OFICINA DE POSGRADOS

TEMA:

PRUEBA DE CONCEPTO PARA EXTRAER INFORMACIÓN CON HERRAMIENTAS DE ANALISIS FORENSE OPEN-SOURCE EN DISPOSITIVOS ANDROID

Proyecto de investigación previo a la obtención del título de Magister en Ciberseguridad

Línea de Investigación:

Seguridad de la Información

Autor:

Darwin Rolando Chimbo Fernández

Director:

PHD. Gustavo David Salazar Chacón

Ambato – Ecuador

Diciembre 2022

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

PRUEBA DE CONCEPTO PARA EXTRAER INFORMACION CON HERRAMIENTAS DE ANALISIS FORENSE OPEN-SOURCE EN DISPOSITIVOS ANDROID

Línea de Investigación:

Seguridad de la Información

Autor:

Darwin Rolando Chimbo Fernández

Gustavo David Salazar Chacón, Ing. PHD. f._____

Firmado electrónicamente por:
GUSTAVO DAVID SALAZAR CHACON

CALIFICADOR

Enrique Xavier Garces Freire, Ing. Mg. f._____

CALIFICADOR

José Marcelo Balseca Manzano, Ing. Mg. f._____

CALIFICADOR

Juan Carlos Acosta Teneda, P. Mg. f._____

COORDINADOR DE LA OFICINA DE POSGRADOS

Hugo Rogelio Altamirano Villarroel, Dr. f._____

SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
DIRECCIÓN CENTRO DE POSGRADOS
Sede Ambato

Pontificia Universidad Católica del Ecuador
SECRETARÍA GENERAL
PROCURADURÍA

Ambato – Ecuador

Diciembre 2022

DECLARACIÓN DE AUTENCIDAD Y RESPONSABILIDAD

Yo: **DARWIN ROLANDO CHIMBO FERNANDEZ**, con CC. **020168391-9**, autor del trabajo de graduación intitulado: "**PRUEBA DE CONCEPTO PARA EXTRAER INFORMACION CON HERRAMIENTAS DE ANALISIS FORENSE OPEN-SOURCE EN DISPOSITIVOS ANDROID**", previa a la obtención del título profesional de Magister en Ciberseguridad, de la oficina de posgrados.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Ambato, diciembre 2022

DARWIN ROLANDO CHIMBO FERNANDEZ

CC. 0201683919

AGRADECIMIENTO

A Dios por haberme dado el conocimiento y la fuerza necesaria para concluir con éxito una más de mis metas planteadas. A mi esposa e hija por su comprensión y apoyo incondicional en todo momento. Por estar pendiente siempre de mis estudios y así culminarlo de la mejor manera.

A mis padres por haberme dado ánimo y seguirme inculcando valores. Al PHD. Gustavo Salazar mi Director de Tesis por su colaboración y apoyo en el desarrollo de este trabajo.

Darwin Rolando Chimbo Fernandez

DEDICATORIA

A mi esposa e hija quienes con su amor, cariño y comprensión me permitieron cumplir satisfactoriamente otro de mis objetivos trazados, por darme ánimo y fuerza para continuar con mi estudio hasta culminarlo con éxito.

Darwin Rolando Chimbo Fernandez

RESUMEN

En la actualidad, se ha evidenciado que la mayoría de los delitos informáticos, se han realizado desde dispositivos móviles, esto debido a que una gran cantidad de personas cuentan con un equipo móvil desde, el cual, acceden a todas sus redes sociales e incluso para realizar transacciones en línea. Es por eso que el presente trabajo de investigación tiene por objetivo realizar una prueba de concepto para extraer información de dispositivos móviles con sistema operativo Android mediante herramientas de análisis forense *open-source*, existe una carencia de herramientas de software libre para ser usado por los analistas forenses y así realicen extracción de información necesaria que aporte en la investigación de algún caso forense relacionado con equipos móviles. La metodología que, se aplica para el desarrollo del proyecto es una investigación bibliográfica de métodos y normativas existentes que permitan: identificar el dispositivo móvil, extraer información mediante el método manual, lógico y físico cada uno con su respectiva herramienta; y presentar resultados obtenidos en el formato de informe pericial alineado a la normativa legal vigente. Terminado la extracción en los escenarios propuestos tanto en un equipo móvil real como en un equipo móvil emulado, se realiza la comparación de la información obtenida con cada herramienta, de esta manera, se comprueba la factibilidad del desarrollo del presente trabajo, adquirir información mediante el uso de software libre que sea utilizado por los peritos informáticos en sus investigaciones.

Palabras claves: dispositivos móviles, Android, informe pericial.

ABSTRACT

Currently, it has been shown that most computer crimes have been carried out from mobile devices, this is due to the fact that most people have a mobile device, from which they access all their social networks and even carry out online transactions. That is why this study aims to carry out a proof of concept to extract information from mobile devices with the Android operating system using open-source forensic analysis tools since currently, forensic analysts lack free software tools which allows them to extract the necessary information that can contribute to the investigation of a forensic case related to mobile equipment. The methodology that is applied for the development of the project is bibliographical research of existing methods and regulations that allow to identify the mobile device, extracting information through the manual, logical and physical methods, each with its respective tool; and submitting a report of the results obtained in the format of an expert report in line with current legal regulations. Once finished the extraction in the proposed scenarios, both in the real mobile equipment and in the emulated mobile equipment; and made the comparison of the information obtained with each tool, the feasibility of the development of this study is verified since information can be acquired using free software, which can be used by computer experts in their investigations.

Keywords: mobile devices, android, expert report.

ÍNDICE

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

En la actualidad, la evolución de los dispositivos móviles ha incrementado notablemente, han pasado de ser simples celulares a ser computadores de mano. Razón, por la cual, las actividades cotidianas de las personas como revisar correos electrónicos, redes sociales, sitios de interés, incluso realizar transacciones bancarias *online* lo hacen mediante los dispositivos móviles. Estos dispositivos móviles en su mayoría tienen sistema operativo Android, es la plataforma más popular entre los usuarios y, también, entre los cibercriminales, es el principal blanco entre todas las plataformas móviles.

El uso de los dispositivos móviles ha crecido notablemente por tal razón los servicios ofrecidos, las aplicaciones cada día son más numerosas, es posible estar conectado desde cualquier lugar a la hora que desee. Esto ha traído grandes beneficios para los usuarios por la comodidad; para las empresas porque ofrecen un mejor servicio, pero, también, llama la atención de personas y cibercriminales que han visto un gran mercado y que en los últimos años su explotación ha estado en aumento, con esto obtiene provecho para sus intereses personales o económicos a través de los diferentes delitos informáticos. Los dispositivos móviles están expuestos a un sinnúmero de peligros, al igual que los computadores y otros equipos que estén conectados a la red. Los peligros a los que están expuesto los usuarios de un dispositivo móvil son los mismos que para cualquier usuario de otro equipo informático (Andrade-Salinas et al., 2019). Algunas de estas amenazas son: *malware, spam, phishing*, robo o extravío físico del dispositivo.

