PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE

INGENIERA EN SISTEMAS Y COMPUTACIÓN

"DESARROLLO DE UNA GUÍA DE PROCEDIMIENTOS EN BASE AL ESTUDIO DE MODELOS DE ANÁLISIS FORENSE DE DATOS, APLICADA EN ANÁLISIS A DISPOSITIVOS MÓVILES"

KATHERINE ALEXANDRA JAYA CÁCERES

QUITO – ECUADOR

2017

DEDICATORIA

A mis padres por ser el pilar fundamental en todo lo que soy, en toda mi educación, tanto académica, como de la vida, por su incondicional apoyo perfectamente mantenido a través del tiempo.

Todo este trabajo ha sido posible gracias a ellos.

RESUMEN

En la actualidad los dispositivos móviles son los más utilizados por las personas alrededor del mundo, lo que ha llevado a que los mismos pudieran estar relacionados con algún incidente de seguridad como: extorsión, fraude, robo o pérdida del dispositivo, razones que han hecho que la rama de la informática forense incremente su popularidad en los últimos años y haciendo necesario el uso de un proceso que se enfoque en este tipo de dispositivos.

En el marco antes descrito, se menciona la necesidad de contar con un proceso de análisis forense orientado a dispositivos móviles, lo que hace de la presente investigación su principal objetivo como es la propuesta de desarrollo de una guía de procedimientos de análisis forense en base al estudio de modelos existentes, dicha guía busca cubrir de la mejor manera el proceso completo llevado a cabo durante un análisis de este tipo, dentro del cual se encuentra desde el aseguramiento de la escena, pasando por la recolección y análisis de la evidencia, hasta finalizar en la entrega del informe correspondiente con los resultados obtenidos de la investigación.

Para cumplir con el objetivo propuesto se abordó todo tipo de términos considerados importantes para el desarrollo de la guía, tanto como definiciones, teorías, técnicas metodologías y herramientas de software relacionadas con la informática forense y los dispositivos móviles, concluyendo y dando como resultado una guía de procedimientos practica y fácil de usar.

ÍNDICE GENERAL

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

INTRODUCCIÓN

Hoy en día el campo de la informática forense se ha convertido en un área fundamental para la seguridad informática, debido al incrementado de la tecnología que ha ocasionado el desarrollo de diferentes tipos de delitos que involucran directamente esta área. En este sentido, a causa de varios avances en la tecnología se presentan una gran cantidad de vulnerabilidades y opciones para romper la ley, siendo los dispositivos móviles los más involucrados y atractivos para este tipo de actividades ilícitas.

Los dispositivos móviles actualmente considerados no solo como un lujo, sino más bien convertidos en una necesidad de las personas al estar involucrados en sus actividades cotidianas. Dispositivos móviles como los teléfonos celulares que aparte de cumplir con sus funciones básicas de comunicación, han incluido nuevas funcionalidades especiales como envió de correos electrónicos, navegar en internet, acceso a diferentes redes sociales y permitir portar datos personales de manera práctica, fácil y cómoda, siendo este el tipo de información vulnerable y susceptible a un ataque o robo de información. Por estas razones, surge la necesidad de tener un procedimiento que permita realizar un análisis correcto de las evidencias, que podrían involucrarse en una investigación de tipo legal donde los teléfonos celulares sean el dispositivo vulnerado.

Como resultado se propone, una guía de procedimientos de análisis forense de datos enfocado a los teléfonos celulares, dicha guía permitirá obtener un informe detallado de las actividades realizadas.

En el primer capítulo, se realiza una recopilación, definición y entendimiento de todos los términos implicados en el análisis forense y dispositivos móviles. Al inicio se define términos como evidencia digital, delitos informáticos, y se enumera una lista de ventajas y

desventajas de llevar a cabo un análisis forense digital. Como parte importante del capítulo se revisa las herramientas de software para el análisis forense de datos en diferentes áreas. Para terminar con una revisión de todo lo que se refiere a dispositivos móviles como es sistemas operativos, seguridad y vulnerabilidades.

El segundo capítulo muestra un estudio de los modelos de análisis forense, para este análisis se examina cuatro modelos considerados desde un punto de vista personal como los más conocidos, dichos modelos cuentan con procedimientos que ayudan en el desarrollo de la guía propuesta.

En el capítulo tres, previo al desarrollo de la guía de procedimientos propuesta se realiza un análisis comparativo y un estudio de las fases fundamentales de un análisis forense, todo esto ayudara para finalmente desarrollar una guía práctica y fácil de usar.

Finalmente, desarrollada la guía se procede a realizar la aplicación de la misma en un escenario de prueba simulado, dicha aplicación podría desde un punto de vista validar la propuesta y mostrar el uso e importancia de su aplicación en una investigación de informática forense.

OBJETIVOS

Objetivo General

Desarrollar una guía de procedimientos en base al estudio de modelos de análisis forense de datos, orientada al análisis de dispositivos móviles.

Objetivos Específicos

- Revisar conceptos fundamentales y procedimientos que son relevantes dentro de la informática forense.
- Examinar ventajas y desventajas de efectuar un análisis forense de datos, para de esta manera constatar los beneficios e inconvenientes que se presentan en dicho análisis.
- Analizar herramientas de análisis forense de datos que en la actualidad son utilizadas para descubrir incidentes en dispositivos móviles, redes, correos electrónicos y bases de datos.
- Estudiar los modelos de análisis forense de datos, para un entendimiento más amplio de los procedimientos que se requieren en una investigación forense de datos.
- Realizar un análisis comparativo de los modelos estudiados, lo cual servirá de base para el desarrollo de la guía de procedimientos propuesta.
- Realizar un análisis aplicando la guía desarrollada a dispositivos móviles.

CAPÍTULO I

FUNDAMENTACIÓN TEÓRICA

1.1. Análisis Forense

El análisis forense es un área que toma fuerza en los últimos años debido al incremento de incidentes de seguridad especialmente en el ámbito de la tecnología, es parte de la seguridad informática que busca examinar y reconstruir como se ha vulnerado un sistema. De esta forma es necesario para el desarrollo de nuestra guía el conocer y comprender términos referentes a la informática forense. Se inicia con una revisión de algunos conceptos envueltos en el área de la computación o informática forense, además de analizar las ventajas y desventajas de llevar a cabo una investigación de análisis forense.

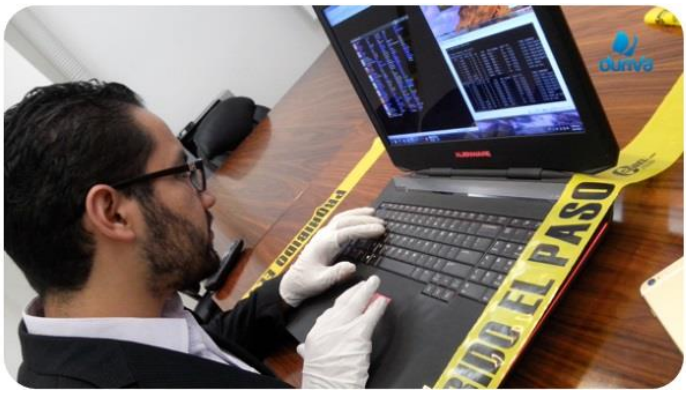


Ilustración 1 Análisis Forense

Fuente: https://peritajeinformatico.com.mx/wp-content/uploads/2015/10/computo-forense-delitos.jpg

1.1.1. Evidencia digital

En cuanto al término Evidencia Digital o también conocida como prueba electrónica, no es fácil encontrar una definición única y universal. Sin embargo, desde el punto de vista del ámbito probatorio se lo puede definir como cualquier tipo de información de modo digital que es almacenada o transmitida, además podrá ser manejada en un juicio de comprobarse que constituye una dependencia entre un delito y su autor.

Como señala Jeimy J. Cano, en su artículo "Introducción a la Informática Forense", donde detalla que la evidencia digital se considera un término amplio que permite describir "cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal". (Cano, 2011)

Es importante destacar, que para garantizar una validez probatoria de la evidencia digital, esta debe cumplir con ciertos requerimientos como es: ser admisible, autentica, completa, creíble, segura y confiable. De igual forma cabe mencionar que la evidencia digital se clasifica en tres categorías:

- ***Registros almacenados en equipos de tecnología informática.*** Son todos los documentos creados y almacenados por el usuario en el equipo de tecnología informática.
- ***Registros generados por equipos de tecnología informática.*** Son todos los documentos que son el resultado del uso del equipo de tecnología informática, el usuario no los puede alterar.

- ***Registros híbridos.*** Conformados por los registros almacenados y generados por equipos de tecnología informática**.**

1.1.2. Delitos informáticos

En lo que respecta a Delitos Informáticos para ofrecer un concepto adecuado, es recomendable realizar una revisión de los conceptos propuestos por algunos autores y organismos, los cuales han aportado desde distintas perspectivas y matices al concepto.

Para empezar, según el "Convenio de Ciberdelincuencia del Consejo de Europa", delitos informáticos define como: "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos". (Consejo de Europa, 2001)

Desde el punto de vista de Parker, define a los delitos informáticos como "todo acto intencional asociado de una manera u otra a los computadores; en los cuales la victima ha o habría podido sufrir una perdida; y cuyo autor ha o habría podido obtener un beneficio". (Romeo Casabona, 1988)

Hecha la observación anterior se puede definir que los Delitos Informáticos son actos ilegales y no éticos, que involucran todo en cuanto a lo referente a equipos de tecnología informática, redes de datos[1] y datos informáticos; en donde se encuentran implicados un autor y una víctima.

[1] Redes de datos: Conjunto de ordenadores conectados entre sí, con el objetivo de compartir recursos...

Ilustración 2 Delitos informáticos

Fuente: http://www.ohmygeek.net/wp-content/uploads/2012/10/Cibercrimen-Virus-650x256.jpg

1.1.3. Definición de análisis forense digital

Informática forense, computación forense o examinación forense, estas son algunas de las formas como también es conocido el análisis forense digital. El análisis forense en el campo de la informática es una ciencia moderna, que ha tomado fuerza en los últimos años debido al incremento elevado del uso de la tecnología en la vida diaria de las personas.

Este término se define como un proceso el cual aplica un conjunto de técnicas que permiten la extracción de información de equipos de tecnología informática, técnicas que permiten identificar, preservar, analizar y presentar información que se encuentre implicada en un proceso legal. Esta información puede ayudar en la reconstrucción tras un incidente de seguridad, de manera que se podrá saber lo sucedido. A continuación se describe de manera breve los propósitos del análisis forense digital:

- Identificar de manera clara las vulnerabilidades que permitieron que se lleve a cabo el incidente de seguridad.

- Identificar el origen y quien fue el perpetrador[2] del incidente de seguridad.
- Determinar qué acciones se realizaron en el incidente, además los métodos y herramientas utilizados en este.
- Establecer medidas que ayuden dentro de la seguridad, para evitar la repetición del incidente.

1.1.4. Ventajas y desventajas de efectuar un análisis forense

Llevar a cabo un proceso de análisis forense no es sencillo, teniendo en cuenta que se nos puede presentar ciertos inconvenientes en la obtención de la evidencia, lo cual es una desventaja al efectuar un análisis forense. De la misma manera que podemos encontrar desventajas dentro de la aplicación de un análisis forense en un proceso investigativo, así también tenemos ventajas. A continuación algunas de estas ventajas y desventajas.

1.1.4.1. Ventajas del análisis forense

- Eficiencia y rapidez en la capacidad de búsqueda dentro de una cantidad amplia de datos.
- Análisis de datos completo, rápido y en diferentes idiomas, sin que el tamaño de estos sea un obstáculo.

[2] Perpetrador: Persona que comete un delito o una falta grave.

- Permite el rastreo del autor del incidente, mediante la obtención de información esencial, que se manejó en el dispositivo antes de der eliminada.

1.1.4.2. Desventajas del análisis forense

- Los costos elevados, debido a los equipos que se requiere para realizar el análisis.
- Preocupación en el ámbito legal, por temas de privacidad de los propietarios de los equipos de tecnología.
- Corrupción de datos, es decir, posible alteración de la información al momento de extraerla.

1.2. Herramientas Tecnológicas para Análisis Forense

Con respecto a las herramientas tecnológicas para el análisis forense, en la actualidad se ha encontrado una gran variedad. Muchas de estas herramientas facilitan llevar a cabo la investigación de los delitos en los organismos de investigación y en los departamentos de policía.

Estas herramientas tecnológicas para el análisis forense se pueden clasificar en diferentes áreas de análisis; algunas de estas herramientas son pagadas, pero también cuentan con una versión gratuita no obstante esta tiene ciertas

limitaciones en sus funciones. A continuación se detalla las herramientas que son utilizadas en algunas de estas áreas de análisis.

1.2.1. Herramientas para el análisis de redes

En referencia a la clasificación anterior, una de las categorías en las que se enfoca el análisis forense es el campo de las redes de datos. La aplicación de análisis forense en las redes de datos tiene como objetivos principales:

- Analizar el tráfico cifrado de la red.
- Buscar actividades maliciosas dentro de la red.
- Identificar conexiones sospechosas que generan ataques de seguridad en la red.

Entre las herramientas que ayudan en la ejecución de un análisis forense en las redes de datos tenemos las siguientes:

- ***Wireshark.*** Software considerado como una de las mejores herramientas analizadoras de paquetes de red[3], permitiendo un nivel de análisis profundo y detallado de lo que sucede en la red. Utilizada en su mayoría para examinar problemas de seguridad y solución de estos dentro de la red. Entre las ventajas de utilizar esta herramienta tenemos que es multiplataforma[4], además es libre y de código abierto[5].

[3] Paquete de red: Conocido también como paquete de datos, es cada bloque en que se divide la…
[4] Multiplataforma: Es una característica que se asigna a programas que tienen el poder de funcionar…
[5] Código abierto: Termino usado para definir programas que son distribuidos libremente, y además su…

Ilustración 3 Logo WIRESHARK

Fuente: https://www.wireshark.org/assets/theme-2015/images/wireshark_logo.png

- ***NetworkMiner.*** Es un producto de software para llevar a cabo diferentes tareas de análisis forense de red en diferentes sistemas operativos de una forma sencilla, clara y rápida. Esta herramienta permite realizar capturas de paquetes, con el fin de detectar todo tipo de problemas que pueden presentar un riesgo para la seguridad. Una característica fuerte de la herramienta es su interfaz, la cual facilita las tareas de análisis, búsqueda y comprensión de los resultados obtenidos.

  NetworkMiner cuenta con dos versiones, NetworkMiner (edición gratuita) y NetworkMiner Professional.

- ***Xplico.*** Herramienta de software enfocada principalmente en el análisis forense de red, a través de la extracción de los paquetes capturados del tráfico de red[6]; permitiendo de esta manera realizar una evaluación de los datos que viajan por la red, y además los sistemas que se encuentran presentes. Xplico es una herramienta de software libre y código abierto.

[6] Tráfico de red: Es la cantidad de datos enviados y recibidos que viajan a través de la red.

1.2.2. Herramientas para el análisis de correos electrónicos

Los correos electrónicos se han convertido en un canal de comunicación electrónica principalmente en el ámbito empresarial y profesional, a través del cual se presentan cualquier tipo de negociación y cierre de transacciones. Como consecuencia del incremento de comunicación por este medio, en los últimos años se ha presentado un aumento en denuncias como insultos, amenazas y numerosas actividades criminales fomentadas a través de emails.

Es evidente entonces buscar herramientas que faciliten la investigación y detección de los delitos cometidos a través de este medio. Para ilustrar esto tenemos a continuación algunas herramientas utilizadas para el análisis forense en correos electrónicos.

- ***Aid4Mail.*** Conocida como una herramienta de software esencial dentro de la informática forense enfocada al análisis de correos electrónicos. Es una herramienta con una interfaz de fácil aprendizaje, compuesta por poderosas funciones de búsqueda que entregan información relevante y de manera rápida.

Ilustración 4 Logo Aid4Mail

Fuente: http://www.aid4mail.com/style/template/images/logo.png

Aid4Mail posee diferentes versiones pagadas, cuenta también con una versión trial gratuito con limitaciones en sus funcionalidades.

- ***eMailTrackerPro.*** Es una herramienta antiespam[7] principalmente utilizada para el rastreo de un correo electrónico, lo cual lo realiza a través del encabezado del mismo. Además de esto, también cuenta con un avanzado filtro, que permite el análisis de los mensajes y previene al correo de phishing[8], virus, spam[9], entre otros.

  eMailTrackerPro es una herramienta pagada, pero si se desea realizar una prueba antes de adquirirlo brinda un trial gratuito por 15 días.

- ***Paraben's Email Evidence Examination.*** Producto de software que permite hacer una lectura de archivos email, a través del análisis de los encabezados de los correos, el cuerpo y archivos adjuntos de estos; además se puede recuperar correos electrónicos eliminados. Es una herramienta fácil de utilizar, entrega un análisis detallado de los correos investigados.

Ilustración 5 Paraben's Email Evidence Examination

Fuente: https://www.paraben.com/images/products/e3-emx/emx.png

[7] Antiespam: Herramienta que se encarga de controlar el correo basura en los servidores de email o…
[8] Phishing: Método utilizado por delincuentes para obtener datos personales e información confidencial…
[9] Spam: Son los mensajes no solicitados, también conocido como correo basura o correo no deseado.

Paraben’s Email Evidence Examination es una herramienta comercial, también dispone de un demo con una duración de 15 días o un límite de 7 ejecuciones.

1.2.3. Herramientas para el análisis de base de datos

En la actualidad, las bases de datos se las considera como una ventaja competitiva dentro de las organizaciones debido a que facilitan el manejo de una gran cantidad de datos, permitiendo el ahorro del espacio físico y tiempo al momento de realizar consultas de la información contenida en estas. Esta concentración de datos, puede también ser utilizada para cometer delitos de diferente índole, por esta razón se ve la necesidad de la utilización de herramientas para análisis forense las cuales ayudan en esclarecimiento de hechos delictivos informáticos.

A continuación se menciona algunas de las herramientas que son utilizadas para aplicar la informática forense a bases de datos:

- ***Windows Forensic Tool Chest.*** Software comercial diseñado para brindar un enfoque estructurado y repetible respuesta forense en vivo, que ofrece consultar incidentes, auditoria o recolección de información relevante en un sistema Windows. Esta herramienta es muy útil para un profesional de la seguridad, ya que entre sus principales ventajas le permite buscar indicios de un incidente, de intrusos, o mal uso en la configuración del equipo, a través de una metodología efectiva de recogida de datos.

- ***SQLCMD.*** A diferencia de lo descrito anteriormente esto no es un software, es considerado como una utilidad mediante línea de comandos de Windows. Esta utilidad permite el manejo de la base de datos, pero su utilización se la debe considerar como uno de los últimos recursos cuando la base de datos principal o master se corrompe, es decir se presenta una falla en el sistema.

- ***MD5SUM.*** De la misma manera que el ejemplo descrito anteriormente esta también es una utilidad, que tuvo sus inicios en Unix[10] pero se ha ido adaptando para otras plataformas[11]. La utilidad de seguridad tiene como objetivo principal la verificación de la integridad de los datos, lo cual lo efectúa a través del cálculo de la huella digital de un archivo.

1.2.4. Herramientas para el análisis de teléfonos móviles

Los teléfonos móviles se han convertido en una herramienta esencial en la vida diaria de las personas debido a la facilidad de accesos a diferentes funciones y servicios que estos brindan. Muchas de estas funciones y servicios se han convertido en primordiales dentro de un teléfono móvil, un ejemplo de esto son la cámara para plasmar fotografías y videos, posicionamiento global, capacidad de ejecución de diferentes aplicaciones, además de acceso a internet el cual permite mantener una conexión y comunicación constante de todo lo que sucede alrededor del mundo.

[10] Unix: Es un sistema operativo multiusuario, multitarea, portable, con distintos intérpretes de comandos…
[11] Plataforma: Es un sistema que sirve como base para la ejecución de aplicaciones compatibles con el…

Frente a todo lo positivo en servicios y funciones que los teléfonos brindan también se han transformado en una herramienta para el delito, por esta razón se han desarrollado una gran variedad de herramientas para el análisis forense de estos dispositivos. A continuación se describe algunas de estas herramientas.

- ***MOBILedit! Forensic.*** Es un programa o herramienta de software que se utiliza para la recuperación de datos de un teléfono, además cuenta con una interfaz fácil de usar y entrega de informes detallados y difícil manipulación. La recuperación incluye datos como mensajes de texto, archivos, historial de llamadas, recordatorios, notas, contraseñas, entre otros.

Ilustración 6 MOBILedit! Forensic

Fuente: http://softwarecrackworks.com/wp-content/uploads/2013/09/MO-6.9.0.2...[12]

MOBILedit! Forensic compatible con los diferentes fabricantes y sistemas operativos; es un software comercial de pago que cuenta

[12] http://softwarecrackworks.com/wp-content/uploads/2013/09/MOBILedit-Forensic-6.9.0.2876-FULL-+-Serial.jpg

también con una versión gratis, dicha versión presenta ciertos limitantes en sus funciones.

- ***Oxygen Forensic Suite.*** Herramienta de software de gran utilidad para los expertos forenses, desarrollada para la extracción y análisis de información de teléfonos. Cuenta con una amplia variedad de funciones entre sus principales la recuperación de mensajes de texto tanto enviados, recibidos como eliminados, historial de contactos, calendarios, cache web de los navegadores, registro de eventos, entre otras.

  Oxygen Forensic Suite es un software compatible con 1500 modelos de dispositivos y las diferentes plataformas. Esta herramienta ofrece una versión gratis con ciertas restricciones y la versión pagada disponible para un mejor análisis en los dispositivos.

- ***Dr.Fone.*** Es un software de recuperación de datos que ofrece una diversidad de funciones las cuales consienten en la recuperación de fotos, mensajes de texto, contactos perdidos o eliminados, archivos de diferente tipo e información de algunas aplicaciones como Whatsapp.

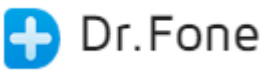


Ilustración 7 Logo Dr.Fone

Fuente: http://drfone.wondershare.net/es/

El programa recuperador de datos Dr.Fone tiene versiones para plataformas como iOS y Android, a pesar de que es un programa óptimo para la recuperación de datos una de sus desventajas es el pago por la licencia, para su prueba también dispone de una versión gratuita valida por 30 días.

- ***Paraben's E3: Universal.*** Es una herramienta de software que combina tres áreas principales en cuanto a análisis de evidencia digital, entre los cuales tenemos: unidad de disco duro, móviles (smartphone) e IoT[13], facilitando el proceso de análisis, haciéndolo más eficiente y eficaz. En cuanto a dispositivos móviles entre sus principales funcionalidades nos permite realizar adquisición de evidencia lógica y física.

Ilustración 8 Paraben E3: Universal

Fuente: https://www.paraben.com/images/products/e3-u/e3-big.png

El programa E3: Universal es comercial, pero también posee una versión trial con una duración de 15 días.

[13] IoT: Internet of Things

1.3. Dispositivos Móviles

En términos generales al referirnos a dispositivos móviles, lo primero que se piensa es en teléfonos móviles. No obstante, este término describe diversos dispositivos móviles que se encuentran en el mercado, como pueden ser: computadores portátiles, agendas digitales, cámaras, teléfonos, tabletas, etc. Cada uno de estos dispositivos se encuentra programados con características únicas, teniendo una memoria y un lenguaje que permite navegar a través de un entorno determinado.

Ilustración 9 Dispositivos móviles

Fuente: http://cio.com.mx/wp-content/uploads/2015/01/dispositivos-moviles.jpg

De este modo, en este documento nos vamos a enfocar en el análisis de un dispositivo móvil en específico, el cual es reconocido como teléfono celular debido a su amplia penetración en el mercado y gran volumen de dispositivos vendidos a nivel mundial y por tanto el más utilizado. De esta manera se presenta una definición general en cuanto a dispositivos móviles, que ayuda a obtener una definición que engloba las características de nuestro dispositivo en específico.

Así mismo, a nivel técnico se describirá algunos de los sistemas operativos utilizados por estos dispositivos móviles.

Por otro lado, se toma en cuenta ciertos temas que serán un gran aporte para el desarrollo del documento como son la seguridad y las vulnerabilidades que se pueden presentar en estos dispositivos móviles.

1.3.1. Definición de dispositivos móviles

Dispositivo móvil se define como un aparato de tamaño pequeño, con características específicas de procesamiento, almacenamiento de información limitada y con capacidad de conectarse a internet. Diseñados para realizar una función en específico, y son transportados por los usuarios de manera fácil.

Después de las consideraciones anteriores y basándose en la significado anterior, se presenta una definición en cuanto a uno de los dispositivos conocido como teléfono celular.

Se conoce como teléfonos móviles a dispositivos inalámbricos que facilitan la comunicación desde casi cualquier lugar, dado que tiene un acceso a la red de telefonía celular. Cabe agregar que a pesar de que su objetivo principal es la comunicación, en los últimos años se ha ido desarrollando y se ha incorporado nuevas funcionalidades como cámara, reproductor de audio, acceso a internet y GPS[14].

[14] GPS: Global Positioning System

1.3.2. Sistemas operativos

Un sistema operativo es considerado un programa dedicado al control del dispositivo, en otras palabras la interacción entre los programas o aplicaciones instaladas por el usuario y el hardware del dispositivo como es la pantalla, la cámara, el teclado, etc. Inicialmente estos programas fueron desarrollados para la interacción en los PCs, pero con el paso del tiempo los teléfonos móviles han ido avanzando hasta convertirse en un computador de bolsillo en un medio donde el cliente busca la opción de realizar varios tipos de tareas en un solo dispositivo.

Es importante destacar que en el mundo se presenta una gama amplia en cuanto a sistemas operativos de teléfonos móviles, muchos de sus fabricantes compiten por lograr un software que incorpore todas las necesidades del usuario y llegar a ser líderes en el mercado. En este sentido los principales y más utilizados sistemas operativos en teléfonos móviles tenemos iOS y Android. Cada uno de estos sistemas cuentan con características específicas las cuales los hacen líderes en el mercado y un reto para sus competidores.

Tal como se ha mencionado anteriormente existe una variedad de sistemas operativos diferentes; por ejemplo entre los más populares Android, iOS, Windows Phone y Blackberry, y menos conocidos como Symbian, Firefox OS, Ubuntu Touch, Tizen, WebOS. Si bien en el fondo cumplen las mismas funciones, cada uno posee importantes diferencias.

1.3.2.1. Android

Android es un sistema operativo inicialmente creado para ser usado en teléfonos móviles, que con el paso del tiempo evolucionaria y se convertiría en un sistema operativo de televisores, relojes inteligentes y automóviles. Este sistema operativo ha sido creado por Android INC., compañía que respaldo y más tarde adquirió Google, programa basado en Linux como un sistema operativo multiplataforma, libre y sobre todo gratuito.

Ilustración 10 Logo Android

Fuente: http://www.brandemia.org/wp-content/uploads/2012/10/logo_principal.jpg

El sistema ha ido progresando en busca de ampliar su mercado, cada vez mejorando e incorporando nuevas características y funcionalidades a su sistema. Posee una forma muy característica de nombrar a las versiones del sistema operativo, lo que quiere decir que utiliza términos de postres y dulces en inglés; desde su primera versión Apple Pie (Tarta de manzana) se ha tenido grandes avances hasta llegar a sus últimas versiones Marshmallow (Malvavisco) y Nougat (Turrón), que lo ha colocado como el sistema operativo de teléfonos más vendido en el mundo.

