UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CARRERA DE SOFTWARE

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIEROS EN SOFTWARE

FORMA: PROYECTO DE INVESTIGACIÓN

TEMA:

ANÁLISIS FORENSE UTILIZANDO HERRAMIENTAS OPEN-SOURCE EN DISPOSITIVOS MÓVILES DETERIORADOS

AUTORES:

Jerson Ismael Chimbo Fernández
Henry Estiben Sinche Pilco

DIRECTOR:
Ing. Jesús Coloma

GUARANDA-ECUADOR

2023

TEMA DEL PROYECTO DE INVESTIGACIÓN

ANÁLISIS FORENSE UTILIZANDO HERRAMIENTAS OPEN-SOURCE EN DISPOSITIVOS MÓVILES DETERIORADOS.

AGRADECIMIENTO

Agradecido con Dios por brindarme salud y vida en todo momento, también a la "Universidad Estatal de Bolívar" por haberme permitido formarme en ella y obtener un gran conocimiento impartido por todos los docentes que han sido parte de mi formación profesional, y a la vez agradecerle de manera especial, al Ingeniero Jesus Coloma director de mi proyecto de investigación quien nos ha guiado con su paciencia, con su dirección, conocimiento, enseñanza y colaboración para la culminación de nuestro proyecto con éxito.

También agradezco a mis padres María Fernandez y Segundo Chimbo, hermanos y familiares quienes han sido muy importantes en mi formación académica, quienes me han inculcado muchos valores, humildad, perseverancia, valentía y responsabilidad en mi para así lograr cumplir mis metas.

Chimbo Fernandez Jerson Ismael

Agradezco a la "Universidad Estatal de Bolívar" por ser escenario del conocimiento obtenido, a sus docentes quienes han compartido su conocimiento siendo guía durante esta etapa de mi vida.

A mi familia, en especial a mi madre Gloria Pilco y a mi padre Milton Sinche quienes han sido cimiento para mi formación académica, quienes han inculcado en mí responsabilidad, perseverancia, humildad y valentía, quienes me han brindado apoyo incondicional convirtiéndose en inspiración para alcanzar mis metas.

Sinche Pilco Henry Estiben

DEDICATORIA

Este trabajo dedico primordialmente a Dios, quien ha sido mi guía y me ha dirigido por el camino correcto, por brindarme sabiduría y fuerza para poder alcanzar cada una de mis metas tanto personal como profesional.

Con mucho amor y gratitud a mis padres, por su amor, por los consejos, valores, principios y apoyo incondicional, lo que me ha dado la fortaleza necesaria para continuar en este arduo camino hacia el éxito de mi carrera profesional.

Chimbo Fernandez Jerson Ismael

Todos mis triunfos y logros se los he dedicado a Dios y mi familia, dedico este logro a mis padres que sé que cada triunfo mío es un triunfo para ellos, ellos que son quienes me apoyan y brindar su amor incondicional, están conmigo en cada momento, así este logro es mas de ellos que mío y se los dedico con todo mi cariño.

Sinche Pilco Henry Estiben

UEB
UNIVERSIDAD ESTATAL DE BOLIVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CERTIFICADO DE VALIDACIÓN

Ing. Jesús Coloma, Dra. Edelmira Guevara y Lic. Edgar Rivadeneira, en su orden Director y Pares Académicos del Trabajo de Integración Curricular "ANÁLISIS FORENSE UTILIZANDO HERRAMIENTAS OPEN SOURCE EN DISPOSITIVOS MÓVILES DETERIORADOS" desarrollado por los señores Chimbo Fernández Jerson Ismael y Sinche Pilco Henry Estiben.

CERTIFICAN

Que, luego de revisado el Trabajo de Integración Curricular en su totalidad, cumple con las exigencias académicas de la carrera SOFTWARE, por lo tanto, autorizamos su presentación y defensa.

Guaranda, 17 de noviembre del 2022

Ing. Jesús Coloma
Director

Dra. Edelmira Guevara
Par Académico

Lic. Edgar Rivadeneira
Par Académico

DERECHOS DE AUTOR

Nosotros, **Jerson Ismael Chimbo Fernandez y Henry Estiben Sinche Pilco** portadores de las cédulas de identidad **N° 0202123691** y **0250136330** respectivamente**,** en calidad de autores y titulares de los derechos morales y patrimoniales del Trabajo de Titulación: **ANÁLISIS FORENSE UTILIZANDO HERRAMIENTAS OPEN-SOURCE EN DISPOSITIVOS MÓVILES DETERIORADOS**, modalidad Trabajo de Integración Curricular, de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, concedemos a favor de la Universidad Estatal de Bolívar, una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservamos a mi/nuestro favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizamos a la Universidad Estatal de Bolívar para que realice la digitalización y publicación de este trabajo de titulación el Repositorio Digital, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El (los) autor (es) declara (n) que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Firmado electrónicamente por:
JERSON ISMAEL CHIMBO FERNANDEZ

Jerson Ismael Chimbo Fernandez
CI. 0202123691

Firmado electrónicamente por:
HENRY ESTIBEN SINCHE PILCO

Henry Estiben Sinche Pilco
CI. 0250136330

ÍNDICE DE CONTENIDO

TABLA DE ILUSTRACIONES

TABLAS

INTRODUCCIÓN

En la actualidad, el uso de los dispositivos móviles con sistema operativo Android ha tenido un crecimiento significativo e innovador en la comunicación, sin embargo, el uso de la tecnología ha fomentado el crecimiento de actividades ilícitas por lo que surge la necesidad de realizar investigaciones periciales a través del análisis forense. Estos actos ilícitos nos conducen hacia el ámbito de la informática forense, misma que aplica métodos, técnicas y herramientas que permitirá realizar la extracción de información de dispositivos con sistema operativo Android y como resultado obtener pruebas que sirvan como evidencia en un proceso judicial.

El ámbito del análisis forense, es un campo muy amplio, que cada vez va ganando terreno debido a diferentes situaciones que implican el uso de la tecnología, estas situaciones varían desde ambientes laborales hasta asuntos de seguridad nacional.

Según (Lopez L. F., 2017) el FBI define a la informática forense como: "la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en medios computacionales". Es necesario una descripción detallada de cada una de las fases para comprender su significado:
La adquisición: es la recolección del dispositivo para su posterior análisis.
La preservación: mantiene el dispositivo móvil tal cual como se lo adquirió sin afectar su integridad, es decir evita su alteración con el fin de preservar la información contenida en el dispositivo.
La obtención: es el proceso de validación y obtención de la imagen forense.
La presentación: en esta fase se expone los resultados obtenidos luego del análisis forense. La presente investigación tiene por objetivo la extracción de información a través de análisis forense de dispositivos móviles deteriorados usando herramientas de software libre y consta de 4 capítulos. Estos capítulos tocan temas como los antecedentes donde se detallan las investigaciones previas sobre la informática forense; así como su definición; selección de la metodología adecuada; las herramientas y técnicas a utilizar de acuerdo los escenarios planteados. Así mismo, todo el reglamento legal que respalda la investigación.

De igual forma detalla los procedimientos que deben llevar a cabo para la extracción de información a través del análisis forense, además, aporta información acerca de las herramientas del software libre utilizados en la ejecución de este proyecto para su correcto manejo y comprensión, de esta manera garantizar que la evidencia digital extraída mantenga los principios autenticidad e integridad y así obtener un resultado exitoso.

RESUMEN

Hoy en día, se ha podido ver un aumento significativo en el cometimiento de delitos en los que se encuentran involucrados dispositivos móviles con sistema operativo Android, mismo que se ha convertido en el número uno a nivel mundial al ser la plataforma más utilizada; el presente trabajo de investigación tiene por objetivo extraer información de dispositivos móviles que presentan daños en su estructura, es decir, cuando los dispositivos por a o b circunstancia se han visto dañados el procedimiento se llevara a cabo con ayuda de herramientas de análisis forense open-source y de técnicas invasivas para la obtención de la información, ya que, en este sentido existe desconocimiento sobre las herramientas de software libre orientadas al análisis forense de la misma manera existe desconocimiento sobre las técnicas invasivas de adquisición y del procedimiento a seguir cuando un dispositivo se encuentra averiado.

La metodología que se aplica en este trabajo es una investigación de carácter bibliográfico sobre modelos y normas legales nacionales que permitan identificar el dispositivo móvil, asegurar el escenario motivo de investigación, preservar, adquirir la información por medio cada técnica y haciendo uso de su respectiva herramienta, así como analizar los resultados y presentar informes de ser el caso. Finalizado el proceso de extracción en los escenarios propuestos, se comprueba que mediante la documentación realizada en cada fase del método utilizado se facilita al perito la realización del informe pericial, por tal razón, se justifica así la factibilidad del desarrollo del presente trabajo.

PALABRAS CLAVE

Extraer información, técnicas invasivas, dispositivos móviles, herramientas open-source.

ABSTRACT

Nowadays, there has been a significant increase in the commission of crimes involving mobile devices with Android operating system, which has become the number one worldwide as the most widely used platform; The present research work aims to extract information from mobile devices that have been damaged in their structure, that is, when the devices by a or b circumstances have been damaged, the procedure will be carried out with the help of open-source forensic analysis tools and invasive techniques for obtaining information, since, in this sense there is ignorance about the free software tools oriented to forensic analysis in the same way there is ignorance about the invasive techniques of acquisition and the procedure to follow when a device is damaged.

The methodology applied in this work is bibliographic research on models and national legal standards to identify the mobile device, ensure the scenario under investigation, preserve, acquire information through each technique and using their respective tool, as well as analyze the results and submit reports if necessary. After the extraction process in the proposed scenarios, it is verified that through the documentation made in each phase of the method used, it is easier for the expert to make the expert report, for this reason, the feasibility of the development of this work is justified.

KEYWORDS
Information extraction, invasive techniques, mobile devices, open-source tools.

CAPITULO I

FORMULACIÓN GENERAL DEL PROYECTO

1.1 Descripción del Problema

Increíblemente, los delincuentes de hoy utilizan la tecnología para facilitar el crimen y escapar de las autoridades. Este hecho dificulta la labor de la Policía Nacional, la fiscalía general del Estado y la Función Judicial deben especializarse y capacitarse en las nuevas tecnologías que se convierten en herramientas necesarias para el auxilio a la Justicia y para la persecución del delito y el delincuente.

En el proceso de extracción de información de dispositivos móviles, muchas veces los peritos se encuentran con serias dificultades en su tarea, esto se debe principalmente a que se debe trabajar con equipos que han sufrido algún tipo de daño en su estructura física, generalmente se trata de pantallas rotas, interruptores rotos, golpes, incinerados, expuestos a largos periodos de humedad y sumamente deteriorados dando como resultado la afectación de sus componentes, todo esto demanda una mayor cantidad de recursos para lograr encontrar evidencia digital que sirva como elemento probatorio del posible cometimiento de un delito; todo esto encarece el proceso muchas de las veces por encima de las posibilidades de los investigadores.

Con base a lo mencionado anteriormente el daño a los componentes de los dispositivos móviles genera inconvenientes graves al analista forense de dispositivos móviles al dificultarse la recuperación y extracción de la información de documentos, archivos de audio, multimedia, contactos, mensajes, llamadas, y otros archivos. Como consecuencia la labor de extracción de las evidencias digitales en dispositivos móviles con sistema operativo Android con componentes dañados se vuelve una tarea ardua y compleja debido a que necesita realizar procedimientos avanzados como el uso de técnicas invasivas de adquisición aplicado a la memoria y procesador del dispositivo móvil, tomando en cuenta que no se debe afectar la integridad del dispositivo o poniendo en riesgo la perdida de la información.

1.2 Formulación del Problema

¿De qué manera se podrá extraer evidencia digital forense de dispositivos móviles con sistema operativo Android cuando sus componentes han sido afectados?

1.3 Preguntas de Investigación

¿Qué métodos y técnicas de análisis forense permitirán la extracción de información de un dispositivo móvil cuando sus componentes han sido afectados?
¿Cuáles serán las herramientas open source adecuadas para extraer información de dispositivos móviles Android con componentes en mal estado?
¿Al aplicar una técnica invasiva de extracción de información será posible obtener evidencia digital de dispositivos móviles Android con componentes afectados?

1.4 Justificación

Es importante la obtención de elementos de convicción (Información) esto se constituye en una de las facetas útiles dentro del éxito de en una investigación criminal, aspecto que demanda de los investigadores encargados de la recolección, preservación, análisis y presentación de las evidencias digitales una eficaz labor que garantice la autenticidad e integridad de dichas evidencias, a fin de ser utilizadas posteriormente ante el Tribunal Penal.
La investigación es de suma importancia ya que permitirá adquirir y aportar con conocimiento a la sociedad principalmente para quienes se dedican a la labor del análisis forense en dispositivos móviles bajo plataformas Android, ya que, al encontrarse con dispositivos móviles con componentes deteriorados, rotos la pantalla, incinerados, expuestos a humedad o cualquier otro factor que dificulte la extracción de información digital que permita ser utilizada como evidencia. Cabe mencionar que para cada proceso de análisis forense existente técnicas, fases, métodos que se combinan permitiendo la extracción de la información, sin afectar la integridad de la evidencia en el dispositivo móvil.
El presente trabajo de investigación es motivado por adquirir nuevos conocimientos y aportar a la sociedad en la solución de problemas, además recalcar que nos gusta el campo de la auditoria informática, por lo tanto, nuestro objetivo es extraer evidencia digital por medio de técnicas y herramientas open source de auditoria

forense cumpliendo con todos requerimientos que establece la normativa legal de Ecuador.

Los beneficiarios directos serán los peritos e investigadores forenses dedicados a esta profesión sirviendo de guía para el desarrollo del proceso, herramientas y materiales adecuados para la extracción de información mediante técnicas invasivas en dispositivos móviles cuando sus componentes son deteriorados.

La investigación se enfocará en la siguiente línea de investigación: Ingeniería De Software, Redes y Telecomunicaciones en la sub línea seguridad de aplicaciones.

1.5 Objetivos:

Objetivo General:

Aplicar un análisis forense utilizando herramientas open source en dispositivos móviles cuando sus componentes están deteriorados para la extracción de evidencia digital.

Objetivos Específicos:

- Seleccionar las técnicas y métodos adecuados para la extracción de información en dispositivos móviles Android con componentes deteriorados.
- Establecer las herramientas open source adecuadas para la extracción de información de dispositivos móviles Android.
- Extraer evidencia digital de dispositivos móviles Android con el uso de herramientas open source para el análisis forense.

1.6 Hipótesis

Al utilizar técnicas invasivas de análisis forense se podrá extraer evidencia digital de dispositivos móviles Android cuando sus componentes están deteriorados.

1.7 Variables

Independiente

Técnicas Invasivas de Análisis forense

Dependiente

Evidencia digital

Operacionalización de Variables

Tabla 1

Operacionalización de la variable independiente

Variable Independiente: Técnicas Invasivas de Análisis forense				
Concepto	**Categoría**	**Indicadores**	**Ítems**	**Técnicas e instrucciones**
Es un conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial. (Lopez, 2007)	Métodos y técnicas invasivas de extracción de información. Proceso de adquisición. Leyes y reglamentos.	Número de herramientas open-source para el análisis forense validas / total de herramientas. Número de procesos o fases válidas para la extracción de información/total de fases o procesos. Número de artículos empleados para la validación de la evidencia digital.	¿Qué herramientas open-source existen para la extracción de información en dispositivos móviles en terminales Android? ¿Cuáles son las técnicas invasivas para la extracción de información en dispositivos móviles con componentes afectados?	Fichas de Observación Técnica.