Es así que, con el aumento del mercado móvil, la cantidad y la importancia de la información que, se confía a estos dispositivos, también, crecerán los ataques, intrusiones y demás peligros informáticos. Por eso es necesaria la implementación de políticas que ayuden a mitigar estos ataques, la sensibilización a los usuarios y, en el caso que ocurra una intrusión poder establecer las acciones relevantes en la investigación y esclarecer los mismos, es allí donde entra la informática forense.
La informática forense es la ciencia que aplica las técnicas informáticas para el proceso de adquirir, preservar, obtener y presentar datos que han sido analizados

electrónicamente y almacenados en un medio electrónico, los cuales, serán utilizados en el ámbito judicial debido a su relevancia (Ramon, 2006).

Debido a su importancia la informática forense es utilizada tanto en el sector público como en el sector privado, a pesar que en las entidades públicas en proceso judicial a las evidencias forenses encontradas, se da un juicio de valor para determinar una sentencia. Mientras que, en la parte privada, se realizan todas las investigaciones del caso sin la necesidad de llegar a instancias legales.

Es así que existe ya un modelo a seguir para realizar un análisis forense a dispositivos móviles con sistema operativo Android que sigue todas las fases que contempla en la informática forense (Tapia & Washington, 2021). Además, también, se ha evidenciado la existencia de una Metodología de análisis forense para dispositivos móviles alineado a leyes del Ecuador (Cajías, 2018).

Lo anterior evidencia que actualmente la extracción de información en dispositivos móviles es lo más importante para un análisis forense, esta información posteriormente con el cumplimiento de la cadena de custodia es considera evidencia. Sin embargo, en la extracción de información del dispositivo móvil, se utiliza muchas técnicas/métodos y software pero, se ha demostrado que el método más efectivo para extraer información es aquella que considere la recuperación de información mediante una imagen forense completa del sistema operativo del dispositivo móvil, ya que recupera información eliminada y/o modificada.

Si, se realiza actos ilícitos por medio de dispositivos móviles estos, se convierten en un punto clave de la investigación sobre, el cual, se realiza un peritaje informático. Al permitir a los peritos informáticos obtener evidencias digitales estos asumen el rol más importante de la investigación forense. Sin embargo, las herramientas de software propietario agregan una problemática a la recolección y almacenamiento de la información por su dificultad de acceso al pago, razón que es más evidente si el perito informático necesita realizar un análisis forense y no cuenta con la metodología y las herramientas adecuadas de software libre.

Con base en lo mencionado, se evidencia el siguiente problema: ¿Es posible extraer información de dispositivos móviles para el análisis forense mediante herramientas *open-source* en su totalidad y ser considerada valida? Para encontrar la solución al problema mencionado, se plantea la siguiente hipótesis: con el uso de software libre, se verificó la factibilidad de la extracción de información para un análisis forense eficiente de dispositivos móviles. Con el fin de demostrar la hipótesis propuesta al desarrollar el presente trabajo de investigación, se plantea el objetivo general y los objetivos específicos.

Objetivo General

Realizar una prueba de concepto para extraer información mediante herramientas de análisis forense open-source en dispositivos Android

Objetivos Específicos

1. Documentar el estado del arte para el análisis informático forense en dispositivos de software libre.
2. Analizar el proceso existente aplicable al análisis forense en dispositivos móviles según la normativa ecuatoriana de software libre.
3. Identificar los KPI técnicos más importantes para la comparación de las herramientas de extracción de información a ejecutarse en las pruebas de concepto.
4. Diseñar pruebas de concepto en entorno real y simulado sobre extracción de información en dispositivos móviles de software libre.

Se utilizó la siguiente metodología con la finalidad de cumplir con las actividades definidas. La metodología hipotético-deductivo utiliza procedimientos inductivos y deductivos para llegar a una conclusión y así poder comprobar la hipótesis planteada, se selecciona esta metodología porque tiene características más acordes al proyecto de estudio. La metodología fue aplicada con un enfoque cualitativo con diseño transversal debido a que la misma prueba de concepto, se aplicaran a varios dispositivos móviles. Las pruebas mencionadas, se realizaron de acuerdo a las siguientes fases: Identificación y preservación de la evidencia,

adquisición o extracción de las evidencias, análisis de la evidencia y generación/presentación del informe técnico.

En la actualidad los dispositivos móviles por sus grandes facilidades de utilización y prestaciones que ofrece, entre ellos: gran cantidad de espacio para almacenamiento, procesamiento, mensajería instantánea (*WhatsApp, Telegram*), redes sociales (*Twitter, Instagram y Facebook*), interacción constante con internet, *email* tanto como personal como empresarial, banca *online*, bolsa de valores, cámaras fotográficas de alta resolución, video conferencia, y aplicaciones de geolocalización, entre otros. Al brindar estos beneficios, los mismos llegaran a convertirse en riesgos de igual o mayor magnitud para el propietario; de esta manera un pirata informático obtiene beneficiarse de la información que un dispositivo móvil almacena de su propietario con fines delictuosos, ya sea mediante acceso no autorizado al dispositivo o a través de vulnerabilidades encontradas en el software o hardware del dispositivo, en esta época la información es el activo más importante tanto para una persona natural como ara una organización.

Como en el dispositivo móvil, se almacena toda la información y actividades del propietario logra reflejar su preferencia social, preferencia religiosa, tendencia política, gustos para entretenimiento, preferencias consumistas, es ahí donde radica el interés de los piratas informáticos, que mediante programas maliciosos en algunos casos con la inserción en aplicaciones legitimas, hacen uso de la información o funcionalidad de los equipos móviles para beneficio delictivo. Luego que, se ha cometido una actividad maliciosa el propietario, se ve involucrado en actos delictivos por lo que es necesario realizar el análisis forense digital a fin de demostrar la inocencia o culpabilidad del usuario. Es así que para realizar el proceso de extracción de evidencia digital en los dispositivos móviles es necesario contar con las herramientas *open-source* que cumplan y provean todas las funcionalidades que proporciona una herramienta de propietario. Con esto, se pretende ayudar a los peritos informáticos del país y del mundo la alternativa de realizar sus peritajes con herramientas de software libre, ofrecen los mismos beneficios y cumplen con las normativas que los rige. Y de esta manera no solo

depender para este tipo de actividades de unas cuantas empresas existentes y, además, ampliar el campo laboral para los profesionales de esta área.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Informática Forense

La Informática Forense es la ciencia que permite la adquisición, el análisis, la preservación y presentación de datos procesados electrónicamente y almacenados en dispositivos de almacenamiento (Di Iorio et al., 2017). A la informática forense, también, se la conoce como Análisis Forense Digital, el cual, logra definirse como el conjunto de principios y técnicas que comprende adquirir, conservar, documentar, analizar y presentar las evidencias digitales.