Android ha desarrollado características que lo han llevado a ser un fuerte competidor con otro de los sistemas que lidera el campo de telefonía móvil como es iOS de Apple. Algunas de estas características son:

- Siendo un sistema operativo de uso libre este puede ser implementado y adaptado en dispositivos móviles de cualquier compañía que lo requiera.
- Disponibilidad de descarga de una gran diversidad de aplicaciones ya sean pagadas o gratuitas como juegos o herramientas que ayudan en la optimización del sistema.
- Android un sistema fácilmente adaptable que forma parte de un gran número de dispositivos de todo tipo desde teléfonos móviles, tabletas, televisores y últimamente se está implementando en automóviles.

1.3.2.2. iOS

El sistema operativo iOS diseñado y desarrollado por Apple una de las empresas de tecnología más grandes del mundo. Inicialmente desarrolla el sistema para uno de sus productos más conocido el iPhone, para luego ser usado en otros dispositivos como el iPad, iPod Touch y Apple TV. iOS proviene de MacOS el cual está basado en Darwin BSD[15], por esta razón es un sistema operativo tipo Unix.

[15] Darwin BSD: Es el sistema operativo base para la construcción del sistema operativo de Apple, con…

Ilustración 11 Logo iOS

Fuente: http://www.greenhat.mx/wp-content/uploads/2016/08/apple-logo.png

Apple desde el 2007 que hizo su anuncio del iPhone, en aquel entonces se lo conocía con el nombre de iPhone OS el cual poseía aplicaciones básicas preinstaladas sin la posibilidad de instalar aplicaciones de terceros. Apple frente a un mercado competitivo muy amplio se ha visto obligado a mejorar su sistema e implementar funciones que brinden al usuario una de las experiencias más cómodas del mercado y que también le permita obtener una ventaja frente a su competencia.

iOS está ubicado en los primeros lugares de los mejores sistemas operativos en telefonía, algunos de los puntos fuertes que lo han colocado aquí son:

- La respuesta inmediata a posibles vulnerabilidades o errores después del lanzamiento de una nueva versión del sistema.
- Conexión e interacción con los dispositivos dentro del hogar sean estos productos Apple como iPad, Apple TV, Mac, Apple Watch, funcionando como uno solo.
- Sistema diseñado para aprovechar al máximo el hardware, logrando así una mejor fluidez en el funcionamiento del dispositivo y una mejor gestión de la energía.

- Mayor seguridad a través del seguimiento de aplicaciones y evitar el acceso de estas a la información del usuario sin su consentimiento.

1.3.2.3. Windows Phone

Windows Phone presentado como un sistema operativo para móviles diseñado y desarrollado por Microsoft, el cual surge como sucesor de Windows Mobile. Sistema operativo cuya visión es enfocarse en un mercado de consumo y dejando de lado el mercado empresarial. Teniendo presente un mercado muy competitivo dentro del ámbito tecnológico en telefonía móvil han logrado una posición importante en el medio debido a su alianza con Nokia.

Ilustración 12 Logo Windows Phone

Fuente: https://i2.wp.com/windtux.com/wp-content/uploads/2016/01/wind...[16]

Microsoft diseña un sistema con una interfaz que tenga un comportamiento estable y un mejor control de las plataformas de hardware que lo ejecutan,

[16] https://i2.wp.com/windtux.com/wp-content/uploads/2016/01/windows_phone_logo.jpg?ssl=1

dicha interfaz incluye ciertos servicios propios de la empresa como Skype, OneDrive y Xbox Live; todo esto encaminado a conseguir una única experiencia e integración del teléfono, la web y la PC, a través de servicios y aplicaciones. Entre algunas de las características de Windows Phone importantes tenemos:

- La interfaz es bastante intuitiva convirtiéndose en una de las más sencillas de usar para el usuario.
- Permitir una conexión a cualquier subdirección que se encuentre en los servidores[17] de Windows Live, de esta forma tener acceso a la cuenta de correo, contactos y algunos servicios de Microsoft.
- Interacción con los dispositivos del ecosistema de Microsoft, es decir con una PC, smartphone o Xbox manteniendo de esta manera la información importante sincronizada.

La empresa anuncio en enero del 2015 que dará de baja a su sistema Windows Phone para centrarse en un nuevo sistema más versátil y disponible para cualquier tipo de plataformas conocido como Windows 10 Mobile.

[17] Servidor: Es una unidad informática que realiza tareas y brinda diversos servicios a otros ordenadores…

1.3.2.4. BlackBerry OS

BlackBerry OS diseñado y desarrollado por la compañía RIM[18], es un sistema operativo de código cerrado diseñado utilizado en los dispositivos móviles de la empresa. En 1999 su aparición con los primeros handheld[19], dispositivos móviles que además de sus funciones habituales incorporaron también acceso a correo electrónico, una navegación web y una sincronización con ciertos programas como Lotus Note y Microsoft Exchange.

Ilustración 13 Logo BlackBerry OS

Fuente: http://vignette2.wikia.nocookie.net/telefono/images/5/5c/BlackB...[20]

La empresa BlackBerry se encuentra enfocada en un mercado corporativo y no corporativo. Gracias a que cuenta con un nivel alto en cuanto a seguridad del que otros sistemas operativos carecen, es un sistema operativo altamente usado por empresarios y profesionales. De la misma manera un usuario particular también puede gozar de estos beneficios de seguridad al contratar el paquete de datos proporcionado por el sistema BlackBerry.

[18] RIM: Research In Motion
[19] Handheld: Se define como un dispositivo o computador portátil, de tamaño reducido que pueda…
[20] http://vignette2.wikia.nocookie.net/telefono/images/5/5c/BlackBerry_OS_logo.png/revision/latest/scale-to-width-down/640?cb=20131231031627&path-prefix=es

BlackBerry OS cuenta con características propias que lo han acercado a su competencia, un ejemplo de esto es:

- Incluye un gestor de correo electrónico y agenda lo han hecho llamativo en el ámbito profesional, usuarios que buscan seguridad y protección de sus datos privados.
- Cuenta con una interfaz más fluida, en efecto ha incorporado un teclado inteligente y táctil más limpio.

1.3.3. Seguridad en dispositivos móviles

En la actualidad el incremento de usuarios de teléfonos móviles ha ido en aumento siendo este un objeto imprescindible que forma parte de nuestra vida diaria. Como consecuencia de esto los ataques a este tipo de dispositivos son más frecuentes convirtiéndose en una de las razones para que la seguridad en estos sea una prioridad en los últimos años.

Ilustración 14 Seguridad de dispositivos móviles

Fuente: http://www.tecnolatinos.com/wp-content/uploads/2015/03/segurid...[21]

[21] http://www.tecnolatinos.com/wp-content/uploads/2015/03/seguridad-dispositivos-moviles.png

Teniendo en cuenta que cada dispositivo está diseñado para que el usuario pueda manejar una cantidad importante de información ya sea personal o empresarial como contraseñas, fotografías, videos, contactos y en algunas ocasiones hasta datos de tarjetas de crédito. De la misma forma la conexión a internet de los dispositivos móviles nos brinda una facilidad de intercambio de información y la realización de distintas transacciones en línea.

El avance de la tecnología en los dispositivos móviles brinda una mejor comunicación, sin embargo nos exponen al usuario a peligros y ataques de personas que buscan extraer información sin ningún consentimiento o aprobación; de la misma manera dispositivos que pueden ser utilizados para el cometimiento de delitos como la extorsión.

Dadas las condiciones que anteceden se debería tener en cuenta ciertos aspectos que pueden ayudar a mantener un adecuado control de seguridad en nuestros dispositivos móviles, por ejemplo:

- Mantener un control adecuado de los datos que son compartidos
- Contralar la forma de acceso al dispositivo
- Crear copias de seguridad son una opción para respaldar los datos más importantes
- Instalar aplicaciones que sean seguras
- Las actualizaciones son importantes

1.3.4. Tipos de vulnerabilidad

En los últimos años el crecimiento de la telefonía móvil ha traído consigo un efecto negativo, como es los ataques informáticos a estos dispositivos; los ataques y vulnerabilidades aumentan a la misma velocidad como crece la telefonía, presentándose de diferentes formas. Siendo este un problema en el que cada empresa de telefonía busca mejorar y brindar la mayor seguridad a sus usuarios.

Muchas de estas vulnerabilidades son comunes entre las diferentes plataformas, a continuación algunas son:

- Dispositivos móviles que no cuentan con contraseñas que verifique el acceso del usuario a estos.
- Redes de acceso inalámbrico públicas que no tienen una encriptación adecuada de los datos que se transmiten a través de estas.
- Dispositivos móviles con algún tipo de malware el cual es resultado de descargar aplicaciones que contiene software malicioso.
- Falta de software de seguridad en los dispositivos móviles, por desconocimiento del usuario sobre la instalación de dicho software.
- Mantener abiertos canales de comunicación como el Bluetooth lo que permite que el dispositivo sea visto por otros usuarios.

CAPÍTULO II

MODELOS DE ANÁLISIS FORENSE

Los modelos de análisis forense han sido desarrollados principalmente para formar parte de una ayuda a los investigadores de esta área. Desde sus inicios cada modelo busca mejorar el proceso por el cual pasa la información, es decir desde la extracción de datos hasta llegar a su etapa final que es la entrega del informe pericial. De esta manera se ha determinado ciertas características que debería poseer un modelo óptimo de análisis forense, como son:

1. Identificar los objetivos potenciales de la investigación sin dejar de lado el ámbito de la aplicación de la ley, en otras palabras considerar el sistema completo.
2. Considerar los principios básicos para el manejo de la evidencia, preservando esta ante posibles fallos en el sistema.
3. Considerar no solo las acciones de los eventos sino también los efectos que los origina e identificar cada una de las partes involucradas dentro de un análisis forense.
4. Considerar el contexto, es decir el entorno y el método que ayudan en la interpretación y comprensión de un evento.
5. Presentar un informe claro y conciso de los eventos, que sea de fácil entendimiento y análisis para los investigadores forenses.

Es importante destacar que en la búsqueda de mejorar el proceso y teniendo en cuenta las características antes mencionadas se ha desarrollado numerosos modelos. Esto nos lleva a realizar una revisión de algunos de los más destacados modelos de análisis, para

alcanzar un entendimiento eficaz de los procedimientos y estándares dentro del área de la informática forense.

2.1. Modelo - Digital Forensic Research Workshops (DFRWS)

En el año 2001, Nueva York fue sede para llevar a cabo el primer Digital Forensic Research Workshops o también conocido por sus siglas en ingles DFRWS. Tuvo como objetivo principal reunir un extenso número de comunidades académicas, investigativas y profesionales para compartir sus conocimientos en el ámbito de la informática forense. Teniendo como audiencia a profesionales, civiles y militares se crea un documento de consenso que contenía la esencia de la informática forense en ese momento, proponiendo un proceso de investigación dividido en siete fases secuenciales.

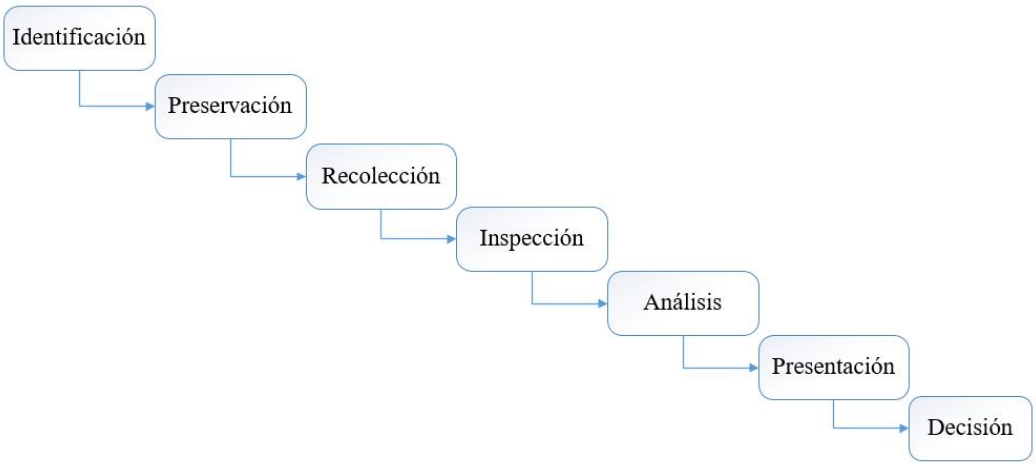


Ilustración 15 Diagrama Modelo Digital Forensic Research Workshops (DFRWS)

Fuente: Traducción de (Sachowski, 2016)

1. **Identificación.** En esta fase se efectúa un reconocimiento y se determina el tipo de incidente, a través de una detección tanto de posibles perfiles como de indicadores del mismo.

2. **Preservación.** Esta fase comienza con un proceso de gestión de casos e incluye la cadena de custodia[22]. Cabe mencionar que se considera una fase crítica para garantizar que la información obtenida esté libre de contaminación.

3. **Recolección.** En esta fase los datos o información pertinentes son recogidos, a través de herramientas de software autorizadas las cuales utilizan diversas técnicas y métodos de recuperación.

4. **Inspección.** Es considerada una de las fases críticas de la investigación donde la información es examinada profundamente, mediante técnicas de validación y filtrado que permiten obtener evidencia clave para la reconstrucción del incidente o escena del crimen.

5. **Análisis.** Siendo esta otra de las fases críticas donde se reconstruye la escena del crimen, mediante las pruebas obtenidas de la recopilación y reunión de información esencial dentro de la investigación.

6. **Presentación.** En esta fase la explicación de las respectivas conclusiones y el resumen de la información contenida en la investigación es documentada, para ser presentada como testimonio o informe del incidente.

[22] Cadena de custodia: El mecanismo que garantiza la autenticidad de los elementos de prueba…

7. **Decisión.** En la fase final se toma una decisión sobre el incidente y se presenta una sentencia, basados en los testimonios e informes presentados ante un tribunal de justicia.

VENTAJAS

- Modelo enfocado en que todas sus fases cubran lo necesario dentro de una investigación forense.
- Prioriza de manera efectiva la conservación de la integridad de la información y mantener la cadena de custodia.
- Recurre a técnicas que permitan la extracción de información oculta.
- Modelo cuya metodología se actualiza de manera constante.

DESVENTAJAS

- Las fases en el modelo son muy generales de manera que no define un procedimiento concreto para la ejecución de las actividades.
- Es un modelo ligeramente rígido, de tal manera que es efectivo cuando el investigador conoce con exactitud los pasos de las actividades de investigación.

2.2. Modelo - Abstract Digital Forensics Model (ADFM)

El Modelo Forense Digital Abstracto o en ingles conocido como Abstract Digital Forensics Model (ADFM), es un modelo propuesto en el 2002 por Mark Reith, Clint Carr y Gregg Gunsch. Basado en la recopilación de fases comunes de los modelos existentes principalmente del modelo DFRWS, por esta razón se lo considera una evolución o mejora del modelo antes mencionado. Añadiendo tres fases nuevas en el proceso, teniendo como resultado nueve fases.

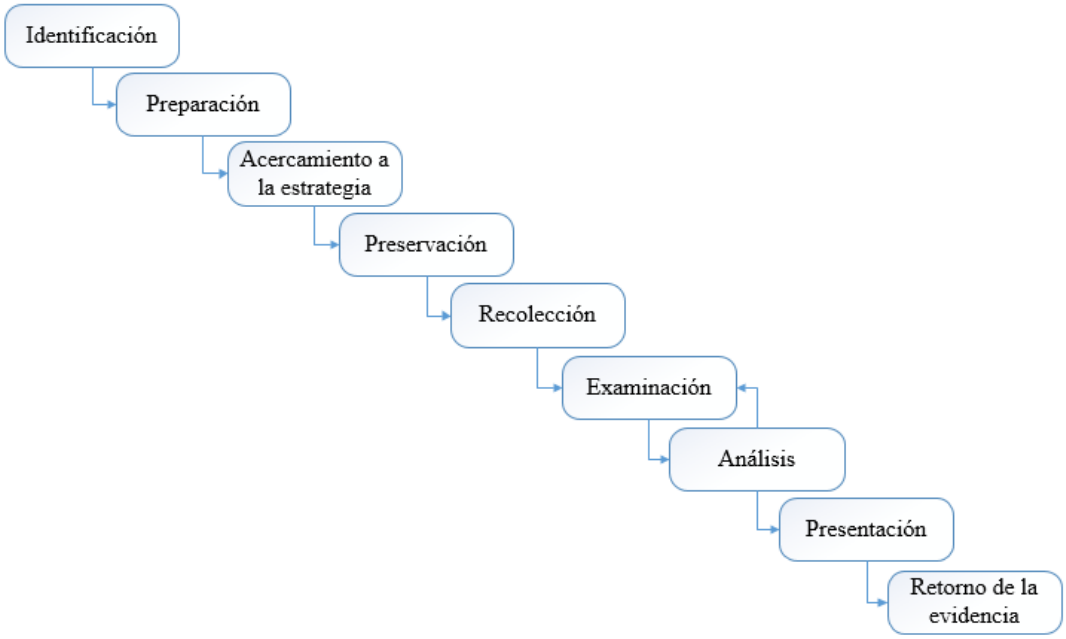


Ilustración 16 Diagrama Modelo Abstract Digital Forensics Model (ADFM)

Fuente: Traducción de (Sachowski, 2016)

1. **Identificación.** Esta fase tiene un impacto importante en las etapas siguientes de la investigación siendo su objetivo principal el reconocimiento del incidente y sus indicadores, además la determinación del tipo de incidente.

2. **Preparación.** Fase encargada de preparar las herramientas, técnicas y órdenes de búsqueda, además de administrar las autorizaciones de seguimiento y apoyo a la gestión.

3. **Acercamiento a la estrategia.** La fase consiste en una maximización de la recolección de las pruebas o evidencia sin ninguna alteración, esto a través de la generación de un plan que permita además minimizar el impacto a la víctima.

4. **Preservación.** Fase en la cual la evidencia es lo primordial y tiene como objetivo aislar, asegurar y preservar las pruebas de manera que no sean alteradas o perdidas por cualquier persona implicada dentro de la investigación.

5. **Recolección.** En esta fase es necesario obtener una grabación y registro al momento de llegar a la escena, es decir antes de realizar cualquier manipulación de la evidencia. Realizar una duplicación de la evidencia utilizando procedimientos estandarizados y reconocidos mundialmente.

6. **Examinación.** En esta fase se realiza una búsqueda profunda y sistemática de evidencia esencial en la investigación, además es necesario realizar una documentación detallada de la misma.

7. **Análisis.** La fase consiste en realizar un examen exhaustivo de la evidencia, de este modo se podrá reconstruir datos que ayuden a obtener conclusiones sobre la investigación en base a la evidencia analizada.
8. **Presentación.** En esta fase se presentan las conclusiones obtenidas en base a la evidencia previamente analizada y un resumen de todo lo investigado.
9. **Retorno de la evidencia.** Fase encargada de garantizar que toda la evidencia física y digital que pueda ser entregada, sea devuelta a su dueño o propietario apropiado en óptimas condiciones.

VENTAJAS

- Considerado un modelo bastante completo en sus procedimientos tanto antes como después de la investigación.
- Incluye tres fases nuevas que ayudan a mejorar el proceso de investigación, estas son la preparación, acercamiento a la estrategia y retorno de la evidencia.

DESVENTAJAS

- No es aplicable para muchos de los casos de investigación, a pesar de que incluye en su procedimiento características importantes de modelos anteriores.

2.3. Modelo - Cyber Forensics Field Triage Process Model (CFFTPM)

Cyber Forensics Field Triage Process Model (CFFTPM), modelo propuesto en el 2006 por Rogers cuyo enfoque es identificar, examinar e interpretar la evidencia digital al instante en el que la investigación empieza, en otras palabras el modelo presenta un enfoque de análisis en sitio/campo, omitiendo la necesidad de que la evidencia encontrada en la escena del crimen sea llevada a un laboratorio forense para un análisis profundo. Este modelo busca recoger la máxima cantidad de evidencia en un tiempo relativamente corto, debido a que algunas de las investigaciones requieren ser resueltas de forma inmediata. Para la recolección de esta evidencia se toma en cuenta ciertos detalles que puede presentar cada caso a investigar, cabe mencionar que las características que presentan cada uno de los casos son diferentes, en efecto una investigación de pornografía infantil es diferente a una investigación sobre delitos financieros o tráfico de drogas. De la misma forma el modelo posee ciertas guías para la investigación y manipulación de la evidencia como son:

1. Buscar y encontrar evidencia esencial utilizable de manera inmediata
2. Identificar a víctimas en situación de riesgo potencial
3. Guía de la investigación en curso
4. Identificar posibles involucrados
5. Evaluar el peligro que produce el delincuente a la sociedad

Además de lo antes mencionado se debe tener en cuenta que es fundamental proteger la integridad de la evidencia y de pruebas que requieran un examen o análisis más profundo.

Las fases del modelo CFFTPM se derivan de dos modelos anteriores como son el modelo Integrated Digital Investigation Process (IDIP) desarrollado en el 2002 por Carrier y Spafford y el modelo Digital Crimen Scene Analysis (DCSA) desarrollado por Rogers en el 2006. El modelo está formado por 6 fases primarias, las cuales se subdivide en 6 subclases. Se considera que el proceso utilizado por este modelo cumple los principios forenses ampliamente practicados.

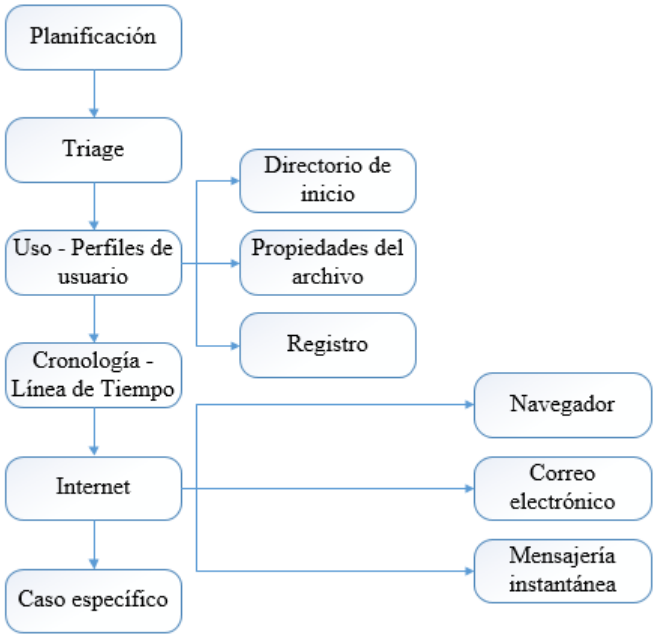


Ilustración 17 Diagrama Modelo Cyber Forensics Field Triage Process Model (CFFTPM)

Fuente: Traducción de (Sachowski, 2016)

1. **Planificación.** Siendo esta la primera fase del modelo se debe considerar realizar una planificación adecuada lo que permitirá asegurar una mejora en el porcentaje de éxito de la investigación. Es importante que el investigador principal se encargue de elaborar una matriz que permita cuantificar puntos importantes dentro de una escena del crimen, permitiéndole registrar y definir lo que conoce y ayudarle a determinar lo que se sabe y no se conoce. Dicha matriz debe contener los hechos, el sospechoso, la evidencia digital y además un punto que permita calificar la experiencia al resto del equipo que participa en la investigación.

2. **Triage.** Fase fundamental dentro del proceso al igual que la planificación adecuada son consideradas como la base sobre las cuales se construyes las demás fases del modelo CFTTPM. Esta fase se relaciona de forma directa con la escena del crimen teniendo en cuenta tanto la evidencia física como digital, y el sospechoso. Toda la evidencia obtenida dentro de la investigación debe ser debidamente clasificada en orden de prioridad o importancia, es decir, evidencia que sea más importante o más volátil deberá ser procesada en primera instancia.

3. **Uso / perfiles de usuario.** Después de haber obtenido evidencia importante a través del examen y análisis de la información en las fases previas. La fase de uso / perfil de usuario permite hacer una reconstrucción del caso y crear la relación entre la evidencia examinada y un posible sospechoso identificable e idóneo, de tal manera que si la evidencia es presentada al sospechoso este pueda sentirse obligado a admitir su culpabilidad. Para llevar a cabo una correcta evaluación del perfil del usuario es necesario analizar las horas y fechas asociadas con

aparatos digitales, esto permite identificar el tiempo de acceso del que disponía el sospechoso a la evidencia.

- ***Directorio de inicio.*** El Directorio de Inicio o Home Directory es accesible solamente a través de la cuenta del usuario asociada. Dicho directorio permite el almacenamiento dentro de subcarpetas información relacionada a diferentes aplicaciones instaladas en el dispositivo; carpetas como "Mis documentos", "Escritorio" y "Favoritos" pueden contener archivos incriminatorios, al ser examinados nos ayudan a comprobar si el sospechoso era el único con acceso a esta información o existe más personas con acceso que podrían estar involucradas.

- ***Propiedades del archivo.*** Puede llegar a ser de gran eficacia y utilidad en cierto punto de la investigación comprobar las propiedades y seguridad de un archivo. A pesar de tener gran importancia dentro de la investigación se pueden presentan inconvenientes al momento de establecer y leer los permisos, debido a que estos no están disponibles en FAT y en Windows se encuentran desactivados de manera predeterminada, de tal manera que limita establecer la culpabilidad de los involucrados.

- ***Registro.*** El examinador o investigador debe tener claro lo que está buscando y exactamente a qué lugar debe acceder para encontrarlo, bajo estas condiciones el examinar el registro sería un fuerte indicador para ayudar a identificar al posible sospechoso, caso contrario el análisis del registro puede llegar a ser una pérdida de tiempo valioso.

El examinar el perfil de usuario se considera una parte indispensable para la investigación aunque puede llegar a ser la parte más costosa de esta en cuanto a tiempo utilizado.

4. **Cronología / línea de tiempo.** En una investigación la evidencia se encuentra determinada por un valor temporal, en este caso conocido como tiempo MAC, teniendo sus siglas un significado especifico como son:

    - ***Modification.*** Es el tiempo/fecha de alteración o cambio de un archivo.
    - ***Access time.*** Es el tiempo/fecha de acceso o vista de un archivo.
    - ***Created time.*** Es el tiempo/fecha de creación de un archivo.

    Este tiempo MAC puede contener ciertas inconsistencias y funcionar de diferente manera en sistemas operativos utilizados por teléfonos móviles.

    El investigador debe cuantificar diferentes parámetros una vez que haya obtenido el acceso a los archivos y sus tiempos MAC. Entre las cuantificaciones que es requerido realizar tenemos:

    - Examinar los tiempos de uso del dispositivo por parte del sospechoso y demás usuarios.
    - Analizar e identificar archivos y aplicaciones instaladas en el dispositivo que han sido utilizadas en tiempos determinados, estas podrían contener información significativa para la investigación.
    - Finalmente, identificar y reconocer información almacenada reciente, incluyendo también accesos a los que tienen ciertos

servicios como internet como puede ser las cookies del navegador o la caché.

5. **Internet.** Consiste en un análisis de los dispositivos relacionados con actividades de internet que pueden revelar información esencial para la investigación. Entre las actividades más importantes a examinar está el correo electrónico, navegación web y mensajería instantánea.

   Para disminuir la pérdida de tiempo y los costos que este análisis conlleva, se debe tener en cuenta que tipo de investigación se está realizando, cuales son las posibles aplicaciones involucradas y además si el dispositivo pertenece al sospechoso o a la víctima. Entre algunos de los elementos principales que el investigador debería evaluar tenemos:

   - ***Navegador.*** El análisis de los sitios visitados en la web es importante y se debe tomar en cuenta que la mayoría de los navegadores utiliza métodos para almacenar las "cookies" como archivos permitiendo identificar el sitio que ha visitado a través del nombre de la cookie, esto debido a que la mayoría de veces el nombre coincide con el URL del sitio. La fecha y hora también son necesarias para relacionar las cookies y determinar cuándo se accedió al sitio.

