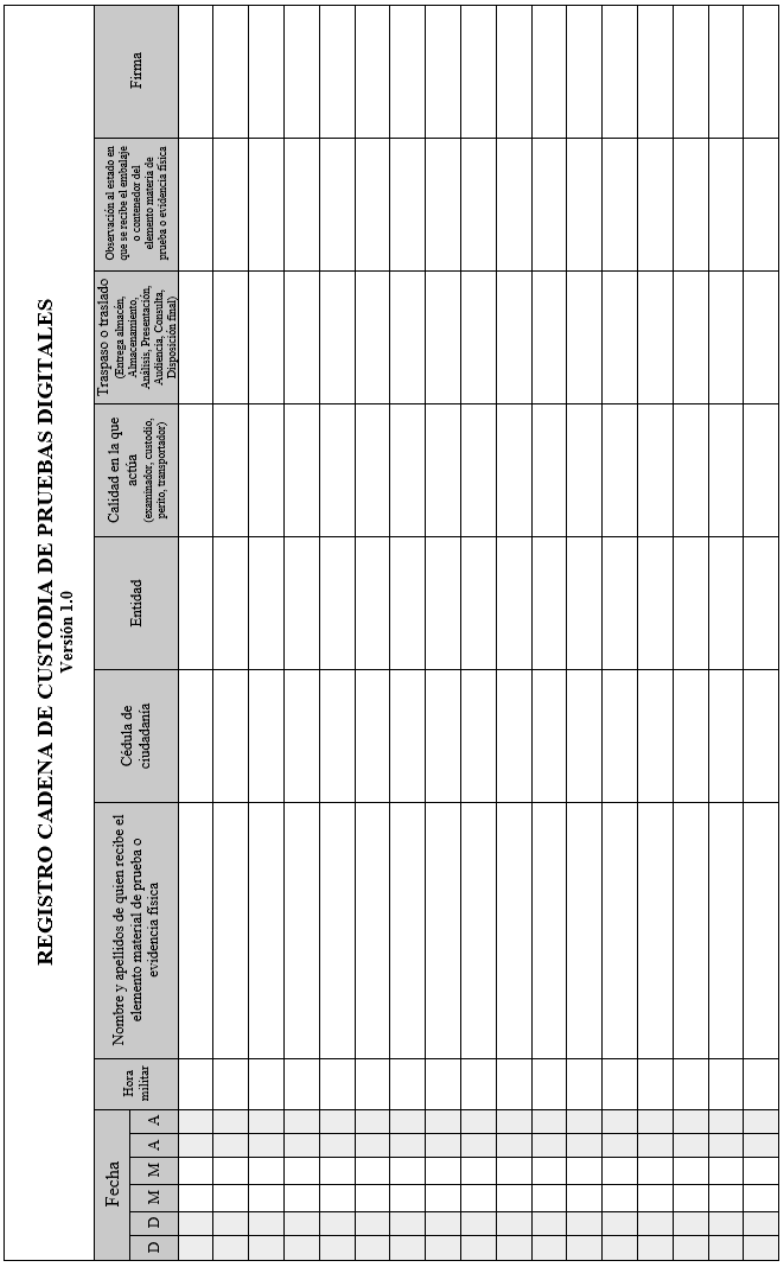
[92] Formato basado en el Manual de procedimientos para la cadena de custodia de la Fiscalía General de la Nación.

3. Registro de continuidad de los elementos materia de prueba o evidencia													
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 (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								

NOTA:

1) Nunca interrumpa el registro de cadena de custodia.
2) el registro de cadena de custodia siempre debe acompañar al elemento materia de prueba o evidencia física.
3) si esta hoja no alcanza para diligenciar los registros de continuidad de cadena de custodia, se puede utilizar tantas hojas adicionales sean necesario. De ser así, en la parte superior derecha de cada hoja se indicara el número único del caso y el de la hoja a que corresponde del total de hojas que conforman el registro de continuidad.