La evidencia digital o prueba electrónica en informática forense es uno de los términos más abordados, el cual, se define como el conjunto de datos en formato binario que comprende los ficheros, su contenido o referencias a éstos (meta-datos) que, se encuentren en los soportes físicos o lógicos, es decir, toda la información que, se encuentra almacenada o transmitida en el dispositivo en análisis. Para que la evidencia digital tenga validez probatoria tiene que ser: admisible, auténtica, completa, creíble, segura y confiable. Como ya, se mencionó anteriormente la evidencia digital es la materia prima para cualquier investigación forense, entonces es necesario tener un protocolo de actuación que, se sigue durante toda la vida útil de la evidencia digital, es decir, desde el momento que, se adquiere los datos hasta que, se destruye o ya no sea importante para la investigación.

Al proceso donde, se garantiza que la evidencia digital va ser la misma durante todas las fases del análisis forense digital, se lo conoce como Cadena de Custodia. Este procedimiento tiene que ser riguroso, tanto con las pruebas, los hechos, así como, también, con el personal que tiene acceso a la evidencia. Mientras que, la línea temporal o línea de tiempo es fundamental para indagar la información requerida en base a un criterio de tiempo determinado que es útil para la investigación. Cualquiera que sea el análisis, se crea una línea temporal, es decir, los acontecimientos o actividades que el dispositivo ha tenido en manos del propietario.

Con la Informática Forense es posible detectar y recuperar datos e información digital y utilizar la misma como evidencia en el esclarecimiento de un acto ilícito o no autorizado. La importancia de la informática forense radica en que, se enfoca en la investigación de actos delictivos que han ocurrido en computadores, dispositivos móviles, así como, también, en un sistema informático, con el fin de encontrar evidencias digitales que sean utilizadas como prueba valida en un proceso judicial.

Debido al acelerado desarrollo tecnológico en la actualidad, también, los piratas informáticos han creado nuevas formas de ejecutar sus actividades delictivas, al saber que actualmente los usuarios tienen sus dispositivos conectados al internet, los peritajes informáticos va en un constante crecimiento, porque, las evidencias digitales, se han constituido en una información muy importante al momento de la reconstrucción de los hechos dentro de una investigación, incluso, se han utilizado como pruebas determinantes dentro de un proceso judicial informático.

Esto hace evidente la necesidad de contar con personal técnico capacitado en el área de análisis forense, el cual, tiene conocimientos sólidos que le permitan actuar ordenadamente, sistemáticamente y apliquen técnicas con el fin de, identificar, adquirir, recuperar y analizar la información ya sea que ésta, se encuentre visible u oculta (Di Iorio et al., 2017). La Informática Forense aparece como la necesidad en la investigación de los diferentes delitos que, afectan día a día a entes gubernamentales y a la sociedad común, esta tiene como propósito comprobar los responsables de los delitos y aclarar el origen de un suceso, mediante la recolección de pruebas digitales para fines investigativos a través de los diferentes métodos.

Tipos de análisis forense digital

Si, 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, así entre ellos, se tiene.

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* entre otros.)

Análisis forense de sistemas. - este tipo de análisis forense hace referencia a la investigación realizada en servidores y estaciones de trabajo, se enfoca en el tipo de sistema operativo (Windows, UNIX, Linux, MAC OS) que tenga el equipo.

Análisis forense de sistemas embebidos. – este análisis forense hace referencia a la investigación en dispositivos móviles, asistente personal digital (PDA), entre otros, 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 apoyar lo anteriormente mencionado y salvaguardar el objetivo principal de la informática forense, que es el de brindar pruebas ante un juez existen unos principios generales que serán aplicadas en cualquier proceso de informática forense.

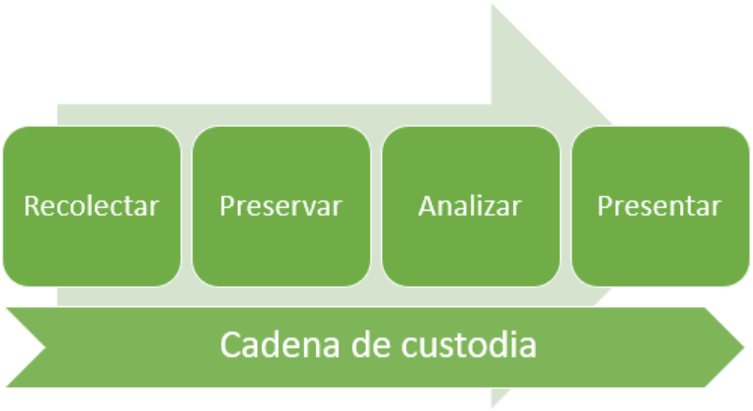
Actuar metódicamente: El investigador es su propio custodio durante el proceso, por cual, cada uno de los pasos ejecutados, herramienta utilizada y resultados obtenidos, estarán bien documentados.

Evitar la contaminación: Evitar a toda costa la inapropiada manipulación de la evidencia analizada, con el objetivo de evitar incurrir en una interpretación o análisis incorrecto.

Controlar la cadena de custodia: Responder a una diligencia y formalidad especial con el fin de documentar cada evento realizado con la evidencia.

Fases del análisis forense digital

Figura 1. Fases del análisis forense digital



Fuente: elaboración propia

El proceso general de un análisis forense consta de las siguientes fases: recolectar, preservar, analizar y presentar (Ayers et al., 2014) , los cuales, se detalla, a continuación:

Recolectar. - Es el primer paso para realizar en un análisis forense informático, en, el cual, la finalidad es obtener todas las evidencias del dispositivo que sean de interés para la investigación. En la extracción de la información, se tiene en cuenta la integridad del mismo, para, lo cual, se utiliza algoritmos de hash.

Preservar. - En esta fase es fundamental revisar si la información que, se recolectó en la fase anterior es la misma que, se tiene para analizar, para validar la integridad de la evidencia es necesario cumplir con la cadena de custodia, el cual, utiliza métodos de verificación y comprobación de evidencia mediante el uso de funciones *hash* (MD5 o SHA1).

Analizar. - En esta fase, se centra toda la investigación, es donde al utilizar herramientas de análisis forense hay que ser capaz de identificar cualquier cambio o acceso no autorizado realizado ya sea al software o hardware del dispositivo móvil. Tener en consideración que estos cambios van desde alteraciones físicas en el sistema de ficheros, sistema operativo hasta el simple acceso.

Además, con las revisiones realizadas es posible realizar la reconstrucción de los hechos, lo que permite al investigador y a la parte interesada entender y esclarecer cómo, se ejecutó el posible delito. Por último, con el análisis realizado, se da a conocer quién es el autor de los hechos, desde que Dirección lógica del equipo o dirección física del equipo del ordenador, se ejecutaron los actos ilícitos.

Presentar. - Esta es la fase final de un análisis forense donde, se consolida toda la información recopilada con el fin de evidenciar todo el análisis realizado en un informe técnico.