   - ***Correo electrónico.*** Un análisis de correo electrónico puede llegar a ser costoso en tiempo, dado que indagar el correo electrónico de un sospechoso puede tomar varias horas. Sin embargo de encontrarse contenido incriminatorio puede tener un peso importante en la investigación.

- ***Mensajería instantánea.*** Muchas de las aplicaciones de mensajería instantánea almacenan las conversaciones de los usuarios en sus servidores dificultando el trabajo del investigador de recuperar esta información como también datos de posibles contactos. Por otro lado en la actualidad se ha incluido en algunas aplicaciones una posibilidad de activar la capacidad de almacenar y grabar online las conversaciones y contactos, con herramientas tecnológicas se podría recuperar y analizar esta información.

6. **Caso específico.** Todo investigador debe ser capaz y tener la habilidad de ajustar los detalles de cada investigación a un tipo de caso en específico, tomando en cuenta las circunstancias que se presentan. Además teniendo en cuenta que, el principal enemigo de un investigador es el tiempo y esto implica un costo importante, debe aprender a priorizar sus objetivos de búsqueda. La planificación y la capacidad para obtener información fiable antes del ingreso a la escena del crimen, juegan un papel importante para que el investigador distribuya su tiempo de búsqueda de la mejor manera posible.

VENTAJAS

- Modelo que propone una investigación en sitio/campo, reduciendo positivamente la pérdida de tiempo y los obstáculos logísticos.
- No descarta la posibilidad de que la evidencia sea enviada a los laboratorios para un análisis exhaustivo.
- Enfoque importante en las aclaraciones del caso investigado.

DESVENTAJAS

- Presenta una orientación hacia un modelo forense digital computarizado, restringiendo su utilidad al no tomar en cuenta la evidencia física.
- Los escenarios y casos de investigación que utilizan el modelo son muy pocos y limitados.

2.4. Modelo - Generic Computer Forensic Investigation Model (GCFIM)

Generic Computer Forensic Investigation Model es el resultado de una investigación realizada por Yunus Yusoff y sus colegas, en dicha investigación se revisó y se analizó los modelos de análisis forense desde el año de 1985 hasta el 2011. Tras la investigación se obtuvo 5 fases genéricas comunes presentes entre los modelos previos, siendo estas principales en los modelos anteriores dan origen al proceso del nuevo modelo GCFIM.

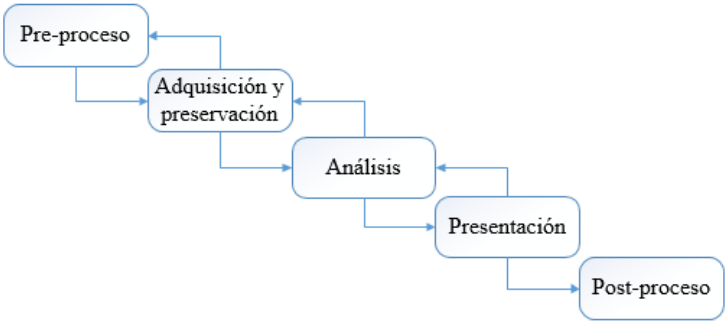


Ilustración 18 Diagrama Modelo Generic Computer Forensic Investigation Model (GCFIM)

Fuente: Traducción de (Sachowski, 2016)

1. **Pre-proceso.** En esta fase lo básico o primordial es una preparación adecuada que sea de ayuda para las fases siguientes. Verificar que las herramientas de análisis tengan un funcionamiento apropiado y que el grupo de investigación se encuentre preparado eficientemente, además de encargarse de gestionar procesos necesarios para la ejecución de la investigación como accesos, privilegios y aprobaciones.

2. **Adquisición y preservación.** Fase encargada de una parte importante dentro del proceso de la investigación abarca subprocesos como son la identificación y recolección de la evidencia en la escena del crimen, además de proporcionar transporte y almacenamiento adecuados con las debidas seguridades para evitar la alteración de los datos que serán preparaos para el análisis en la siguiente fase.

3. **Análisis.** En esta fase se examina de forma minuciosa el contenido y el contexto de la evidencia recuperada en la fase anterior, además se encarga de clasificar la información colocando de manera prioritaria lo que se considera importante para la investigación y desechando información que no se relacione con el caso.

4. **Presentación.** Básicamente en esta fase se prepara toda la documentación de la investigación, es decir todo lo referente a posibles hipótesis, resultados del análisis de la fase previa y todo tipo de reportes del caso.

5. **Post-proceso.** Esta fase engloba todo lo referente a la presentación de informes ante un tribunal judicial para determinar sentencias sobre los involucrados en la investigación. Del mismo modo la evidencia que deba ser entregada a su propietario sea devuelta en buenas condiciones.

VENTAJAS

- Es un modelo flexible y adaptable a una gama amplia de escenarios y casos de investigación.
- Gracias a que hace hincapié en elementos esenciales dentro de un proceso de investigación forense, es apto para el campo en constante evolución como lo es la tecnología.

DESVENTAJAS

- Por la simplicidad del procedimiento y ya que sus fases son muy generales es más conocido como un marco de referencia y no como un modelo de investigación.

CAPÍTULO III

DESARROLLO DE LA GUÍA

Hoy en día los dispositivos móviles conocidos como teléfonos celulares almacenan y manejan una cantidad importante de información. Muchos de los usuarios que utilizan este tipo de dispositivo guarda información tanto personal o empresarial.

Los atentados y vulnerabilidades que presentan estos dispositivos se incrementan diariamente lo que provoca que empresas que comercializan teléfonos celulares busquen la forma de garantizar a sus clientes la protección del dispositivo. La evidencia digital contenida en teléfonos celulares es altamente frágil y vulnerable. De ahí que es necesario determinar un procedimiento estándar que nos permita realizar un análisis profundo y confiable de la evidencia implicada en un posible incidente de tipo judicial. Para el diseño de la guía que ayude con lo mencionado anteriormente se requiere realizar una comparación de los modelos forenses establecidos en la actualidad y detallados en el capítulo anterior, además de un estudio de las fases básicas para este tipo de análisis, hechas las observaciones anteriores lograremos como resultado una guía de procedimientos práctica y fácil de seguir.

3.1. Análisis Comparativo de los Modelos Estudiados

La informática forense nos ofrece en la actualidad una amplia variedad de modelos de investigación. En este caso se efectúa una comparación de los modelos de análisis considerados y detallados en el capítulo anterior;

comparación que ayude en el desarrollo de la guía de procedimientos propuesta. Cada modelo consta de características, ventajas y desventajas a través de las cuales podemos plantear un análisis comparativo.

Características	**Modelos de Análisis Forense**			
	DFRWS[23]	***ADFM***[24]	***CFFTPM***[25]	***GCFIM***[26]
Contiene las etapas o fases generales para un análisis forense informático	X	X	X	X
Implementación en cualquier tipo de escenarios y casos de investigación	X	X		X
Maneja una planificación estratégica		X	X	X
Administra una cantidad amplia de información	X	X		X
Sellado o cierre de la escena del crimen			X	
Identifica evidencia esencial de la escena del crimen	X	X	X	X
Responde a técnicas de protección y ocultamiento de información	X	X	X	X
Extracción de evidencia importante	X	X	X	
Conservación de la evidencia	X	X		X
Especifica procedimientos para la ejecución de actividades		X	X	

Tabla 1 Comparación entre modelos de análisis forense

Fuente: (Jaya, 2017)

[23] DFRWS: Digital Forensic Research Workshops.
[24] ADFM: Abstract Digital Forensics Model.
[25] CFFTPM: Cyber Forensics Field Triage Process Model.
[26] GCFIM: Generic Computer Forensic Investigation Model.

Como resultado del análisis comparativo de estos cuatro modelos de análisis forense, cuyo enfoque es realizar una comparación de características entre cada modelo. Se observa que para este caso el ADFM es el modelo más óptimo para una investigación de informática forense, con características que pueden servir para la guía propuesta en este capítulo, por las siguientes razones:

- Considerado como uno de los pocos modelos que facilitan al investigador en la ejecución de actividades, debido a que este modelo especifica de una manera más estructurada los procedimientos para realizar las actividades de investigación.
- Engloba la mayoría de las características de los modelos con los que es comparado; características importantes como es identificación, extracción y conservación de evidencia significativa.

Por otra parte, los modelos DFRWS y CFFTPM carecen de ciertas características, convirtiéndose estas en desventajas importantes para llevar a cabo su aplicación. Como es en el modelo DFRWS la característica que impide que el modelo sea considerado óptimo es la falta de especificación del proceso para la ejecución de actividades dificultando el trabajo del investigador. Asimismo el CFFTPM es un modelo con pocos y limitados escenarios siendo esto una desventaja al no ser aplicable a cualquier tipo de investigación.

Finalmente, el modelo GCFIM en este caso es considerado como el menos óptimo por la privación de algunas características, además de ser considerado como un marco de referencia y no como un modelo por la sencillez que presenta su proceso.

3.2. Estudio de las Fases Fundamentales de un Análisis Forense

A lo largo del tiempo se ha desarrollado un gran número de modelos con diferentes fases con el propósito de ayudar al investigador en el proceso de análisis forense informático. Cada modelo tiene ventajas y desventajas, además de tener etapas similares entre ellos, también poseen características que los hacen únicos y diferentes. En este sentido, se detalla a continuación cuatro de las fases o etapas esenciales que deben ser consideradas para mantener la idoneidad del proceso en un modelo de análisis forense informático.

3.2.1. Fase de identificación de la escena

Considerada la primera fase y base para las siguientes fases de una investigación de análisis forense involucra dos puntos importantes como es la identificación, búsqueda y recopilación de evidencias. Es esencial que el investigador genere un documento donde se registre datos informativos del incidente y todo tipo de información que también sea considerada importante para dar inicio al proceso de análisis investigativo. Una vez iniciado el proceso de investigación e identificado ciertos indicios del incidente comienza otra parte importante como es la búsqueda y recopilación de evidencia. La evidencia obtenida debe ser debidamente clasificada para facilitar la manipulación de esta en las siguientes fases.

3.2.2. Fase de preservación de la evidencia

En esta fase es importante llevar una documentación de los métodos para el almacenamiento y etiquetado de la evidencia, en otras palabras como se realiza la preservación de la evidencia; todo esto en base a que posteriormente puede ser requerida dicha información. La evidencia debe estar intacta para su conservación, por lo cual es necesario realizar copias de todos los dispositivos que contienen datos como evidencia, y además mantener la cadena de custodia.

3.2.3. Fase de análisis de la evidencia

Para dar inicio con la fase de análisis es necesario contar con las autorizaciones correspondientes, además de las herramientas y técnicas adecuadas para la manipulación de la evidencia. Esta fase tiene como objetivo la reconstrucción de los hechos del incidente desde el inicio del ataque hasta el momento de su hallazgo, se dará por concluida cuando se descubra como se produjo el ataque, quien lo ejecuto y bajo qué condiciones se llevó a cabo el incidente, además de conocer con qué objetivo y que consecuencias tuvo.

3.2.4. Fase de documentación del incidente.

Es importante documentar cada una de las actividades que se realizan durante el proceso de investigación desde que se descubre el incidente hasta terminar con la etapa de análisis de la evidencia. Los documentos generados en las fases

previas permitirán desarrollar un informe final donde se expondrán los resultados de la investigación y los hechos más destacados de lo sucedido.

3.3. Desarrollo de la Guía

Una vez realizada la comparación de los modelos de análisis forense y el estudio de las fases fundamentales de la investigación forense, temas contenidos en el presente capítulo. En esta sección del documento se presenta la propuesta de una guía de procedimientos para el análisis forense de datos, basada en el estudio y entendimiento de los conceptos y modelos de análisis expuestos en los capítulos anteriores.

3.3.1. Alcance de la guía

Los modelos de análisis propuestos son diversos, en el capítulo II se revisa algunos de los modelos considerados desde un punto de vista personal como más significativos. Cada modelo maneja características diferentes, y a pesar de que algunos son debidamente estructurados muchos de estos trabajan bien con un tipo de investigación particular. Hecha la revisión de los modelos de investigación forense no se logró determinar un modelo que se enfoque específicamente en el análisis forense a teléfonos celulares, dispositivos móviles a los cuales se dirige el proceso de nuestra guía propuesta.

Para el desarrollo de la guía de procedimientos propuesta se considera aquellos conocimientos y métodos estándar existentes en el área de la investigación

forense física y digital. El presente modelo busca mejorar algunas de las deficiencias de los modelos previamente analizados, e incluir procedimientos que permitan obtener una guía práctica y fácil de usar con un enfoque hacia los teléfonos celulares.

3.3.2. Fases de la guía propuesta y sus procedimientos

En esta sección del documento, se detallan cada una de las fases y procedimientos que contiene la guía de procedimientos de análisis forense de datos, cuyo enfoque es el análisis de teléfonos celulares.

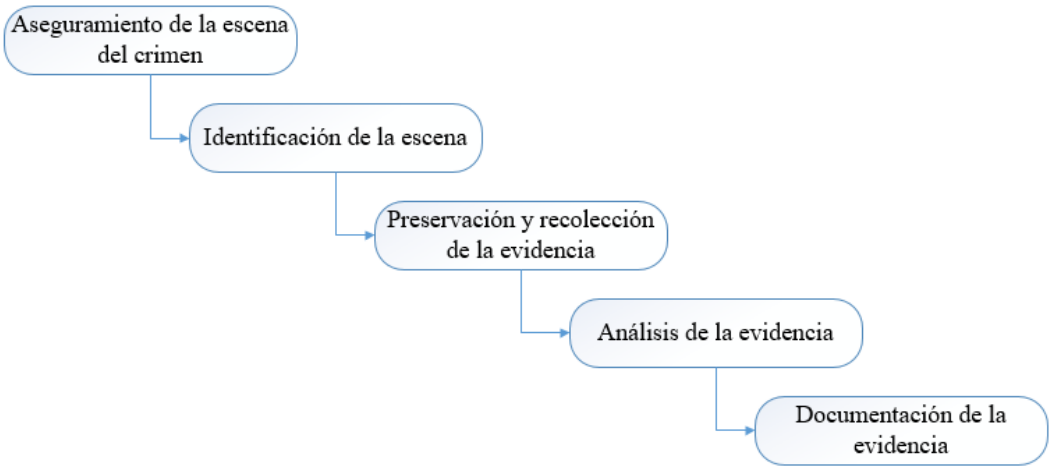


Ilustración 19 Diagrama Modelo de la Guía de Análisis Forense de Datos Propuesto

Fuente: (Jaya, 2017)

3.3.2.1. Fase de aseguramiento de la escena del crimen

Ilustración 20 Aseguramiento de la escena del crimen

Fuente: http://www.andresvelazquez.com/wp-content/uploads/2013/05/Escena-del-Crimen.jpg

La fase de aseguramiento de la escena tiene como objetivo la protección y preservación del lugar de los hechos, conseguir que cada persona designada a participar en el caso de investigación actúe de manera coordinada y estructurada, de forma que permita evitar el ingreso de personas no autorizadas a la escena del crimen que podría alterar las evidencias. Esta fase refleja dos partes importantes para lograr un adecuado aseguramiento del lugar de los hechos o escena del crimen.

Ilustración 21 Diagrama Fase de aseguramiento de la escena del crimen

Fuente: (Jaya, 2017)

1. *Medidas de protección.*

En esta parte se contempla todo lo relacionado con generar o crear actividades y medidas que protejan y preserven el lugar de los hechos a investigar. Para mantener una apropiada protección y aseguramiento de la escena, evitar la contaminación, perdida, alteración y sustracción de evidencia es necesario tener en cuenta lo siguiente:

- Conservar el lugar de los hechos en su forma original.
- Establecer un perímetro dentro del cual se supone existe la mayor cantidad de evidencia.
- Proteger la escena de manera constante durante el allanamiento del lugar y mientras los investigadores realizan su labor, dicha protección finaliza cuando las autoridades correspondientes dispongan lo contrario.

- Delimitar áreas de libre acceso que no afecten a la evidencia, ni alteren el lugar de los hechos o escena del crimen.

2. *Designación de responsables.*

La designación de responsables antes de iniciar con el proceso de análisis forense es importante y juega un papel esencial dentro de la investigación. Al definir o designar responsables aseguramos mantener una organización adecuada durante el proceso de análisis y otorgar responsabilidades a cada miembro del personal involucrado en el caso.

- *Peritos.* Es el personal encargado de ejecutar y monitorear de manera adecuada las actividades relacionadas a la recolección, aseguramiento y preservación de la evidencia, manejando y manteniendo la cadena de custodia.

- *Técnicos forenses.* Conformado por personal autorizado para confiscar el dispositivo, encargarse de la identificación, recolección y análisis de la evidencia, manteniendo y preservando la integridad de la información. Los técnicos forenses llevan un registro de las actividades realizadas que sirve de base para la entregar de informes donde se detallan los resultados de la investigación.

- *Custodios de la evidencia.* Personal encargado de manejar la protección de la evidencia recolectada, manteniendo una cadena de custodia justa; además se encargan de que los datos o información obtenidos en la escena estén correctamente identificados.

- *Investigadores forenses.* Es el personal encargado de diseñar y mantener una planificación apropiada. Las actividades de las fases o etapas del análisis forense deben contar con un orden y un período definido de ejecución.

- *Examinadores forenses.* Conformado por personal altamente preparado que se encarga de extraer y recuperar la mayor cantidad de evidencia del dispositivo, a través de herramientas de software, ingeniería reversa, entre otros métodos. No se recomienda la presencia de examinadores forenses y técnicos forenses al mismo tiempo.

- *Analistas forenses.* Personal encargado de interpretar, evaluar y dar significancia incriminatoria en el caso investigado, a los resultados obtenidos por los examinadores forenses.

Finalmente, para mantener un manejo y control adecuado de la designación de responsables, se propone el llenado del siguiente formulario:

Fecha de designación de roles						
Código del caso						
Descripción del caso						
Rol designado	**Nombre**	**Apellido**	**Fecha de designación de rol**	**Cédula**	**Teléfono**	**Firma**

Tabla 2 Formulario de Designación de responsables

Fuente: (Jaya, 2017)

3.3.2.2. Fase de identificación de la escena

La fase de identificación de la escena del crimen tiene como objetivo recopilar información básica y general de dónde y cómo se encuentra el lugar de los hechos, información que ayude a tomar decisiones sobre las acciones necesarias a seguir para el análisis forense. Así mismo, esta fase pretende obtener información clave de los involucrados, tanto del dueño del dispositivo como de posibles sospechosos presentes en la escena del crimen. Para una adecuada identificación de la escena se debe tener en cuenta los siguientes puntos:

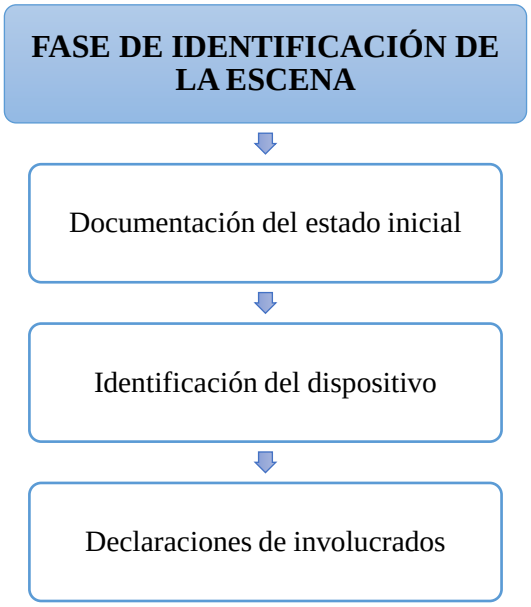


Ilustración 22 Diagrama Fase de identificación de la escena

Fuente: (Jaya, 2017)

1. *Documentación del estado inicial.*

El levantamiento de información inicial para el análisis forense es de gran importancia para el proceso investigativo, de esta manera se podrá recolectar información esencial que podría ser necesaria en un juicio legal. La documentación del estado inicial debe contener información de:

- *Escena del crimen.* Para registrar el estado de la escena del crimen es necesario la toma de fotografías y videos de cómo se encuentra el lugar de los hechos antes de iniciar con cualquier tipo de actividad, sea esta de recolección o análisis de evidencia. Así como también se requiere el registro en un documento donde conste todo tipo de información que describa el delito. Dicho documento debe incluir la siguiente información:

    1. Fecha del incidente
    2. Código del caso
    3. Detalles del incidente
    4. Dirección del incidente
    5. Nombre y apellidos del investigador responsable
    6. Fotografías y videos de la escena

- *Dispositivos.* Se debe tomar registro a través de fotografías o videos que muestren el estado inicial del dispositivo a ser incautado, que en este caso son los teléfonos celulares. Sin embargo, es necesario también documentar todos los dispositivos (computadores, portátiles, etc.) que se encuentren en el lugar de los hechos y sean considerados como evidencia.

Para resumir los dos puntos mencionados anteriormente, que deberían constar en la documentación del estado inicial, tenemos el siguiente formulario:

Fecha del incidente:				
Código del caso:				
Detalles del incidente:				
Dirección del incidente:				
Nombre y apellidos del investigador responsable:				
FOTOGRAFÍAS				
Escena del crimen				
Dispositivo				
Existencia de VIDEOS	**SI**		**NO**	

Tabla 3 Formulario de Documentación del estado inicial

Fuente: (Jaya, 2017)

2. *Declaraciones de involucrados.*

Ilustración 23 Declaraciones de involucrados

Fuente: http://www.actitudfem.com/media/files/styles/large/public/images/2015/03/notaentrevista.jpg?itok=tD9LUWpP

Las declaraciones de los involucrados, juega un papel importante dentro de la investigación, nos ayudan a obtener información sobre los sucesos del incidente e indicios que permitan comenzar con el proceso de análisis de la información. Dentro de los involucrados se debe tener en cuenta las declaraciones de:

- *Dueño del dispositivo.* De estar presente en el lugar de los hecho es la persona que proporcionará información importante sobre el dispositivo, sea esto sucesos extraños en el dispositivo, conexiones, perdida de información, entre otros.

- *Testigos/Sospechosos.* Personas que se encuentren en la escena y podrían brindar cualquier tipo de información sobre los hechos del incidente, así como dar pistas de lo sucedido.

3. *Identificación del dispositivo.*

Cada uno de los dispositivos involucrados en el caso debe ser debidamente identificado. Para su identificación es necesario tener en cuenta tanto el estado y sus características como la documentación existente del dispositivo; a continuación se describe lo que se requiere en cada uno de estos puntos para una identificación apropiada.

- *Estado y características del dispositivo.* Para llevar un mejor control del dispositivo incautado se debe justificar y documentar el adecuadamente, por tanto, el registro debe constar de:

  1. Estado del Dispositivo: Encendido/Apagado
  2. Protegido por clave: Sí o No
  3. Tipo de protección
  4. Marca del teléfono
  5. Modelo del teléfono
  6. Número de teléfono
  7. Operadora del servicio
  8. Número Serial (IMEI[27])

[27] IMEI: International Mobile Station Equipment Identity, identificador único de los dispositivos móviles…

- *Documentación extra del dispositivo.* Documentar las características y el estado del dispositivo son importantes, pero además se debe registrar la existencia de otros elementos que tengan relación con este, para facilitar el acceso y la extracción de evidencia del mismo. Entre estos elementos tenemos:

    1. Manuales de usuario
    2. Memorias extraíbles
    3. Cargadores
    4. Facturas de adquisición
    5. Códigos de acceso

Para la identificación del dispositivo, contamos con el siguiente formulario que incluye lo puntos mencionados previamente.

ESTADO Y CARACTERÍSTICAS DEL DISPOSITIVO				
Estado del dispositivo	**Encendido**		**Apagado**	
Protegido por clave	**SÍ**		**NO**	
En caso de tener protección (Tipo)				
Contraseña				
PIN				
Patrón				
Huella digital				
Reconocimiento facial				
Otro tipo de protección (Especifique)				
Características				
Marca del teléfono				
Modelo del teléfono				
Número de teléfono				
Operadora del servicio				
Numero serial IMEI				
DOCUMENTACIÓN EXTRA DEL DISPOSITIVO				
	SÍ		**NO**	
Manuales de usuario				
Memorias extraíbles				
Cargadores				
Facturas de adquisición				
Códigos de acceso				

Tabla 4 Formulario de Identificación del dispositivo

Fuente: (Jaya, 2017)

3.3.2.3. Fase de preservación y recolección de la evidencia

La fase de preservación y recolección de la evidencia consiste en la recaudación de datos y cualquier tipo de información considerada como evidencia. Podemos encontrar tanto evidencia física como evidencia lógica relacionada con nuestro dispositivo móvil en investigación, se debe mantener un cuidado pertinente en la preservación de la integridad de los datos, para ello la evidencia será manipulada de manera correcta, y manejará una cadena de custodia adecuada.

En esta fase también se debe seleccionar una herramienta de software apropiada para la recolección de evidencia, que será clasificada de acuerdo a un orden de prioridad para su posterior análisis. A continuación, se describe las partes a considerar dentro de la presente fase como es:

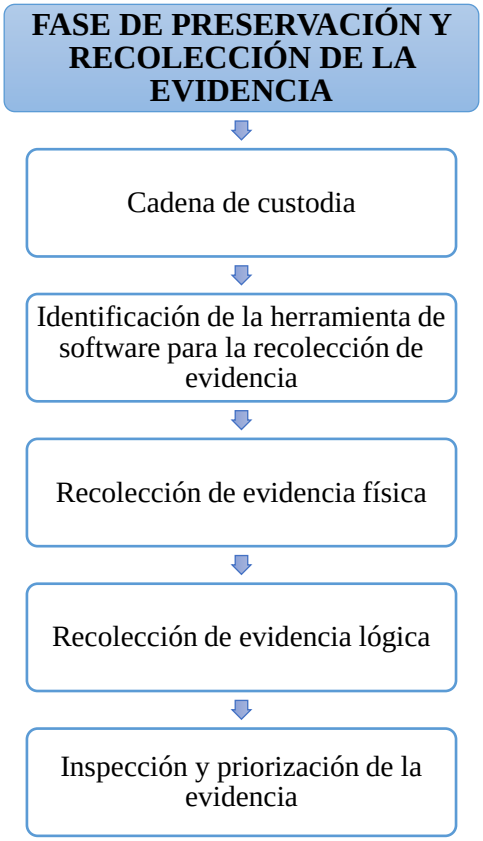


Ilustración 24 Diagrama Fase de preservación y recolección de la evidencia

Fuente: (Jaya, 2017)

4. *Cadena de custodia.*

La cadena de custodia se define como: “el mecanismo que garantiza la autenticidad de los elementos de prueba recolectados y examinados,

esto es, que las pruebas correspondan al caso investigado, sin que dé lugar a confusión, adulteración, ni sustracción alguna." (Fuertes Rocañin, Cabrera Forneiro, & Fuertes Iglesias, 2007)

La aplicación de la cadena de custodia es de suma importancia y da un valor altamente significativo a la investigación, de manera que garantice que el procedimiento empleado ha sido exitoso y que la evidencia recolectada no sufra ninguna alteración para poder ser utilizada y presentada ante un tribunal.

En cuanto a la evidencia dentro de la escena y el tratamiento de esta en el proceso investigativo, es importante tener en cuenta lo siguiente:

- Los elementos de prueba encontrados dentro del lugar de los hechos debe tener un trato adecuado en la recolección de los mismos.
- Los elementos de prueba deben tener un mantenimiento adecuado para su conservación, mientras dure el proceso investigativo.
- La entrega de los elementos de prueba deben ser debidamente fiscalizada.