Anexo F: Registro de cadena de custodia digital



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, Archivo, Custodia, 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							

Anexo G: Registro responsables de la cadena de custodia

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
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

Anexo H: Descripción de herramientas

En este anexo de describen las características de las herramientas elegidas para la realización de esta guía. Las herramientas forenses se orientó de dos formas: La primera, es la selección de las herramientas individuales propiamente dicha. Estas se clasificaron en herramientas para la adquisición, para la examinación, el análisis y otras herramientas necesarias para el análisis forense en un dispositivo Android. La segunda forma, se eligió una suite de herramientas – una distribución GNU/Linux- especializada en el análisis forense en dispositivos móviles.

Esta orientación se hizo por la siguiente razón, la cual es no limitar las herramientas a una distribución específica. Sino que en caso de querer instalar las herramientas necesarias para el análisis forense móvil en una estación forense más completa se pueda hacer.

HERRAMIENTAS PARA LA ADQUISICIÓN

Comando dc3dd: Creada en el Centro del Ciber Crimen del Departamento de Defensa de los Estados Unidos. Es una modificación del comando dd, incluye características que facilitan la adquisición de imágenes forenses. Permite dividir la salida en distintos archivos con extensión secuencial (imagen.dd.000, imagen.dd.001, etc.) y calcula el *hash* para cada uno de los archivos comparando contra el disco de origen. Entre los algoritmos de *hash* que soporta son md5, sha1, sha256 o sha512. El *hash* se va calculando en paralelo a la realización de la imagen, una vez termina el proceso se calcula el *hash* de salida y se contrasta con el de origen.

AFLogical OSE: Es la edición *Open Source* de la herramienta AFLogical desarrollada por ViaForensic[93]. Esta aplicación proporciona un marco de trabajo básico para la extracción de datos de los dispositivos Android mediante proveedores de contenidos y luego guarda los datos en la tarjeta SD del dispositivo incluyendo: Contactos, registro de llamadas, SMS, MMS, partes MMS, información del dispositivo.

Esta aplicación fue liberada para el uso de personal de las fuerzas de la ley, sino para los aficionados Android y para gurús forenses. Para el personal de las fuerzas de la ley está disponible la versión completa de forma gratuita pero bajo registro, en el cual se debe indicar el país y el departamento al cual pertenecen.

HERRAMIENTAS PARA LA EXAMINACIÓN

Foremost. Es una aplicación de línea de comandos para el análisis forense, que permite recuperar archivos basados en sus encabezados, pies de página, y las estructuras de datos internas. Este proceso se conoce como 'tallado de datos' (*Data Carving*). El principal puede trabajar en archivos de imagen, tales como los generados por dd, Safeback, Encase,

[93] ViaForensics pasó a llamarse NowSecure

etc., o directamente en una unidad. Este breve artículo muestra cómo puede utilizar sobre todo para recuperar archivos borrados.

Photorec[94]**.** Es un software diseñado para recuperar archivos perdidos incluyendo videos, documentos y archivos de los discos duros y CD así como imágenes perdidas (por eso el nombre *PhotoRecovery*) de las memorias de las cámaras fotográficas, MP3 *players*, *PenDrives*, etc. PhotoRec ignora el sistema de archivos y hace una búsqueda profunda de los datos, funcionando incluso si su sistema de archivos está muy dañado o ha sido re-formateado. Para más seguridad, PhotoRec usa un acceso de sólo lectura para manejar el disco o la memoria de donde se recobrará los datos perdidos.

Testdisk[95]**.** Es un potente software de recuperación de datos gratuito. Fue diseñado principalmente para ayudar a recuperar particiones perdidas y/o hacer discos no booteables booteables nuevamente cuando estos síntomas son causados por software defectuoso: ciertos tipos de virus o error humano (como borrar accidentalmente una tabla de particiones).

Myrescue. Es un programa para rescatar a los datos aún legibles desde un disco duro dañado. El proyecto es similar en propósito a dd_rescue, sino que trata de salir rápidamente de las áreas dañadas de manejar primero la parte aún no dañados del disco y volver más tarde.