1.2. Análisis forense digital en dispositivos móviles Android

El entorno de los dispositivos móviles ha evolucionado de una manera acelerada en los últimos años provocado principalmente por su adopción masiva por parte de los usuarios, los cuales, llegan a tener de manera simultánea varios terminales con diferentes objetivos como uso profesional, uso personal, entre otros. Hay apreciaciones que indican que en la actualidad hay más de 7.500 millones de dispositivos móviles (Parrales et al., 2021), lo que supone una cifra superior al de la población mundial. En ellos, se almacena multitud de información que resulta determinante a la hora de resolver un incidente como, por ejemplo, historial de llamadas tanto entrantes como salientes, mensajes de texto y multimedia, correos electrónicos, historial de navegación, fotos, videos, documentos, información en redes sociales, información en servicios de almacenamiento online, entre otros. e incluso es posible recuperar información eliminada previamente (Martínez Ródenas, 2020).

El sistema operativo móvil Android es el más usado en el mundo, supera al sistema operativo Windows. Esta popularidad ha provocado que Android sea el sistema

operativo móvil más atacado y, con gran capacidad de cómputo que disponen las actuales terminarles, han contribuido a que cada día, se presenten ataques más sofisticados para esta plataforma. Los cibercriminales han tenido en cuenta este nuevo objetivo y han migrado los ataques que tradicionalmente era para los equipos de escritorio y laptops hacia los dispositivos móviles, y entre las amenazas que enfrentan los usuarios, se encuentra una gran variedad de *malware*, algunos tan particulares como el *ransomware* y *botnets* creadas con dispositivos Android. Si ocurre un incidente de seguridad o, se sospecha que un equipo informático ha sido comprometido, es donde la informática forense tiene su campo de aplicación, para determinar lo qué pasó, cómo ocurrió y determinar quién es el responsable.

Por otra parte con la finalidad de corregir vulnerabilidades existentes las empresas que desarrollan los sistemas operativos envían actualizaciones constantes para que los usuarios actualicen sus equipos y así de alguna manera estar protegidos, el internet a dado paso a la conexión de una red global entre dispositivos móviles, por lo que, la seguridad en este, se ha convertido en un desafío para los desarrolladores, cada día aparece millones de ataques por parte de ciberdelincuentes a entidades gubernamentales, empresas privadas y usuarios comunes, de esta manera la informática forense, se ha convertido en la parte fundamental para esclarecer estos actos delictivos.

La informática forense es una disciplina que, se define como el proceso de aplicar métodos científicos para recopilar y analizar datos e información que es utilizada como evidencia. Esta disciplina trabaja con evidencia digital, y mantiene los principios de las ciencias forenses como es la rigurosidad del manejo de la evidencia, el principio de Locard y los retos a los que, se enfrentan el equipo de peritos informáticos, como son las técnicas anti forenses, que buscar impactar de manera negativa la identificación, la disponibilidad, la confiabilidad y la relevancia de la evidencia encontrada en un peritaje.

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

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

Preservación. - Corresponde a la fase en la que, se identifican los dispositivos a analizar y garantizar que no, se pierdan las evidencias que serán recopiladas para su posterior análisis. El desconocimiento provoca la invalidación automática de las pruebas, por ejemplo, por no solicitar una autorización expresa por escrito para realizar el proceso o que, se pierda información relevante que resulta 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.

Así mismo, se tiene que 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, pasa 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 van a ser transportados, realizar con sumo cuidado, evitar que la información sea alterada o que, se vea expuesta a temperaturas extremas o campos electromagnéticos.

Adquisición. - Una evidencia es definida como cualquier prueba que es utilizada en un proceso legal. Es por ello que tiene las siguientes características:

- Auténtica: ser verídica y no haber sufrido manipulación alguna.
- Completa: representa la prueba desde un punto de vista objetivo y técnico, sin valoraciones personales, ni prejuicios.
- Creíble: ser comprensible.

- Confiable: las técnicas utilizadas para la obtención de la evidencia no generaran ninguna duda sobre su veracidad y autenticidad.
- Admisible: tener valor legal.

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

Análisis. - A la hora de realizar el análisis de la información recopilada, se considera el tipo de incidente al que, se pretende ofrecer respuesta, según el caso resulta necesario realizar un análisis más profundo de determinados aspectos.

Documentación. - Un aspecto fundamental en el proceso del análisis forense es la documentación, por lo que, se realiza dicha fase de una manera muy metódica y detallada. Se realizarán, entre otras, las siguientes acciones:

- 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, entre otros.
- Documentar todos los pasos realizados durante el proceso, mantiene una bitácora con fechas y horas de cada acción realizada sobre las evidencias e incluye las herramientas utilizadas.
- Elaborar dos tipos de informe de conclusiones: uno ejecutivo y uno técnico.

Presentación. - La fase de presentación de la información es tan importante o más que las anteriores, se harán accesibles y comprensibles las conclusiones que, se han obtenido del proceso del análisis forense. Para ello, es recomendable seguir las siguientes pautas:

- Preparar una presentación de manera pedagógica que sea fácilmente comprensible.
- Detallar las conclusiones.

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

1.3. Metodología de extracción de información en dispositivos móviles

La información que, se extrae gracias a una de las fases de análisis forense, en la actualidad para un proceso judicial es muy importante ya en base a esta, se desarrollaran las siguientes fases. Es por esto que es necesario una extracción completa e integra de la imagen forense en el dispositivo móvil a analizar.

La adquisición y el análisis forense de teléfonos móviles implican esfuerzo manual y el uso de herramientas automatizadas. Hay una variedad de herramientas disponibles. para realizar análisis forense móvil. Todas las herramientas tienen sus pros y sus contras, y es fundamental que entiendas que ninguna herramienta es suficiente para todos los propósitos. Entonces, comprender varios tipos de herramientas forenses móviles es importante para los examinadores forenses. Al identificar las herramientas adecuadas para la adquisición forense y análisis de teléfonos móviles, una clasificación de herramientas forenses de dispositivos móviles es la pirámide desarrollado por Sam Brothers (Rohit Tamma & Heather Mahalik, s. f.), el cual, se muestra en la figura 2.

Figura 2. Pirámide de clasificación de herramientas de análisis forense para dispositivos móviles

Fuente: Adaptado de *Practical Mobile Forensics Third Edition* (Rohit Tamma & Heather Mahalik, s. f.)

Esta pirámide pretende servir de guía para clasificar las herramientas de análisis forense de acuerdo a diferentes criterios como:

- Complejidad
- Tiempo de análisis requerido
- Riesgo de pérdida o destrucción de evidencias
- Nivel invasivo
- *Forensically sound* que, se refiere al nivel de fiabilidad, aunque, se trata únicamente de una percepción, todas las herramientas y técnicas utilizadas tendrán una fiabilidad contrastada.

La manera de interpretar el esquema es desde abajo de la pirámide hacia arriba, de modo que las capas superiores poseen una complejidad técnica mayor, un mayor tiempo requerido y más *forensically sound*.

De acuerdo al *Guidelines on Mobile Device Forensics* (Ayers et al., 2014), la extracción manual es el nivel 1 donde los datos son adquiridos al acceder directamente al dispositivo analizado, aquí, se requiere utilizar el teclado del dispositivo. Para obtener información, se utiliza una cámara externa digital que

grabe lo explorado. En este nivel no es posible recuperar los datos borrados del dispositivo y la extracción de datos tarda mucho.