Finalmente, para mantener la adecuada cadena de custodia se llenara el siguiente formulario:

FORMULARIO DE CADENA DE CUSTODIA											
Información general											
Institución o persona											
Lugar del hecho								**Hora**			
Tipo de hecho								**Fecha del hecho**			
Datos del indicio/Evidencia/Bien incautado											
Tipo de Indicio-Evidencia-Bien		**Número de serie**						**Número (IMEI)**			
Marca								**Modelo**			
Estado	**Bueno**			**Regular**					**Malo**		
Color								**Tamaño**			
Volumen								**Peso**			
Tiempo estimado de caducidad o deterioro								**No perecible**			
Fecha	**Hora**	**Nombre completo del receptor de la evidencia**			**Motivo**			**Observaciones**		**Firma**	

Tabla 5 Formulario de Cadena de custodia

Fuente: (Jaya, 2017)

5. *Identificación de la herramienta de software para la recolección de evidencia.*

La determinación de una herramienta de software enfocada en el análisis forense de teléfonos celulares es importante, de manera que permita obtener una cantidad amplia de información del dispositivo,

que contenga datos relacionados con el caso investigado. Para elegir una herramienta adecuada se debería considerar:

- Realizar una selección de posibles herramientas a ser utilizadas en el caso, donde se determine cuáles son las más adecuadas y compatibles con el fabricante del teléfono celular.
- Establecer una breve comparación de funcionalidades entre las herramienta previamente seleccionas en el punto anterior, de forma que se determine las más óptimas para el caso. Para esto se propone el siguiente cuadro de selección como fuente de ayuda

Características de adquisición de evidencia	(Nombre software 1)	(Nombre software 2)	(Nombre software 3)
Adquisición física			
Fabricante			
Modelo			
IMEI			
Archivos			
Llamadas (realizadas, recibidas)			
Tareas			
Análisis (mensajes, contactos, memoria)			
Recuperación de información eliminada			
Verificación de integridad de archivos			
Generación de reportes			
Total/11			

Tabla 6 Cuadro de selección de herramientas de software

Fuente: (Jaya, 2017)

- Finalmente, es necesario documentar la/las herramientas seleccionadas.

6. *Recolección de evidencia física.*

Dentro de la recolección de la evidencia tenemos la evidencia física, que consiste en la realización de una copia bit a bit de la memoria del dispositivo. Además de obtener una imagen de la tarjeta SIM, la cual podría almacenar algún tipo de información del dispositivo, considerando que dicha información puede ser importante en el caso investigado.

3. *Recolección de evidencia lógica.*

Ilustración 25 Recolección de evidencia lógica

Fuente: http://peritoinformaticozaragoza.com/wp-content/uploads/2016/03/forense-movil-1.png

La recolección de la evidencia lógica consiste en adquirir todo tipo de información contenida en el dispositivo referente a:

- Lista de contactos
- Fotos
- Videos
- Mensajes
- Lista de llamadas (recibidas, perdidas, realizadas), etc.

4. *Inspección y priorización de la evidencia.*

Una vez realizada la recolección de la evidencia es recomendable realizar una inspección y priorización de esta. Dicho procedimiento es necesario previamente a la ejecución de la siguiente fase que es el análisis de la evidencia del teléfono móvil. Para una inspección y priorización adecuada se debe:

- Realizar un análisis breve del tipo de caso que se está investigando, y conectar la evidencia que se encuentra más relacionada con este incidente.
- Establecer un orden o grado de importancia de la evidencia encontrada, basada en el análisis del punto anterior.

3.3.2.4. Fase de análisis de la evidencia

La fase de análisis de la evidencia se considera una parte importante de la investigación, ya que tiene como objetivo obtener respuestas a las preguntas planteadas sobre el incidente que causó el inicio de la investigación, además de generar la mayor cantidad de información para la entrega de informes en la fase final. Para adquirir dicha información es necesario aplicar ciertos procesos, métodos y técnicas a la evidencia previamente recolectada, de manera que se pueda establecer de la mejor manera posible los hechos de los eventos ocurridos en cuanto al incidente investigado.

Ilustración 26 Análisis de la evidencia

Fuente: http://www.securityartwork.es/wp-content/uploads/2016/01/img1-300x239.jpg

La fase comprende dos partes importantes dentro de la ejecución de la misma.

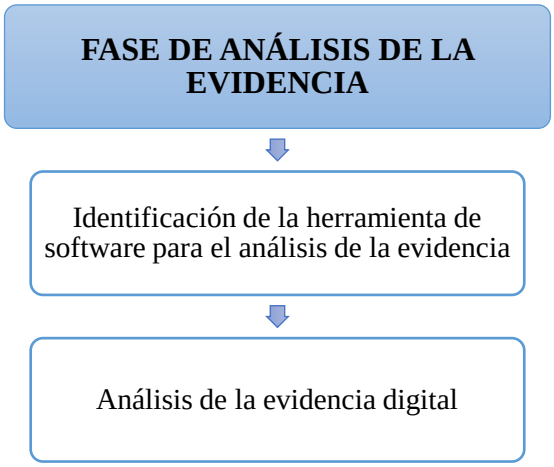


Ilustración 27 Diagrama Fase de análisis de la evidencia

Fuente: (Jaya, 2017)

1. *Identificación de la herramienta de software para el análisis de la evidencia.*

   Al igual que en la fase previa de recolección de la evidencia, es importante seleccionar una herramienta de software a ser usada en la fase actual que permita realizar un análisis minucioso de la evidencia recogida. Para la ejecución de este punto se debe tener en cuenta las mismas consideraciones citadas anteriormente en el punto 2 de la fase de preservación y recolección de la evidencia, es decir en la parte de "identificación de la herramienta de software para la recolección de la evidencia". Cabe destacar que, si las herramientas usadas en la recolección de la evidencia, nos permiten llevar a cabo el análisis de las mismas, es necesario solo enumerarlas.

2. *Análisis de la evidencia digital.*

Para el análisis de la evidencia digital se debe examinar todo tipo de información que pueda estar relacionada con el incidente y con nuestro dispositivo incautado. Por lo cual se debe tener en cuenta lo siguiente:

- Análisis de información almacenada
- Recuperación de archivos eliminados
- Identificación de aplicaciones instaladas
- Análisis de archivos sospechosos
- Identificación de archivos involucrados en el caso
- Construcción de la línea de tiempo

3.3.2.5. Fase de documentación del incidente

La última fase del análisis forense es la documentación del incidente, implica un informe final de todo el procedimiento llevado a cabo, donde se justifica y demuestra todo tipo de hallazgos obtenidos, acciones y hechos durante el proceso de investigación.

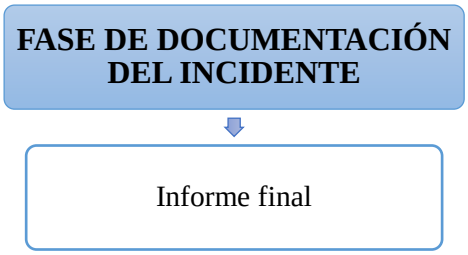


Ilustración 28 Diagrama Fase de documentación del incidente

Fuente: (Jaya, 2017)

1. *Informe final*

El informe final debe ser redactado de forma clara y concisa, es decir que pueda ser comprensible para el público lector de este documento como son los jueces, facilitándoles la tarea en cuanto a la revisión de los hechos y evidencias del incidente. La estructura del informe final debe contar con lo siguiente:

- Periodo de investigación (fecha de inicio, fecha de cierre)
- Nombre del perito o emisor del informe
- Asunto
- Resumen (identificación de la escena, recolección de información, descripción de evidencia)
- Resultados del análisis de la evidencia
- Conclusiones
- Archivos adjuntos

3.3.3. Recomendaciones de aplicación de la guía

La presente guía debe ser usada como una ayuda para la realización de una investigación forense digital, y aplicarla en casos donde estén involucrados dispositivos móviles. Teniendo en cuenta que la guía requiere de la aplicación de herramientas de software para la recolección y análisis de la evidencia, se debe evaluar correctamente el tipo de software a utilizar, dado que los dispositivos móviles presentan diferente tipo de sistema operativo. Además, cabe destacar que se debe emplear los procedimientos y metodologías de la guía en el orden correcto, es decir según lo propuesto; de manera que se pueda garantizar que la evidencia no sufra ninguna alteración durante todo el proceso investigativo y que el mismo permita llevar a cabo un análisis forense integral y estructurado.

CAPÍTULO IV

IMPLEMENTACIÓN DE LA GUÍA EN ANÁLISIS A DISPOSITIVOS MÓVILES

Este capítulo pretende implementar y ejecutar la guía propuesta en análisis a dispositivos móviles, de manera que se demuestre la importancia y eficacia que tiene seguir un proceso adecuado de análisis forense de datos. Además de aplicar de manera correcta las fases que incluye la guía de procedimientos detallada en el capítulo anterior.

A continuación, como resultado y validación de la guía propuesta, se procede a aplicar la misma en un escenario de prueba simulado.

4.1. Escenario de Prueba

El escenario de prueba con el cual será ejemplificada y simulada la aplicación y ejecución de la guía de procedimientos de análisis forense de datos, es el siguiente:

- El 10 de enero del 2017, la empresa TechMart dedicada a la comercialización de equipos tecnológicos, solicita la realización de un análisis forense a los dispositivos móviles entregados por la empresa a su personal, debido a las constantes quejas de sus clientes por la falta de respuesta inmediata en la atención que brindan. Los dispositivos fueron entregados para el uso exclusivo de funciones relacionadas con la empresa.

Finalmente, la empresa desea conocer qué tipo de información es manejada en el dispositivo que pueda estar interfiriendo en las actividades diarias de su personal.

4.1.1. Selección y especificación del dispositivo

El dispositivo que será usado como objeto de pruebas para el análisis forense de datos, tiene las siguientes características:

- Smartphone con sistema operativo Android
- Android versión 6.0.1

4.1.2. Especificación de herramientas a aplicar

Las herramientas de software para la guía de procedimientos de análisis forense propuesta, aplicada en el caso de prueba, en las fases de recolección y análisis de la evidencia, son las siguientes:

- MOBILedit! Forensic
- Paraben E3: Universal

Las herramientas antes mencionadas son comerciales y debido al elevado costo de adquisición, se utilizara la versión de prueba que proveen cada uno de los respectivos propietarios de distribución del software y que está disponible por un tiempo limitado.

4.2. Aplicación de la Guía

Una vez descrito el escenario de prueba, especificado el dispositivo y enumeradas las herramientas a ser utilizadas dentro de la guía de análisis forense de datos, se procede a continuación al desarrollo de la aplicación de la misma.

4.2.1. Fase de aseguramiento de la escena del crimen

Medidas de protección

Para definir las medidas de protección, se tiene en cuenta que muchas de estas son tomadas por el personal oficial que hace el primer ingreso a la escena del crimen. Para la presente investigación, teniendo conocimiento que la misma es de carácter académico y es un escenario de prueba simulado, las medidas de protección que se considera deberían ser tomadas son las siguientes:

- Mantener una custodia adecuada para los dispositivos incautados, considerados como evidencia para el caso investigado.
- Proteger la integridad de la información contenida en cada dispositivo durante todo el proceso.

Designación de responsables

Dentro de la presente investigación se llevara a cabo una distribución de roles, de acuerdo con lo planteado en la guía propuesta. No obstante, por la falta de personal se definirá 4 de los 6 roles propuestos en la guía, y considerados desde el punto de vista personal los más importantes para el desarrollo de la investigación. Dichos roles serán asumidos por la autora de la presente investigación y para la constancia de los mismos se llenará un formulario como el siguiente:

Fecha de designación de roles	12/01/2017					
Código del caso	P001					
Descripción del caso	Caso de Prueba					
Rol designado	**Nombre**	**Apellido**	**Fecha de designación de rol**	**Cédula**	**Teléfono**	**Firma**
Custodio de la evidencia	Katherine	Jaya	12/01/2017	1720579233	0984664253	
Investigador forense	Katherine	Jaya	12/01/2017	1720579233	0984664253	
Examinador forense	Katherine	Jaya	12/01/2017	1720579233	0984664253	
Analista forense	Katherine	Jaya	12/01/2017	1720579233	0984664253	

Tabla 7 Formulario Designación de responsables (Caso de Prueba)

Fuente: (Jaya, 2017)

4.2.2. Fase de identificación de la escena

A continuación, se recopila la información necesaria para el registro de la escena del crimen.

Documentación del estado inicial

Fecha del incidente:	10/01/2017			
Código del caso:	P001			
Detalles del incidente:	Seguimiento de actividades en dispositivos empresariales			
Dirección del incidente:	De los Pinos y Av. Eloy Alfaro			
Nombre y apellidos del investigador responsable:				
Katherine Jaya Cáceres				
FOTOGRAFÍAS				
Escena del crimen				
 *Ilustración 29 Personal de la empresa* Fuente: http://www.liderhoy.com/imagenes/personal-de-la-empresa -y-ejecutivos.jpg				
Dispositivo				
 *Ilustración 30 Dispositivo objeto de análisis* Fuente: (Jaya, 2017)				
Existencia de VIDEOS	**SÍ**		**NO**	X

Tabla 8 Formulario Documentación del estado inicial (Caso de Prueba)

Fuente: (Jaya, 2017)

Declaraciones de involucrados

Con enfoque al presente caso de prueba algunas de las preguntas que se debería realizar al portador o dueño del dispositivo, son las siguientes:

1. *¿Es usted propietario o dueño del teléfono celular?*

   Soy el usuario regular del dispositivo, pero no lo he adquirido.

2. ~~*En caso de ser el propietario, ¿Cómo adquirió el dispositivo?*~~

3. *Si no le pertenece, ¿Quién es el propietario?*

   Dado que el dispositivo fue entregado por la empresa, la empresa es propietaria del mismo.

4. *¿Para qué utiliza habitualmente el dispositivo?*

   Fundamentalmente lo utilizo para comunicarme, además contiene información de contactos que son clientes de la empresa.

5. *¿Cuándo uso el dispositivo por última vez?*

   La mañana del 10 de enero de 2017, antes de entregar el dispositivo para el análisis.

6. *Además de usted, ¿Hay alguien más que tiene acceso al dispositivo?*

   No, soy la única persona que ocupa el teléfono celular.

7. *¿El dispositivo posee algún tipo de protección de acceso?*

   Sí, el dispositivo tiene una protección de acceso.

8. *¿Qué tipo de protección de acceso posee?*

Un PIN de seguridad.

9. *¿Podría entregarme las claves de acceso del dispositivo?*

   Claro, el PIN es 23071986

Identificación del dispositivo

ESTADO Y CARACTERÍSTICAS DEL DISPOSITIVO				
Estado del dispositivo	**Encendido**	X	**Apagado**	
Protegido por clave	**SI**	X	**NO**	
En caso de tener protección (Tipo)				
Contraseña				
PIN	23071986			
Patrón				
Huella digital				
Reconocimiento facial				
Otro tipo de protección (Especifique)				
Características				
Marca del teléfono	Samsung			
Modelo del teléfono	Galaxy J5			
Número de teléfono	0998735493			
Operadora del servicio	Movistar			
Numero serial IMEI	352141078496649			
DOCUMENTACIÓN EXTRA DEL DISPOSITIVO				
	SI		**NO**	
Manuales de usuario	X			
Memorias extraíbles	X			
Cargadores	X			
Facturas de adquisición	X			
Códigos de acceso	X			

Tabla 9 Formulario Identificación del dispositivo (Caso de Prueba)

Fuente: (Jaya, 2017)

4.2.3. Fase de preservación y recolección de la evidencia

Cadena de custodia

FORMULARIO DE CADENA DE CUSTODIA						
Información general						
Institución o persona	Katherine Jaya					
Lugar del hecho	De los Pinos y Av. Eloy Alfaro			**Hora**	10h35	
Tipo de hecho	Seguimiento de actividades en dispositivos empresariales			**Fecha del hecho**	10/01/2017	
Datos del indicio/Evidencia/Bien incautado						
Tipo de Indicio-Evidencia-Bien	Teléfono celular	**Número de serie**	RV8GB2A9NEK	**Número (IMEI)**	352141078496649	
Marca	Samsung			**Modelo**	Galaxy J5	
Estado	**Bueno**	X	**Regular**		**Malo**	
Color	Blanco			**Tamaño**	126,3mm	
Volumen	$88{,}11 cm^3$			**Peso**	146g	
Tiempo estimado de caducidad o deterioro				**No perecible**	X	

Fecha	**Hora**	**Nombre completo del receptor de la evidencia**	**Motivo**	**Observaciones**	**Firma**
10/01/2017	10h35	Katherine Jaya	Preservación de la evidencia		
12/01/2017	09h30	Katherine Jaya	Identificación de la evidencia		
15/01/2017	10h00	Katherine Jaya	Recolección física de la evidencia		
16/01/2017	10h00	Katherine Jaya	Recolección lógica de la evidencia		
17/01/2017	08h00	Katherine Jaya	Análisis de la evidencia adquirida		

Tabla 10 Formulario Cadena de custodia (Caso de Prueba)

Fuente: (Jaya, 2017)

Identificación de la herramienta de software para la recolección de evidencia

Para el dispositivo que será analizado en el caso de prueba en la aplicación de la guía, se presenta una lista de herramientas de software compatibles con el dispositivo en cuestión, estas son:

- MOBILedit! Forensic
- Oxygen Forensic
- Paraben E3: Universal
- Dr.Fone

De las herramientas mencionadas anteriormente, se realiza un breve análisis de tipo funcional, basándonos en el siguiente cuadro de selección de herramientas:

Características de adquisición de evidencia	MOBILedit! Forensic	Oxygen Forensic	Paraben E3: Universal	Dr.Fone
Adquisición física			X	
Fabricante	X	X	X	X
Modelo	X	X	X	X
IMEI	X	X	X	X
Archivos	X	X		X
Llamadas (realizadas, recibidas)	X	X	X	X
Tareas	X	X		
Análisis (mensajes, contactos, memoria)	X	X	X	
Recuperación de información eliminada	X		X	X
Verificación de integridad de archivos	X		X	X
Generación de reportes	X	X	X	
Total/11	10	8	9	7

Tabla 11 Cuadro de selección de herramientas de software

Fuente: (Jaya, 2017)

Como resultado del análisis anterior las herramientas que darán un mejor resultado y que pueden ser usadas en la presente investigación, son las siguientes:

- MOBILedit! Forensic
- Paraben E3: Universal

Estas herramientas de software cumplen con la mayor cantidad de características funcionales que facilitan este trabajo de investigación.

Recolección de evidencia física

Para la recolección de la evidencia física se usara uno de los productos de software distribuidos por Paraben Corporation[28].

- ***Creación del caso de prueba en la herramienta de software***

Previo a la recolección de la evidencia se procede a la creación de un nuevo caso dentro de la herramienta, como se muestra a continuación:

1. Ejecutamos la herramienta de software E3:Universal

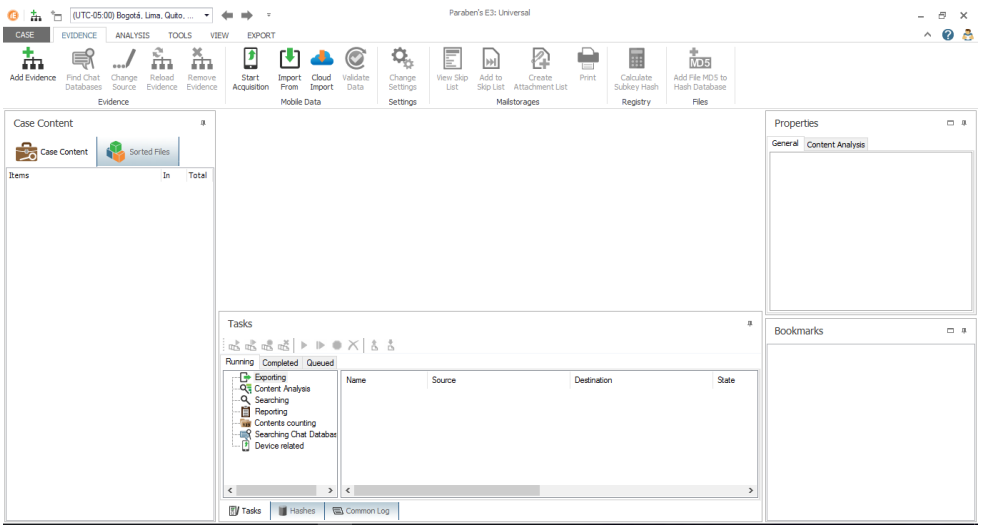


Ilustración 31 Pantalla principal de la herramienta E3: Universal

Fuente: (Jaya, 2017)

[28] Paraben Corporation: Paraben es una empresa que propone soluciones para dispositivos móviles…

2. Para la creación del nuevo caso, seleccionamos CASE y luego Create New Case...

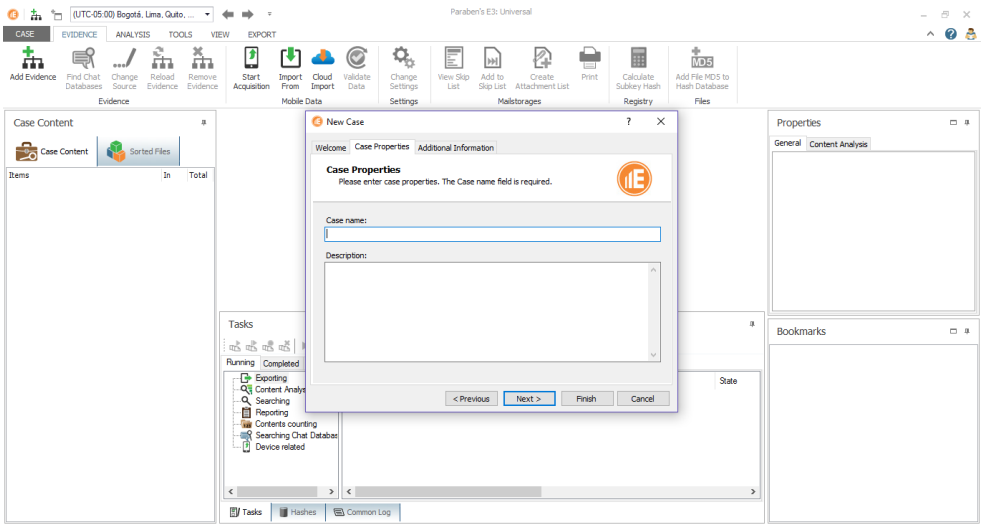


Ilustración 32 Ventana de asistente de creación de nuevo caso (E3: Universal)

Fuente: (Jaya, 2017)

3. Ingresamos el nombre del caso y una breve descripción del mismo, presionamos *Next*.

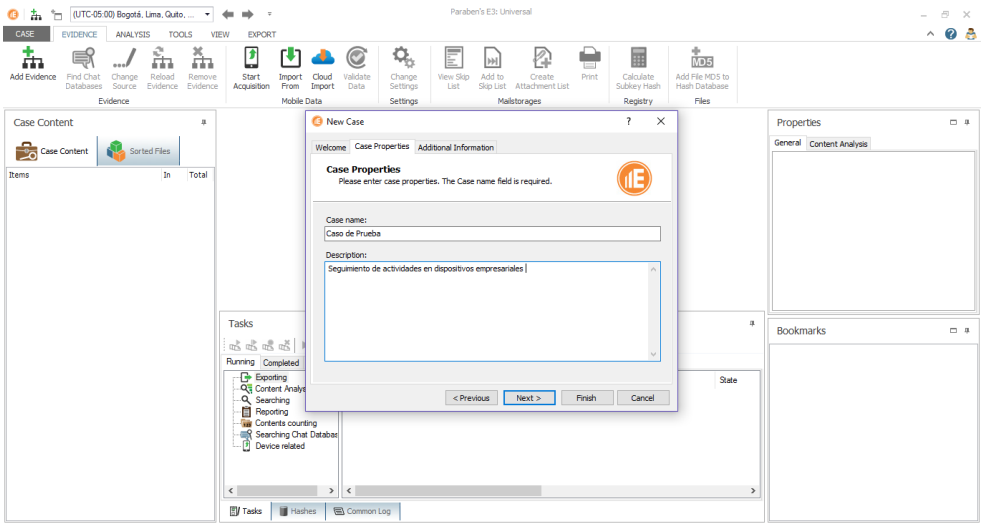


Ilustración 33 Ventana de propiedades del caso (E3: Universal)

Fuente: (Jaya, 2017)

4. A continuación, se ingresa información adicional sobre el caso en investigación.

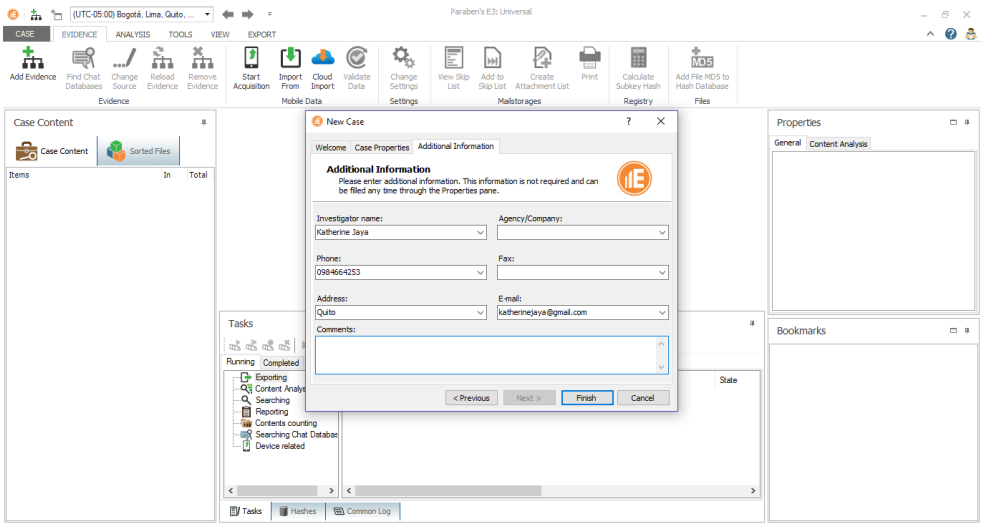


Ilustración 34 Ventana de información adicional del caso (E3: Universal)

Fuente: (Jaya, 2017)

5. Presionamos *Finish*, y seleccionamos el lugar para almacenar el caso. Finalmente, tendremos nuestro caso nuevo creado para incluir todas las evidencias a ser analizadas.

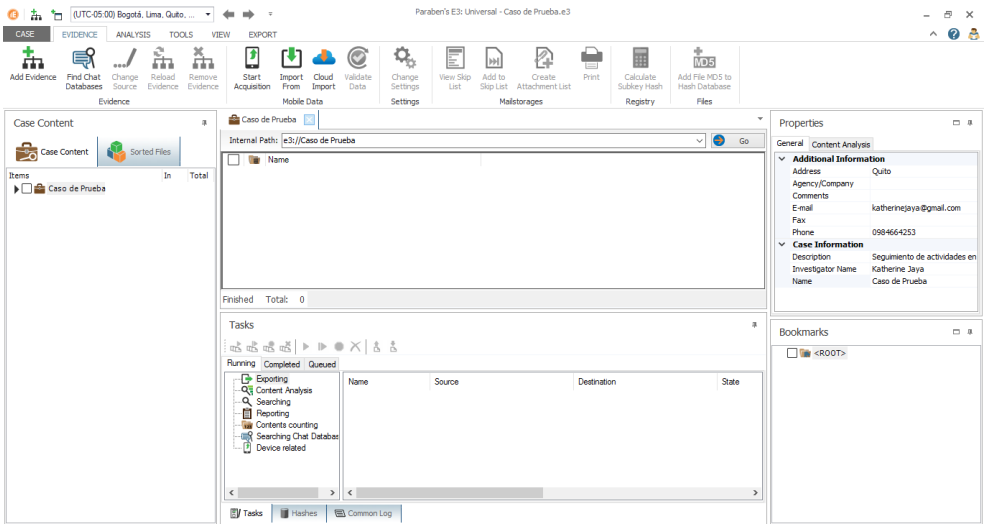


Ilustración 35 Pantalla del nuevo caso creado (E3: Universal)

Fuente: (Jaya, 2017)

- ***Recolección de la evidencia física en la herramienta de software***

Una vez creado nuestro caso, procedemos a la recolección de la evidencia física de nuestro objeto de prueba, en este caso el dispositivo móvil.