HERRAMIENTAS PARA EL ANÁLISIS

The Sleuth Kit (TSK)[96]**.** Es una biblioteca y colección de herramientas de línea de comandos que permite investigar imágenes de disco. Su funcionalidad principal es la de analizar los volumen de datos y del sistema de archivos. Cuenta con un marco de plug-in le permite incorporar módulos adicionales para analizar el contenido del archivo y construir sistemas automatizados.

Permite examinar un ordenador de forma no intrusiva debido a que las herramientas no se basan en el sistema operativo para procesar los sistemas de archivos, borrado y el contenido oculto se muestra. Se ejecuta en plataformas Windows y Unix (ha sido probado en Linux, Mac OS X, CYGWIN, Open & FreeBSD y Solaris).

TSK soporta los sistemas de archivos NTFS, FAT, UFS 1, UFS 2, EXT2FS, EXT3FS, Ext4, HFS, ISO 9660, y yaffs2 (incluso cuando el sistema operativo host no o tiene un orden endian diferente).

De las técnicas de búsqueda se puede decir que:

---

[94] Sitio web del proyecto http://www.cgsecurity.org/wiki/PhotoRec
[95] Sitio web del proyecto http://www.cgsecurity.org/wiki/TestDisk
[96] Sitio web del proyecto TSK www.sleuthkit.org/sleuthkit/

- Lista asigna y elimina nombres ASCII y archivos Unicode.
- Muestra los detalles y contenidos de todos los atributos NTFS (incluyendo todas las secuencias de datos alternativas).
- Muestra del sistema de archivos y metadatos detalles de la estructura.
- Crear líneas de tiempo de actividad de los archivos, que se puede importar en una hoja de cálculo para crear gráficos e informes.
- Hashes de archivos de búsqueda en una base de datos de hash, como el NIST NSRL, Hash Guardián, y bases de datos personalizados que se han creado con la herramienta 'md5sum'.
- Organizar los archivos en función de su tipo (por ejemplo, se separan todos los ejecutables, archivos JPEG y documentos). Páginas de miniaturas se pueden hacer de las imágenes gráficas para el análisis rápido.

Autopsy[97]**.** Es una plataforma de análisis forense digital y la interfaz gráfica de The Sleuth Kit y otras herramientas forenses digitales. Es utilizado por las fuerzas del orden, los militares y los examinadores corporativos para investigaciones.

Fue diseñada para intuitiva, de fácil instalación una plataforma de extremo a extremo con módulos que vienen con él fuera de la caja y otros que están disponibles a partir de terceros. Autopsy tiene las siguientes características:

- **Análisis de la línea de tiempo**: Muestra los eventos del sistema en una interfaz gráfica para ayudar a identificar la actividad.
- **Búsqueda por palabra**: extracción de texto y el índice de búsquedas en módulos que permiten encontrar los archivos que mencionan términos específicos y encontrar patrones de expresiones regulares.
- **Artefactos Web**: Extractos de actividad web de los navegadores comunes para ayudar a identificar la actividad del usuario.
- **Análisis del Registro**: Usa RegRipper para identificar los documentos usados recientemente y dispositivos USB.
- **Análisis de archivo LNK**: Identifica atajos y documentos accedidos
- **Análisis de correo electrónico**: Analiza MBOX mensajes de formato, tales como Thunderbird.
- **EXIF**: Extrae la ubicación geográfica y la información de la cámara de los archivos JPEG.
- **Selección tipo archivo**: Los archivos de grupo por su tipo de encontrar todas las imágenes o documentos.
- **Soporte de reproducción**: Ver vídeos e imágenes en la aplicación y no requiere de un visor externo.
- **Visor de miniaturas**: muestra en miniatura de las imágenes para ayudar al acceso rápido de las mismas.