Tabla 2

Operacionalización de la variable dependiente

Variable dependiente: Evidencia Digital				
Concepto	**Categoría**	**Indicadores**	**Ítems**	**Técnicas e instrucciones**
La evidencia digital se entiende al conjunto de datos en formato binario, esto es, comprende los ficheros, su contenido o referencias a estos (metadatos) que se encuentren e los soportes físicos o lógicos del sistema atacado. (Lopez, 2007)	Metadatos Soportes físicos Soportes lógicos	Número de evidencias extraídas de un dispositivo móvil validas. Número de técnicas invasivas validas /total de técnicas	¿Qué tipos de evidencia se puede obtener a través del análisis forense en dispositivos móviles afectados sus componentes?	Fichas de Observación Técnica.

CAPITULO II

MARCO TEÓRICO

2.1 Antecedentes

En la actualidad, Ecuador tiene la Dirección Nacional de Comunicaciones que se encarga de la detección de delitos informáticos que son realizados por ciber piratas los cuales tienen como finalidad provocar daños en dispositivos informáticos de una organización. El departamento se creó en el año 2016 con alrededor de 200 agentes de la policía judicial mismos que han ido trabajando de manera operativa y preventiva, la función de estos agentes policiales es la de identificar y monitorear accesos ilícitos a los sistemas de información, contenido pornográfico, tráfico de órganos, prostitución infantil, venta de drogas y armas por internet. (Aguirre, 2020)

El análisis forense en dispositivos móviles en la actualidad es una disciplina que ha tomado fuerza debido a que la información digital almacenada en estos dispositivos es importante en el ámbito judicial al momento de determinar la situación de crimen o acto delictivo. La aplicación de técnicas que ayuden a esclarecer ciertos hechos ocurridos en la red surge a partir del siglo XIX. Por tal razón, Rodríguez menciona que "las huellas digitales, con valor identificativo, no fueron usadas hasta finales del siglo XIX. Las pruebas genéticas fueron utilizadas por primera vez en un tribunal a finales del siglo XX, en el año 1996". A partir de lo ocurrido, la ciencia forense dedicada al análisis de dispositivos móviles ha evolucionado a la par del avance tecnológico que se da en la actualidad con la finalidad de ser un aporte a la solución de hechos suscitados mediante el uso indebido de los dispositivos móviles. Muchas son las definiciones de informática forense que podemos encontrar en un gran número de publicaciones, pero todas ellas -de una u otra manera- hacen hincapié en ciertos puntos esenciales; así, de una forma sencilla, podríamos definir la informática forense como un proceso metodológico para la recogida y análisis de los datos digitales de un sistema de

dispositivos de forma que pueda ser presentado y admitido ante los tribunales. (Ferro, 2002)

Según (Pinto, 2014) en su artículo "Metodología de análisis forense orientada a incidentes en dispositivos móviles" menciona "El crecimiento de incidentes en los que intervienen dispositivos móviles plantea la necesidad de tener una metodología para estas tecnologías, ya que, al existir diferentes fabricantes, cada uno tiene diversos criterios en el manejo de la información sin seguir ningún estándar". Además, menciona que en la investigación llevada a cabo las que utilizo no cubrían por completo el proceso de análisis forense en dispositivos móviles, razón por la cual invita a las universidades a desarrollar este tipo de herramientas. (Pinto, 2014)

La dificultad que implica el análisis forense a un dispositivo móvil, esto debido a la diferencia existente entre los dispositivos de diferentes fabricantes, de la misma forma, como a las numerosas y significativas diferencias existentes entre modelos del mismo fabricante. Además, resalta la importancia de la creación de una herramienta forense especializada en el SO Symbian, que en este caso es el SO en el cual se realiza el análisis forense, y que contemple mejoras significativas respecto a las debilidades que presentas las herramientas con las cuales se trabajó. (Agualimpia & Hernández, 2009)

Según (Granda, 2016) menciona que en dispositivos con tecnología más avanzada se requiere aplicar metodología y procedimiento específicos con el fin de asegurar la integridad de la evidencia.

Según (Avendaño, 2012) manifiesta que: "Las herramientas disponibles en internet ayudan a la propagación de ese comportamiento en las víctimas que reciben malos tratos de sus iguales, sea a través de ridiculizaciones, amenazas, chantajes, discriminaciones u ofensas, todo ello de manera anónima para que éste desconozca quien es su agresor lo cual infunde más temor a la víctima".

En las últimas décadas ha existido un mayor interés por la informática forense, en la que los profesionales en informática forense realizan la función de

extraer información almacenada en un medio digital. Además, estos profesionales analizan archivos digitales como: documentos, videos, audios, correos electrónicos, etc., con el objetivo de recopilar toda la evidencia posible en un proceso judicial. La informática forense se ha desarrollado rápidamente ya que reúne varias ramas relacionadas con redes informáticas, bases de datos, dispositivos móviles, ordenadores todo esto con la ayuda de herramientas software especializadas ya tengan estas un costo de adquisición o no. (Aguirre, 2020)

2.2 Marco Científico

Informática Forense

La informática forense es la disciplina de identificar, recolectar, preservar y analizar evidencia a través de la investigación usando modelos y técnicas forenses en áreas específicas de casos penales y civiles, ayuda a resolver disputas legales ante los tribunales, para que los investigadores y profesionales tengan conocimiento en áreas técnicas. La computación forense permite detectar y recuperar información y datos digitales y utilizarlos como evidencia para restablecer un hecho y, por lo tanto, se utiliza como valor probatorio. Debido a los desarrollos tecnológicos ha estado expuesto en los últimos tiempos, la demanda de habilidades informáticas está en constante aumento, debido a que la prueba digital se ha convertido en información muy importante al momento de reproducir eventos en el contexto de una encuesta, incluso se utilizaron como juicios de decisión en proceso pericial. Se requiere personal técnico con sólidos conocimientos para que el opere de manera ordenada y sistemática y aplique métodos para "identificar, adquirir, recuperar y analizar información, ya sea visible u oculta" (Di lorio, y otros, 2017).

La Informática Forense surgió como una necesidad para la investigación de diferentes delitos que afectan a la sociedad a diario, su finalidad es identificar a los responsables de los delitos y esclarecer el origen de los hechos, mediante la recopilación de pruebas con fines de investigación a través de diversas técnicas. Es importante que la información no se altere de ninguna manera, ya que es necesario para mantener la integridad de la evidencia, por lo tanto, es necesario seguir la metodología, la especificación técnica de la información ISO/IEC 27037:2012 Norma Directrices para la identificación, recopilación, recopilación y conservación

de evidencia digital, la proporciona modelos para la identificación, sistematización, recopilación, recopilación y retención de la información, esta norma se basa en tres factores: la relevancia, la confiabilidad y la integridad (Fennema et al., 2017).

Análisis Forense

El análisis forense es un campo que ha crecido rápidamente en los últimos años debido al aumento de los incidentes de seguridad, especialmente en el área de la tecnología que es parte de la seguridad informática que busca probar y refactorizar cómo se ha vulnerado un sistema. Por lo tanto, es necesario para el desarrollo de nuestra guía el conocer y comprender términos relacionados con la informática forense. También consiste en la aplicación de técnicas científicas y analíticas especializadas a una infraestructura tecnológica que permite identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. El análisis 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. (Jaya, 2017)

Tipos de análisis forense digital

Cuando se va a realizar un análisis forense es muy importante tener en cuenta que existen varios tipos, y que además va depender mucho del punto de vista desde el que se va a analizar la información.

Según (Mendillo, 2018) existen tres tipos de análisis forense:

a) **Análisis forense de redes.** - este tipo de análisis forense considera el medio de comunicación por el que viaja la información, aquí están las redes (cableadas, inalámbricas, Bluetooth, etc.)
b) **Análisis forense de sistemas.** - este tipo de análisis forense hace referencia a la investigación realizada en servidores y estaciones de trabajo enfocándose en el tipo de sistema operativo (Windows, UNIX, Linux, MAC OS) que tenga el equipo.
c) **Análisis forense de sistemas embebidos**. – este análisis forense hace referencia a la investigación en dispositivos móviles, PDA (asistente

personal digital), PDS, etc., debido a que un sistema embebido se asemeja a la de un ordenador, desde el punto de vista estructural y de arquitectura.

Para la informática forense sin importar el tipo de análisis que vaya a realizar tiene tres objetivos definidos: la compensación de los daños causados por los criminales o intrusos; la persecución y procesamiento judicial de los criminales y por último la creación y aplicación de medidas para prevenir actos delictivos. Pero para cumplir estos objetivos es necesario realizar una recolección adecuada de la evidencia digital.

Principios del análisis forense digital

Para respaldar lo anterior y defender el propósito principal de la informática forense, es decir, proporcionar evidencia ante un juez, existen ciertos principios generales que se pueden aplicar en cualquier proceso de informática forense que cuenta.

Según (Rueda & Rico, 2016) los principios del análisis forense que se deben seguir son tres, los cuales se mencionan a continuación:

a) **Actuar de manera metódica:** El investigador debe ser su propio supervisor en todo el proceso, en el que cada paso que se da, las herramientas que se utilizan y los resultados obtenidos quedan plenamente documentados.
b) **Evitar la contaminación**: Evitar a toda costa el manejo inadecuado de las pruebas analizadas, para evitar malas interpretaciones o análisis erróneos.
c) **Cadena de Custodia:** Respondiendo a un cuidado particular y forma de dejar constancia de cada evento se hace con evidencia.

Fases del análisis forense digital

El proceso general de un análisis forense incluye las siguientes etapas: recolección, preservación, análisis y presentación (Ayers, Brothers, & Jansen, 2014) las cuales se detallan a continuación:

a) Recolectar. Este es el primer paso a dar en el análisis forense informático, donde el objetivo es recopilar todas las pruebas del dispositivo de interés para la investigación. En la extracción de información se debe tener en

cuenta la integridad de la información, a partir de la cual se pueden utilizar algoritmos hash.

b) Preservar**.** Durante esta etapa es fundamental verificar que la información recolectada en la etapa anterior sea la misma que la información analizada, para confirmar la integridad de la evidencia es necesario respetar la cadena de custodia utilizar métodos de verificación y verificar la prueba mediante un hash función (MD5 o SHA1).

c) Analizar. Toda la investigación se centra en esta etapa, es aquí donde mediante el uso de herramientas de análisis forense debemos ser capaces de identificar cualquier cambio o acceso no autorizado al software o hardware de los dispositivos móviles. Cabe señalar que estos cambios van desde cambios físicos del sistema de archivos, del sistema operativo hasta simples accesos.

Además, con el examen realizado, es posible reconstruir los hechos, lo que permitirá al investigador y al litigante comprender y esclarecer cómo pudo ocurrir el delito. Finalmente, con el análisis realizado, es posible revelar quién es el autor de los comportamientos, a partir de los cuales la IP (dirección lógica del dispositivo) o MAC (la dirección real del dispositivo) de la computadora realizada (Ayers, Brothers, & Jansen, 2014)

d) Presentar. Esta es la etapa final del análisis forense donde toda la información recopilada se agregará para corroborar todos los análisis realizados en un informe técnico.

Informática forense en dispositivos móviles Android

El entorno de los dispositivos móviles ha evolucionado rápidamente en los últimos años, principalmente debido a su gran aceptación por parte de los usuarios que disponen simultáneamente de múltiples dispositivos para diferentes propósitos como uso laboral, uso personal, etc. Algunas estimaciones indican que en la actualidad hay más de 7.500 millones de dispositivos móviles, más que la población mundial. Almacenan una gran cantidad de información que puede ser decisiva a la hora de resolver una incidencia, como, por ejemplo: historial de llamadas entrantes y salientes, mensajes de texto y multimedia, correo electrónico, historial de

navegación, fotos, vídeos, documentos, etc. redes, información en servicios de almacenamiento en línea, etc. e incluso puede recuperar información previamente eliminada. (Martinez, 2020)

El sistema más utilizado en dispositivos móviles es Android. Las empresas desarrolladoras de sistemas operativos envían actualizaciones constantes con la finalidad de solucionar las vulnerabilidades existentes, Internet ha dado paso a las redes globales entre dispositivos móviles, por lo que la seguridad se ha convertido en un reto. Para los desarrolladores, cada día aparecen millones de ataques cibercriminales para organismos gubernamentales, empresas privadas y usuarios comunes, de esta manera, la investigación forense se convierte en un elemento fundamental para esclarecer las verdades de los delincuentes. (Martinez, 2020)

Como menciona (Martinez, 2020), la investigación forense realiza un análisis completo de los registros. almacenado en un sistema. Es importante revisar el directorio que permite la gestión causa de pericia, para proporcionar un informe detallado, el investigador ellos tienen; estándares, lineamientos y metodologías tales como:

a) **ISO/IEC 27037:** Directrices para la identificación, recopilación, adquisición y preservación de la evidencia digital. Es un documento que publicó la Organización Internacional para la estandarización (ISO).
b) **RFC 3227:** Guía para recolectar y archivar evidencia. Proporciona sistemas, directrices para la recopilación y archivo de las pruebas en un incidente de seguridad.
c) **UNE 71505:** Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales. Proporcionan la información sobre los sucesos en un sistema de información.
d) **UNE 71506:** Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas. Define los procesos del análisis forense dentro del ciclo de gestión de evidencias electrónicas.

Para realizar un análisis forense a los dispositivos móviles existen algunas fases, ya que, pese a que tiene aspectos comunes con otro tipo de análisis forense como por ejemplo el de computadores, también tiene diferencias que se deben tener en cuenta.

Pero de una manera global se puede identificar las siguientes: preservación, adquisición, análisis, documentación y presentación los cuales se detalla a continuación:

a) Preservación. - Corresponde a la fase en la que se deben identificar los dispositivos a analizar y garantizar que no se pierdan las evidencias que deben ser recopiladas para su posterior análisis. El desconocimiento puede provocar la invalidación automática de las pruebas, por ejemplo, por no solicitar una autorización expresa por escrito para poder realizar el proceso o que se pierda información relevante que puede resultar decisiva para la resolución del incidente. Aspectos tan sencillos como preservar el dispositivo en una jaula de Faraday con el fin de aislarlo de cualquier tipo de señal o activar el modo avión evita, por ejemplo, la posibilidad de realizar un borrado remoto del terminal. (Martinez, 2020)

Así mismo, se debe mantener un registro continuo del tratamiento realizado sobre el material con el fin de mantener la validez jurídica del proceso, en el caso de que sea necesario. Para ello, se requiere la presencia de un fedatario público: secretario judicial o notario que dé fe a la cadena de custodia, es decir, que garantice la integridad física y lógica de las pruebas. Este aspecto abarca desde la identificación y obtención de las mismas, pasando por el registro, almacenamiento, traslado, análisis final, y la entrega de éstas a las autoridades en caso de que sea necesario. Por otra parte, si los materiales deben ser transportados, se debe realizar con sumo cuidado, evitando que la información sea alterada o que se vea expuesta a temperaturas extremas o campos electromagnéticos. (Martinez, 2020)

b) Adquisición. - Una evidencia puede ser definida como cualquier prueba que pueda ser utilizada en un proceso legal. Es por ello que debe tener las siguientes características:
    a. Auténtica: debe ser verídica y no haber sufrido manipulación alguna.
    b. Completa: debe representar la prueba desde un punto de vista objetivo y técnico, sin valoraciones personales, ni prejuicios.
    c. Creíble: debe ser comprensible.

d. Confiable: las técnicas utilizadas para la obtención de la evidencia no deben generar ninguna duda sobre su veracidad y autenticidad.
e. Admisible: debe tener valor legal.