1. Procedemos añadir una nueva evidencia en el caso, presionando en 

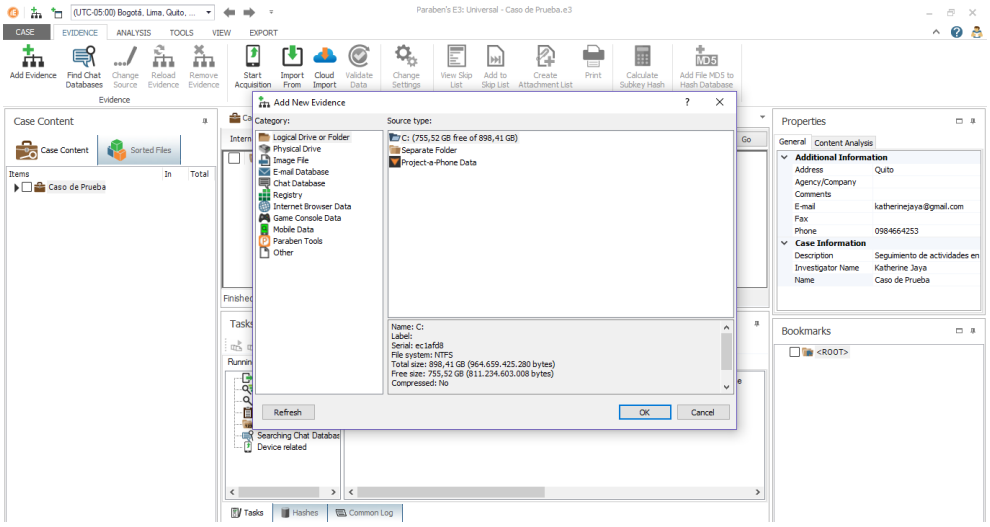


Ilustración 36 Ventana de asistente de nueva evidencia (E3: Universal)

Fuente: (Jaya, 2017)

2. Se abre el cuadro de asistencia para añadir la evidencia, donde seleccionamos en la categoría *Mobile Data* y en el tipo de origen *Mobile Data Acquisition*, finalmente presionamos *OK*.

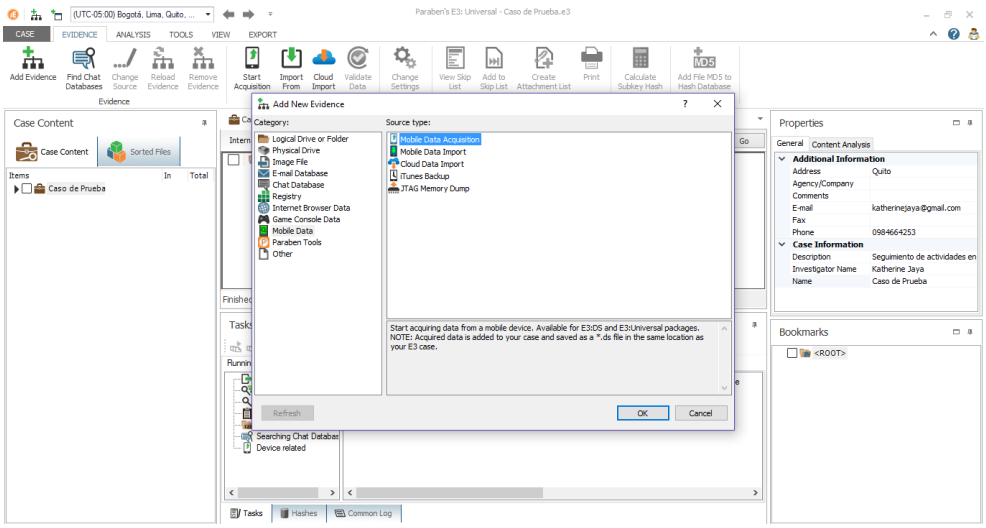


Ilustración 37 Ventana de selección de origen de la adquisición (E3: Universal)

Fuente: (Jaya, 2017)

3. Se conecta el dispositivo para su detección, y se selecciona el dispositivo de adquisición. En este caso *Android*.

Ilustración 38 Ventana de selección del tipo de dispositivo de adquisición de datos (E3: Universal)

Fuente: (Jaya, 2017)

4. Se elige el tipo de adquisición que vamos a realizar.

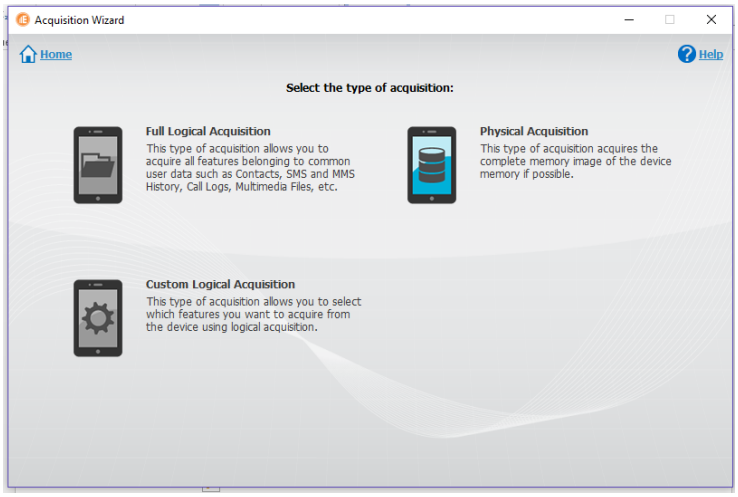


Ilustración 39 Ventana de selección del tipo de adquisición (E3: Universal)

Fuente: (Jaya, 2017)

5. Seleccionamos las acciones que deseamos que se ejecuten en el dispositivo.

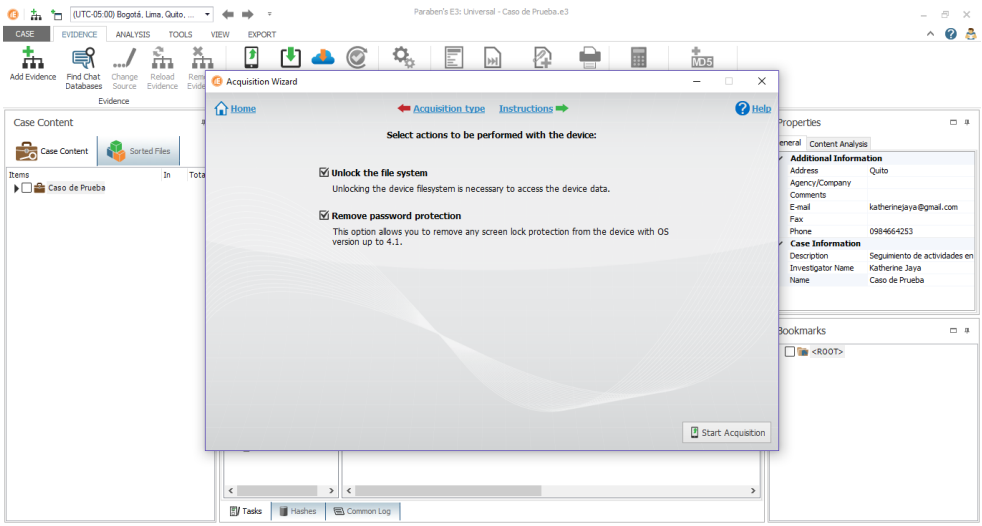
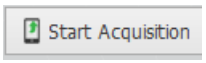


Ilustración 40 Ventana de selección de acciones para la adquisición (E3: Universal)

Fuente: (Jaya, 2017)

6. Presionamos  para dar inicio a la recolección física de evidencia. Una vez terminada la adquisición aparecerá la palabra *OK* y se presionará *Finish*.

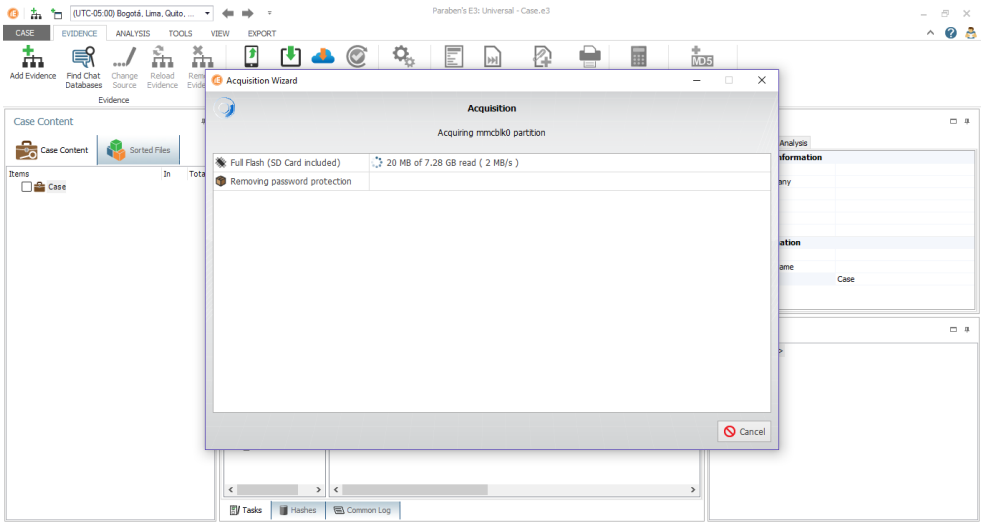


Ilustración 41 Ventana del proceso de adquisición físico (E3: Universal)

Fuente: (Jaya, 2017)

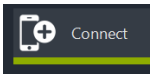
Recolección de evidencia lógica

La recolección de la evidencia lógica se realizó de la siguiente manera, a través de la herramienta de software MOBILedit! Forensic.

1. Ejecutamos la herramienta MOBILedit! Forensic.

Ilustración 42 Pantalla principal de MOBILedit! Forensic

Fuente: (Jaya, 2017)

2. Seleccionamos la opción  para iniciar la conexión entre el dispositivo y el software.

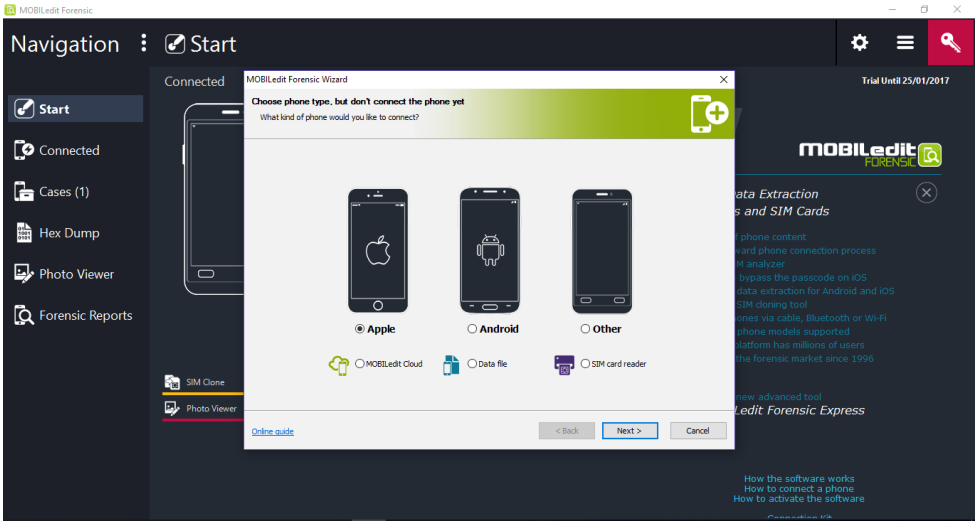


Ilustración 43 Pantalla de inicio para la conexión del dispositivo (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

3. En este caso, seleccionamos *Android* y presionamos siguiente (*Next*).

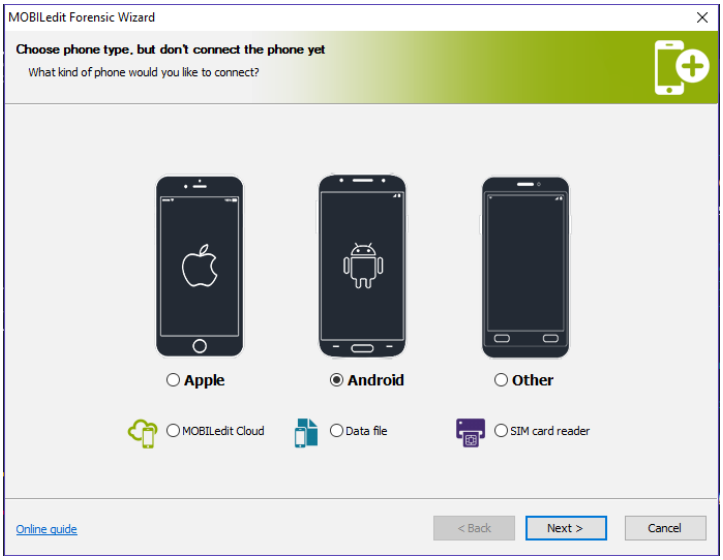


Ilustración 44 Ventana de selección del dispositivo a conectar (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

4. Seleccionamos el tipo de conexión que se va a tener con el dispositivo, y presionamos siguiente (*Next*). En este caso será por el cable del dispositivo.

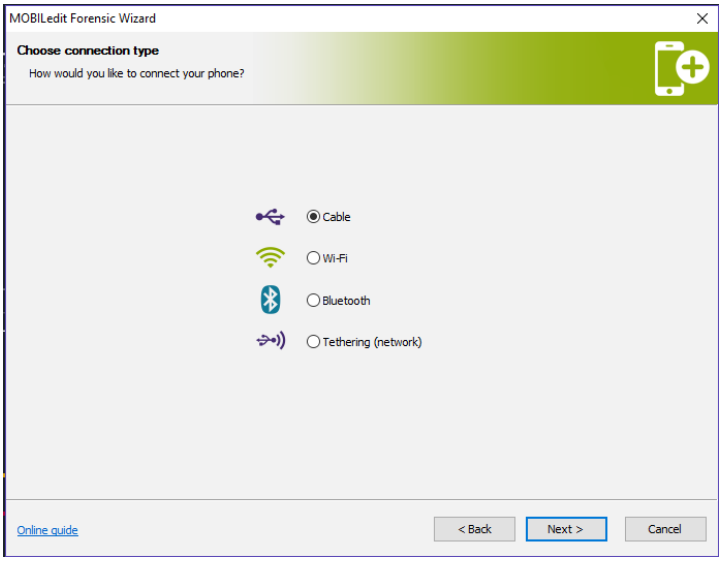


Ilustración 45 Ventana de tipo de conexión (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

5. En esta parte se verifica si se necesita la instalación de algún driver, caso contrario se presiona siguiente (*Next*).

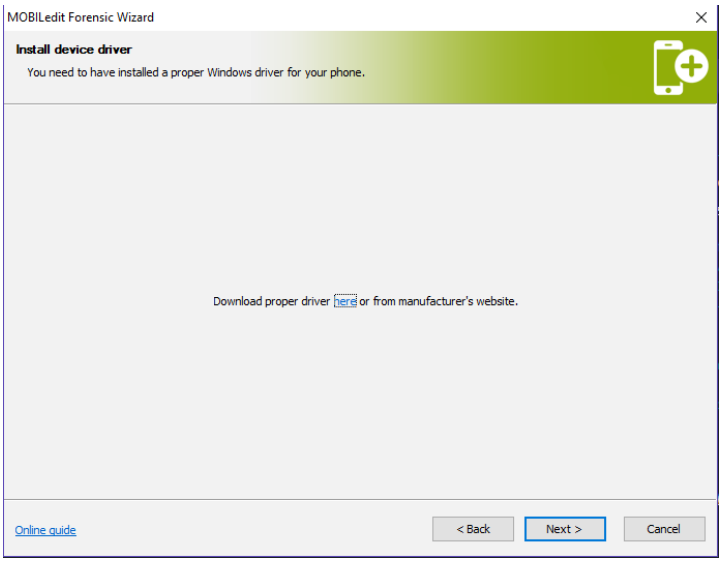


Ilustración 46 Ventana de instalación de drivers del dispositivo (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

6. Se da indicaciones para la activación del modo desarrollador en el dispositivo y como activar la depuración USB, que se requiere para la conexión.

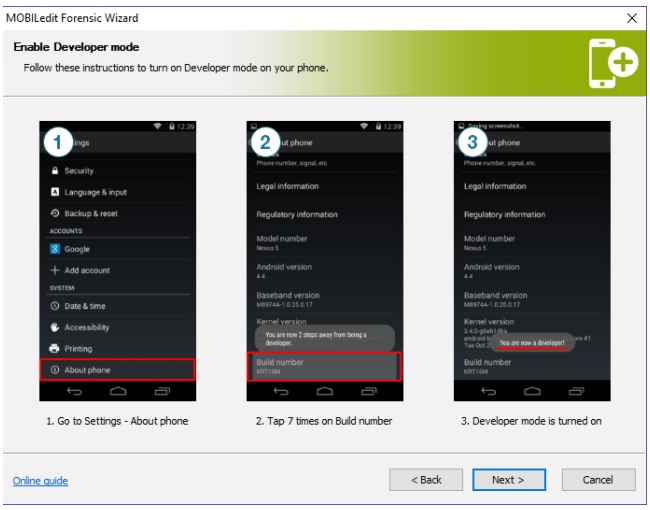


Ilustración 47 ventana guía para activación del modo programador (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

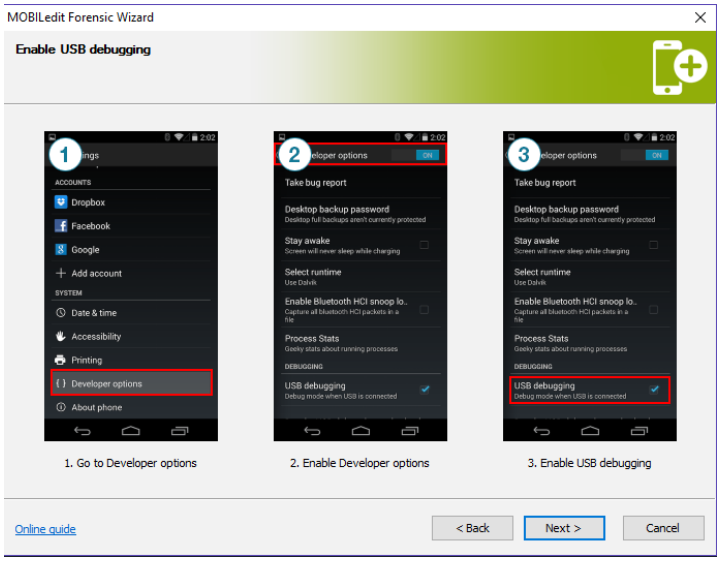


Ilustración 48 Ventana guía para activación de la depuración USB (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

7. Se conecta el dispositivo, una vez detectado lo seleccionamos y presionamos finalizar (*Finish*).

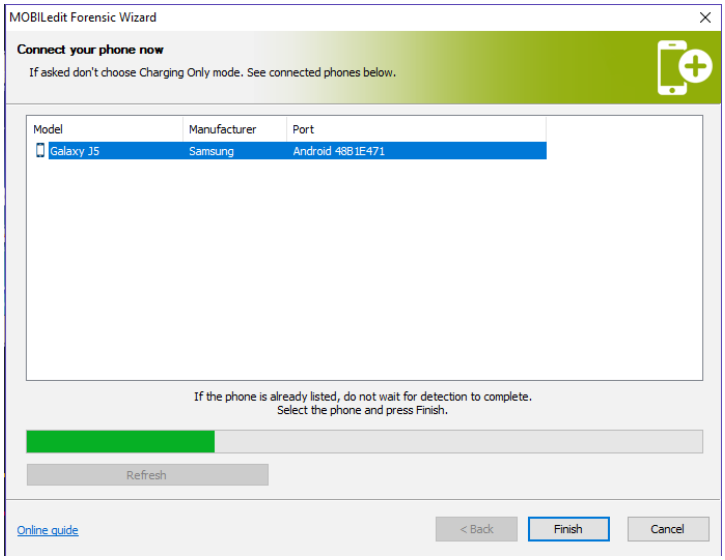


Ilustración 49 Ventana de conexión del dispositivo (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

8. Una vez reconocido el dispositivo, se procede a la extracción de la evidencia.

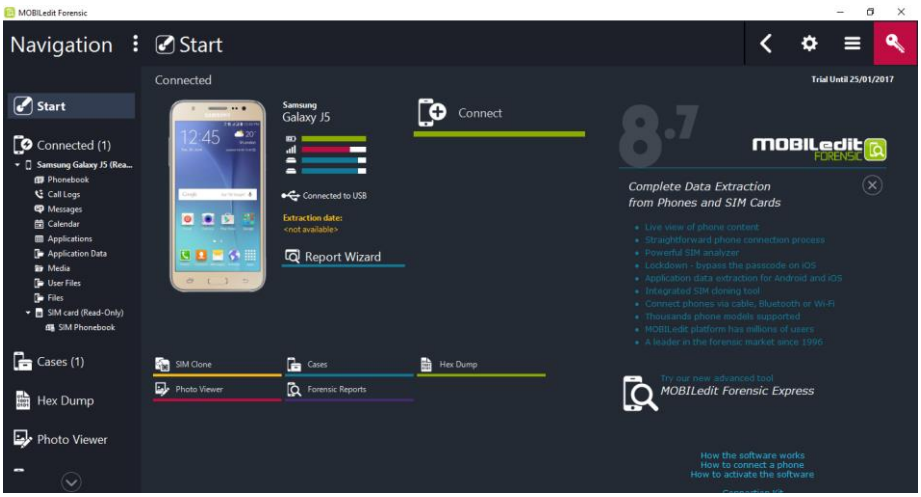
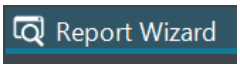


Ilustración 50 Pantalla de conexión del dispositivo (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

9. Hacemos clic en 

y se verifica que se desea extraer, y luego siguiente (*Next*).

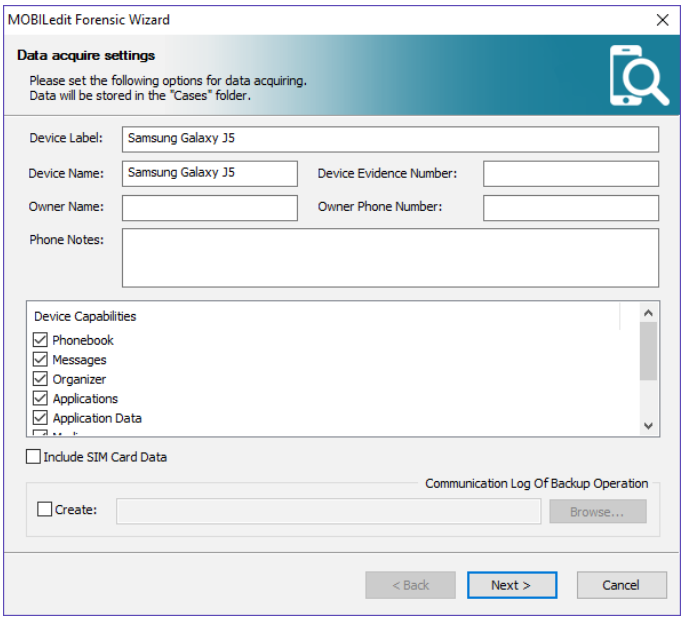


Ilustración 51 Ventana de ajustes para la adquisición de datos (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

10. Seleccionamos que archivos del sistema necesitamos adquirir, de acuerdo a las opciones que se presenta. Para nuestro caso serán todos los archivos del sistema (*Whole file system*).

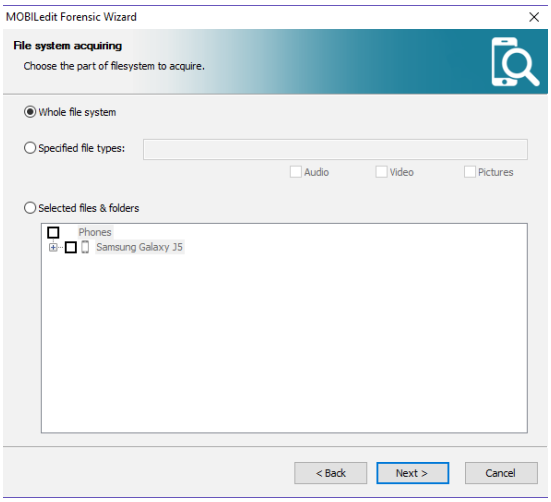


Ilustración 52 Ventana de selección para adquisición de archivos del sistema (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

11. Presionamos siguiente (*Next*), iniciando de esta manera con la obtención de la evidencia.

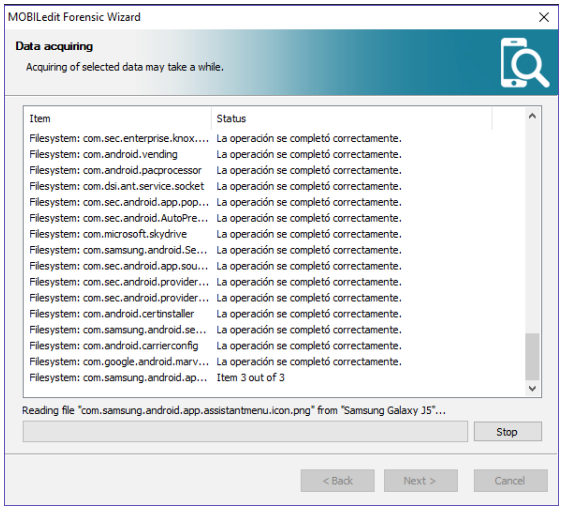


Ilustración 53 Ventana de proceso de adquisición de datos (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

12. Una vez terminado el proceso de adquisición presionamos siguiente (*Next*).

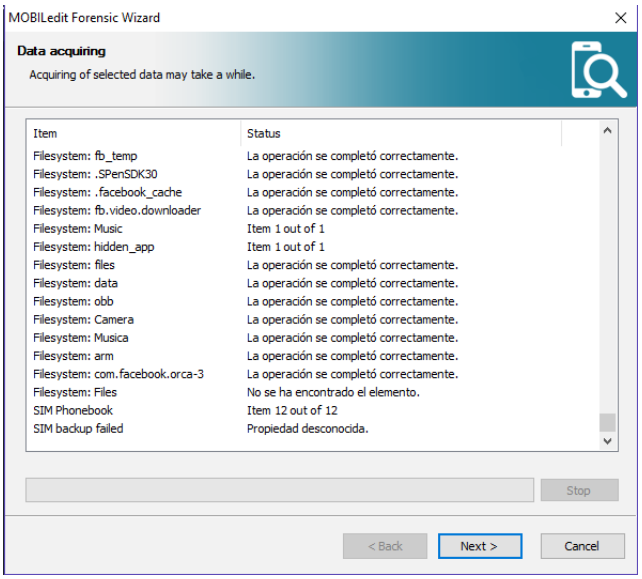


Ilustración 54 Ventana del proceso de adquisición de datos finalizada (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

13. Seleccionamos un caso nuevo, presionamos siguiente y procedemos a llenar los datos para la creación del caso investigado.