[97] Sitio web de Autopsy http://www.sleuthkit.org/autopsy/index.php

- **Análisis del sistema de archivo robusto**: Soporte para sistemas de archivos comunes, incluyendo NTFS, FAT12 / FAT16 / FAT32 / ExFAT, HFS +, ISO9660 (CD-ROM), Ext2 / Ext3 / Ext4, yaffs2 y UFS de The Sleuth Kit.
- **Hash Set Filtrado**: Filtra archivos buenos conocidos usando NSRL y archivos malos conocida usando hashsets personalizados en HashKeeper, md5sum y formatos EnCase.
- **Etiquetas**: archivos de etiquetas con nombres de etiquetas arbitrarias, tales como "marcador" o "sospechoso", y añadir comentarios.
- **Extracción de string unicode**: Extrae las cadenas de espacio no asignado y tipos de archivos desconocidos en muchos idiomas (árabe, chino, japonés, etc.).
- Tipo de archivo de detección basada en firmas y detección de falta de coincidencia de extensión.
- Módulo de archivos interesante será archivos bandera y carpetas basándose en el nombre y la ruta.
- Soporte Android: extrae datos de SMS, registros de llamadas, contactos, Tango, palabras con los amigos, y más.

Autopsy analiza imágenes de disco, unidades locales o carpetas de archivos locales. Los formatos de disco pueden estar en formato Raw, dd o E01. El soporte para E01 es proporcionada por libewf. También cuenta con una estructura de información que permite la generación de informes.

Nota: Autopsy es una herramienta que se ejecuta en principio en la plataforma Windows, así que la versión 3.0 no está disponible para otras plataformas hasta el momento. Si se quiere ejecutar Autopsy en Linux y OS X debe usar la versión 2.0.

log2timeline[98] es una herramienta diseñada para extraer las marcas de tiempo de varios archivos encontrados en un sistema informático típico y agregarlos a la línea del tiempo.

OTRAS HERRAMIENTAS NECESARIAS PARA EL ANÁLISIS FORENSE

Comando ADB (*Android Debug Bridge*)[99]. Es una herramienta de línea se comandos versátil que le permite comunicarse con una instancia del emulador o dispositivo Android conectado. Es un programa cliente-servidor que incluye tres componentes:

1. Un cliente, que se ejecuta en el equipo de desarrollo. Se puede invocar un cliente desde un *shell* mediante la emisión de un comando adb. Otras herramientas de Android, como el *plugin* ADT y DDMS también crean clientes adb.
2. Un servidor, que se ejecuta como un proceso en segundo plano en el equipo de desarrollo. El servidor gestiona la comunicación entre el cliente y el demonio adb se ejecuta en un emulador o dispositivo.

[98] Sitio web del proyecto https://github.com/log2timeline/plaso
[99] Documentación sobre ADB en Android Developers http://developer.android.com/tools/help/adb.html

3. Un demonio, que se ejecuta como un proceso en segundo plano en cada emulador o dispositivo instancia.

SUITE DE HERRAMIENTAS

DEFT (*Digital Evidence & Forensic Toolkit*) [100]. Es una distribución que se compone de GNU/Linux y DART (Kit de herramientas de Respuesta Digital Avanzada). Esta suite está dedicada al análisis forense digital y actividades de inteligencia.

La versión 8.2 está basada en Ubuntu 12.10 y cuenta con DART es su versión 2. DART es una suite para la gestión y respuesta ante incidentes desde sistemas operativos Windows, que incluye un lanzador de herramientas para este sistema operativo.

Hay ciertas características a DEFT que minimizan el riesgo de alterar los datos que están siendo sometidos a análisis (Fratepietro, Rossetti, & Dal Checco, 2012). Algunas de estas características son:

1. En el arranque, se analiza el sistema no utiliza las particiones de intercambio en el sistema.
2. Durante el inicio del sistema no hay guiones automáticos de montaje.
3. No existen sistemas automatizados para cualquier actividad durante el análisis de las pruebas;
4. Todas las herramientas de almacenamiento y adquisición de tráfico de red en masa no alteran los datos que se adquirieron.

DEFT nos ofrece sus herramientas distribuidas entre las siguientes categorías (Guasch, 2013):

- ***Analysis*** - Herramientas de análisis de ficheros de diferentes tipos
- ***Antimalware*** - Búsqueda de *rootkits*, virus, *malware*, así como PDF con código malicioso.
- ***Data recovery*** - Software para recuperación de ficheros
- ***Hashing*** - Scripts que permiten la realización de cálculo de hashes de determinados procesos (SHA1, SHA256, MD5...)
- ***Imaging*** - Aplicaciones que podemos utilizar para realizar los clonados y adquisición de imágenes de discos duros u otras fuentes.
- ***Mobile Forensics*** - Análisis de Blackberry, Android, iPhone, así como información sobre las típicas bases de datos de dispositivos móviles en SQLite utilizadas por las aplicaciones.