Algunos ejemplos de evidencias digitales son: fotos, vídeos, documentos, registro de llamadas, correos electrónicos, mensajes de WhatsApp, etc. En el caso de los dispositivos móviles es importante tener en cuenta que las tarjetas de memoria que habitualmente utilizan pueden tener información de gran relevancia por lo que es necesario tenerla muy presente en esta fase.

c) Análisis. - A la hora de realizar el análisis de la información recopilada se debe considerar el tipo de incidente al que se pretende ofrecer respuesta, ya que dependiendo del caso puede resultar necesario realizar un análisis más profundo de determinados aspectos.

d) Documentación. - Un aspecto fundamental en el proceso del análisis forense es el de la documentación, por lo que, se debe realizar dicha fase de una manera muy metódica y detallada. Se pueden realizar, entre otras, las siguientes acciones:
   a. Fotografiar los dispositivos móviles y anotar su marca, modelo e información identificativa como el IMEI o IMSI, y su estado inicial: encendidos o apagados, bloqueados o no, etc.
   b. Documentar todos los pasos realizados durante el proceso, manteniendo una bitácora con fechas y horas de cada acción realizada sobre las evidencias e incluyendo las herramientas utilizadas.
   c. Elaborar dos tipos de informe de conclusiones: uno ejecutivo y uno técnico.

e) Presentación. - La fase de presentación de la información es tan importante o más que las anteriores ya que se deben hacer accesibles y comprensibles las conclusiones que se han obtenido del proceso del análisis forense. Para ello, es recomendable seguir las siguientes pautas:
   a. Preparar una presentación de manera pedagógica que sea fácilmente comprensible.

b. Detallar las conclusiones.
c. Explicar de manera clara el proceso que se ha llevado para la obtención de las evidencias.
d. Evitar las afirmaciones no demostrables o los juicios de valor.
e. Elaborar las conclusiones desde un punto de vista objetivo.

2.3 Marco Conceptual

Auditoria Informática

La Auditoría informática es una modalidad de auditoría que concierne a la evaluación en profundidad de los recursos informáticos y tecnológicos de una organización. También se refiere a la revisión práctica que se realiza sobre los recursos informáticos con que cuenta una entidad con el fin de emitir un informe o dictamen sobre la situación en que se desarrollan y se utilizan esos recursos. (López, 2007).

Evidencia Digital

Según (Jaya, 2017) "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".

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:

a) Registros almacenados en equipos de tecnología informática. Son todos los documentos creados y almacenados por el usuario en el equipo de tecnología informática.
b) 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.
c) Registros híbridos. Conformados por los registros almacenados y generados por equipos de tecnología informática.

Herramientas para el Análisis Forense

Andriller

Andriller es una aplicación multiplataforma para Microsoft Windows, Ubuntu y Linux, es un software utilitario con una colección de herramientas forenses para smartphones. Realiza adquisiciones forenses de solo lectura y no destructivas desde dispositivos Android. Esta herramienta es realmente útil al tener que trabajar sobre sistemas operativo Android y es especialmente requerida en casos de peritajes de WhatsApp. Tiene características, como el poderoso descifrado del patrón de la pantalla de bloqueo, código PIN o contraseña; decodificadores personalizados para datos de aplicaciones de bases de datos de Android (algunos Apple iOS y Windows) para decodificar comunicaciones. La extracción y los decodificadores producen informes en formatos HTML y Excel. (Sacco, 2021)

Características:

a) Extracción de datos automatizado y parsing de datos.
b) Extracción de datos en teléfonos no-rooteados a través de la copia de seguridad (en Android 4.x).
c) Extracción de datos con permisos de root: root ADB daemon, CWM recovery mode, o SU binary (Superuser/SuperSU).
d) Parsing de la estructura de carpetas, archivos Tarball y Android Backup.
e) Selección de los decodificadores de la base de datos individuales para Android y Apple.
f) Descifrado de base de datos de WhatsApp (msgstore.db. crypt, msgstore.db. crypt5, msgstore.db. crypt7 y msgstore.db. crypt8).
g) Craqueo de patrón, PIN y contraseña.
h) Desempaqueta archivos de backup Android

Autopsy

Autopsy es un programa forense digital de código abierto basado en GUI para analizar discos duros y teléfonos inteligentes de manera eficiente. Miles de usuarios en todo el mundo utilizan Autopsy para investigar lo que sucedió en la computadora o un dispositivo móvil. (Chandan, 2022)

Características:

a) Análisis de correo electrónico

b) Detección de tipo de archivo
c) Reproducción multimedia
d) Análisis de registro
e) Recuperación de fotos de la tarjeta de memoria
f) Extraiga información de la cámara y la ubicación geográfica de archivos JPEG
g) Extrae la actividad web de un navegador
h) Mostrar eventos del sistema en una interfaz gráfica
i) Análisis de la línea de tiempo
j) Extraiga datos de Android: SMS, registros de llamadas, contactos, etc.
k) Tiene informes extensos para generar en formato de archivo HTML, XLS.

Santoku

Santoku Linux es una distribución basada en Linux especialmente desarrollada para auditar dispositivos móviles en busca de vulnerabilidades, fallos o simplemente cualquier aspecto que pueda comprometer nuestra privacidad al utilizar cualquiera de estos dispositivos móviles y gratuito de código abierto. (Martínez, 2020)

Características:

a) Ejecución de herramientas para adquisición y análisis de datos de manera forense.
b) Gestión de la comunicación entre el dispositivo móvil con sistema operativo Android y el equipo con sistema operativo Santoku.
c) Herramientas de imagen para NAND, tarjetas de medios y RAM
d) Scripts y utilidades útiles diseñados específicamente para análisis forense móvil
e) Análisis tanto la memoria interna como la ROM y la RAM en busca de información residente en dichas memorias.

Modelo de Análisis forense en dispositivos móviles

Los peritajes informáticos necesitan modelos de eficiencia que ayuden a mejorar procedimientos realizados en el marco del análisis forense, es fundamental que estas actividades sean de conformidad con las normas legales aplicables, durante la extracción de datos, su estructura no debe ser modificada para su análisis

y posterior emisión del informe pericial, Se analiza los diferentes modelos de diferentes autores para elegir los más efectivos, lo que permite lograr resultados óptimos en el análisis forense (Jaya, 2017).

Model Digital Forensic Research Workshops (DFRWS)

Este modelo (DFRWS), propone un proceso de investigación segmentado en siete etapas lineales, como se muestra en la ilustración 1 (Jaya, 2017).

Ilustración 1

Diagrama Model Digital Forensic Research Workshops (DFRWS) Fuente: (Jaya, 2017)

a) Identificación. - En esta etapa permite ejecutar el reconocimiento y determinar el tipo de suceso.
b) Preservación. - Esta etapa contiene la cadena de custodia, para que los datos no sean manipulados.
c) Recolección. - Los datos son recolectados mediante la utilización de herramientas tecnológicas tanto de software como de hardware.

d) Inspección. - Se analizan los datos recogidos los que, permitirán la reconstrucción de los hechos.
e) Análisis. - Mediante el resultado del análisis de los datos se realiza la reconstrucción de los hechos.
f) Presentación. - Se emite el informe pericial documentado con sus respectivas conclusiones.
g) Decisión. - La información obtenida se constituye en un factor decisivo en el dictamen de la sentencia (Jaya, 2017).

Técnicas invasivas de adquisición de datos en dispositivos Android

Chip-off

Consiste en la extracción del chip de memoria de la placa electrónica, a día de hoy no es muy común. Hay dos tipos:

a) Extracción caliente (thermal): mediante la aplicación de calor. Es la más popular y la más agresiva, ya que aplicamos temperaturas superiores a 230 º C.
b) Extracción fría (non thermal): mediante técnicas de lijado, fresado y corte.

Antes de realizar un chip off debemos saber que es el último recurso e investigar sobre el dispositivo (marca, modelo, SO, chip), si el dispositivo está cifrado o si podemos realizar otras técnicas de extracción menos agresivas. Con una extracción caliente el 5% de las memorias quedan dañadas de forma total. (Velasco, 2022)

Hex Dump/JTAG

Extrae todos los datos del teléfono haciendo una copia bit a bit del contenido. Este proceso requiere que el equipo se conecte a los puertos de acceso de prueba del equipo (TAP). El resultado es un archivo binario que requiere de un perfil técnico que pueda interpretarlo. Las herramientas disponibles para esta técnica son más sofisticadas. Algunas son: UFED Ultimate de Cellebrite, XRY Complete de MSAB, MD Box de Hancom, Riff Box, Moorc o Easy JTag plus. (Ayers, Brothers, & Jansen, 2014)

2.4 Marco Legal

Al tratarse del análisis forense para la extracción de información en dispositivos Android surge la necesidad de considerar la normativa legal vigente en el Ecuador. Se describen algunos artículos y reglamentos relacionados con el presente trabajo de investigación.

Código orgánico integral penal

Artículo 69 (2a)

En el artículo 69 inciso 2 manifiesta que:

2- Comiso penal, procede en todos los casos de delitos dolosos y recae sobre los bienes, cuando estos son instrumentos, productos o réditos en la comisión del delito. No habrá comiso en los tipos penales culposos. En la sentencia condenatoria, la o el juzgador competente dispondrá el comiso de: a) Los bienes, fondos o activos, o instrumentos equipos y dispositivos informáticos utilizados para financiar o cometer la infracción penal o la actividad preparatoria punible. (ASAMBLEA NACIONAL, 2018)

Artículo 178.- Violación a la intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley (ASAMBLEA NACIONAL, 2018).

Artículo 190.- Apropiación fraudulenta por medios electrónicos. - La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o

modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes (ASAMBLEA NACIONAL, 2018).

Artículo 193.- Reemplazo de identificación de terminales móviles. - La persona que reemplace las etiquetas de fabricación de los terminales móviles que contienen información de identificación de dichos equipos y coloque en su lugar otras etiquetas con información de identificación falsa o diferente a la original, será sancionada con pena privativa de libertad de uno a tres años (ASAMBLEA NACIONAL, 2018)

Artículo 456.- Cadena de custodia. - Se aplicará cadena de custodia a los elementos físicos o contenido digital materia de prueba, para garantizar su autenticidad, acreditando su identidad y estado original; las condiciones, las personas que intervienen en la recolección, envío, manejo, análisis y conservación de estos elementos y se incluirán los cambios hechos en ellos por cada custodio. La cadena inicia en el lugar donde se obtiene, encuentra o recauda el elemento de prueba y finaliza por orden de la autoridad competente. Son responsables de su aplicación, el personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, el personal competente en materia de tránsito y todos los servidores públicos y particulares que tengan relación con estos elementos, incluyendo el personal de servicios de salud que tengan contacto con elementos físicos que puedan ser de utilidad en la investigación (ASAMBLEA NACIONAL, 2018).

Artículo 471.- Registros relacionados a un hecho constitutivo de infracción.- No requieren autorización judicial las grabaciones de audio, imágenes de video o fotografía relacionadas a un hecho constitutivo de infracción, registradas de modo espontáneo al momento mismo de su ejecución, por los medios de

comunicación social, por cámaras de vigilancia o seguridad, por cualquier medio tecnológico, por particulares en lugares públicos y de libre circulación o en los casos en que se divulguen grabaciones de audio o video obtenidas por uno de los intervinientes, en cuyo caso se requerirá la preservación de la integralidad del registro de datos para que la grabación tenga valor probatorio. En estos casos, las grabaciones se pondrán inmediatamente a órdenes de la o el fiscal en soporte original y servirán para incorporar a la investigación e introducirlas al proceso y de ser necesario, la o el fiscal dispondrá la transcripción de la parte pertinente o su reproducción en la audiencia de juicio (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2018).

Artículo 498.- Medios de prueba. - Los medios de prueba son: El documento, El testimonio, La pericia (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2018).

Artículo 500.- Contenido digital. - El contenido digital es todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí. En la investigación se seguirán las siguientes reglas: 1) El análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de técnicas digitales forenses. 2) Cuando el contenido digital se encuentre almacenado en sistemas y memorias volátiles o equipos tecnológicos que formen parte de la infraestructura crítica del sector público o privado, se realizará su recolección, en el lugar y en tiempo real, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido. 3) Cuando el contenido digital se encuentre almacenado en medios no volátiles, se realizará su recolección, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido. 4) Cuando se recolecte cualquier medio físico que almacene, procese o transmita contenido digital durante una investigación, registro o allanamiento, se deberá

identificar e inventariar cada objeto individualmente, fijará su ubicación física con fotografías y un plano del lugar, se protegerá a través de técnicas digitales forenses y se trasladará mediante cadena de custodia a un centro de acopio especializado para este efecto (ASAMBLEA NACIONAL, 2018).

Ley de comercio electrónico, firmas y mensajes de datos

La presente ley tiene como objeto regular y sancionar las infracciones que se atribuyen a lo relacionado con los sistemas de información, redes electrónicas e internet.

Art. 5.- Confidencialidad y reserva. - Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia (CONGRESO NACIONAL, 2021).

Art. 8.- Conservación de los mensajes de datos. - Toda información sometida a esta ley, podrá ser conservada; este requisito quedará cumplido mediante el archivo del mensaje de datos, siempre que se reúnan las siguientes condiciones: a) Que la información que contenga sea accesible para su posterior consulta; b) Que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida; c) Que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado; y, d) Que se garantice su integridad por el tiempo que se establezca en el reglamento a esta ley. Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo. La información que tenga por única finalidad facilitar el envío o recepción del mensaje de datos, no será obligatorio el cumplimiento de lo establecido en los literales anteriores.(CONGRESO NACIONAL, 2021)

Art. 10.- Procedencia e identidad de un mensaje de datos. - Salvo prueba en contrario se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe, para actuar conforme al contenido del mismo, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica, excepto en los siguientes casos: a) Si se hubiere dado aviso que el mensaje de datos no proviene de quien conste como emisor; en este caso, el aviso se lo hará antes de que la persona que lo recibe actúe conforme a dicho mensaje. En caso contrario, quien conste como emisor deberá justificar plenamente que el mensaje de datos no se inició por orden suya o que el mismo fue alterado; y, b) Si el destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o hizo caso omiso de su resultado (CONGRESO NACIONAL, 2021).

Art. 52.- Medios de prueba. - Los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta ley, cualquiera sea su procedencia o generación, serán considerados medios de prueba. Para su valoración y efectos legales se observará lo dispuesto en el Código de Procedimiento Civil(CONGRESO NACIONAL, 2021).

Art. 55.- Valoración de la prueba. - La prueba será valorada bajo los principios determinados en la ley y tomando en cuenta la seguridad y fiabilidad de los medios con los cuales se la envió, recibió, verificó, almacenó o comprobó si fuese el caso, sin perjuicio de que dicha valoración se efectúe con el empleo de otros métodos que aconsejen la técnica y la tecnología. En todo caso la valoración de la prueba se someterá al libre criterio judicial, según las circunstancias en que hayan sido producidos. Para la valoración de las pruebas, el juez o árbitro competente que conozca el caso deberá designar los peritos que considere necesarios para el análisis y estudio técnico y tecnológico de las pruebas presentadas (CONGRESO NACIONAL, 2021)

Reglamento del Sistema Pericial Integral de la Función Judicial

Artículo 4: Calidad de perito. - Toda persona para ser considerada como perito, debe estar previamente calificada por el Consejo de la Judicatura de conformidad con el Código Orgánico General de Procesos y este Reglamento. No será obligatoria la calificación en caso de que se trate de una o un experto que no tenga su domicilio en el Ecuador y que sea designada o designado como tal para un juicio, cuando no existan peritos de la especialidad correspondiente en el país. En casos extraordinarios, cuando en una fase pre procesal o proceso judicial se requiera una o un perito en determinada especialidad para la cual no existan peritos calificados, excepcionalmente se requerirá la participación de una experta o experto en la especialidad requerida, en cuyo caso no se exigirá la calificación y se procederá conforme a lo establecido en este Reglamento (CONSEJO DE LA JUDICATURA, 2022).