La extracción lógica es el nivel 2, aquí, se accede a los datos a través de conexión USB, *Wifi o Bluetooth*. Las herramientas utilizadas envían una serie de comandos al dispositivo móvil, las cuales, responde como resultado los datos almacenados.

La extracción hexadecimal es el nivel 3, aquí, también, es necesario conectar por USB o por *Wifi* la herramienta y el dispositivo, y de esta manera, se accede a la información almacenada en la memoria *flash*. En esta extracción, se inserta un programa en un área de memoria protegida del sistema, conecta un dispositivo de unidad *flash* en el puerto de datos del equipo móvil. Los datos de la memoria flash son capturados luego de que el dispositivo *flash* envíe los comandos necesarios.

La extracción *Chip-Off* es el nivel 4, este nivel radica en remover la tarjeta de memoria flash del equipo móvil que vaya a ser analizado, el cual, permite la creación de la imagen binaria de los datos almacenados en la tarjeta. Esta extracción es similar a realizar una imagen forense de un disco duro.

La lectura microscópica es el nivel 5, este nivel permite realizar grabaciones de las observaciones físicas del equipo móvil en una tarjeta NAND o NOR, para, lo cual, se utiliza un microscopio electrónico.

Herramientas para extracción de información de dispositivos móviles

Existen algunas de las herramientas gratuitas que servirán al momento de realizar la extracción de información en equipos móviles como las que, se menciona, a continuación:

AFLogical OSE - Open source Android Forensics app and framework. – según (Aji et al., 2020) es una aplicación en formato APK que necesita ser previamente instalada en el terminal Android. Una vez finalizado el proceso permite extraer información variada a la tarjeta SD (registro de llamadas, listado de contactos y de aplicaciones instaladas, mensajes de texto y multimedia) y posteriormente ésta

recuperada o bien a través de la conexión de la tarjeta a un dispositivo externo o mediante el *Android Debug Bridge* (ADB).

Linux Memory Extractor (LIME). - según (Martinez, 2016) es un software que permite la obtención de un volcado de memoria volátil de un dispositivo basado en Linux como es el caso de los teléfonos móviles Android. Así mismo, presenta la ventaja de que es ejecutado remotamente vía red.

Android Data Extractor Lite (ADEL). - es una herramienta desarrollada en *Python* que permite conseguir un flujograma forense a partir de las bases de datos del dispositivo móvil. Para realizar este proceso, se necesita que el dispositivo móvil tenga privilegios de usuario *root* o tener instalado un *recovery* personalizado (Araujo-Costa-Silva, 2019).

Android Debug Bridge (ADB). – según (Yunia Pasa & Hariyadi, 2020) es una herramienta de línea de comandos que permite la comunicación con el dispositivo móvil. Con el comando *adb*, se realiza varias acciones en el equipo como, por ejemplo, instalación y depuración de aplicaciones, además, provee acceso a una *shell* de Unix en donde, se ejecuta diferentes comandos en el dispositivo según lo que, se necesite. Esta herramienta tiene una arquitectura cliente-servidor que contiene tres elementos:

- **Cliente. -** es el que envía comandos, este cliente, se ejecuta en el computador del investigador. Para invocar un cliente desde un terminal de línea de comandos, se lo realiza con la ejecución de un comando adb.
- **Daemon (adbd). -** es el que realiza la ejecución de comandos en un dispositivo móvil. En cada dispositivo móvil el Daemon, se ejecuta como un proceso en segundo plano.
- **Servidor. -** es el que realiza la administración de la comunicación entre el cliente y el daemon. Al igual que el cliente, el servidor, se ejecuta en el computador del investigador como un proceso en segundo plano.

Andriller. – según (Yuliani & Riadi, 2019) es un software que contiene una colección de herramientas forenses para equipos móviles. Permite realizar adquisiciones forenses sin modificar datos desde dispositivos Android. Su utilidad radica en la facilidad de su uso y en especial debido a que en más ocasiones es requerido para peritaje informático de la aplicación *Whatsapp.* Ofrece funcionalidades como: descifrado del patrón de la pantalla de bloqueo, código PIN o contraseña; decodificadores personalizados para datos de aplicaciones de bases de datos que permiten decodificar comunicaciones. A demás, se obtiene informes en formatos HTML y Excel de la extracción realizada (Rahman & Riadi, 2019). Las principales características de esta herramienta son:

- Permite extraer datos de manera automatizada y, también, realizar *parsing* de datos.
- Permite extraer datos en teléfonos no-rooteados a través de la copia de seguridad.
- Permite extraer datos con privilegios de *root.*
- Permite seleccionar los decodificadores de la base de datos individuales para *Android* y *Apple*.
- Permite descifrar la base de datos de *WhatsApp* (*msgstore.db.crypt, msgstore.db.crypt5, msgstore.db.crypt7 y msgstore.db.crypt8*).
- Permite el craqueo de patrón, PIN y contraseña.
- Permite desempaquetar archivos de *backup* de sistemas Android.

Santoku. - es una distribución de Linux gratuita de código abierto enfocado al análisis forense en dispositivos móviles, la seguridad móvil y el análisis de malware móvil. Proporciona herramientas para; analizar y adquirir datos, examinar malware en equipos móvil, desamblar y evaluar aplicaciones móviles con scripts diseñados para detectar problemas comunes en aplicaciones móviles. Además, proporciona algunas herramientas para el análisis del tráfico de red y de imágenes (Rivera, s. f.).

Herramienta dd. - el dd (por sus siglas en ingles *Dataset Definition*), en el análisis forense es utilizado para realizar imagen forense de un dispositivo que, se necesite

extraer información, esta herramienta permite obtener una copia bit a bit de toda la información almacenada en alguna partición o incluso de unidades completas (Díaz Muñoz, 2015). La sintaxis para su uso es la siguiente:

```
dd if=/dev/mmcblk1 of=/home/andorid.dd bs=4096
conv=notrunc,noerror,sync
```

Donde if=/dev/mmcblk1 hace referencia a lo que, se va a copiar, el of=/home/andorid.dd hace referencia a la ruta donde, se va a copiar la imagen forense y el bs=4096 hace referencia a la velocidad con la que, se procesa la copia forense.

Para no tener errores durante la ejecución, se ejecuta el comando mencionado en el dispositivo móvil con permisos de *root*.

Autopsy. - es una herramienta de código abierto utilizado para el análisis forense informático. La herramienta tiene interfaz gráfica por, lo cual, su utilización es fácil, tiene la capacidad para analizar imágenes forenses de discos duros, tarjetas de memoria, celulares y otros dispositivos de almacenamiento de datos. Permite analizar los discos de sistemas Windows, UNIX y sistemas de archivos (NTFS, FAT, UFS1 / 2, Ext2 / 3). Además, mediante esta herramienta, se recupera datos eliminados, realizar búsquedas mediante palabras claves, ver metadatos, extraer información EXIF de imágenes y vídeos. Es utilizado por peritos informáticos para investigar lo que ocurrió en un computador (*Autopsy* | *Digital Forensics*, s. f.).