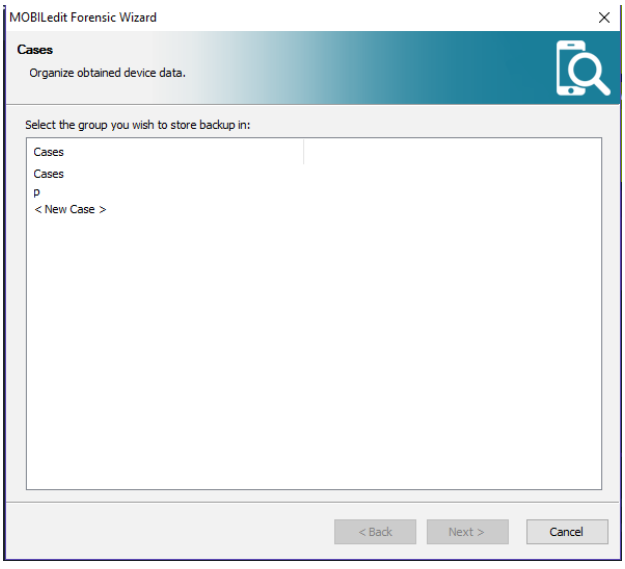


Ilustración 55 Ventana de selección de casos (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

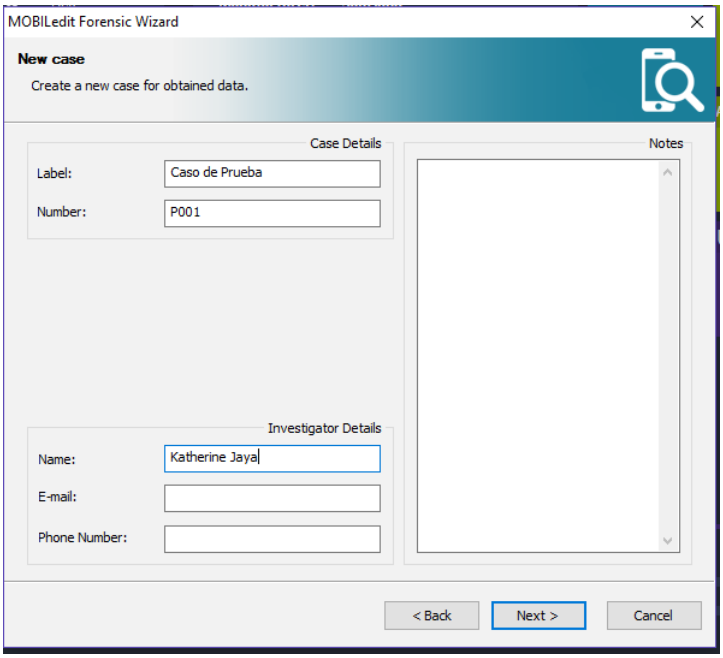


Ilustración 56 Ventana de información del nuevo caso (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

14. Seleccionamos la forma de exportación de los datos, cual es el origen de estos y que tipo de datos contendrá este documento.

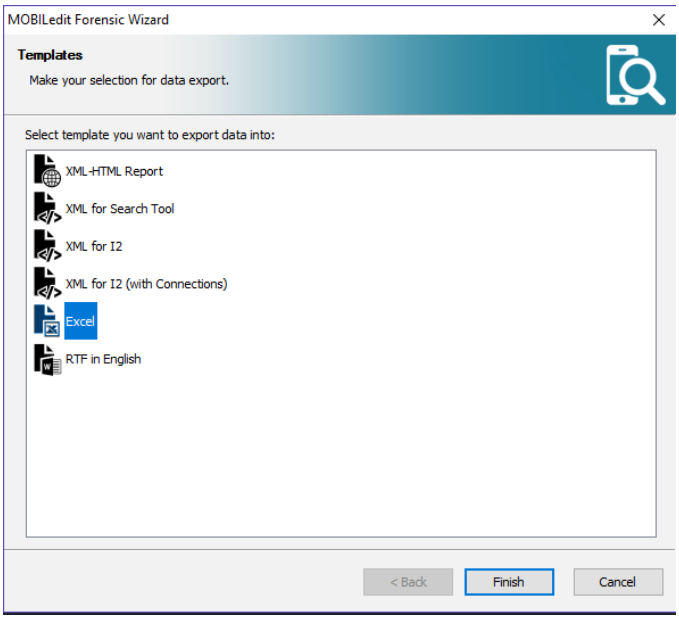


Ilustración 57 Ventana de selección de plantilla para la exportación de datos (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

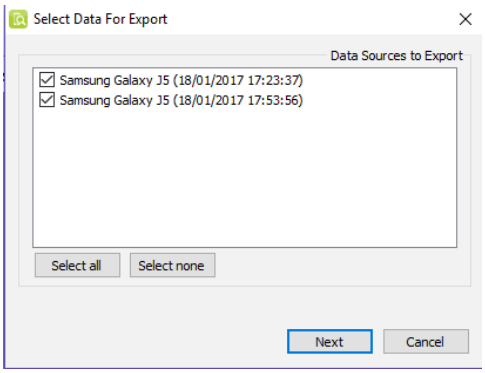


Ilustración 58 Ventana de selección de datos a exportar (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

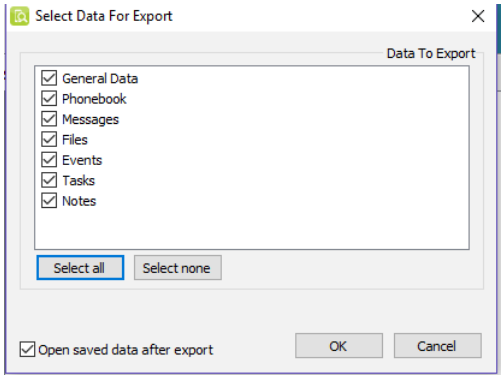


Ilustración 59 Ventana de selección de datos para la exportación (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

15. Seleccionamos el lugar donde deseamos almacenar la exportación.

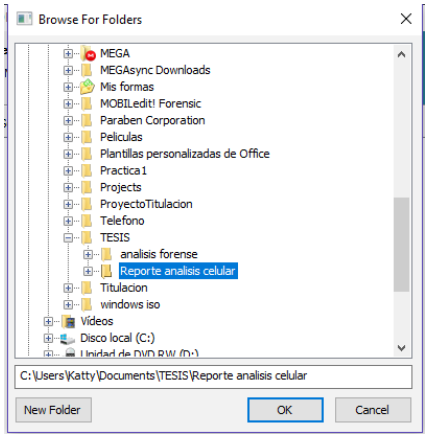


Ilustración 60 Ubicación de almacenamiento de archivo de exportación (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

16. Finalmente, se genera un informe de la recolección o adquisición de datos lógicos.

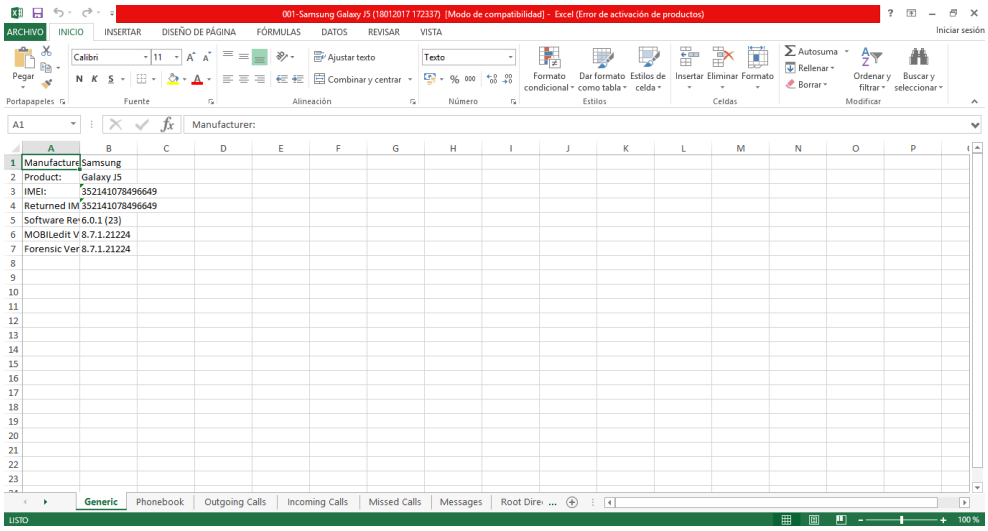


Ilustración 61 Archivo con datos exportados

Fuente: (Jaya, 2017)

Inspección y priorización de la evidencia

Por las razones que se solicitó la presente investigación forense los principales puntos a enfocarse en el análisis son:

- Aplicaciones
- Mensajería

4.2.4. Fase de análisis de la evidencia

Identificación de la herramienta de software para el análisis de la evidencia

La herramienta de software utilizada para el análisis de la evidencia es:

- MOBILedit! Forensic

Análisis de la evidencia digital

Recolectada la información, se procede a continuación al análisis de la misma en la respectiva herramienta de software.

Ilustración 62 Pantalla principal con datos generales del dispositivo (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

- *Información básica del dispositivo*

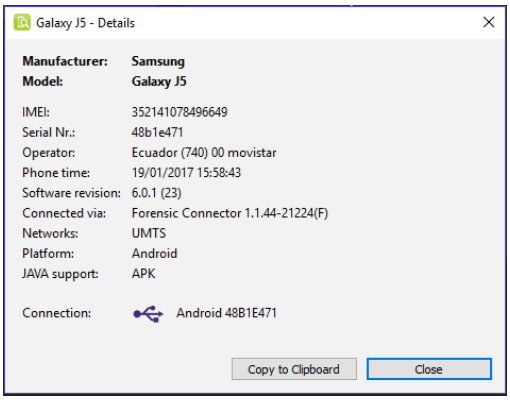


Ilustración 63 Ventana de información básica del dispositivo (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

La ilustración muestra los detalles principales del dispositivo como son: fabricante, modelo, IMEI, número de serial, operadora, plataforma, versión del sistema operativo, entre otros. Además de este tipo de información también se puede ver el porcentaje de batería y la capacidad de memoria del teléfono y de la tarjeta.

Ilustración 64 Ventana con de información extra del dispositivo (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

- *Directorio telefónico*

Se logró adquirir un total de 82 contactos con sus nombres de registro y números telefónicos. La herramienta permitió identificar como 12 contactos en SIM, 34 en Google y 36 en la aplicación de WhatsApp.

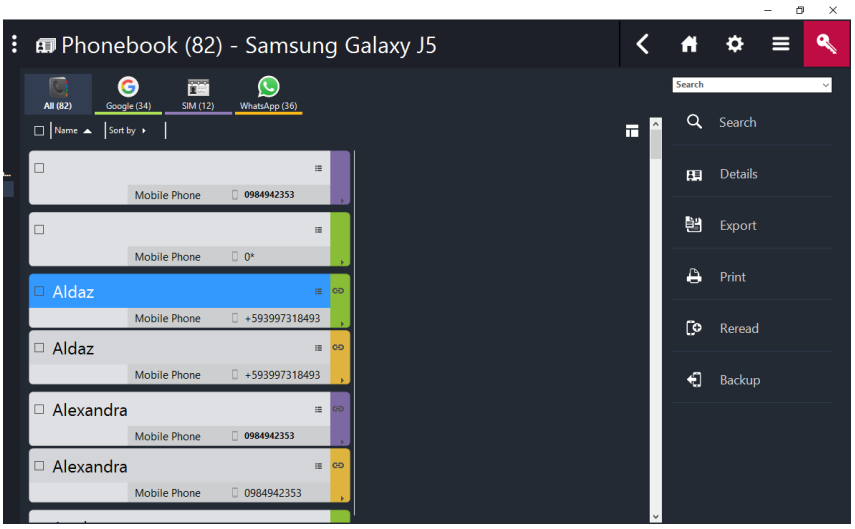


Ilustración 65 Ventana de análisis del directorio telefónico (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

- *Registro de llamadas*

Recuperado un total de 42 llamadas, de las cuales 15 son llamadas perdidas, 23 realizadas y 4 recibidas. Se puede ver tanto el nombre del contacto, el número, la fecha y hora de cada llamada.

Ilustración 66 Ventana de análisis del registro de llamadas (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

En caso de que se requiera un análisis más profundo en cada contacto se puede tener la hora de inicio de la llamada y a qué hora finalizo la misma.

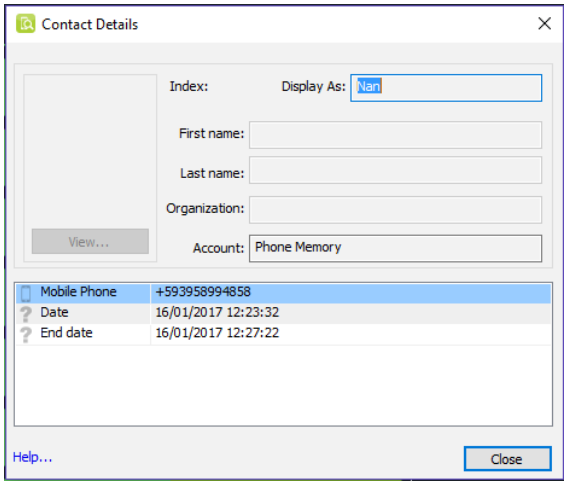


Ilustración 67 Ventana de detalles del contacto (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

- *Mensajes*

Se identificó un total de 7 mensajes de 4 cuatro conversaciones, mostrándonos el contenido del mensaje, el nombre del remitente, además de la fecha y hora que estos fueron recibidos o enviados.

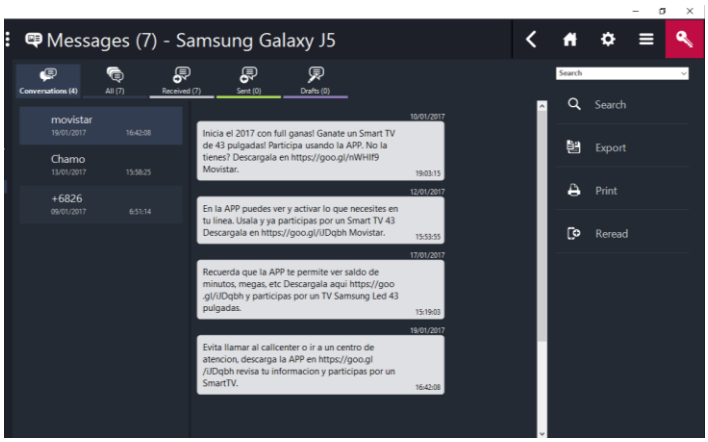


Ilustración 68 Ventana de análisis de mensajes (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

- *Calendario*

No se registró ningún tipo de evento almacenado en el calendario.

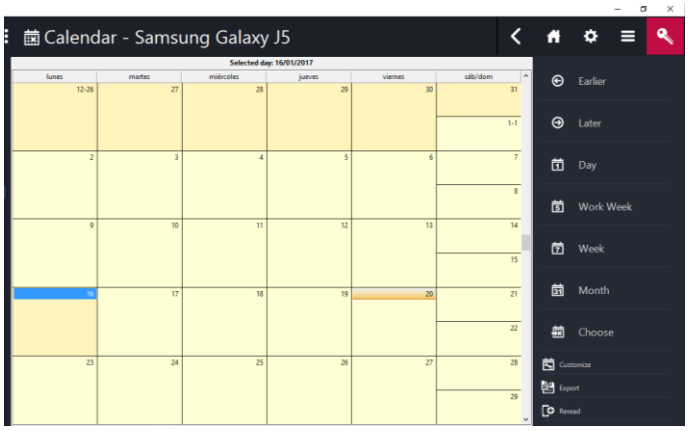


Ilustración 69 Ventana de análisis del calendario (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

- *Aplicaciones*

Se encontró un total de 242 aplicaciones, las cuales se dividen aplicaciones propias del sistema y de usuario. Cada una de estas se las puede distinguir por una barra de color al lado izquierdo de cada una.

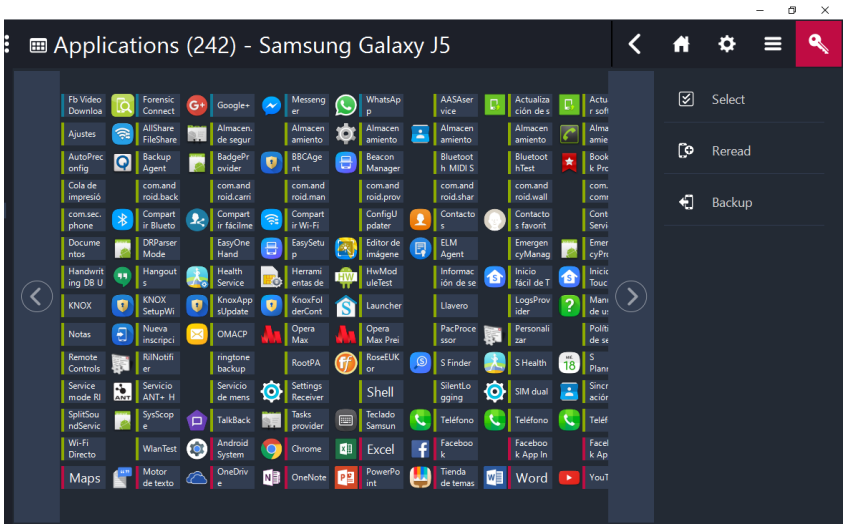


Ilustración 70 Ventana de análisis de las aplicaciones (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

- *Datos de la aplicación*

En esta parte se encuentra lo relacionado al contenido de los proveedores de las aplicaciones, contenido basura de los mismos, datos de cuentas de usuario, y algunos logs.

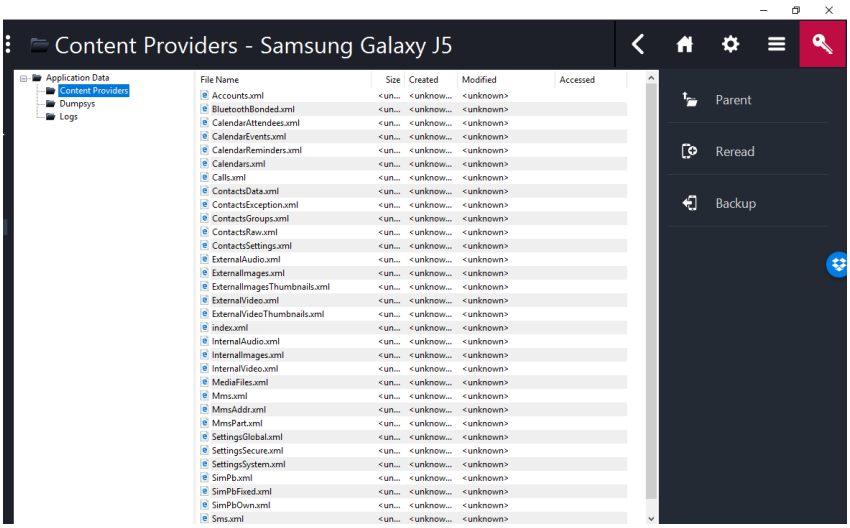


Ilustración 71 Ventana de análisis de los datos de aplicaciones (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

- *Media*

Muestra todo el contenido multimedia almacenado en el dispositivo como fotografías, videos, música, entre otros. Entre lo que se logró identificar un total de 219 fotografías y 64 videos.

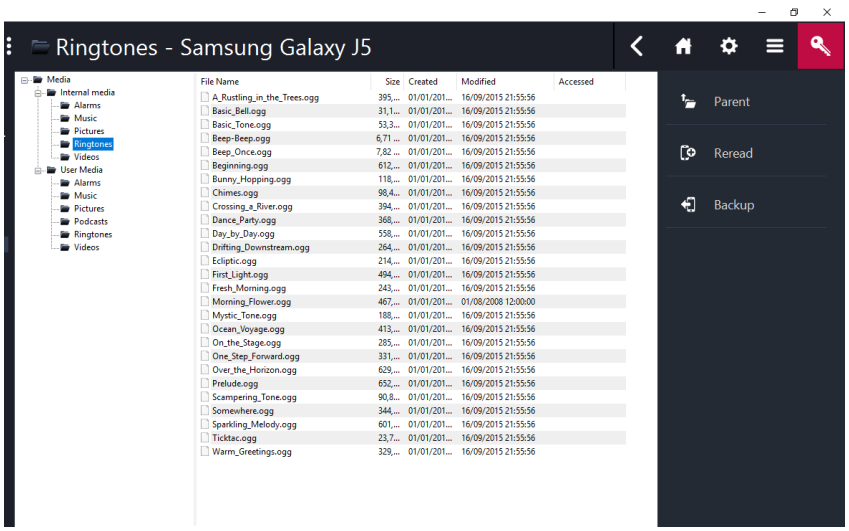


Ilustración 72 Ventana de análisis del contenido multimedia (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

- *Archivos de usuario*

Permitió la identificación de contenido fotográfico, descargas, contenido de la aplicación de WhatsApp como: fotos, audios, videos.

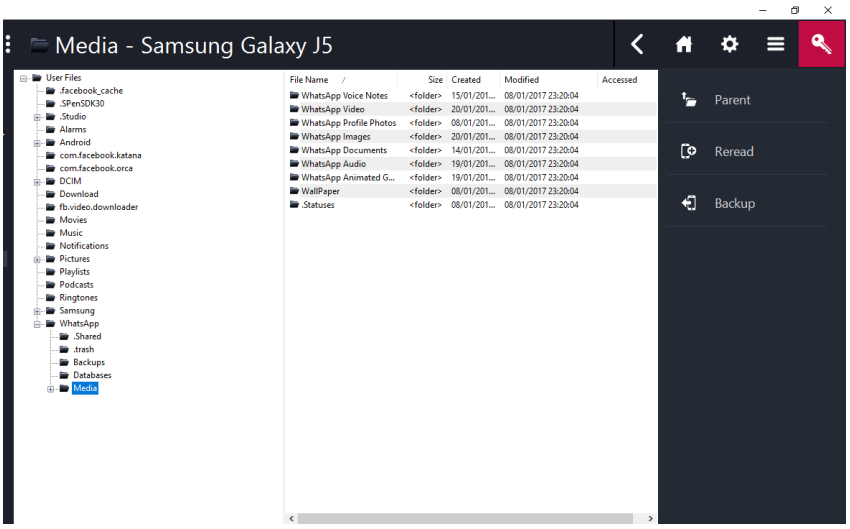


Ilustración 73 Ventana de análisis de archivos de usuario (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

- *Archivos*

Muestra el contenido almacenado en el dispositivo, aquí también encontramos el ejecutable de las aplicaciones instaladas en el dispositivo.

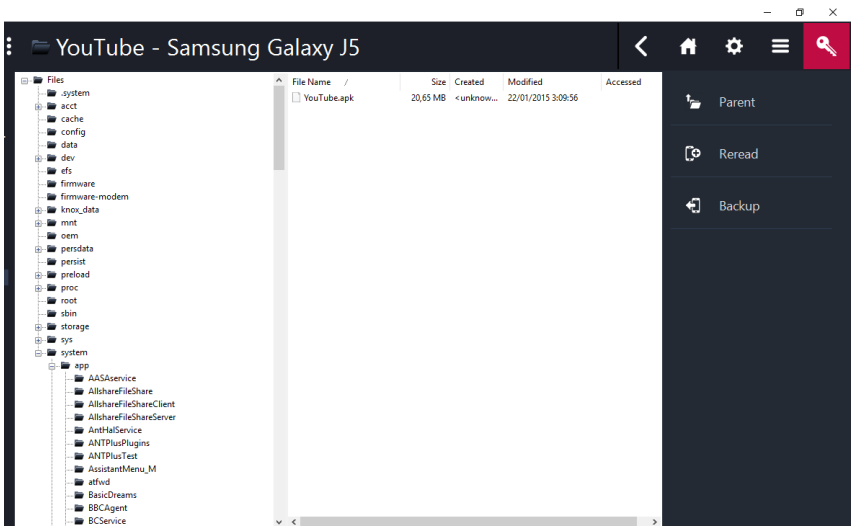


Ilustración 74 Ventana de análisis de archivos (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

- *Tarjeta SIM*

Para finalizar se muestra información de la tarjeta SIM del dispositivo.

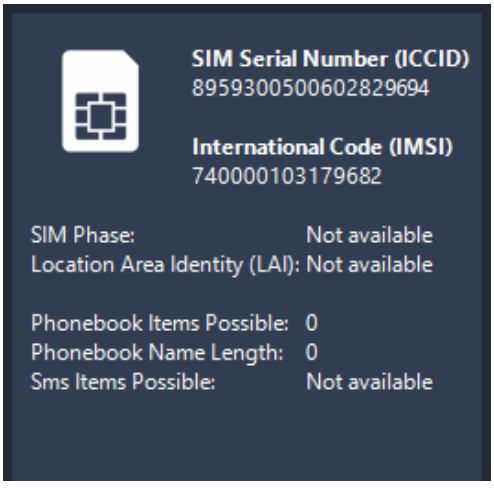


Ilustración 75 Ventana de información de la tarjeta SIM (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

- *Construcción de la línea de tiempo*

La herramienta ayuda con la construcción de la línea de tiempo de los eventos, sean estos en días, semanas, meses o años.

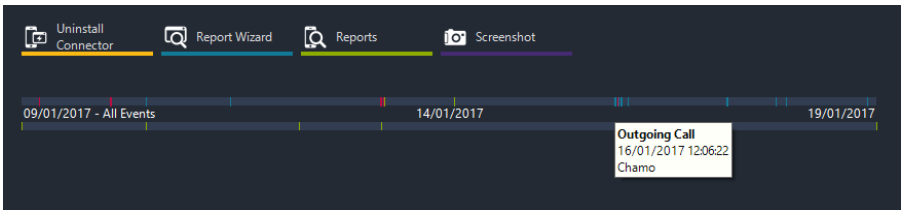


Ilustración 76 Línea de tiempo 1 de todos los eventos (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

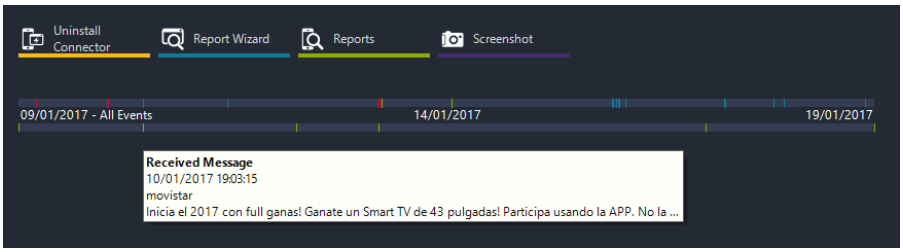


Ilustración 77 Línea de tiempo 2 de todos los eventos (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

Ilustración 78 Línea de tiempo en meses (MOBILedit! Forensic)

Fuente: (Jaya, 2017)

4.2.5. Fase de documentación del incidente

Informe final

Para nuestro caso de prueba, los archivos adjuntos no se incluirán en esta sección, como debería constar en el informe final según la guía propuesta, debido a la extensión del documento serán incluidos en la sección de los Anexos, al final de la presente investigación.

El informe tendrá la siguiente estructura, como fue definida en la guía propuesta.