Artículo 22: Obligaciones generales. - Las y los peritos calificados se desempeñarán como auxiliares de la justicia con objetividad, imparcialidad, independencia, responsabilidad, oportunidad, puntualidad, rectitud, veracidad, corrección y honestidad. Su trabajo deberá enmarcarse en todo momento en la ética, con la presentación de su criterio técnico y especializado, exento de juicios de valor de ningún tipo. La obligación de la o el perito es única e integral y comprende las siguientes actividades: cumplir con la designación dispuesta por la autoridad judicial competente, la presentación del informe verbal y/o escrito, la presentación de aclaraciones, ampliaciones u observaciones al informe, la defensa y/o exposición del informe en audiencias orales, de prueba o de juicio; así como cualquier otra actividad necesaria dispuesta por autoridad judicial competente. En el caso de las personas jurídicas, las obligaciones serán cumplidas por cada uno de los expertos que formen parte de ellas y se hayan calificado como peritos; la persona jurídica calificada como perito tendrá responsabilidad solidaria respecto al cumplimiento de dichas obligaciones, debiendo garantizar que sus condiciones de organización, físicas y tecnológicas permitan a sus peritos cumplir sus funciones a cabalidad (CONSEJO DE LA JUDICATURA, 2022).

Código orgánico General de Procesos (COGEP)

PERITO

Art. 221.- Perito. Es la persona natural o jurídica que, por razón de sus conocimientos científicos, técnicos, artísticos, prácticos o profesionales está en condiciones de informar a la o al juzgador sobre algún hecho o circunstancia relacionado con la materia de la controversia. Aquellas personas debidamente acreditadas por el Consejo de la Judicatura estarán autorizadas para emitir informes periciales, intervenir y declarar en el proceso. En el caso de personas jurídicas, la declaración en el proceso será realizada por el perito acreditado que realice la pericia. En caso de que no existan expertos acreditados en una materia específica, la o el juzgador solicitará al Consejo de la Judicatura que requiera a la institución pública, universidad o colegio profesional, de acuerdo con la naturaleza de los conocimientos necesarios para la causa, el envío de una terna de profesionales que puedan acreditarse como peritos para ese proceso en particular (ASAMBLEA NACIONAL, 2022).

Art. 222.- Declaración de peritos. (Reformado por el Art. 30 de la Ley s/n, R.O. 517-S, 26-VI-2019). - La o el perito será notificado en su dirección electrónica con el señalamiento de día y hora para la audiencia de juicio o única, dentro de la cual sustentará su informe. Su comparecencia es obligatoria. En caso de no comparecer por caso fortuito o fuerza mayor, debidamente comprobado y por una sola vez, se suspenderá la audiencia, después de haber practicado las demás pruebas y se determinará el término para su reanudación. En caso de inasistencia injustificada, su informe no tendrá eficacia probatoria y perderá su acreditación en el registro del Consejo de la Judicatura. En la audiencia las partes podrán interrogarlo bajo juramento, acerca de su idoneidad e imparcialidad y sobre el contenido del informe, siguiendo las normas previstas para los testigos. Las partes tendrán derecho, si lo consideran necesario, a interrogar nuevamente al perito, en el orden determinado para el testimonio. En ningún caso habrá lugar a procedimiento especial de objeción del informe por error esencial, que únicamente podrá alegarse y probarse en la audiencia. Concluido el contrainterrogatorio y si existe divergencia con otro peritaje, la o el juzgador podrá abrir el debate entre peritos de acuerdo con

lo previsto en este Código. Finalizado el debate entre las o los peritos, la o el juzgador, abrirá un interrogatorio y contrainterrogatorio de las partes, exclusivamente relacionado con las conclusiones divergentes de los informes. La o el juzgador conducirá el debate. (ASAMBLEA NACIONAL, 2022)

Art. 223.- Imparcialidad del perito. La o el perito desempeñará su labor con objetividad e imparcialidad. Durante la audiencia de juicio o única podrán dirigirse a la o al perito, preguntas y presentar pruebas no anunciadas oportunamente orientadas a determinar su parcialidad y no idoneidad, a desvirtuar el rigor técnico o científico de sus conclusiones, así como cualquier otra destinada a solventar o impugnar su credibilidad (ASAMBLEA NACIONAL, 2022)

INFORME PERICIAL

Art. 224.- Contenido del informe pericial. Todo informe pericial deberá contener, al menos, los siguientes elementos: 1) **N**ombres y apellidos completos, número de cédula de ciudadanía o identidad, dirección domiciliaria, número de teléfono, correo electrónico y los demás datos que faciliten la localización del perito, 2) La profesión, oficio, arte o actividad especial ejercida por quien rinde el informe, 3) El número de acreditación otorgado por el Consejo de la Judicatura y la declaración de la o del perito de que la misma se encuentra vigente, 4) La explicación de los hechos u objetos sometidos a análisis, 5) El detalle de los exámenes, métodos, prácticas e investigaciones a las cuales ha sometido dichos hechos u objetos, 6) Los razonamientos y deducciones efectuadas para llegar a las conclusiones que presenta ante la o el juzgador; Las conclusiones deben ser claras, únicas y precisas (ASAMBLEA NACIONAL, 2022).

Art. 225.- Solicitud de pericia. Cuando alguna de las partes justifique no tener acceso al objeto de la pericia, solicitará en la demanda o contestación, reconvención o contestación a la reconvención, que la o el juzgador ordene su práctica y designe el perito correspondiente. El informe pericial será notificado a las partes con el término de por lo menos diez días antes de la audiencia, término que podrá ser ampliado a criterio de la o del juzgador y de acuerdo con la complejidad del informe (ASAMBLEA NACIONAL, 2022).

Art. 226.- Informe pericial para mejor resolver. En caso de que los informes periciales presentados por las partes sean recíprocamente contradictorios o esencialmente divergentes sobre un mismo hecho, la o el juzgador podrá ordenar el debate entre sí de acuerdo con lo dispuesto en el presente Código. Si luego del debate entre las o los peritos, la o el juzgador mantiene dudas sobre las conclusiones de los peritajes presentados, ordenará en la misma audiencia un nuevo peritaje, para cuya realización sorteará a una o un perito de entre los acreditados por el Consejo de la Judicatura, precisando el objeto de la pericia y el término para la presentación de su informe, el mismo que inmediatamente será puesto a conocimiento de las partes. En aquellos casos en que una de las partes sea representada por una o un defensor público o demuestre tener escasos recursos económicos, los honorarios y gastos del peritaje, podrán ser cubiertos por el Consejo de la Judicatura, a petición de esta. (ASAMBLEA NACIONAL, 2022).

Art. 227.- Finalidad y contenido de la prueba pericial. La prueba pericial tiene como propósito que expertos debidamente acreditados puedan verificar los hechos y objetos que son materia del proceso. Las partes procesales, podrán sobre un mismo hecho o materia, presentar un informe elaborado por una o un perito acreditado (ASAMBLEA NACIONAL, 2022).

CAPITULO III

METODOLOGÍA

La metodología a ser empleada en el desarrollo del presente trabajo parte de la investigación documental argumentativa o exploratoria hasta llegar a la investigación aplicada, mediante la correcta selección de procesos de extracción de información en los dispositivos móviles con componentes deteriorados se logrará cumplir los objetivos planteados. Para la presente investigación, se ha elegido los siguientes métodos de investigación:

3.1 Tipo de Investigación

Investigación Aplicada

Para el desarrollo del proyecto se selecciona la investigación aplicada, que tiene por objetivo buscar la solución a un problema específico enfocándose en la búsqueda y consolidación del conocimiento. Esta depende de la recolección de información de las distintas teorías y procesos de análisis forense, y así en base a la teoría recolectada se puede generar conocimiento práctico para la extracción de información.

3.2 Enfoque de la investigación

Para la extracción de información en dispositivos móviles con componentes deteriorados bajo terminales Android se establecerá la utilización del enfoque mixto que representa la integración o combinación entre los enfoques cualitativo y cuantitativo. El enfoque cuantitativo se fundamenta en un esquema deductivo y lógico que busca formular preguntas de investigación e hipótesis para posteriormente probarlas y por otro lado el enfoque cualitativo permite la obtención de información, recolección de datos y herramientas utilizadas para la extracción de información, también permite definir las diferentes características de cada de una de las herramientas y métodos utilizados, así como sus ventajas y desventajas. (Sampieri, 2014)

3.3 Métodos de Investigación

Método Bibliográfico

Se eligió este método de investigación porque se centra en el análisis de tesis, modelos, estudios, revistas, artículos científicos, libros desarrollados para profundizar en los lineamientos relacionados con el análisis de investigación, con el fin de aportar un valor agregado al objeto que se está tratando, estudio de las leyes y reglamentos vigentes en el país como el COIP, COGEP y Ley del comercio electrónico, firmas y mensajes de datos.

El avance continuo de la tecnología, así como el desarrollo, el uso de dispositivos y la creación de nuevas formas de cometer delitos a través de dispositivos móviles demuestran la necesidad de métodos y herramientas de software libre para la extracción de información. Para llevar a cabo este proceso, se seleccionarán los equipos e instrumentos disponibles, siguiendo una metodología basada en un estudio bibliográfico de métodos nacionales e internacionales. A través de esta investigación se establecerá el valor de la información almacenada en los dispositivos móviles, de ahí la importancia de investigar fuentes bibliográficas confiables que ayuden a organizar la información para la redacción y elección una metodología para análisis forense. lo que contribuirá al hallazgo de la evidencia digital.

3.4 Técnicas e Instrumentos de Recopilación de Datos

En este proyecto se utilizará la técnica de la observación y recopilación bibliográfica para contar con material informativo como son: videos tutoriales, guías, libros, artículos y sitios web, con el objetivo de determinar la importancia de cada metodología, utilización de diferentes técnicas invasivas y las herramientas necesarias para el proceso de análisis forense y así lograr extraer la información de dispositivos móviles deteriorados.

Metodología de desarrollo del análisis forense

Para la metodología de desarrollo se va a utilizar la revisión de trabajos, herramientas, métodos existentes y relacionados con el tema de investigación propuesto.

Para la extracción de información de los dispositivos móviles se utilizará la metodología (DFRWS), lo cual se van a tomar las fases necesarias para su desarrollo. En la siguiente figura se proporciona una descripción del proceso a considerar para la extracción de la evidencia en dispositivos móviles con sistema operativo Android.

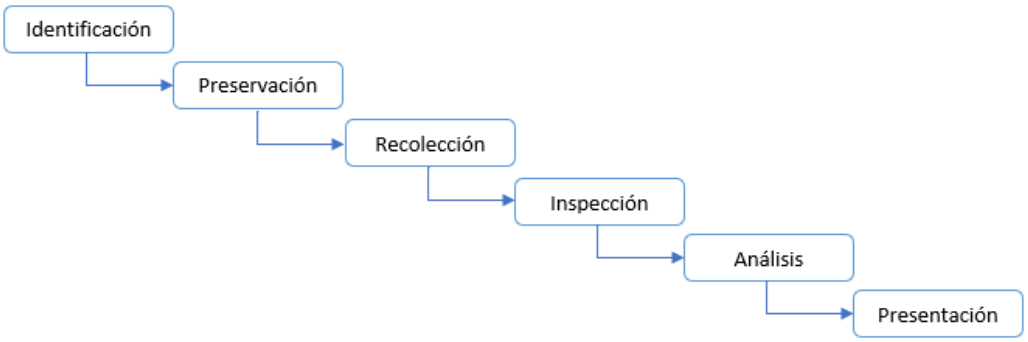


Ilustración 2

Diagrama Model Digital Forensic Research Workshops (DFRWS) Fuente: Traducido y adaptado de *(Sachowski, 2019)*

Como se muestra en la ilustración 2, para la extracción de información en un dispositivo móvil deteriorado se consideran las siguientes fases: Identificación, preservación, recolección, inspección, análisis y presentación. Para la ejecución del proyecto se ha definido trabajar sobre un escenario con equipos reales, para la extracción de información en casos extremos se van utilizar las herramientas y modelos seleccionados con anterioridad con el objetivo de obtener evidencia digital de los dispositivos móviles.

Tabla 3

Características de los equipos

Tipo de Escenario	Equipo	Marca	Modelo	Sistema Operativo	Memoria Ram	Procesador	CPU	Almacenamiento interno
Real	1	SAMSUNG	SM-J510MN	Android 5.1 Lollipop	2 GB	Qualcomm Snapdragon 410 MSM8916	Qualcom adreno 306 1200 MHz	16 GB
Real	1	SAMSUNG	SM-A5	Android OS, v4.4.4 KitKat	2 GB	Qualcomm MSM8916	Snapdragon 410 quad-core 1.2GHz	16 GB

De acuerdo a las fases indicadas anteriormente, a continuación, se detalla el proceso a seguir:

Fases de identificación y preservación

Sobre el proceso mencionado anteriormente, se elabora la documentación con la información más relevante del dispositivo a analizar, además se llevará un detalle documental de las pruebas que se realicen en cada dispositivo, que servirá para verificar y evaluar los resultados. La información que se registra es marca, modelo, serie, versión de sistema operativo, memoria RAM, capacidad de almacenamiento interno, etc.

Siguiendo el modelo propuesto se procede con el registro de información del equipo para nuestro caso de estudio. Las actividades a realizar en esta fase son:

a) Evidenciar la imagen del equipo a analizar
b) Registrar información del equipo en una ficha

Se inicia la identificación del dispositivo móvil objeto de investigación, se realiza la inspección visual con la finalidad de conocer el estado del equipo y si está operativo se procede a registrar en la ficha como se puede ver en la ilustración 3 y tabla 4.

Ilustración 3

Equipo destinado a analizar Samsung Galaxy A5

Ilustración 4

Equipos destinados a analizar Samsung Galaxy J5

Tabla 4

Ficha de registro de información del dispositivo móvil Samsung Galaxy J5

Ficha técnica de dispositivos móviles						
Perito	Jerson Chimbo Henry Sinche					
Numero de caso	002					
Fecha	05 de septiembre de 2022					
Hora	10:00					
Ítem	**Tipo**	**Marca**	**Serie**	**Modelo**	**Estado**	**Observaciones**
1	Celular	Samsung	RV8J40W5WLR	SM-J510MN	Dañado	El teléfono presenta indicios de haber sido estrellado contra el piso, razón por la cual sus

						componentes, (pantalla) se encuentra dañado.

Tabla 5

Ficha de registro de información del dispositivo móvil Samsung A5

Ficha técnica de dispositivos móviles						
Perito	Jerson Chimbo Henry Sinche					
Numero de caso	003					
Fecha	03 de octubre de 2022					
Hora	10:00					
Ítem	**Tipo**	**Marca**	**Serie**	**Modelo**	**Estado**	**Observaciones**
1	Celular	Samsung	RF8K52CNN9J	Samsung Galaxy A5	Dañado	El dispositivo móvil presenta un corto circuito por estar sumergido en agua, por tal razón, la placa de circuitos, el SM-1 y SM-2, los conectores de batería y los componentes conectados directamente a las

	baterías están severamente corroídos, por lo cual el dispositivo se apagó y no volvió a encender.