Además, de las ya mencionadas existen múltiples herramientas más para la extracción de información basadas en software libre entre, las cuales, se tiene: Android SKD, *Androidlocdump, Androidguard, Viaforensic, BitPim y Helix.*

Tal como, se ha visto, cada una de las herramientas de extracción de información para dispositivos móviles permite adquirir cierto tipo de datos del dispositivo según la necesidad que, se presente y en algunos casos, se visualiza lo obtenido sin ningún otro software adicional. Al analizar las características que ofrece cada herramienta citada anteriormente, se determina que la herramienta dd incluye la

mayoría de las funcionalidades para la extracción de datos, esta permite realizar una copia bit a bit (imagen forense) del dispositivo a analizar. Como la imagen forense no es posible visualizarlo directamente es necesario apoyarse de software de análisis forense, para esta, se utiliza la herramienta Autopsy, la cual, provee muchas funcionalidades para realizar una investigación forense digital.

Extracción de datos manual, lógica, física y sistemas de ficheros

(Soto, 2021) indica que para la extracción de datos en los dispositivos móviles existen varias herramientas disponibles tanto a nivel de hardware como a nivel de software. Cada una de las herramientas mencionadas anteriormente ellas tienen sus fortalezas, tener en cuenta que, depende de sus características, modelo, versión del sistema operativo y estado en el que, se encuentre el teléfono (encendido, apagado, bloqueado, entre otros).

La extracción de datos es la fase más compleja, debido a que cada dispositivo móvil tiene su característica propia de seguridad. Por, lo cual, según el sistema operativo, marca y modelo, se selecciona el método más adecuado, según (Mendillo, 2018) los métodos de extracción son manual, lógica, archivos de sistema y física, los cuales, se muestran en la siguiente figura.

Figura 3. Métodos de extracción de datos

Fuente: Adaptado de Análisis forense de dispositivos móviles (Mendillo, 2018)

La extracción de datos fue realizado con referencia a alguno de los siguientes métodos; extracción manual, extracción lógica, extracción física y extracción del sistema de ficheros.
Con base a lo mencionado, se va abordar sobre el proceso que, se realiza, así como que datos adquiere al aplicar cada método.

Extracción manual. - Este método es el más fácil de todos, simplemente, se usa el teclado o la pantalla táctil para navegar en el dispositivo y realizar la búsqueda de la información referente al caso que, se necesite investigar. Para documentar los hallazgos, se toma fotografías o, se realiza grabaciones. A fin de facilitar las búsqueda y visualización de la información existente, se instala un explorador de archivos como ES *File Explorer*.

Extracción lógica. - Este método extrae las carpetas y los archivos que están almacenados en una unidad lógica como una partición del sistema. Para esto, se utilizan los módulos implementados de manera nativa por el fabricante, es decir, aquellos que son utilizados de forma habitual para sincronizar el dispositivo con un computador para solicitar la información deseada al sistema operativo del dispositivo móvil. Para realizar esta extracción, se conecta el dispositivo móvil con el computador mediante un cable USB, Bluetooth. Extrae datos a través de Media Transfer Protocol (MTP), permite transferir todo tipo de archivos. Existen otras herramientas para este tipo de extracción que ya mencionó anteriormente como: *Android Debug Bridge* (ADB), AFLogical.

Extracción física. - Es el método más completo y utilizado normalmente, permite realizar una réplica idéntica del original por lo que, se preservan la totalidad de la información almacenada. Este método realiza una copia bit a bit de toda la memoria interna y externa, así como, también, de algunas de sus particiones mediante software y en algunas ocasiones hardware. Esta extracción permite la búsqueda de archivos que fueron eliminados en el equipo móvil. Para realizar la copia forense del dispositivo móvil, se realiza mediante la herramienta dd (por sus siglas en ingles *Dataset Definition*) y con privilegios de usuario *root*.

Extracción del sistema de ficheros. - Permite obtener todos los ficheros visibles mediante el sistema de ficheros, lo que no incluye ficheros eliminados o particiones ocultas. Según el tipo de investigación resulta suficiente utilizar este método, lo que supone una complejidad menor que la adquisición física.

Para llevarlo a cabo, se aprovecha de los mecanismos integrados en el sistema operativo para realizar el copiado de los ficheros. *Android Debug Bridge* (ADB) en el caso de Android. Mediante este método es posible recuperar cierta información eliminada, algunos sistemas operativos como es el caso de Android e iOS, se valen de una estructura que utiliza bases de datos SQLite para almacenar gran parte de la información. De este modo, si, se eliminan registros de los ficheros, únicamente, se marcan como disponibles para sobreescritura, por lo que temporalmente siguen disponibles y por tanto es posible recuperarlos.

1.4. Normativa legal en el Ecuador

Al tratarse de la extracción de información en dispositivos móviles es necesario, también, considerar la normativa legal vigente del Ecuador y cómo, se aplica en las diferentes fases del análisis forense. A continuación, se describe algunos artículos y reglamentos importantes relacionados con el presente trabajo de investigación tomados del Código Integral Penal.

Código Orgánico Integral Penal (COIP)

El Código Integral Penal establece una serie de sanciones relacionadas con los delitos informáticos y de telecomunicaciones en el Ecuador, algunos de ellos como: **Art. 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 mediante la alteración, manipulación o modificación del funcionamiento de redes electrónicas, programas,

sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, es sancionada con pena privativa de libertad de una tres años.

La misma sanción, se impone 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 (Código Orgánico Integral Penal, COIP, 2021).

Art. 191.- Reprogramación o modificación de información de equipos terminales móviles. - La persona que reprograme o modifique la información de identificación de los equipos terminales móviles, es sancionada con pena privativa de libertad de uno a tres años (Código Orgánico Integral Penal, COIP, 2021).

Art. 232.- Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, es sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena es sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción, se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena es de cinco a siete años de privación de libertad (Código Orgánico Integral Penal, COIP, 2021).

Art. 233.- Delitos contra la información pública reservada legalmente. - La persona que destruya o inutilice información clasificada de conformidad con la Ley, es sancionada con pena privativa de libertad de cinco a siete años.

La o el servidor público que, al utilizar cualquier medio electrónico o informático, obtenga este tipo de información, es sancionado con pena privativa de libertad de tres a cinco años.

Cuando, se trate de información reservada, cuya revelación comprometa gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, es sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no, se configure otra infracción de mayor gravedad (Código Orgánico Integral Penal, COIP, 2021).

Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. - La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o, se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, es sancionada con la pena privativa de la libertad de tres a cinco años (Código Orgánico Integral Penal, COIP, 2021).

Art. 456.- Cadena de custodia. - Se aplica cadena de custodia a los elementos físicos o contenido digital materia de prueba, para garantizar su autenticidad, acreditar 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, incluye, también, el personal de servicios de salud que tengan contacto con elementos físicos que son de utilidad en la investigación (Código Orgánico Integral Penal, COIP, 2021).