INFORME DE LA INVESTIGACIÓN

Periodo de investigación: 10 de enero de 2017 – 25 de enero de 2017

Nombre del perito o emisor del informe: Katherine Alexandra Jaya Cáceres

Asunto: Seguimiento de actividades en dispositivos móviles

Resumen:

La presente investigación forense fue solicitada por la siguiente razón:

- La empresa hizo la entrega de dispositivos móviles a sus empleados para el uso exclusivo de funciones relacionadas con la empresa, no obstante debido a las constantes quejas de sus clientes por la falta de respuesta inmediata en la atención que brindan, la empresa desea conocer qué tipo de información es manejada en el dispositivo que pueda estar interfiriendo en las actividades diarias de su personal.

Los dispositivos incautados como objeto de prueba tienen las siguientes características:

- Samsung Galaxi J5
- Operadora Movistar
- Dispositivos encendidos

Además se entregó documentación extra perteneciente a estos dispositivos, como es:

- Manuales de usuario
- Memorias extraíbles
- Cargadores
- Facturas de adquisición

Resultados del análisis de la evidencia:

Se obtuvo los siguientes resultados de la evidencia recolectada:

- Información básica del dispositivo (marca, modelo, IMEI, número de serie, operadora del servicio, plataforma, versión del sistema operativo entre otros).
- 82 contactos con nombres de registro y números telefónicos
- 42 llamadas registradas (perdidas, realizadas, recibidas)
- 7 mensajes de texto de 4 conversaciones

- Ningún registro en el calendario
- 242 aplicaciones (aplicaciones del sistema y de usuario)
- 219 fotografías
- 64 videos
- Información básica de la tarjeta SIM

Conclusiones:

El análisis de la evidencia nos muestra que la posible causa de la pérdida de tiempo de los empleados de la empresa TechMart, es el uso constante de aplicaciones de mensajería y redes sociales como Facebook, Messenger y WhatsApp; la última aplicación mencionada, de igual forma es utilizada para la comunicación entre los clientes, pero a su vez también es utilizada para comunicarse con familiares, amigos y grupos de chat.

Archivos adjuntos:

Esta parte incluye lo siguiente:

- Formulario de designación de responsables
- Formulario de documentación del estado inicial
- Formulario de identificación del dispositivo
- Reportes generados por las herramientas de software

4.3. Conclusiones del Resultado del Análisis Realizado

Como se puede apreciar en las conclusiones del informe en la sección anterior, y una vez terminado el análisis se pudo concluir que la posible causa de la pérdida de tiempo de los empleados de la empresa TechMart, es el uso constante de aplicaciones de mensajería y redes sociales como Facebook, Messenger y WhatsApp; la última aplicación mencionada, de igual forma es utilizada para la comunicación entre los clientes, pero a su vez también es utilizada para comunicarse con familiares, amigos y grupos de chat.

Por otro lado, la herramienta utilizada para el análisis de la evidencia en su versión comercial, presenta reportes más completos que incluyen datos borrados, contraseñas de cuentas y redes wifi, además de datos y recordatorios de aplicaciones como Skype, Dropbox, Facebook, WhatsApp, entre otros; sin embargo debido a que en este trabajo de disertación se está utilizando una versión trial, no se puede contar con esta información.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- Cumpliendo con el objetivo general del trabajo de disertación, y luego de realizar un estudio de información esencial en el campo de la informática forense, se concluyó con el desarrollo de una guía de procedimientos de análisis forense de datos, que pretende ser un apoyo para el área de análisis a dispositivos móviles.

- Las fases de la guía de procedimientos propuesta, son el resultado de una revisión de varias guías, procedimientos y metodologías empleados en el análisis forense; cada fase desarrollada aporta con procesos y acciones a seguir, e incluyen formularios de ayuda para un mejor control de todas las actividades que son necesarias dentro de una investigación forense.

- Las fases de recolección y análisis de la evidencia son un punto importante al implementar la guía de procedimientos, ya que al ser ejecutadas de una manera adecuada brindan una mayor probabilidad de establecer una ruta hacia los atacantes, y contar con una mayor cantidad de evidencia probatoria para el juzgamiento de los involucrados.

- La guía de procedimientos fue aplicada en un escenario de prueba, diseñado para simular una investigación forense que involucra un incidente con teléfonos celulares, así se pudo validar y mostrar la eficacia

de la guía propuesta, su efectividad en cuanto a evidencia encontrada y entrega de reportes, como también sus limitantes de aplicación.

- Las herramientas de software son un complemento significativo dentro del análisis forense de datos, puesto que brindan un aporte importante y enriquecen los resultados permitiendo tener una mejor perspectiva de la información encontrada; cabe destacar que las herramientas se encuentran en constante evolución y cada vez mejoran sus funcionalidades.

- Con la aplicación de la guía propuesta en el caso de prueba y llevado a cabo el análisis pertinente, se puede apreciar que las herramientas utilizadas sí facilitan el trabajo de análisis forense, permitiendo obtener información como mensajería, registro de llamadas, directorio telefónico, aplicaciones instalas, además de otro tipo de información considerada relevante para una investigación forense digital.

- La guía de procedimientos propuesta se encuentra orientada a la investigación forense en teléfonos celulares, sin embargo, se tiene la posibilidad de ser aplicada a otro tipo de dispositivos móviles realizando algunos cambios de acuerdo con el tipo de dispositivo a ser investigado.

- Debido al crecimiento de los peligros informáticos en el mercado móvil, que son el resultado del aumento en el uso de estos dispositivos, se evidencia que el campo de la informática forense orientada a dispositivos móviles, muestra ser un área interesante y de mucha relevancia en el contexto actual y a futuro, además se abre una importante camino en el área investigativa y profesional.

5.2. Recomendaciones

- La guía de procedimientos de análisis forense desarrollada, podrá ser utilizada como una fuente de ayuda en cualquier caso de investigación forense, donde se encuentren involucrados como parte de la evidencia dispositivos móviles.

- Concientizar a las personas en el tema de la utilización adecuada de la tecnología, de esta forma disminuir el índice de incidentes de seguridad, sean estos robos, amenazas, fraudes o estafas; especialmente en el uso de los dispositivos móviles que en la actualidad son parte de la vida cotidiana de todas las personas.

- Se sugiere la utilización de herramientas de software forense, para la aplicación de la guía, las cuales brindan un soporte y ayuda al investigador, tanto en la recolección como en el análisis de la evidencia dentro de la investigación.

- Es recomendable mantener un seguimiento e informarse de las nuevas herramientas de software forense y las actualizaciones en las mismas, a manera de poder elegir la mejor opción que facilite la recolección y análisis de la evidencia.

- El tema de la informática forense es muy amplio, por lo cual se propone que trabajos futuros se enfoquen en otros campos de análisis como correos electrónicos, bases de datos, redes, entre otros; de esta manera se podrá profundizar y contribuir en el área de la seguridad informática.

BIBLIOGRAFÍA

Agualimpia, C., & Hernandez, R. (s.f.). *Análisis forense en dispositivos móviles con Symbian OS.* Documento de maestría, Pontifica Universidad Javeriana, Dept. Ingeniería electrónica. Obtenido de http://www. criptored. upm. es/guiateoria/gt_m142e1. htm.

Android Developers. (2011). *What is Android?* Obtenido de http://developer.android.com/guide/basics/what-is-android.html

Apple Inc. (s.f.). *iOS*. Recuperado el Noviembre de 2016, de https://www.apple.com/la/

Baz Alonso, A., Ferreira Artime, I., & Alvares Rodriguez, M. (2011). *Dispositivos móviles.* Universidad de Oviedo, EPSIG Ing. Telecomunicación.

BlackBerry Limited. (s.f.). *BlackBerry*. Recuperado el Noviembre de 2016, de http://us.blackberry.com/home.html

Bryant, R., & Bryant, S. (Edits.). (2016). *Policing Digital Crime.* New York: Routledge.

Cano, J. J. (2011). *Computación forense en base de datos: conceptos y reflexiones.* Colombia: Ecopetrol S.A.

Combs, G. (2007). *Wireshark*. Recuperado el Noviembre de 2016, de https://www.wireshark.org/

COMPELSON Labs. (s.f.). *MOBILedit! Forensic*. Recuperado el Noviembre de 2016, de http://www.mobiledit.com/

Consejo de Europa. (2001). *Convenio sobre la CiberDelincuencia.* Obtenido de http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf

Costa, G., & De Franceschi, A. (2007). *Xplico*. Recuperado el Noviembre de 2016, de http://www.xplico.org/

Domínguez, F. L. (2013). *Introducción a la informática forense* . España: RA-MA Editorial.

Fookes Holding Ltd. (2005). *Aid4Mail*. Recuperado el Noviembre de 2016, de http://www.aid4mail.com/

Fuertes Rocañin, J. C., Cabrera Forneiro, J., & Fuertes Iglesias, C. (2007). *Manual de ciencias forenses.* Madrid: Arán Ediciones.

Google. (2014). *Android*. Recuperado el Noviembre de 2016, de https://www.android.com/

Hassanien, A. E., Fouad, M. M., Manaf, A. A., Zamani, M., Ahmad, R., & Kacprzyk, J. (Edits.). (2016). *Multimedia Forensics and Security: Foundations, Innovations, and Applications* (Vol. Volumen 115 de Intelligent Systems Reference Library). Springer.

Jaya, K. A. (2017). Quito, Ecuador.

Kim, K. J. (Ed.). (2015). *Information Science and Applications* (Vol. Volumen 339 de Lecture Notes in Electrical Engineering). Korea: Springer.

Martínez, J. J. (2009). *Computación forense. Descubriendo los rastros informáticos.* México: Alfaomega Grupo Editor S.A.

Microsoft. (s.f.). *sqlcmd (utilidad)*. Recuperado el Noviembre de 2016, de https://technet.microsoft.com/es-es/library/ms162773(v=sql.105).aspx

Monty McDougal. (1998). *Windows Forensic Tool Chest*. Recuperado el Noviembre de 2016, de http://www.foolmoon.net/security/wft/

Netresec. (2010). *NetworkMiner*. Recuperado el Noviembre de 2016, de http://www.netresec.com/?page=NetworkMiner

Oxygen Forensics. (s.f.). *Oxygen Forensic Analyst*. Recuperado el Noviembre de 2016, de https://www.oxygen-forensic.com/es/

Paraben Corporation. (s.f.). *E3:EMX*. Recuperado el Noviembre de 2016, de https://www.paraben.com/products/e3-emx

Perales, D. M. (2013). *UNIX a base de ejemplos.* España: Lulu.

Rios, R., Garcia, E., Garcia Cabot, A., De Marcos, L., Oton, S., Gutierrez Martinez, J. M., . . . Bar Magen, J. (2012). Accesibilidad en Smartphones para el acceso a contenidos e-learning. *III Congreso Iberoamericano sobre Calidad y Accesibilidad de la Formación Virtual (CAFVIR 2012).*

Rogers, M., & Seigfried Spellar, K. C. (Edits.). (2013). *Digital Forensics and Cyber Crime: 4th International Conference, ICDF2C 2012, Lafayette, IN, USA, October 25-26, 2012, Revised Selected Papers* (Vols. Volumen 114 de Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering). Springer.

Romeo Casabona, C. M. (1988). *Poder informático y seguridad jurídica.* Madrid: Fundesco.

Sachowski, J. (2016). *Implementing Digital Forensic Readiness: From Reactive to Proactive Process.* Syngress.

Visualware Inc. (1997). *eMailTrackerPro*. Recuperado el Noviembre de 2016, de http://www.emailtrackerpro.com/

Wondershare. (s.f.). *Dr.Fone*. Recuperado el Noviembre de 2016, de https://drfone.wondershare.com/

GLOSARIO DE TÉRMINOS

ADFM: Abstract Digital Forensics Model.

Antiespam: Herramienta que se encarga de controlar el correo basura en los servidores de email o correo electrónico.

Cadena de custodia: El mecanismo que garantiza la autenticidad de los elementos de prueba recolectados y examinados, esto es, que las pruebas correspondan al caso investigado, sin que dé lugar a confusión, adulteración, ni sustracción alguna. (Fuertes Rocañin, Cabrera Forneiro, & Fuertes Iglesias, 2007)

CFFTPM: Cyber Forensics Field Triage Process Model.

Código abierto: Termino usado para definir programas que son distribuidos libremente, y además su código de desarrollo no es secreto, ni está sujeto a ningún tipo de licencia.

Darwin BSD: Es el sistema operativo base para la construcción del sistema operativo de Apple, conocido como Mac OS X.

DFRWS: Digital Forensic Research Workshops.

GCFIM: Generic Computer Forensic Investigation Model.

GPS: Global Positioning System.

Handheld: Se define como un dispositivo o computador portátil, de tamaño reducido que pueda ser fácilmente sostenido en la mano.

IMEI: International Mobile Station Equipment Identity, identificador único de los dispositivos móviles a nivel mundial.

IoT: Internet of Things

Multiplataforma: Es una característica que se asigna a programas que tienen el poder de funcionar de manera similar en diferentes sistemas operativos o plataformas.

Paquete de red: Conocido también como paquete de datos, es cada bloque en que se divide la información que es enviada a través de la red.

Paraben Corporation: Paraben es una empresa que propone soluciones para dispositivos móviles, smartphone, correo electrónico y sistemas forenses de juegos. Paraben ha estado forjando nuevos enfoques para hacer frente a la evidencia digital, y soporta imágenes lógicas y físicas en dispositivos móviles y en el 100% de los teléfonos inteligentes en el mercado. (Paraben Corporation, n.d.)

Perpetrador: Persona que comete un delito o una falta grave.

Phishing: Método utilizado por delincuentes para obtener datos personales e información confidencial de manera ilícita a través de internet.

Plataforma: Es un sistema que sirve como base para la ejecución de aplicaciones compatibles con el mismo.

Redes de datos: Conjunto de ordenadores conectados entre sí, con el objetivo de compartir recursos, información y servicios.

RIM: Research In Motion.

Servidor: Es una unidad informática que realiza tareas y brinda diversos servicios a otros ordenadores, conocidos como usuarios.

Spam: Son los mensajes no solicitados, también conocido como correo basura o correo no deseado.

Trafico de red: Es la cantidad de datos enviados y recibidos que viajan a través de la red.

Unix: Es un sistema operativo multiusuario, multitarea, portable, con distintos intérpretes de comandos, multiprocesador, multicore, con compiladores propios, con entorno gráfico, entre otras características. (Perales, 2013)

ANEXOS

Anexo A. Archivos adjuntos del informe de la investigación

- **Formulario de designación de responsables**

Fecha de designación de roles	12/01/2017					
Código del caso	P001					
Descripción del caso	Caso de Prueba					
Rol designado	**Nombre**	**Apellido**	**Fecha de designación de rol**	**Cédula**	**Teléfono**	**Firma**
Custodio de la evidencia	Katherine	Jaya	12/01/2017	1720579233	0984664253	
Investigador forense	Katherine	Jaya	12/01/2017	1720579233	0984664253	
Examinador forense	Katherine	Jaya	12/01/2017	1720579233	0984664253	
Analista forense	Katherine	Jaya	12/01/2017	1720579233	0984664253	

Fuente: (Jaya, 2017)

- **Formulario de documentación del estado inicial**

Fecha del incidente:	10/01/2017
Código del caso:	P001
Detalles del incidente:	Seguimiento de actividades en dispositivos empresariales
Dirección del incidente:	De los Pinos y Av. Eloy Alfaro
Nombre y apellidos del investigador responsable:	
Katherine Jaya Cáceres	
FOTOGRAFÍAS	
Escena del crimen	

Ilustración 79 Personal de la empresa

Fuente: http://www.liderhoy.com/imagenes/personal-de-la

-empresa-y-ejecutivos.jpg

Dispositivo				

Ilustración 80 Dispositivo objeto de análisis

Fuente: (Jaya, 2017)

Existencia de VIDEOS	**SI**		**NO**	X

Fuente: (Jaya, 2017)

- **Formulario de identificación del dispositivo**

ESTADO Y CARACTERÍSTICAS DEL DISPOSITIVO				
Estado del dispositivo	**Encendido**	X	**Apagado**	
Protegido por clave	**SI**	X	**NO**	
En caso de tener protección (Tipo)				
Contraseña				
PIN	23071986			
Patrón				
Huella digital				
Reconocimiento facial				
Otro tipo de protección (Especifique)				
Características				
Marca del teléfono	Samsung			
Modelo del teléfono	Galaxy J5			
Número de teléfono	0998735493			
Operadora del servicio	Movistar			
Numero serial IMEI	352141078496649			
DOCUMENTACIÓN EXTRA DEL DISPOSITIVO				
	SI		**NO**	
Manuales de usuario	X			
Memorias extraíbles	X			
Cargadores	X			
Facturas de adquisición	X			
Códigos de acceso			X	

Fuente: (Jaya, 2017)

- **Reportes generados por la herramienta MOBILedit! Forensic**

Información general del dispositivo

MOBILedit FORENSIC

PHONE CONTENT REPORT

Manufacturer	Samsung
Product	Galaxy J5
Platform	android
SW revision	6.0.1 (23)
Returned IMEI	352141078496649
IMEI	352141078496649
Device time	01/25/2017 17:11:38

Device Information

Device Label	Samsung Galaxy J5 (25/01/2017 16:43:39)
Device Name	Samsung Galaxy J5

Sim card

Imsi	740000103179682
Iccid	8959300500602829694

Investigator Information

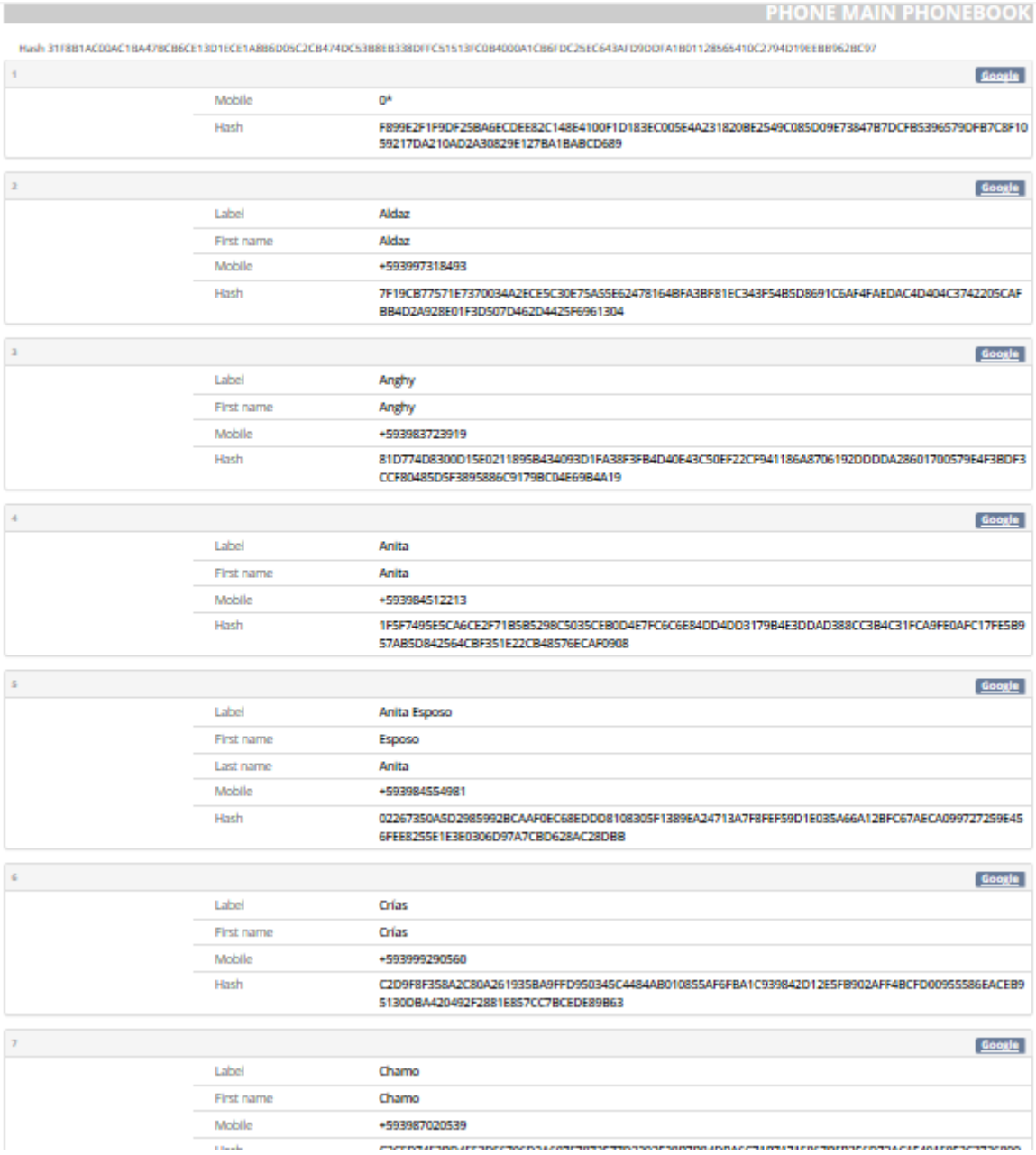
Investigator Name	Katherine Jaya
Investigator Email	
Investigator Phone Number	

Extraction Information

Data Extraction Started	01/25/2017 16:43:33
Data Extraction Finished	01/25/2017 17:07:02
Extracted by	MOBILedit Forensics 8.7.1.21224

Fuente: (Jaya, 2017)

Directorio telefónico (Google)



PHONE MAIN PHONEBOOK

Hash 31F8B1AC00AC1BA478CB6CE13D1ECE1A886D05C2CB474DC53B8EB338DFFC51513FC0B4000A1CB6FDC25EC643AFD9DDCFA1B0112856541OC2794D19EEBB962BC97

1 — Google

Mobile	0*
Hash	FB99E2F1F9DF25BA6ECDEE82C148E4100F1D183EC005E4A231820BE2549C085D09E73847B7DCFB5396579OFB7C8F1059217DA210AD2A30829E127BA1BABCD689

2 — Google

Label	Aldaz
First name	Aldaz
Mobile	+593997318493
Hash	7F19CB77571E7370034A2ECE5C30E75A55E62478164BFA3BF81EC343F54B5D8691C6AF4FAEDAC4D404C3742205CAFBB4D2A928E01F3D507D462D4425F6961304

3 — Google

Label	Anghy
First name	Anghy
Mobile	+593983723919
Hash	81D774D8300D15E0211895B434093D1FA38F3FB4D40E43C50EF22CF941186A8706192DDDDA28601700579E4F3BDF3CCF80485D5F3895886C9179BC04E69B4A19

4 — Google

Label	Anita
First name	Anita
Mobile	+593984512213
Hash	1F5F7495E5CA6CE2F7185B5298C5035CEB0D4E7FC6C6E84DD4DD3179B4E3DDAD388CC3B4C31FCA9FE0AFC17FE5B957AB5D842564CBF351E22CB48576ECAF0908

5 — Google

Label	Anita Esposo
First name	Esposo
Last name	Anita
Mobile	+593984554981
Hash	02267350A5D2985992BCAAF0EC68EDDD8108305F1389EA24713A7F8FEF59D1E035A66A12BFC67AECA0997272S9E456FEE8255E1E3E0306D97A7CBD628AC28DBB

6 — Google

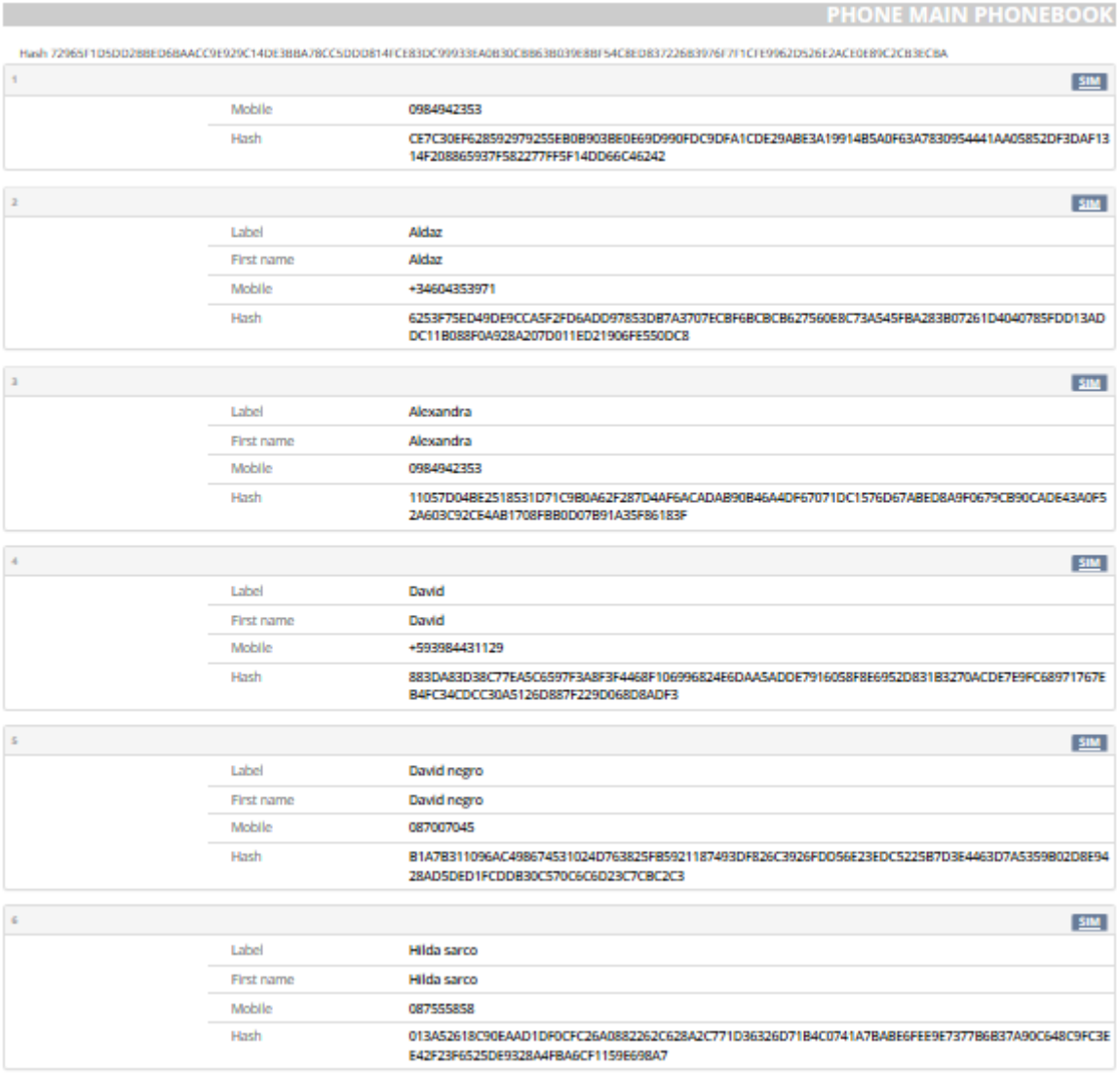
Label	Crías
First name	Crías
Mobile	+593999290560
Hash	C2D9F8F358A2C80A261935BA9FFD950345C4484AB010855AF6FBA1C939842D12E5FB902AFF4BCFD00955586EACEB95130DBA420492F2881E857CC7BCEDE89B63

7 — Google

Label	Chamo
First name	Chamo
Mobile	+593987020539
Hash	

Fuente: (Jaya, 2017)

Directorio telefónico (SIM)