A continuación, se procedió al desensamblaje de los dispositivos móviles para de esta manera obtener la placa del teléfono y poder continuar con el proceso de análisis forense, como se muestra a continuación:

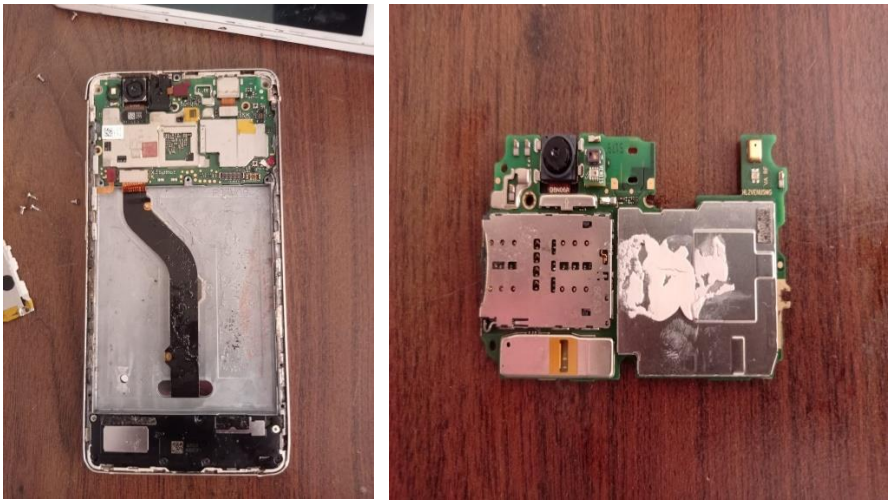


Ilustración 5

Placa base Samsung Galaxy J5

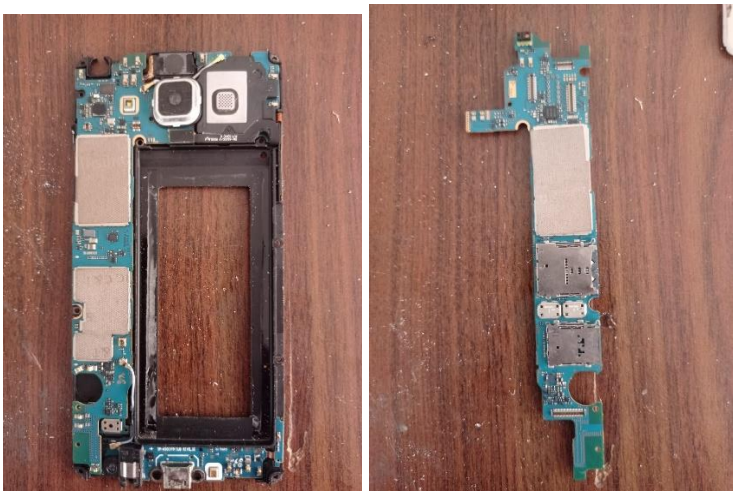


Ilustración 6

Placa base Samsung Galaxy A5

Fases de Recolección e Inspección

En esta fase se procede a realizar una extracción física del dispositivo móvil con la obtención de la información almacenada en la memoria ROM del teléfono, a través de la técnica invasiva chip-off y Hex-Dump/JTAG, se realizó un respaldo exacto de bit a bit de la memoria ROM del dispositivo sin alterar su integridad.

Obtención de la imagen forense del dispositivo móvil Samsung Galaxy A5 mediante la técnica CHIP-OFF

Como se mencionó anteriormente en la **tabla 6** el dispositivo móvil A5 se encontró en un estado avanzado de corrosión por estar expuesto a humedad, por tal razón la placa de circuitos, los conectores de batería y los componentes conectados directamente a la batería están severamente corroídos, por lo que el dispositivo se apagó y no volvió a encender.

Posteriormente se procedió a medir con un multímetro el dispositivo móvil y se comprobó que el ánodo y el cátodo del conector de la batería del dispositivo SM probado estaban en cortocircuito. Por lo tanto, procedimos a secar el dispositivo, eliminamos los contaminantes limpiando la placa de circuito con alcohol isopropílico y un cepillo suave. Después de limpiar y confirmar que ya no haya ningún cortocircuito en el conector de la batería del dispositivo SM, se conectó la

placa de circuito a una fuente de alimentación de carga continua y se procedió a encender, dando como resultado que el dispositivo SM no arrancó correctamente.

Después de determinar que el dispositivo ya no tiene arreglo y los chips de circuitos integrados de gestión de energía (PMIC por sus siglas en inglés) ya no estaban montados correctamente en la placa debido a la pérdida de soldadura y los cortocircuitos ocasionados, por lo tanto, procedimos a extraer con una pistola de calor la memoria ROM del dispositivo SM para poder obtener la información almacenada en el dispositivo.

Mediante la técnica invasiva chip-off se procede a extraer la memoria ROM del teléfono ubicada en la placa base dicho proceso nos permitirá tener acceso a la información para poder generar una imagen forense. Con ayuda de la herramienta Guymager se procede a crear una imagen forense en formato .dd, para lo cual la memoria ROM extraída del dispositivo lo conectamos como USB en el computador, se debe constatar que la memoria se encuentre en modo read-only, esto para asegurarse que en el transcurso del proceso no se vaya a modificar la información que contiene la memoria y de esta manera crear la imagen forense del dispositivo móvil la cual nos permitirá tener acceso información del dispositivo y por ende poder extraer datos como contactos, llamadas, mensajes, cuentas de Gmail, chats de WhatsApp y multimedia. Como se muestra a continuación:

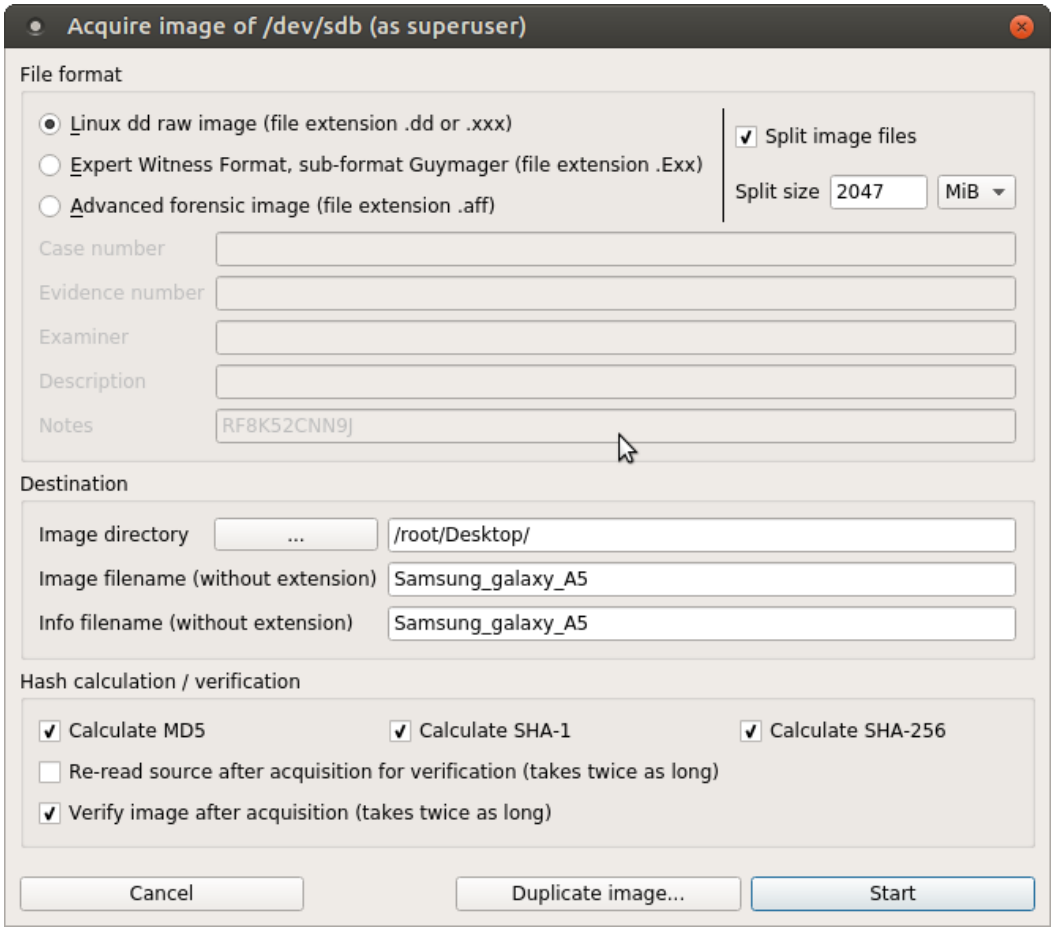


Ilustración 7

Ruta y formato de la Imagen Forense

A continuación, se procede a crear la imagen forense:

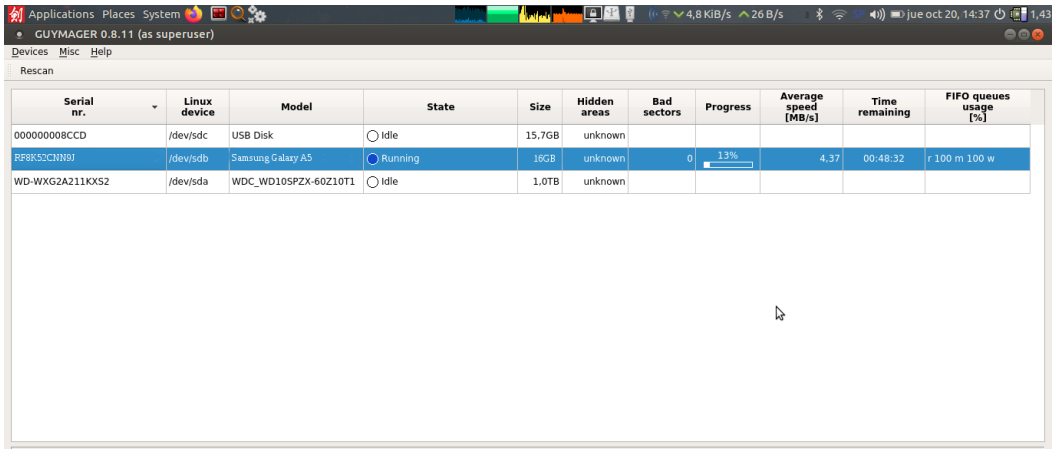
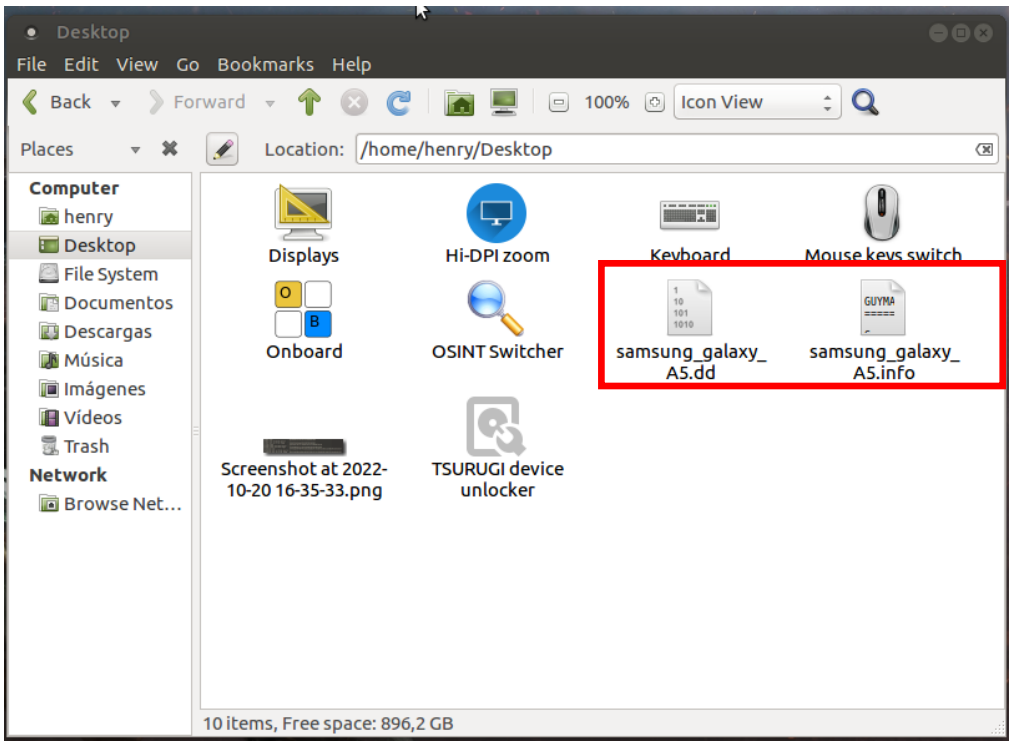


Ilustración 8

Creación de la Imagen Forense

Después de aproximadamente 4 horas finalizo el proceso de extracción y se obtiene la imagen forense creada en el directorio seleccionado.

Ilustración 9



Obtención de la Imagen Forense

Nota: La creación de la imagen forense tarda de acuerdo al espacio de almacenamiento del dispositivo móvil.

Ademas, se obtuvo los hashes (md5, sha1, sha256) de la imagen forense con el proposito de cuidar la integridad de la informacion extraida.

```
89 MD5 hash                   : dd7a60ae67fe2e354a75c09dabaf2629
90 MD5 hash verified source   : --
91 MD5 hash verified image    : 0a0330158116ee9769c00070199e8b22
92 SHA1 hash                  : 4a9f9e6579df72726d607607017c49bb8622a1a6
93 SHA1 hash verified source  : --
94 SHA1 hash verified image   : 7e541098aea1c114229cee690cdafa1a6b7c4847
95 SHA256 hash                : 50f766d2078f90ff41660dc0adb0247175b4d931a482513268ba9022eb513b54
96 SHA256 hash verified source: --
97 SHA256 hash verified image : db6542dd2801dcbb844803d25b68124511459dd6038136ab556c6ea0a6ebe782
```

Ilustración 10

Hashes de la Imagen Forense

Análisis de la imagen forense del dispositivo Samsung Galaxy A5

Para el respectivo análisis de la imagen forense del dispositivo móvil se procedió abrir la imagen forense en la herramienta Autopsy la cual permite visualizar toda la información que contenía el dispositivo como se muestra a continuación:

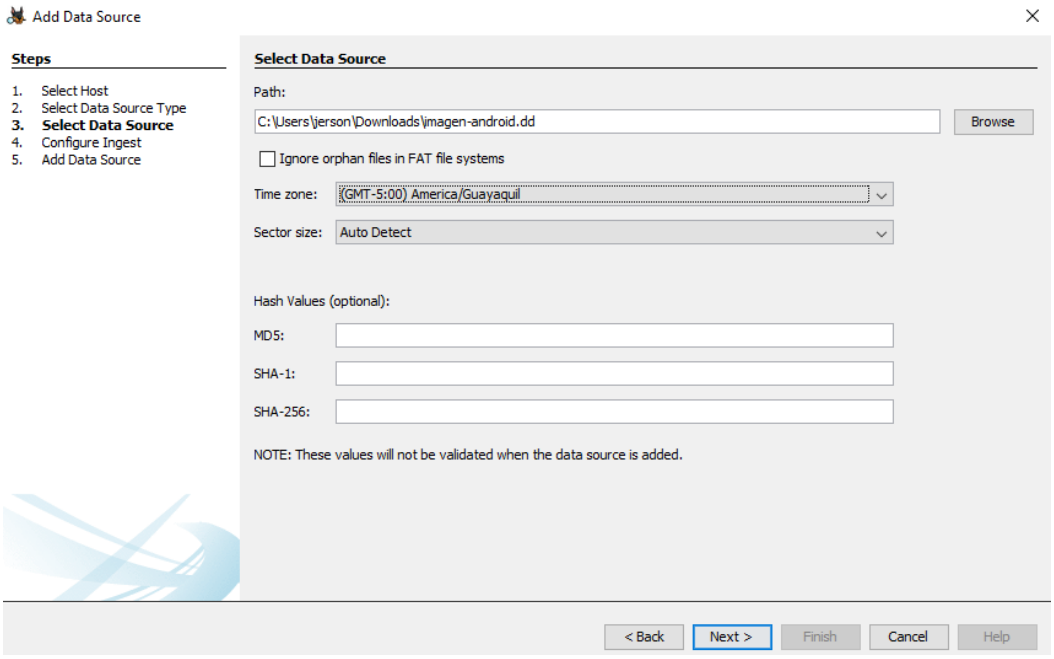


Ilustración 11

Carga de la Imagen Forense

Luego de cargar la imagen forense en Autopsy se pasó a seleccionar los módulos de los cuales se desea obtener la información.