Ley de comercio electrónico, firmas y mensajes de datos

El objeto de la Ley de comercio electrónico, firmas y mensajes de datos es regular y sancionar las infracciones relacionado con los sistemas de información, redes electrónicas e internet, en algunos de ellos como:
Art. 2.- Reconocimiento jurídico de los mensajes de datos. - Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos, se somete al cumplimiento de lo establecido en esta ley y su reglamento (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

Art. 7.- Información original. - Cuando la ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito queda cumplido con un mensaje de datos, si es requerido conforme a la ley, puede comprobarse que ha conservado la integridad de la información a partir del momento en que, se generó por primera vez en su forma definitiva, como mensaje de datos.

Se considera que un mensaje de datos permanece integro, si, se mantiene completo e inalterable su contenido, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación.

Por acuerdo de las partes y con el cumplimiento de todas las obligaciones previstas en esta ley, se desmaterializarán los documentos que por ley deban ser instrumentados físicamente. Los documentos desmaterializados contendrán las firmas electrónicas correspondientes debidamente certificadas ante una de las entidades autorizadas según lo dispuesto en el artículo 29 de la presente ley, y serán conservados conforme a lo establecido en el artículo siguiente (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

Art. 8.- Conservación de los mensajes de datos. - Toda información sometida a esta ley, es conservada; este requisito queda 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 cumple con la conservación de mensajes de datos, al usar 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 es obligatorio el cumplimiento de lo establecido en los literales anteriores (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

Art. 10.- Procedencia e identidad de un mensaje de datos. - Salvo prueba en contrario, se entiende 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 consta como emisor; en este caso, el aviso, se lo hace antes de que la persona que lo recibe actúe conforme a dicho mensaje. En caso contrario, quien conste como emisor justifica 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 (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

Art. 54.- Práctica de la prueba. - La prueba, se practica de conformidad con lo previsto en el Código de Procedimiento Civil y al observar las normas siguientes:

a) Al presentar un mensaje de datos dentro de un proceso judicial en los juzgados o tribunales del país, se adjunta el soporte informático y la transcripción en papel del documento electrónico, así como los elementos necesarios para su lectura y verificación, cuando sean requeridos;
b) En el caso de impugnación del certificado o de la firma electrónica por cualesquiera de las partes, el juez o tribunal, a petición de parte, ordena a la entidad de certificación de información correspondiente, remitir a ese despacho los certificados de firma electrónica y documentos en los que, se basó la solicitud del firmante, debidamente certificados; y,
c) El facsímile, es admitido como medio de prueba, siempre y cuando, haya sido enviado y recibido como mensaje de datos, mantenga su integridad, se conserve y cumpla con las exigencias contempladas en esta ley.

En caso de que alguna de las partes niegue la validez de un mensaje de datos, probará, conforme a la ley, que éste adolece de uno o varios vicios que lo invalidan, o que el procedimiento de seguridad, también, los datos de creación y los medios utilizados para verificar la firma, no serán reconocidos técnicamente como seguros.

Cualquier duda sobre la validez es objeto de comprobación técnica (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

Art. 55.- Valoración de la prueba. - La prueba es valorada bajo los principios determinados en la ley y al tomar 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 somete 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 designa los peritos que considere necesarios para el análisis y estudio técnico y tecnológico de las pruebas presentadas (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

Reglamento del Sistema Pericial Integral de la Función Judicial

El Reglamento del Sistema Pericial Integral de la Función Judicial establece obligaciones específicas que los peritos cumplirán, así como, también, la forma en que, se presenta el informe pericial, en algunos de ellos como:

Art. 19.- Obligaciones Específicas. Son obligaciones específicas de los peritos:
1. (Sustituido por el Art. 15 de la Res. 067-2016, R.O. 756-2S, 17-V-2016). - Cumplir la orden de la autoridad judicial una vez que han sido designados. En caso de que la calificación pericial venza luego de la designación del perito, éste tiene igualmente la obligación de presentar su informe y cumplir con todos los deberes inherentes a la orden judicial. El informe y las actuaciones periciales cumplidas en este supuesto, tendrán toda la validez legal y procesal que el caso lo amerite. Los peritos presentaran su excusa debidamente documentada dentro del proceso, en los siguientes casos:

a) Causas de fuerza mayor o caso fortuito;
b) Ausencia del país previa a la designación;

c) Tener a su cargo más de tres informes periciales pendientes de presentación, tener otra diligencia en otra judicatura o fiscalía; y,
d) Las demás que determine la ley.

2. Presentar el informe correspondiente oportunamente, en la forma, plazos y términos previstos por la normativa o por la autoridad judicial correspondiente. En caso de dificultad o complejidad en su trabajo, tiene la posibilidad de solicitar motivadamente a la autoridad competente, un solo plazo adicional para presentar su informe, la ampliación o aclaración al mismo, salvo que la normativa legal disponga lo contrario. Se solicitarán plazos adicionales al antes establecido de forma excepcional y al tomar en consideración las dificultades para la presentación del informe. La jueza, el juez, o la o el fiscal, motivarán la aceptación o no de esta nueva solicitud de ampliación de plazo que presente la o el perito.

3. (Sustituido por el Art. 15 de la Res. 067-2016, R.O. 756-2S, 17-V-2016). - Presentar el informe correspondiente, de forma verbal y/o escrita, según lo que la normativa procesal establezca, con los requisitos mínimos establecidos en este reglamento y la ley; y, subirlo al Sistema Informático Pericial, en archivo tipo PDF. En el caso de informes de avalúos de bienes, obligatoriamente, se subirán, también, las fotografías de los mismos.

4. Presentar obligatoriamente y dentro del plazo otorgado, las aclaraciones, ampliaciones o complementos al informe presentado que ordene la autoridad judicial competente. Estas aclaraciones, se presentarán de forma verbal y escrita según la normativa que lo establezca.

5. Explicar y defender el informe presentado y sus conclusiones, en las audiencias orales, de prueba, o de juicio para, las cuales, fuere notificado legalmente, si la ley así lo prevé.

6. Presentar conjuntamente con su informe en todos los procesos judiciales o pre procesales, la copia certificada de la factura de honorarios emitida por su persona, por el trabajo pericial realizado.

7. Abstenerse de cobrar valores adicionales a los incluidos en la factura presentada en el proceso judicial o pre procesal, por el informe presentado, por las aclaraciones o ampliaciones hechas, por la defensa del informe en audiencia oral, de prueba o de juicio, o por cualquier otra actividad inherente a su actividad pericial. Los valores de honorarios facturados son únicos, y abarcan todas las obligaciones de los peritos constantes en el presente artículo.

8. Aprobar los cursos de capacitación determinados en el presente reglamento; y,

9. Cualquier otra obligación establecida en la normativa legal, en este reglamento y/o por la o el administrador del sistema pericial (*Reglamento del Sistema Pericial Integral de la Función Judicial*, 2014).

Art. 20.- Forma. - El informe pericial, sus explicaciones o aclaraciones, se presentarán de forma verbal y por escrito, de conformidad con la normativa procesal correspondiente. En caso de que el informe sea escrito, la jueza o juez o la o el fiscal obligatoriamente lo sube sin los anexos al sistema informático que administra el proceso correspondiente, mediante la constancia e inclusión al momento de hacerlo, el número del código de calificación de perito.