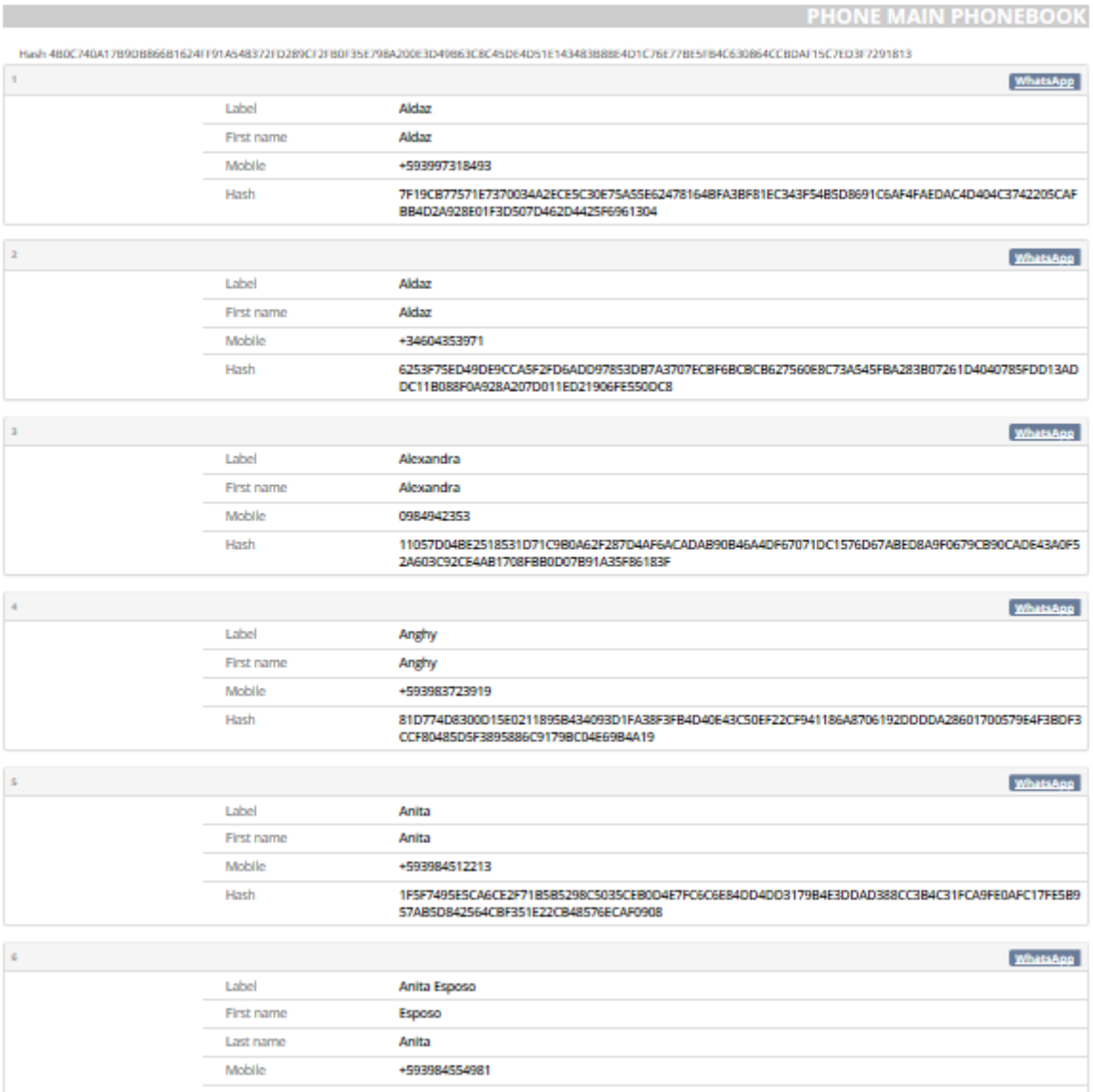
PHONE MAIN PHONEBOOK

Hash: 72965F1D5DD288ED68AACC9E929C14DE3B8A78CC5DDD814FCE83DC99933EA0B30CB863B039E8BF54C8ED837226B3976F7F1CFE9062D5262E2ACE0E89C2CB3ECBA

1		SIM
	Mobile	0984942353
	Hash	CE7C30EF628592979255EB0B903BE0E69D990FDC9DFA1CDE29ABE3A19914B5A0F63A7830954441AA0S852DF3DAF1314F208865937F582277FF5F14DD66C46242
2		SIM
	Label	Aldaz
	First name	Aldaz
	Mobile	+34604353971
	Hash	6253F75ED49DE9CCA5F2FD6ADD97853DB7A3707ECBF6BCBCB627560E8C73A545FBA283B07261D4040785FDD13ADDC11B088F0A928A207D011ED21906FE550DC8
3		SIM
	Label	Alexandra
	First name	Alexandra
	Mobile	0984942353
	Hash	11057D04BE2518531D71C9B0A62F287D4AF6ACADAB90B46A4DF67071DC1576D67ABED8A9F0679CB90CADE43A0F52A603C92CE4AB1708FBB0D07B91A35FB6183F
4		SIM
	Label	David
	First name	David
	Mobile	+593984431129
	Hash	883DA83D38C77EA5C6597F3A8F3F4468F106996824E6DAA5ADDE7916058F8E6952D831B3270ACDE7E9FC68971767EB4FC34CDCC30A5126D887F229D068D8ADF3
5		SIM
	Label	David negro
	First name	David negro
	Mobile	087007045
	Hash	B1A7B311096AC49867453102 4D76382SFB5921187493DF826C3926FDD56E23EDC5225B7D3E4463D7A5359B02DBE9428AD5DED1FCDDB30C570C6C6D23C7CBC2C3
6		SIM
	Label	Hilda sarco
	First name	Hilda sarco
	Mobile	087555858
	Hash	013A52618C90EAAD1DF0CFC26A0882262C628A2C771D36326D71B4C0741A7BABE6FEE9E7377B6B37A90C648C9FC3EE42F23F6525DE9328A4FBA6CF1159E698A7

Fuente: (Jaya, 2017)

Directorio telefónico (WhatsApp)



PHONE MAIN PHONEBOOK

Hash 4B0C740A17B9DB866B1624FF91A548372FD289CF2FB0F35E798A200E3D49863C8C45DE4D51E143483B88E4D1C76E77BE5FB4C630864CCBDAF15C7ED3F7291813

1 — WhatsApp

Label	Aldaz
First name	Aldaz
Mobile	+593997318493
Hash	7F19CB77571E7370034A2ECE5C30E75A55E62478164BFA3BF81EC343F54B5D8691C6AF4FAEDAC4D404C3742205CAFBB4D2A928E01F3D507D462D4425F6961304

2 — WhatsApp

Label	Aldaz
First name	Aldaz
Mobile	+34604353971
Hash	6253F75ED49DE9CCA5F2FD6ADD97853DB7A3707ECBF6BCBCB627560E8C73A545FBA283B07261D4040785FDD13ADDC11B088F0A928A207D011ED21906FE550DC8

3 — WhatsApp

Label	Alexandra
First name	Alexandra
Mobile	0984942353
Hash	11057D04BE2518531D71C9B0A62F287D4AF6ACADAB90B46A4DF67071DC1576D67ABED8A9F0679CB90CADE43A0F52A603C92CE4AB1708FBB0D07B91A35FB6183F

4 — WhatsApp

Label	Anghy
First name	Anghy
Mobile	+593983723919
Hash	81D774D8300D15E0211895B434093D1FA38F3FB4D40E43C50EF22CF941186A8706192DDDDA28601700579E4F3BDF3CCF80485D5F3895886C9179BC04E69B4A19

5 — WhatsApp

Label	Anita
First name	Anita
Mobile	+593984512213
Hash	1F5F7495E5CA6CE2F71B5B5298C5035CEB0D4E7FC6C6E84DD4DD03179B4E3DDAD388CC3B4C31FCA9FE0AFC17FE5B957AB5D842564CBF351E22CB48576ECAF0908

6 — WhatsApp

Label	Anita Esposo
First name	Esposo
Last name	Anita
Mobile	+593984554981

Fuente: (Jaya, 2017)

Registro de llamadas (perdidas)

PHONE MISSED CALLS

Hash 4CB50F4E25C29C66D561BB27CABA60880CCD1BF69A2943C0C92E3B65676159CD16212A51C27B1E916119FAE634C4BD97AEC9ED82C58C33ADAB7D0F4376AAE35C

	Label	From	To	Time	Duration
1	Guichon	0984980331		01/22/2017 17:32:16	00:00:00
2	Guichon	0984980331		01/22/2017 10:47:11	00:00:00
3	Guichon	0984980331		01/22/2017 09:08:00	00:00:00
4	Chamo	0987020539		01/21/2017 13:09:57	00:00:00
5	Chamo	0987020539		01/21/2017 13:07:30	00:00:00
6	Chamo	0987020539		01/21/2017 13:06:17	00:00:00
7	Chamo	0987020539		01/16/2017 13:06:42	00:00:00
8	Chamo	0987020539		01/13/2017 16:27:10	00:00:00
9	Chamo	0987020539		01/13/2017 15:54:32	00:00:00
10	Chamo	0987020539		01/13/2017 15:46:15	00:00:00
11	Chamo	0987020539		01/13/2017 15:45:28	00:00:00
12	Chamo	0987020539		01/13/2017 15:44:43	00:00:00
13	Chamo	0987020539		01/13/2017 15:43:50	00:00:00

Fuente: (Jaya, 2017)

Registro de llamadas (realizadas)

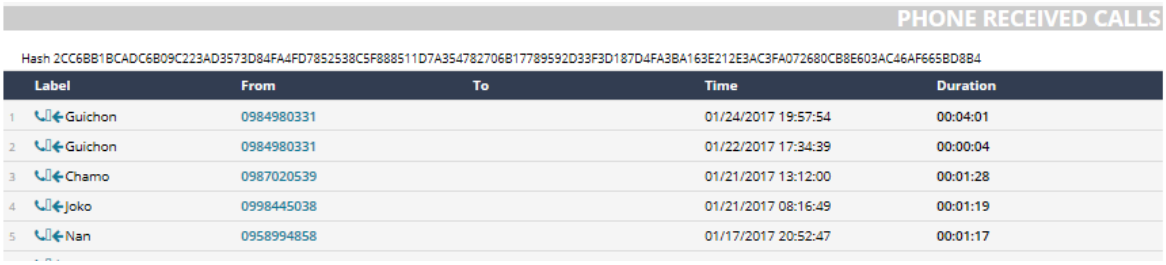
PHONE DIALED NUMBERS

Hash 8A5CF10F26EABF377C52DFAB5A33C93514D2B4986BA966F38A305B3550FE9C5471970C195D63C9E46DC17114971B96A75EDACBA263C4FC5181238986D0CFF832

	Label	From	To	Time	Duration
1	Guichon		0984980331	01/22/2017 17:35:57	00:00:00
2	Guichon		0984980331	01/22/2017 17:35:36	00:00:00
3	Guichon		0984980331	01/22/2017 17:35:06	00:00:00
4	Nan		+593958994858	01/21/2017 21:30:10	00:00:06
5	Nan		+593958994858	01/21/2017 21:04:03	00:00:35
6	Chamo		0987020539	01/21/2017 13:11:22	00:00:15
7	Chamo		+593987020539	01/21/2017 12:53:42	00:00:02
8	Chamo		+593987020539	01/19/2017 13:58:58	00:00:15
9			5939832341215	01/18/2017 14:17:30	00:00:00
10			*001	01/18/2017 11:20:08	00:00:04
11	Katy nena		0984664252	01/18/2017 11:19:46	00:00:00
12	Nan		+593958994858	01/17/2017 21:13:23	00:01:05
13	Nan		+593958994858	01/17/2017 20:59:36	00:01:16

Fuente: (Jaya, 2017)

Registro de llamadas (recibidas)



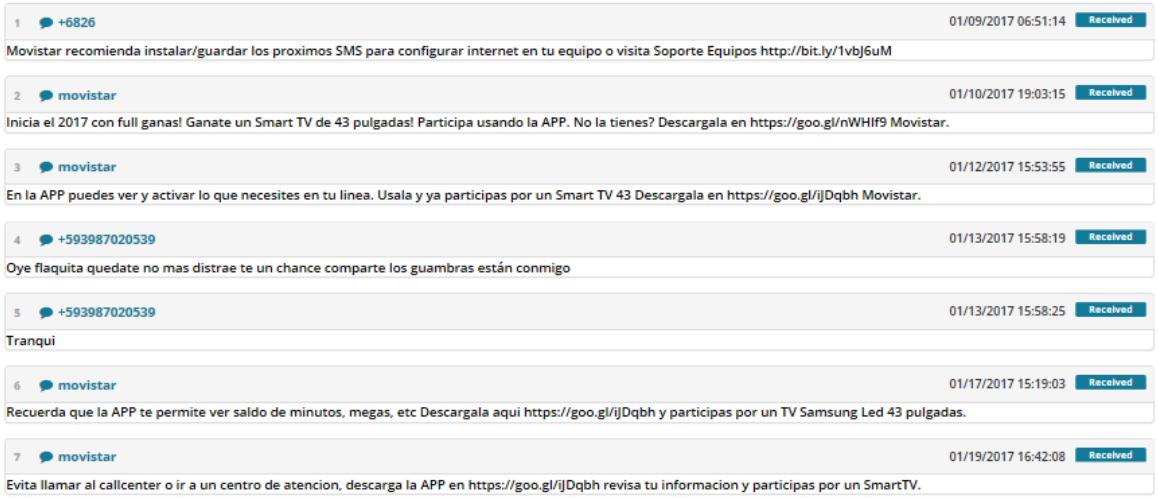
PHONE RECEIVED CALLS

Hash 2CC6BB1BCADC6B09C223AD3573D84FA4FD7852538C5F888511D7A354782706B17789592D33F3D187D4FA3BA163E212E3AC3FA072680CB8E603AC46AF665BD8B4

	Label	From	To	Time	Duration
1	Guichon	0984980331		01/24/2017 19:57:54	00:04:01
2	Guichon	0984980331		01/22/2017 17:34:39	00:00:04
3	Chamo	0987020539		01/21/2017 13:12:00	00:01:28
4	Joko	0998445038		01/21/2017 08:16:49	00:01:19
5	Nan	0958994858		01/17/2017 20:52:47	00:01:17

Fuente: (Jaya, 2017)

Mensajes



1	+6826	01/09/2017 06:51:14	Received

Movistar recomienda instalar/guardar los proximos SMS para configurar internet en tu equipo o visita Soporte Equipos http://bit.ly/1vbJ6uM

2	movistar	01/10/2017 19:03:15	Received

Inicia el 2017 con full ganas! Ganate un Smart TV de 43 pulgadas! Participa usando la APP. No la tienes? Descargala en https://goo.gl/nWHIf9 Movistar.

3	movistar	01/12/2017 15:53:55	Received

En la APP puedes ver y activar lo que necesites en tu linea. Usala y ya participas por un Smart TV 43 Descargala en https://goo.gl/ijDqbh Movistar.

4	+593987020539	01/13/2017 15:58:19	Received

Oye flaquita quedate no mas distrae te un chance comparte los guambras están conmigo

5	+593987020539	01/13/2017 15:58:25	Received

Tranqui

6	movistar	01/17/2017 15:19:03	Received

Recuerda que la APP te permite ver saldo de minutos, megas, etc Descargala aqui https://goo.gl/ijDqbh y participas por un TV Samsung Led 43 pulgadas.

7	movistar	01/19/2017 16:42:08	Received

Evita llamar al callcenter o ir a un centro de atencion, descarga la APP en https://goo.gl/ijDqbh revisa tu informacion y participas por un SmartTV.

Fuente: (Jaya, 2017)

Datos de la aplicación

APPLICATIONS DATA

Filename	Size	Created	Modified	Accessed
Content Providers				
Hash 07D9008D6DF1FD502DA0E6FB114ABF37B28C977C54349FFC18D215004F9D7556ECCD0F1629CF8A6A4379D6E70B3A1E6D9BDC6060596A1E0E895966C05D455594				
Accounts.xml				
Hash BDA4E9EB8D86FE36F8FE4AAEBED9F481E204FE34A365543A1D904E8E988ED9EAA774D3673AF6D7860C57741D5E82AE24F70D8C5C5B10B52EDCACC01BC2AAA5C2				
BluetoothBonded.xml				
Hash 4BC19FA1E3BD3B9A7CE88843281ADADE1B6B55A33707328026BE282E6E7A3954EDE0359C8F62E53B72215667ED38F1B49CDED70EC68038DB6BB5EC0933F33A3B				
CalendarAttendees.xml				
Hash 385A81622F4C521E0ABB184D74A86B639273D974CDCA3EBB2246B61CE32855C88E4C73F78390A5C175BF773E516C02BB5A06EBE7F0B1C6FC9AFB7469B7A95CD2				
CalendarEvents.xml				
Hash 46ABC091FAF44FAD782AE88753D54B1664A383DFF2FD4CE3A2CBB4848A720C06460DFF84F36F23B4DA1A50BF654365F36F5F2C3AB5450502CECB942788EDF3E3				
CalendarReminders.xml				
Hash 41540B9A75E9491D74B56C3DBB95326DDF3BC7BA5E4B71C5E9AFF26407DC8EBF93CC4B7F54C44B8E609C0F6E2D7E3A625622843364E3BA933CE1D7F8E5BAABE2				
Calendars.xml				
Hash C925A2FC0FE86624095CADF272E80A0A86D92EAFE655AE42F51B2FA56E26FAB279826C0C9A48D31A59CAE0C133F08859D4482E55EDA2F5F15E599C4022606D2E				
Calls.xml				
Hash 802918CF5089E26A41974C45237B3D28E1A21BA1A6E8F9A7EAAC62868BDC5ACA8412D92757E8F5DE3A3FA27F4B57CCF6078CDE8971701F89C191D749743E1C96				
ContactsData.xml				
Hash E2E802F07EDA626964689ABBF9A29EFE0BEB326E288F9DEF30BFA691903FA9BDF425ADA2FFE29606S4073977CB006C33FF7DDD166CE6E1DDFF1321107B4EBB70				
ContactsException.xml				
Hash FFE4906C0A06CF3F4B4CDC18F65BB1FD61BEBE9C228EC4D60DF595ECC3F6C10E02A532E8F224FA7E8E5C069232C267838AB3D63FDEE500A3BD30EBA820F927F8				
ContactsGroups.xml				

Fuente: (Jaya, 2017)

Aplicaciones

APPLICATIONS

Filename	Size	Created	Modified	Accessed
parambackup.target				
Hash CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3E				
android				
Hash E16A35873EAB93BD01B5B45AFBB1ECDAFEFE406BAD89BA2C6037A1F121DD6ED0D97AF3EBC001BBED7D5B610F52F6D9149F8EEB57B07BD790A8C2E2A897D24A0D				
description.info				
Hash 1A494A27C41B1183EB12FA1CD0C6AC7792A24ECCB7D7B13972E17B52C954107E3C4495506B4F25E1FFEFFE3A3FBB0D06BCD8A1F9820E7081DF8B5CA71E1A9660				
icon.png				
Hash 2A8E24BCB5A1CDD4E007CC52BCE27CCC02B910BED1C3B0B638C7F08C7838E80C94F7AE4952A597E110C10432B62E4475A8870525F3ABE9C23EF9FFCD38F99572				
com.android.backupconfirm				
Hash 2CA39709172D28F71BABA78111AB55CF834AF712D38735196D5D49B9AB3DD8CBA11B07C7A4630543F14C85337042585B1B4CAA0CCDDF2141B5BD8F4DF27A9946				
description.info				
Hash FFB8C16A2464ACC16D17BFB5EBC52A3C5CC964F8D489CAA2F15389FE226D511CCE2BAED5A60706E6E0A3DD221B3CCCBC3F0604735D2027B55F9FAB6C43724FFB				
com.android.bluetooth				
Hash 7A85270EC9BE5D758D4C52E0A1A5AC0FC383A169F47437F61732ED926448E3F2988FE7FEA67D7A66CB24FAC83B3AB2187EFCEFDE8761E1D900F611B2310F1D28				
description.info				
Hash AC1C3BD8AA266F6595C2821210F13E1C719A96CCE35D1B982144180A1D1D365A642AD2F5C04ADC7F493E4907467B125BCC343377954D33ADA4FEE35EEA2E9540				
icon.png				
Hash D0CA2DEB3FD881CE28A329C0D3D9E7FF6554EA6CFE93C6D497A7D83289C46C2D2D6EFEE5A0A27AEBD369A8CBC0BF5AAF369E9AC78C9B7878EFB20B5E5A661048				
com.android.bluetoothmidiservice				

Fuente: (Jaya, 2017)

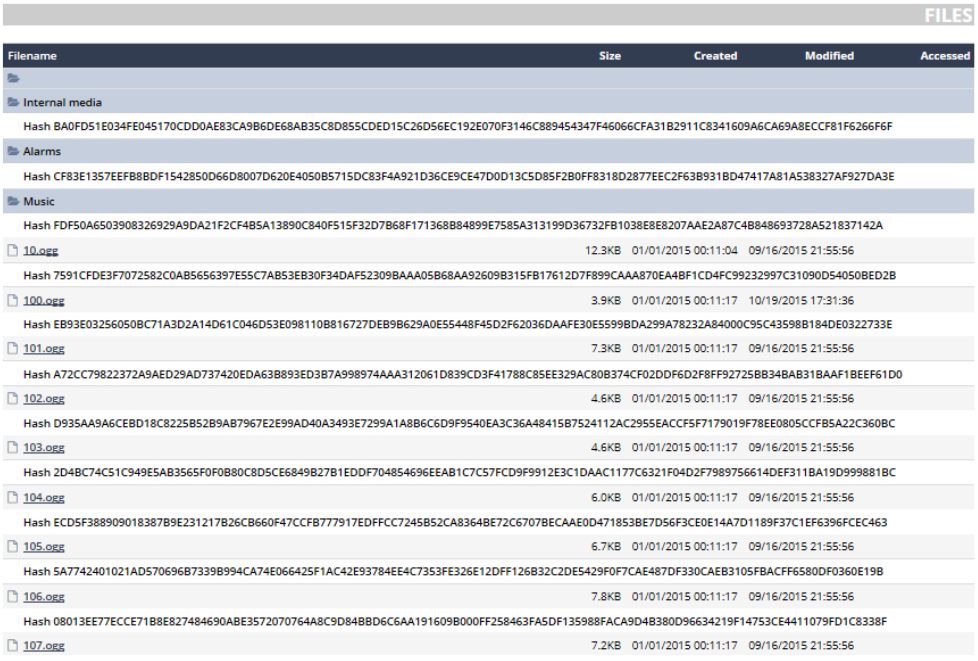
Archivos

FILES

Filename	Size	Created	Modified	Accessed
.SPenSDK30				
Hash A0CE37755F585CED140A9C34C8C4C140A5DF88137AAD719025FCE035B2EC488541A89AB214C6DE3081916EEBA8944178BE8F0E20935706AAE39B0196B1D3012C				
.nomedia	0B	01/12/2017 18:20:25	01/12/2017 18:20:25	
Hash CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3E				
.Studio				
Hash D26481D43670C741DDAF568E3ED09C4D765E59D7DC11E9BF0EFB4FCC1F9F9EE68FEF317767718A876A66046DC5AB2DC11F4AC286AF9B97F95DB6904518F01339				
tempHistoryInfo				
Hash CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3E				
.facebook_cache				
Hash A3B2C17438F6EE951D7B816358945FF80FD4F2531331EC0C9F451EE12728B6AFE71CBF3905FE98FAA152FBC155513069599B483027A7C38AAE379CF008BCDC5F				
journal	31B	01/14/2017 16:44:45	01/14/2017 16:44:45	
Hash 3B1C12394F2D267F56B47E25B4257898008EE55121AEE06DFF09E4372105DD1DA2123BA692C863A2BC3CD8542413DAB7D7CFC88948A7B80279C8D4A3224638DF				
Alarms				
Hash CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3E				
Android				
Hash 8277BB9CD410F9E317CFC882D904C8D0304469548439B10D14197EE57F4AD266B625C78E0C5AD614C15E28464522FF02DEF16CB378C4781EB7F6A5A26522286C				
data				
Hash 95CAC06C7DDA794875909DEF5C6EA093616847CD1A534253AFE64BD854E6A0C082ABA79174E0AC3FF4D58F58F14075DA274A43CFF6A84C80D622FBE791BAEB03				
.nomedia	0B	12/31/2014 19:10:30	12/31/2014 19:10:30	
Hash CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3E				
com.android.calendar				
Hash 3C6B038F81D3DB169D78BA42FB67FF14EBEE609226025E1C0C11F036F4A31FBD62564FC06708AD221A6C3C3523DD4CA8465C7F01BED620254212F3E47DB622A4				

Fuente: (Jaya, 2017)

Archivos multimedia



FILES

Filename	Size	Created	Modified	Accessed
Internal media				
Hash BA0FD51E034FE045170CDD0AE83CA9B6DE68AB35C8D855CDED15C26D56EC192E070F3146C889454347F46066CFA31B2911C8341609A6CA69A8ECCF81F6266F6F				
Alarms				
Hash CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3E				
Music				
Hash FDF50A6503908326929A9DA21F2CF4B5A13890C840F515F32D7B68F171368B84899E7585A313199D36732FB1038E8E8207AAE2A87C4B848693728A521837142A				
10.ogg	12.3KB	01/01/2015 00:11:04	09/16/2015 21:55:56	
Hash 7591CFDE3F7072582C0AB5656397E55C7AB53EB30F34DAF52309BAAA05B68AA92609B315FB17612D7F899CAAA870EA4BF1CD4FC99232997C31090D54050BED2B				
100.ogg	3.9KB	01/01/2015 00:11:17	10/19/2015 17:31:36	
Hash EB93E03256050BC71A3D2A14D61C046D53E098110B816727DEB9B629A0E55448F45D2F62036DAAFE30E5599BDA299A78232A84000C95C43598B184DE0322733E				
101.ogg	7.3KB	01/01/2015 00:11:17	09/16/2015 21:55:56	
Hash A72CC79822372A9AED29AD737420EDA63B893ED3B7A998974AAA312061D839CD3F41788C85EE329AC80B374CF02DDF6D2F8FF92725BB34BAB31BAAF1BEEF61D0				
102.ogg	4.6KB	01/01/2015 00:11:17	09/16/2015 21:55:56	
Hash D935AA9A6CEBD18C8225B52B9AB7967E2E99AD40A3493E7299A1A8B6C6D9F9540EA3C36A48415B7524112AC2955EACCF5F7179019F78EE0805CCFB5A22C360BC				
103.ogg	4.6KB	01/01/2015 00:11:17	09/16/2015 21:55:56	
Hash 2D4BC74C51C949E5AB3565F0F0B80C8D5CE6849B27B1EDDF704854696EEAB1C7C57FCD9F9912E3C1DAAC1177C6321F04D2F7989756614DEF311BA19D999881BC				
104.ogg	6.0KB	01/01/2015 00:11:17	09/16/2015 21:55:56	
Hash ECD5F388909018387B9E231217B26CB660F47CCFB777917EDFFCC7245B52CA8364BE72C6707BECAAE0D471853BE7D56F3CE0E14A7D1189F37C1EF6396FCEC463				
105.ogg	6.7KB	01/01/2015 00:11:17	09/16/2015 21:55:56	
Hash 5A7742401021AD570696B7339B994CA74E066425F1AC42E93784EE4C7353FE326E12DFF126B32C2DE5429F0F7CAE487DF330CAEB3105FBACFF6580DF0360E19B				
106.ogg	7.8KB	01/01/2015 00:11:17	09/16/2015 21:55:56	
Hash 08013EE77ECCE71B8E827484690ABE3572070764A8C9D84BBD6C6AA191609B000FF258463FA5DF135988FACA9D4B380D96634219F14753CE4411079FD1C8338F				
107.ogg	7.2KB	01/01/2015 00:11:17	09/16/2015 21:55:56	

Fuente: (Jaya, 2017)