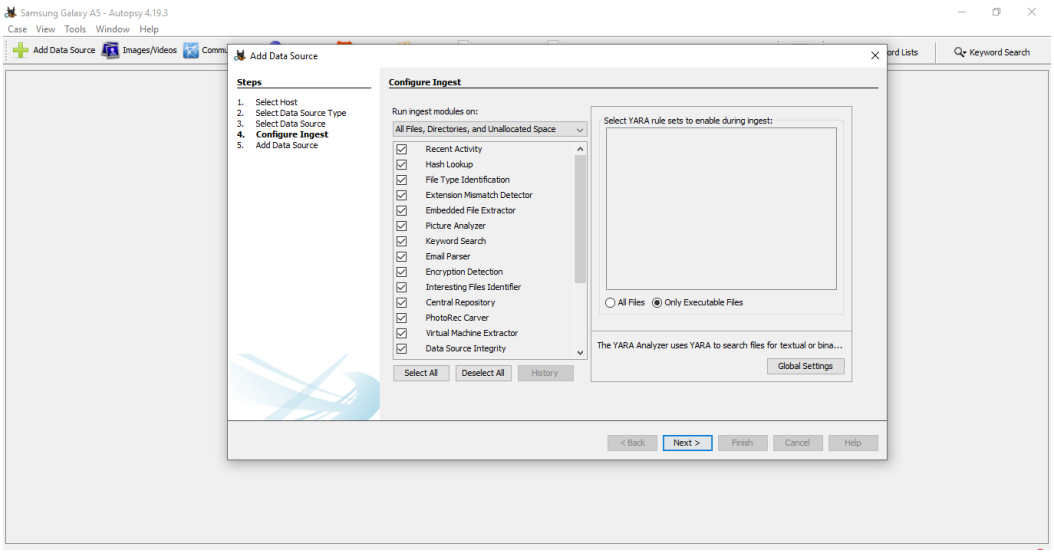


Ilustración 12

Selección de Módulos

Finalizada la carga de la imagen forense se puede visualizar toda la información que estaba dentro de la misma como contactos, registro de llamadas, mensajes, cuentas de Gmail, chats de WhatsApp y archivos de multimedia.

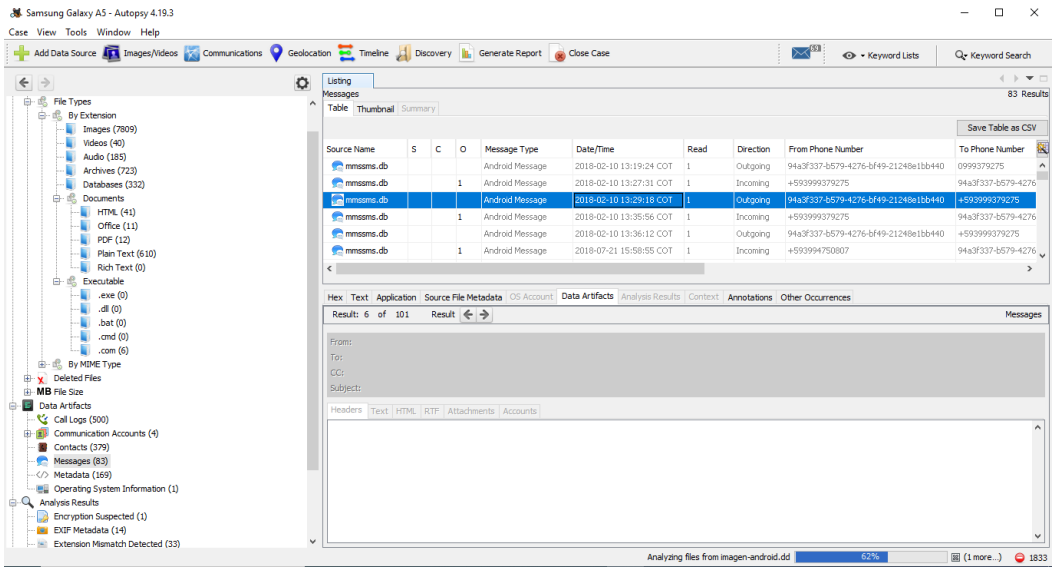


Ilustración 13

Contenido de la Imagen Forense

Teniendo acceso a la información de la imagen forense mediante la herramienta Autopsy se puede tener acceso a logs de llamadas, registro de contactos, imágenes, videos, archivos mp3, mensajes SMS, programas instalados, documentos almacenados, historial web de navegación, cuentas de correo electrónicos, archivos eliminados, entre otros.

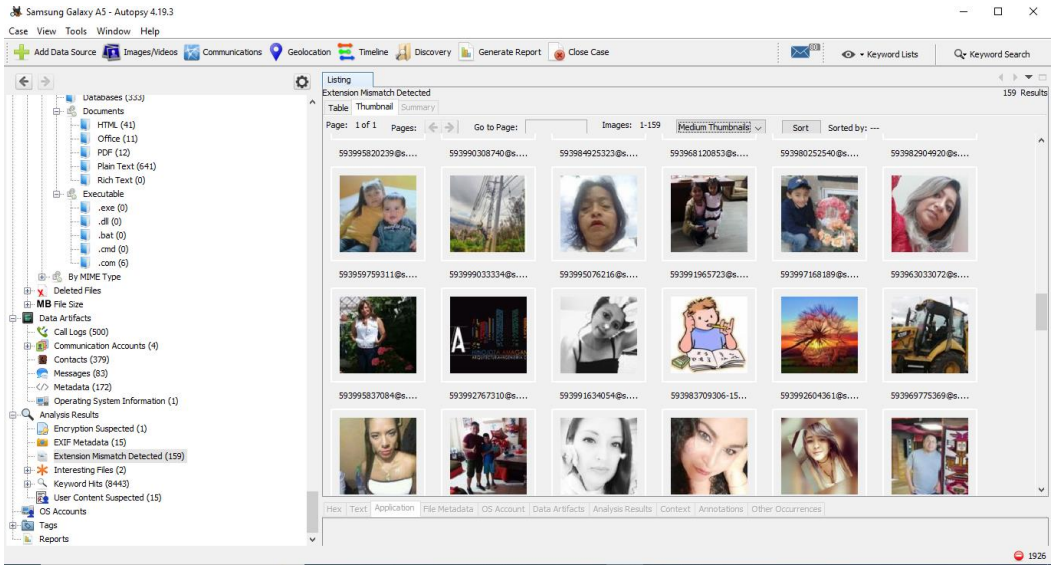


Ilustración 14

Imágenes almacenadas en el dispositivo

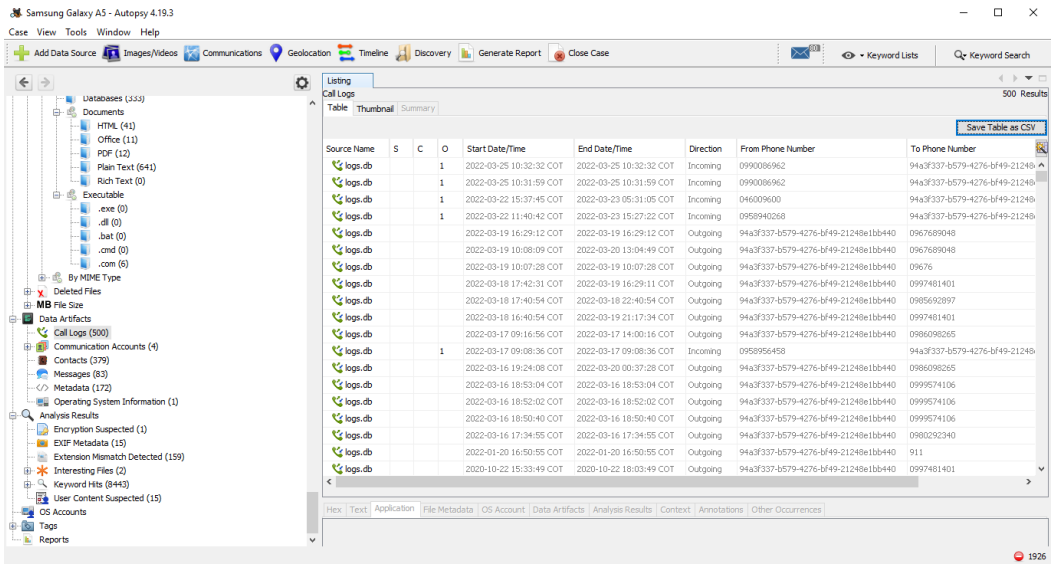


Ilustración 15

Logs de llamadas

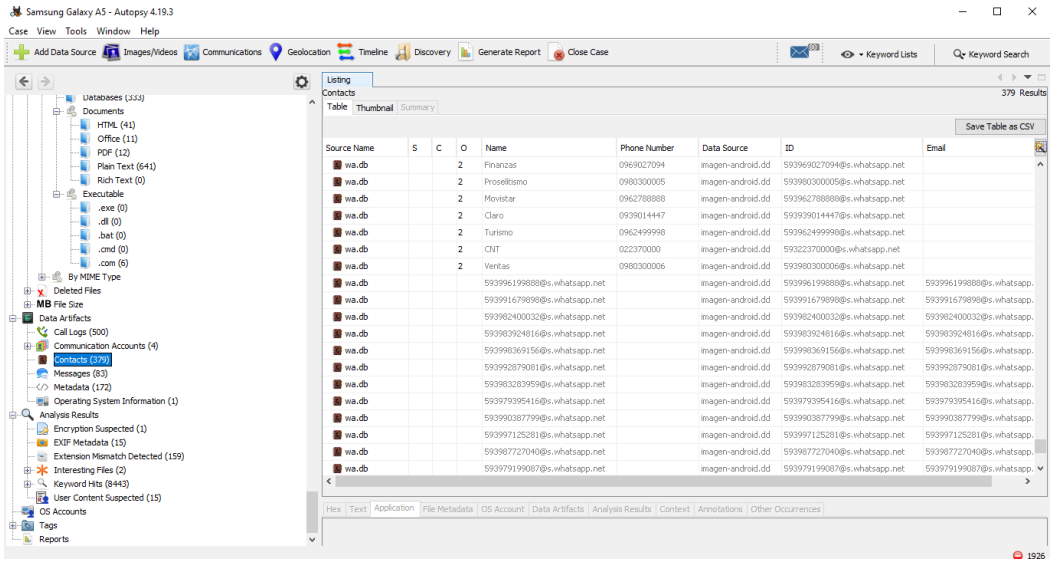


Ilustración 16

Registro de Contactos

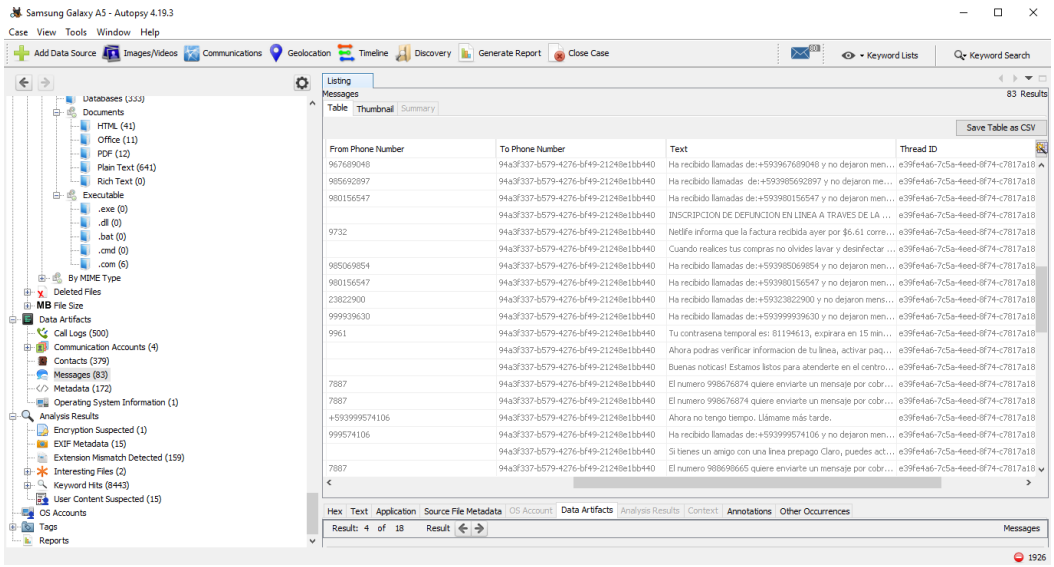


Ilustración 17

Mensajes SMS

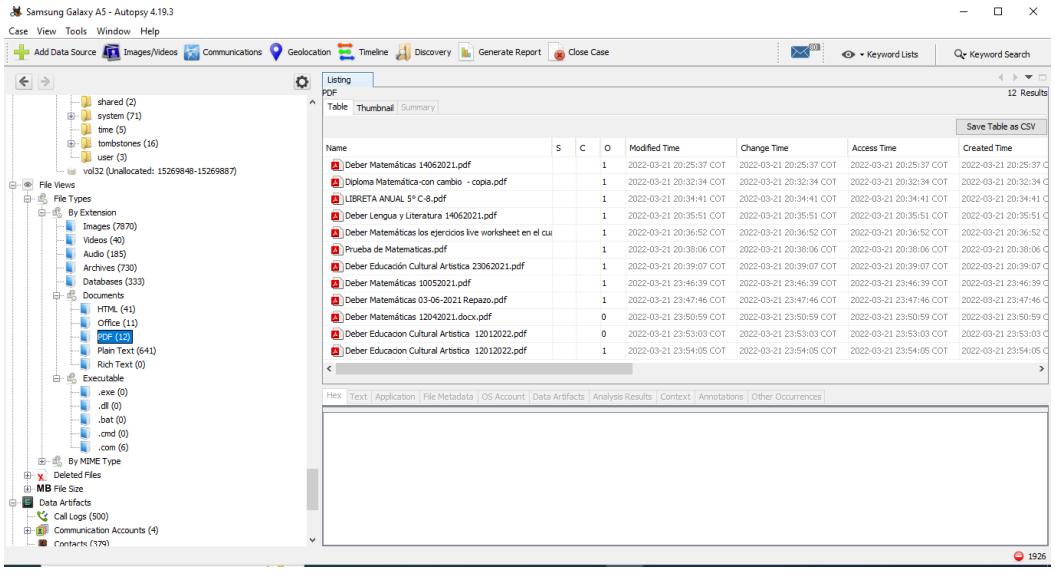


Ilustración 18

Archivos PDF

Obtención de la Imagen forense del dispositivo móvil Samsung J5 mediante la técnica invasiva HEX-DUMP/JTAG

Como se especifica en la **tabla 5,** el dispositivo móvil Samsung J5 no tiene daños muy severos en su arquitectura física, el dispositivo móvil solo presenta daño en uno de sus componentes (pantalla) por tal motivo no es viable aplicar la técnica invasiva del chif-off, también se procedió a realizar las diferentes pruebas con el fin de descartar más daños en sus componentes, dando como resultado que la placa de circuitos, los conectores de batería y los componentes conectados directamente a la batería están funcionando con normalidad, por lo que el dispositivo no presentó ninguna falla al encender.

Después de determinar que el dispositivo si tiene arreglo y los chips de circuitos integrados de gestión de energía (PMIC por sus siglas en inglés) están montados correctamente en la placa, por lo tanto, se puede extraer la información almacenada en el dispositivo.

Por medio la técnica invasiva JTAG se procede a extraer una backup de los archivos que contiene la memoria del dispositivo y si fuera el caso también de la memoria extraíble del teléfono. Con ayuda del SO Tsurugi y de la herramienta adb inicia con el proceso de la creación de la backup del dispositivo, para ello, primero debemos abrir un terminal en Tsurugi con privilegios de super usuario esto para que no nos

genere error alguno al digitar algunos comandos en el terminal, una vez que estemos como root dentro del terminal se procede a digitar la siguiente línea de comando "adb devices" esto con el fin de establecer una conexión con el dispositivo móvil, ver ilustración 9.

Ilustración 19

Conexión con el dispositivo

Una vez que se ha establecido la conexión con el dispositivo se da inicio al proceso de la creación de la backup del dispositivo, para ello se debe digitar el comando "adb backup -all -shared -apk -f samsung_j5.ab" y de esta manera crear una imagen forense parcial del dispositivo móvil la cual nos permitirá tener acceso información del dispositivo y por ende poder extraer datos como contactos, llamadas, mensajes, cuentas de Gmail, chats de WhatsApp y multimedia.