[100] Sitio web del proyecto DEFT http://www.deftlinux.net/

- ***Network Forensics*** - Herramientas para procesamiento de información almacenada en capturas de red
- **OSINT** - Aplicaciones que facilitan la obtención de información asociada a usuarios y su actividad.
- ***Password recovery*** - Recuperación de contraseñas de BIOS, ficheros comprimidos, ofimáticos, fuerza bruta, etc.
- ***Reporting tools*** - Por último, dentro de esta sección encontraremos herramientas que nos facilitarán las tareas de generación de informes y obtención de evidencias que nos servirán para documentar el análisis forense. Captura de pantalla, recopilación de notas, registro de actividad del escritorio, etc.

En abril de 2015 se lanzó DEFT Zero[101], diseñada para ser la versión ligera de DEFT. Está centrado en la copia forense de evidencias digitales (es decir, los discos duros, dispositivos USB y unidades de red), optimizado para correr en solo 400 Mb, permitiendo que se cargue por completo en memoria RAM. Basado en Lubuntu 04.14.02 LTS y se desarrollará en paralelo con las futuras versiones completas de DEFT. Soporta versiones de 32 y 64 bits, con UEFI y arranque seguro.

[101] DEFT Zero http://www.deftlinux.net/2015/04/24/deft-zero-rc1-ready-for-download/

Anexo 2: Ponencias en congresos

Fundación Universitaria Juan de Castellanos

UNAD Universidad Nacional Abierta y a Distancia

Universidad Santo Tomás Primer Claustro Universitario de Colombia T U N J A Experiencia y Calidad

UB Universidad de Boyacá

Certifican que:

JOHAN SMITH RUEDA RUEDA

Participó como Ponente en el

CONGRESO INTERNACIONAL DE INVESTIGACIÓN EN INGENIERÍA DE SISTEMAS

REDIS Nodo Boyacá - Llanos

Con la ponencia

Análisis forense en dispositivos móviles con sistema operativo Android: Estado del arte

Realizado del 23 al 25 de abril de 2014 en Tunja, Boyacá, Colombia.

Mg. Ing. Jorge Gabriel Hoyos Pineda
Decano Facultad de Ingeniería de Sistemas
Universidad Santo Tomás, Seccional Tunja

Mg. Ing. Carmen Inés Báez Pérez
Directora del Programa de Ingeniería de Sistemas
Universidad de Boyacá

Mg. Ing. Iván Andrés Delgado González
Director del Programa de Ingeniería de Sistemas
Fundación Universitaria Juan de Castellanos

Mg. Ing. Leonardo Bernal Zamora
Tutor Especializado CEAD Tunja
Universidad Nacional Abierta y a Distancia

La República de Colombia
y en su nombre

013894

LA UNIVERSIDAD DE PAMPLONA

FACULTAD DE INGENIERÍAS Y ARQUITECTURA

Certifican que:

Johan Smith Rueda Rueda

C.C. 1091667778

PARTICIPÓ COMO PONENTE EN EL

CONGRESO INTERNACIONAL DE ELECTRÓNICA Y TECNOLOGÍAS DE AVANZADA

Con una intensidad de 20 horas

PhD. Aldo Pardo García
Director X CIETA

Pamplona, 26, 27 y 28 de Marzo de 2014

Mg. Jorge Luis Diaz R.
Director Dto EEST

Anexo 3: Articulo en revisión

Del estado del arte realizado en el presente proyecto se realizó un artículo, el cual se encuentra en revisión en la Revista INGE CUC, revista de la Facultad de Ingeniería de la Universidad de la Costa, indexada en la categoría C Publindex e indexada en Ulrich's y Latindex y está registrada con ISSN IMPRESO: 0122-6517 e ISSN ELECTRÓNICO: 2382-470.