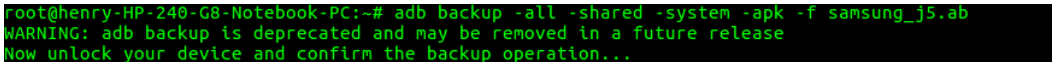


Ilustración 20

Generación de la backup del dispositivo

Debemos confirmar la operación en el dispositivo móvil.

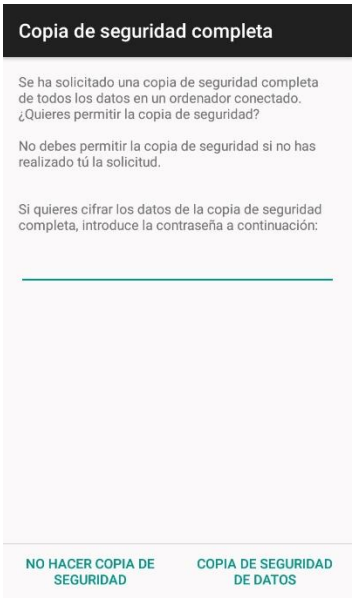


Ilustración 21

Confirmación de la operación en el dispositivo móvil

Después de aproximadamente 30 minutos, la imagen forense se ha creado, cabe recalcar que la imagen se crea solo de las carpetas a las que el usuario tiene acceso como, galería, descargas, entre otras, por tal motivo el tiempo de creación es más corto.

Ilustración 22

Imagen Forense parcial del dispositivo móvil

Una vez obtenida la imagen forense se deben crear los hashes (md5, sha224, sha256), esta acción es necesaria para mantener la integridad de la imagen y de esta manera verificar si se alteró el contenido de información de la imagen forense.

```
henry@henry-HP-240-G8-Notebook-PC:~/38523a1821a36b1/20221012_14_29_12_backup$ md
5sum samsung_j5.ab
04ab341deca3abe566b3371304bd8d88  samsung_j5.ab
henry@henry-HP-240-G8-Notebook-PC:~/38523a1821a36b1/20221012_14_29_12_backup$ sh
a224sum samsung_j5.ab
f24c820a32a16f9be3e219fcf9d10ebfe8a1983027558320493ec8fc  samsung_j5.ab
henry@henry-HP-240-G8-Notebook-PC:~/38523a1821a36b1/20221012_14_29_12_backup$ sh
a256sum samsung_j5.ab
4101446e33f81096bf0afcd54347327c803ce6a305e1a2b12e8884b89a8fae1c  samsung_j5.ab
henry@henry-HP-240-G8-Notebook-PC:~/38523a1821a36b1/20221012_14_29_12_backup$
```

Ilustración 23

Hash de la imagen forense

Análisis de la imagen forense del dispositivo Samsung Galaxy J5

Para el siguiente análisis de la imagen forense del dispositivo móvil SM se procedió a crear el caso y abrir la imagen forense en la herramienta Autopsy la cual permite visualizar toda la información que contenía el dispositivo como se muestra a continuación:

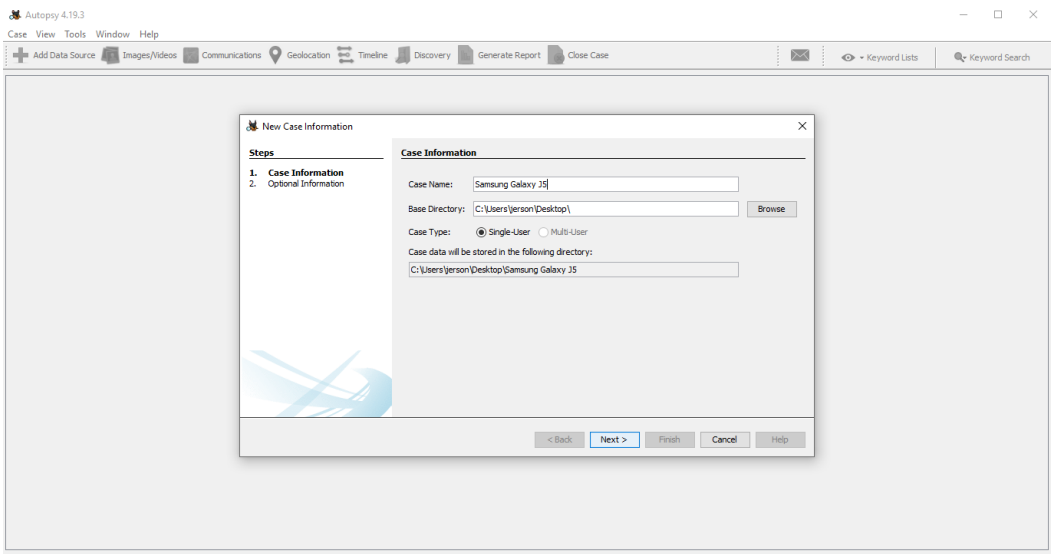


Ilustración 24

Creación del Caso a Analizar

Selección de la ruta de la imagen forense para proceder a cargarlo en Autopsy.

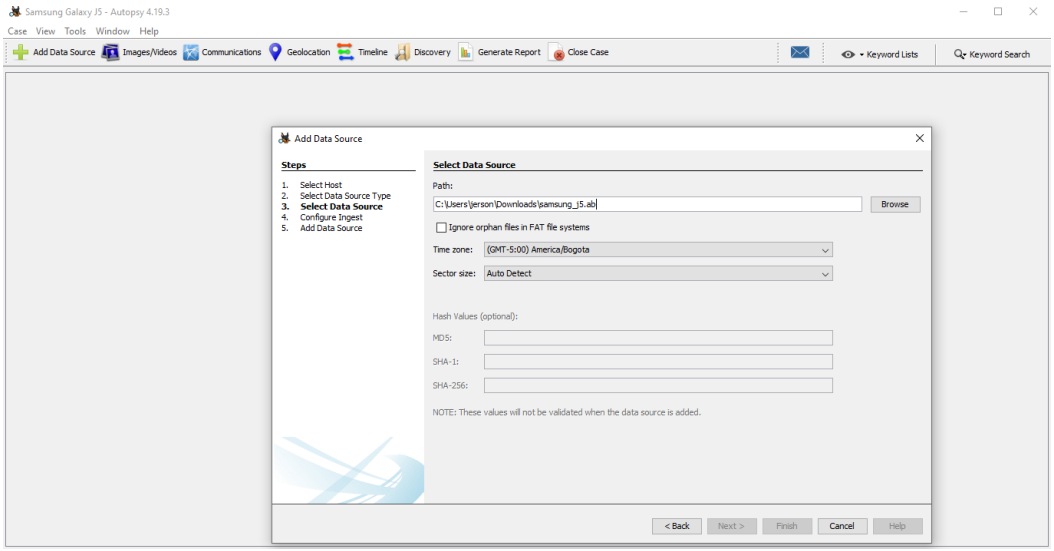


Ilustración 25

Carga de la Imagen Forense SM J5

Una vez cargado la imagen forense en la herramienta Autopsy se procedió a seleccionar los módulos que son necesarios para la adquisición de la información.

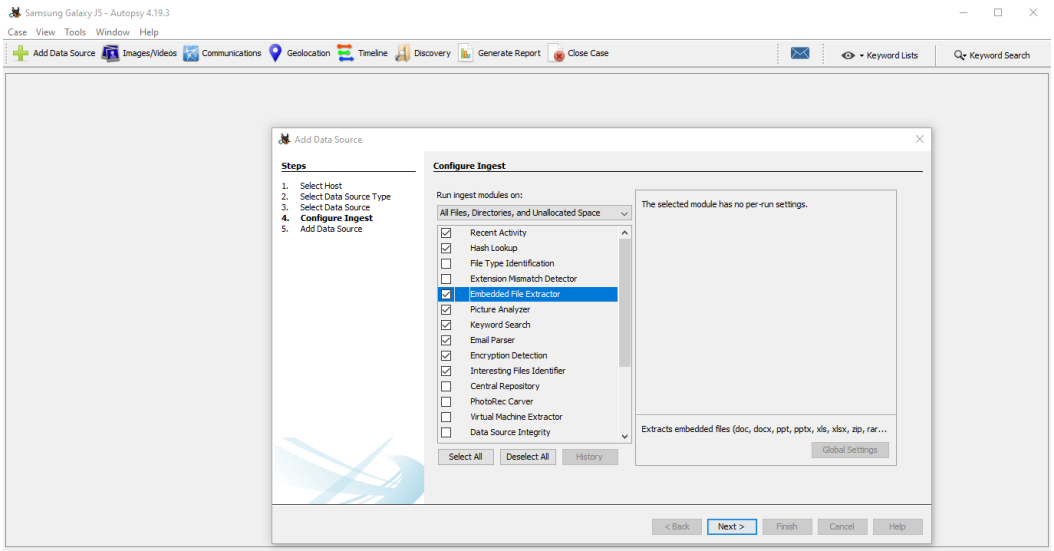


Ilustración 26

Selección de Módulos SM-J5

Terminado la carga de la imagen forense se podrá tener acceso al contenido de la imagen forense y un backup de la base de datos del dispositivo móvil.

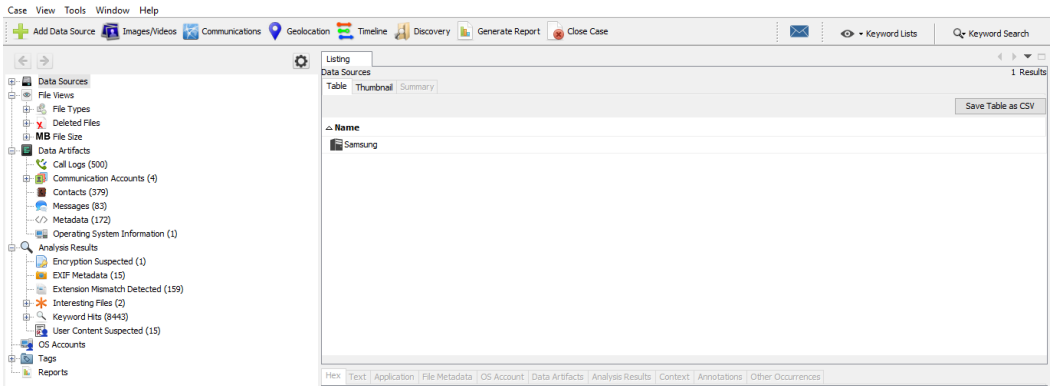


Ilustración 27

Carga Finalizada de la Imagen Forense SM-J5

Teniendo acceso a la información de la imagen forense mediante la herramienta Autopsy se puede tener acceso a logs de llamadas, registro de contactos, mensajes SMS, programas instalados, carpetas de archivos y un backup de todas las bases de datos que contenía el dispositivo móvil.

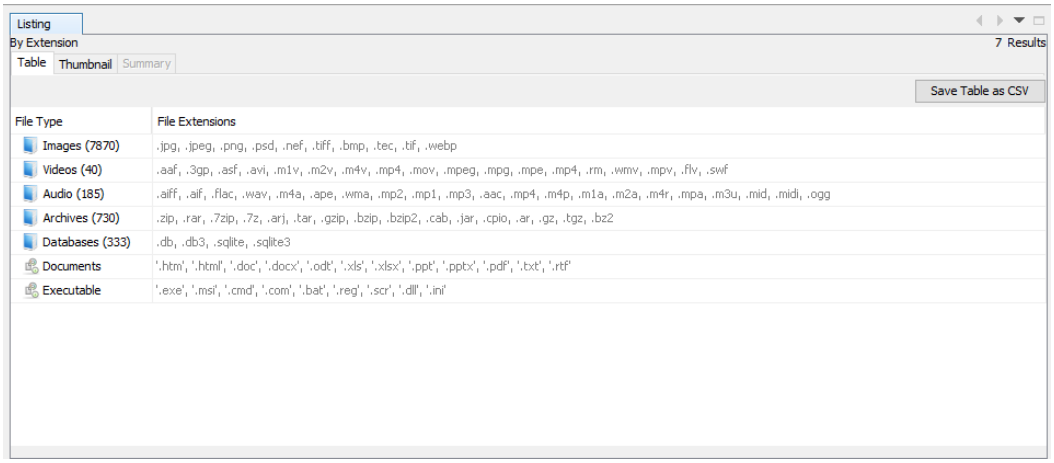


Ilustración 28

Carpeta de Archivos

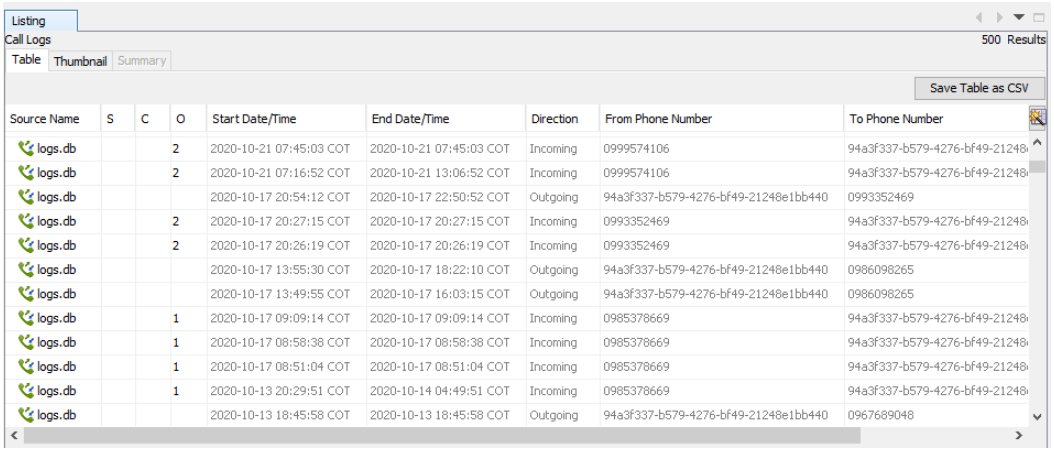


Ilustración 29

Logs de Llamadas

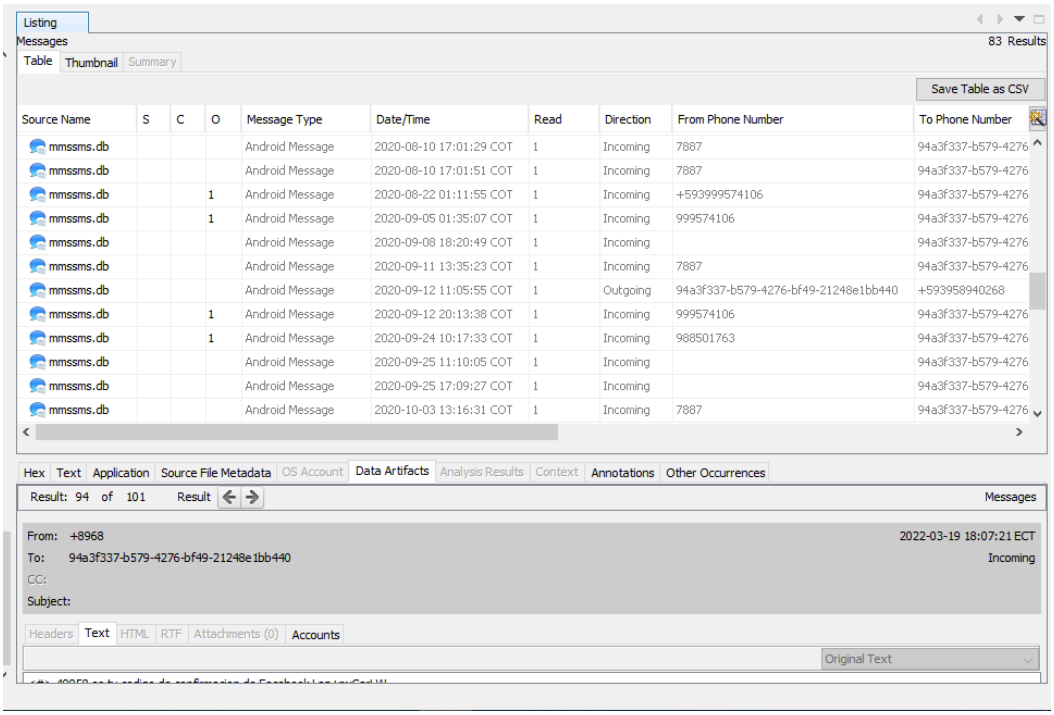


Ilustración 30

Mensajes registrados

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1 Análisis, Interpretación y Discusión de los Resultados

Preguntas de investigación

¿Qué métodos y técnicas de análisis forense permitirán la extracción de información de un dispositivo móvil cuando sus componentes han sido afectados?

Para la extracción de información de dispositivos móviles deteriorados se utilizó la metodología de Model Digital Forensic Research Workshops (DFRWS) aplicando cada una de las fases como son: identificación, preservación, recolección, inspección, análisis y presentación. Se definió dos escenarios con equipos reales para realizar la labor forense, entre las técnicas invasivas utilizadas están el chip-off y hex-dump/JTAG las cuales permitieron extraer gran parte de la información almacenada en el dispositivo móvil.

¿Cuáles serán las herramientas open source adecuadas para extraer información de dispositivos móviles Android con componentes en mal estado?

Las herramientas software que se utilizaron son Guymager y el sistema operativo tsurugi para la creación de la imagen forense del dispositivo móvil, además, una vez obtenida la data se emplea la herramienta Autopsy para poder acceder al contenido de la información extraída del dispositivo móvil deteriorado como chats de WhatsApp, fotos, videos, archivos, correos electrónicos y multimedia.

¿Al aplicar una técnica invasiva de extracción de información será posible obtener evidencia digital de dispositivos móviles Android con componentes afectados?

El uso de la técnica invasiva chip-off permite extraer la memoria ROM de la placa del dispositivo móvil, aun cuando el teléfono haya sido totalmente destruido sus componentes, para luego extraer la imagen forense ya que esta técnica permite realizar una copia exacta de bit a bit de la memoria.

Comprobación de la hipótesis

En los dispositivos móviles con daños causados por el agua, se ha optado por el análisis de chip-off como método eficaz de recuperación de datos. Sin embargo, con la implantación del cifrado de todo el disco, el análisis de chip-off es cada vez menos prometedor. En muchos casos de dispositivos encriptados, la única opción para extraer los datos del usuario con fines forenses digitales es recuperar la función original del dispositivo y luego introducir el código de desbloqueo/desencriptación. Aunque esto podría lograrse trasplantando las partes eléctricas que contienen los datos del usuario y las claves de descifrado a una placa de circuito de un donante, dado el típico retraso de los laboratorios forenses, no es factible realizar este trasplante para todos los dispositivos dañados por el agua, por tal razón las técnicas invasivas se aplicaron de acuerdo a los daños que poseen el dispositivo.

Una vez que el agua a afectado los metales conductores de los electrodos de las placas de circuito impreso se corroen y se pierden, la reparación de los circuitos eléctricos se vuelve muy difícil, por lo que el chip-off o el trasplante de chip son las únicas opciones para recuperar la función original del dispositivo. Por lo tanto, eliminar la batería y la humedad de un dispositivo dañado por el agua es crítico para detener las reacciones de corrosión en su PCB. Además, el estado de funcionamiento del dispositivo cuando entra en contacto con el agua contribuye al nivel de corrosión del metal.

Al aplicar la técnica invasiva chip-off al dispositivo SM-A5 se procede a extraer la memoria ROM de la placa y así conectarlo como una USB al computador y la herramienta Guymager lo detecta al dispositivo y permite extraer la imagen forense del dispositivo móvil SM-A5 en un lapso de 4 a 5 horas esto debido a que su almacenamiento interno es de 16GB, hay que mencionar que una imagen forense es una copia bit a bit de la memoria ROM del dispositivo, una vez obtenida la imagen forense se procedió a cargarlo en la herramienta Autopsy y así poder visualizar la información contenida en el dispositivo para su respectivo análisis de la evidencia digital.

Mientras tanto la técnica invasiva hex-dump/JTAG se procedió aplicar al dispositivo móvil SM-J5 ya que no presento daños significativos en su arquitectura física, el dispositivo móvil únicamente presento daño en uno de sus componentes

(pantalla) por tal razón no es recomendable aplicar la técnica invasiva del chif-off, también se procedió a realizar las diferentes pruebas con el fin de descartar más daños en sus componentes, dando como resultado que la placa de circuitos, los conectores de batería y los componentes conectados directamente a la batería están funcionando con normalidad, por lo que el dispositivo no presentó ninguna falla al encender. Mediante la técnica invasiva JTAG se procede a extraer una backup de los archivos contenidos en la memoria del dispositivo, Con ayuda del SO Tsurugi y de la herramienta adb se da inicio al proceso de la creación de la backup del dispositivo en un tiempo de 1 a 2 horas ya que esta herramienta solo nos permite extraer información parcial del dispositivo móvil en forma de backup. Posterior a esto se procedió a leer el backup en la herramienta Autopsy para su respectivo análisis de su evidencia digital.

Con base a los escenarios realizados a los dispositivos móviles mediante las técnicas invasivas a dispositivos deteriorados mencionadas anteriormente no se ha podido obtener en su totalidad toda la información almacenada en los dispositivos, se logró obtener y visualizar la evidencia digital como logs de llamadas, registro de contactos, videos, imágenes, SMS, registro de aplicaciones instaladas, conversaciones de Facebook, archivos PDF, DOCX y entre otros. Por otra parte, surgieron algunos inconvenientes al momento de visualizar otro tipo de información para evidenciar algún caso, por ejemplo, la base de datos de WhatsApp debido a sus actualizaciones y mejoras en su seguridad no se encontró la herramienta capaz de abrir la base de datos cripto 14 y 15, también no se puede recuperar archivos que ya fueron eliminados en el dispositivo móvil.

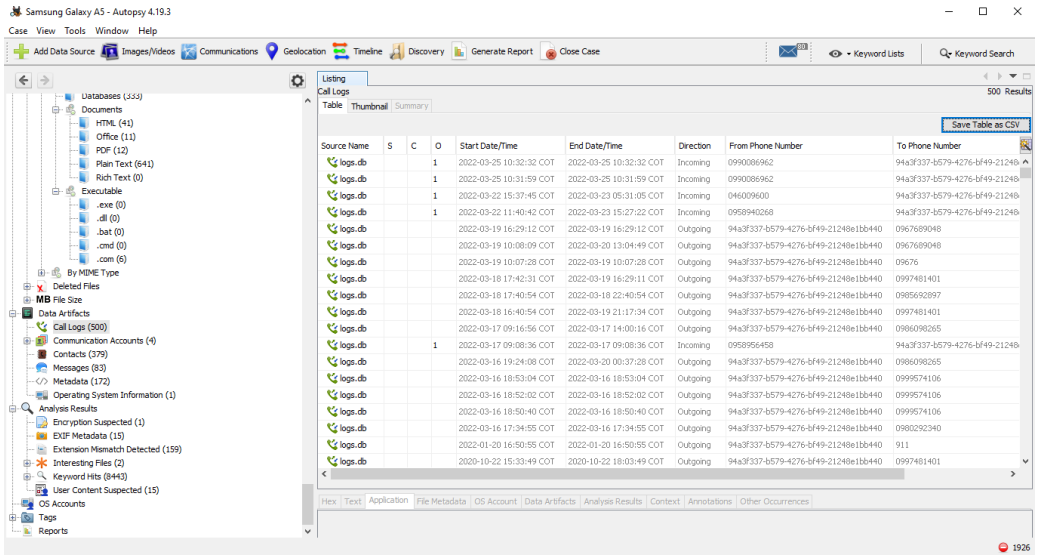


Ilustración 31

Resultados de la Obtención de información

CONCLUSIONES

- En el análisis forense informático existen una gran cantidad de metodologías que pueden utilizarse para realizar el proceso de extracción y búsqueda de información. Cada metodología tiene un enfoque diferente y dependiendo del caso se debe elegir la que mejor se adecue al escenario en el cual se va a trabajar, una elección correcta de la metodología garantizara que el proceso de auditoria forense sea exitoso.
- Al momento de realizar este trabajo, hay algunas herramientas con las cuales no se ha podido trabajar porque han surgido inconvenientes con los procesos de instalación debido a las licencias, pagos o versiones de las mismas. Igualmente ha pasado con las técnicas forenses avanzada de carácter invasiva debido a que usan sistemas específicos como la chip-off, cuyos materiales son costosos y a los cuales no se ha podido tener acceso, por lo cual no se ha podido realizar casos específicos.
- También se ha podido realizar la extracción física y lógica de un dispositivo Android de acuerdo al modelo y versión con la cual hemos verificado cómo acceder a la información del dispositivo y posibles inconvenientes que

pueden surgir relacionados con componentes dañados en casos de pantalla rota, ping de carga dañado y mojados, etc.

- Asimismo, se ha trabajado con varias herramientas con licencias de software libre y se ha podido descargar e instalar en un ordenador para realizar la adquisición y análisis de dispositivos móviles, estas herramientas son Adb, Autopsy y Tsurugi.
- Con la ejecución de técnicas invasivas forenses y los artículos 193, 456 y 500 del COIP mencionan sobre el remplazo de identificación de terminales móviles, cadena de custodio y contenido digital, al remplazar unos de sus componentes no se altera la integridad de la información siempre y cuando se tenga la autorización de la parte competente o juez que son el sustento para un perito informático, quien es el actor facultado de realizar el análisis, estudio técnico y tecnológico para extraer evidencia digital que sirva como prueba para la valoración o criterio ante un tribunal, de acuerdo a la Ley, por lo tanto el presente trabajo de investigación servirá de guía para en casos extremos cuando uno de sus componentes están deteriorados de un dispositivo móvil, considerando que las herramientas a utilizar tienen costos elevados.
- También es importante concluir que la ejecución de los procesos y las herramientas open-source para extraer información almacenada en los dispositivos móviles permitió obtener un sin número de evidencia digital relevante que puede aportar en alguna investigación para esclarecer algún caso, así como también saber qué técnicas y herramientas se pueden utilizar de acuerdo al tipo de extracción que se esté aplicando y qué información se puede adquirir.

RECOMENDACIONES

- Para realizar análisis forense a dispositivos móviles, principalmente cuando estos presentan daños en su integridad, se deben realizar ciertos procedimientos que garanticen la integridad de la información obtenida.
- Con el paso del tiempo las actualizaciones de seguridad en el sistema operativo Android van mejorando lo que hace que el proceso forense sea más complicado, por tal razón, se deben buscar métodos y técnicas que más se adapten a las necesidades al momento de extraer información.
- También es recomendable profundizar el estudio teórico práctico para contribuir con nuevos procedimientos, herramientas software y hardware con el objetivo de dar un uso adecuado de las mismas, a fin de dar soporte en el proceso de búsqueda y recolección de información en cualquier proceso investigativo.

BIBLIOGRAFÍA

Agualimpia, C., & Hernández, R. (2009). Análisis forense en dispositivos móviles con Symbian OS. Documento de maestría, Dept. Ingeniería electrónica, Pontifica Universidad Javeriana. Obtenido de http://www. criptored. upm. es/guiateoria/gt_m142e1. htm.

Ayers, Brothers, & Jansen. (2014). Investigación forense de dispositivos móviles: metodologías y herramientas. Obtenido de https://www.redseguridad.com/especialidades-tic/activos-de-informacion/investigacion-forense-de-dispositivos-moviles-metodologias-y-herramientas_20201021.html

Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on Mobile Device Forensics. doi:Issue: NIST Special Publication (SP) 800-101 Rev. 1

Chandan, K. (05 de Mayo de 2022). GEEKFLARE. Obtenido de https://geekflare.com/es/forensic-investigation-tools/

Di lorio, A., Castellote, M., Constanzo, B., Curti, H., Waimann, J., & Lamperti, S. (2017). El rastro digital del delito: aspectos técnicos, legales y estratégicos de la informática forense. Publisher: Universidad FASTA.

Ferro, J. (2002). CYBERINVESTIGACIÓN. Obtenido de http://www.funcionjudicial.gob.ec/www/pdf/peritos/FORMATO%20DE%20INFO

Granda, M. (2016). ANÁLISIS FORENSE A DISPOSITIVOS MÓVILES CON TECNOLOGÍA IPHONE. Obtenido de http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/11957/T-ESPE-053257.pdf?sequence=1&isAllowed=y

Jaya, K. A. (2017). DESARROLLO DE UNA GUÍA DE PROCEDIMIENTOS EN BASE AL ESTUDIO DE. Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/13484/Trabajo%20de%20Disertaci%C3%B3n%20-%20Katherine%20Jaya.pdf?sequence=1&isAllowed=y

Lopez, M. (Junio de 2007). Análisis Forense Digital. Obtenido de https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

Martinez, C. (2020). Análisis forense en dispositivos móviles: un caso práctico.

Mendillo, V. (2018). Análisis forense de dispositivos móviles., (pág. 131). Caracas (Venezuela). Obtenido de http://mendillo.info/forensica/An%C3%A1lisis%20forense%20de%20dispositivos%20m%C3%B3viles%20-%20V.%20Mendillo.pdf

Pinto, D. (2014). Metodología de análisis forense orientada a incidentes en dispositivos móviles. Maskana, 5.

Rueda, J., & Rico, D. (2016). La informática forense en dispositivos Android. Revista Ingenio, 9, 21-34.

Sacco, L. (21 de 03 de 2021). Peritos Informaticos. Obtenido de https://peritosinformaticos.ar/andriller-2022/

Sachowski, J. (2019). Implementing digital forensic readiness: From reactive to proactive process. CRC Press.

Sampieri, R. (2014). Metodología de la investigación (sexta ed.). Mexico: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V. Obtenido de https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Velasco, M. (04 de Abril de 2022). Técnicas de extracción en dispositivos móviles. Obtenido de https://wdiarium.com/tecnicas-de-extraccion-en-dispositivos-moviles

ANEXOS

Anexo 1. Desensamblaje de los dispositivos móviles

Anexo 2. Modelo de la ficha técnica de dispositivos móviles

Ficha técnica de dispositivos móviles						
Perito						
Numero de caso						
Fecha						
Hora						
Ítem	**Tipo**	**Marca**	**Serie**	**Modelo**	**Estado**	**Observaciones**

ING. JESUS ANTONIO COLOMA GAROFALO EN CALIDAD DE DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR,

CERTIFICA

Que el trabajo de integración curricular denominado "**ANÁLISIS FORENSE UTILIZANDO HERRAMIENTAS OPEN SOURCE EN DISPOSITIVOS MÓVILES DETERIORADOS**", presentado por Jerson Ismael Chimbo Fernández y Henry Estiben Sinche Pilco estudiantes **de la carrea de Software** pasó el análisis de coincidencia no accidental en la herramienta URKUND, reflejando **un porcentaje de similitud del 11%,** como se puede evidenciar en el documento adjunto.

Guaranda, 27 de febrero del 2023

Atentamente,

JESUS ANTONIO COLOMA GAROFALO

Ing. Jesus Antonio Coloma Garofalo
Director

Dirección: Av. Ernesto Che Guevara y Gabriel Secaira
Guaranda-Ecuador
Teléfono: (593) 3220 6059
www.ueb.edu.ec

Ouriginal
by Turnitin

Document Information

Analyzed document	ANÁLISIS FORENSE (tesis final Entregable)-1.docx (D159360782)
Submitted	2/23/2023 10:18:00 PM
Submitted by	
Submitter email	jerchimbo@mailes.ueb.edu.ec
Similarity	11%
Analysis address	jcoloma.ueb@analysis.urkund.com

Sources included in the report

Entire Document

Hit and source - focused comparison, Side by Side

- Submitted text
  As student entered the text in the submitted document.
- Matching text
  As the text appears in the source.