Los informes periciales realizados en procesos calificados por la ley como reservados, o que tienen que ver con información restringida por la ley, no, se subirán al sistema informático que administra el proceso correspondiente (*Reglamento del Sistema Pericial Integral de la Función Judicial*, 2014).

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Caracterización del problema

El presente proyecto de desarrollo, se realizó bajo el esquema de una prueba de concepto, debido a que, se procedió con la extracción de información de dispositivos móviles con sistema operativo Android mediante herramientas *open-sourse*, con el fin de demostrar que es posible obtener evidencia valida del dispositivo móvil. Y así para apoyar en el proceso de un análisis forense a los peritos informáticos le da una alternativa de fácil acceso y que cumpla lo ofrecido por las herramientas comerciales.

Las actividades de extracción de información en los dispositivos móviles, se van a realizar en primera instancia en un emulador en donde, se va a instalar sistemas operativos Android, los cuales, con herramientas de extracción de información, se realizó lo misma, se ejecutaron varias simulaciones, para luego en segunda instancia con los resultados de las primeras pruebas realizar la extracción de información en dispositivos móviles físicos con las mismas herramientas. Debido a que es una prueba de concepto no, se optó por realizar en alguna institución definida, y, también, al saber como premisa que contar con un dispositivo móvil que esté inmerso en un proceso delictivo tiene que cumplir sus etapas y tiempos desde la incautación, aislamiento y entrega a la entidad competente para que realice el análisis forense digital.

2.2. Metodología de la investigación

Con la elección de una correcta metodología el proceso de extracción de información de los dispositivos móviles, se cumplió con el objetivo planteado. Para el presente proyecto de desarrollo, se ha elegido los siguientes métodos de investigación:

Investigación cualitativa

Para la Prueba de concepto (POC) propuesto desarrollado establece la utilización de la investigación cualitativa que, permite la obtención de información y datos de distintos modelos y herramientas para la extracción de información en dispositivos móviles con sistema operativo Android, las características de cada una de las herramientas y métodos existentes, así como, también, que ventajas y desventajas ofrece.

Método bibliográfico

Se ha seleccionado este método debido a que engloba el análisis de tesis, modelos, investigaciones, revistas, artículos, libros, desarrollados para ahondar guías con relación al análisis de la investigación, con el fin de, dar un valor agregado al tema tratado, se profundiza el estudio de las leyes y normativas vigentes en el país.

El constante avance tecnológico junto al crecimiento, utilización de los dispositivos y creación de nuevas formas de realizar actos ilícitos a través de los dispositivos móviles evidencian la necesidad de contar con métodos y herramientas de software libre para la extracción de información. Para realizar el proceso, se procede con la selección del equipo y herramientas disponibles, se utiliza una metodología basada en la investigación bibliográfica de métodos nacionales e internacionales. Mediante esta búsqueda y análisis, se establece lo valiosa que, resulta la información almacenada en dispositivos móviles de allí la importancia de indagar fuentes bibliográficas confiables que, permitan organizar la información para la redacción correcta de este modelo el que, contribuye al esclarecimiento delito informático.

Técnicas e instrumentos de investigación

En el presente proyecto, se va emplear la técnica de la observación mediante la revisión de métodos existentes para la extracción de información en dispositivos móviles con sistema operativo Android, con el objetivo de establecer la importancia de cada uno de los métodos y el aporte que estos han realizado a los profesionales

que realizan el análisis forense. A demás de la observación, se aplica la técnica de análisis documental la que, consiste en el estudio de datos secundarios a través de la recolección de información de fuentes bibliográficas como; libros, revistas, páginas web.

Además, en este proyecto, se utilizó metodología hipotético-deductivo, maneja procedimientos inductivos y deductivos para llegar a una conclusión y así comprobar la hipótesis planteada. Esta metodología es seleccionada porque tiene características más acordes al proyecto de estudio. La metodología fue aplicada con un enfoque cualitativo con diseño transversal debido a que la misma prueba de concepto, se aplicaran a varios dispositivos móviles.

Metodología Hipotético-Deductivo

Para hablar de la metodología hipotético-deductivo es necesario revisar el método experimental, el cual, lo consideran por su gran desarrollo y relevancia un método independiente del método empírico (lógica experimental), este método engloba al método hipotético-deductivo.

El método hipotético-deductivo tiene describe al método científico, basado en un ciclo inducción-deducción-inducción para establecer hipótesis y comprobar o contradecir. Debido a que está compuesto por la observación del fenómeno a estudiar, creación de la hipótesis para explicar dicho fenómeno (inducción), deducción de consecuencias o implicaciones más elementales de la propia hipótesis (deducción) y comprobación o refutación los expuestos deducidos lo compara con la experiencia (inducción).

El presente método obliga al investigador a combinar la reflexión racional o momento racional (la formación de hipótesis y la deducción) con la observación de la realidad o momento empírico (la observación y la verificación). Por esto, se afirma que el método sigue un proceso inductivo (en la observación), deductivo (en el planteamiento de hipótesis y en sus deducciones), y vuelve a la inducción para su verificación. Además, en el caso de que todas las variables sean objeto de estudio,

el último paso sería una inducción completa que daría paso a una ley universal. En caso contrario, la inducción es incompleta y, por lo tanto, la ley obtenida sería una ley probabilística.

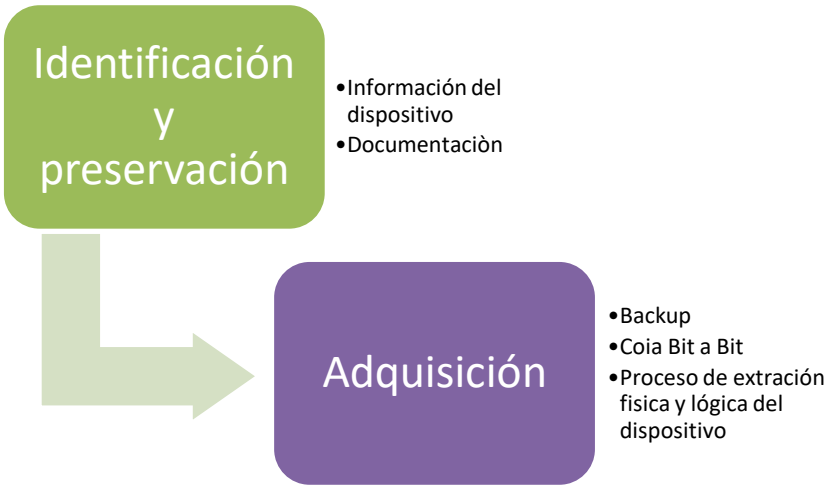
Por las características ofrecidas el método inductivo-deductivo en la POC a realizarse ayuda a evaluar y analizar los resultados de los escenarios a ejecutarse posteriormente, así como, también, en la etapa del desarrollo.

2.3. Metodología de desarrollo

Para la metodología de desarrollo, se utilizó la revisión de trabajos, herramientas, método existentes y relacionados con el análisis forense en dispositivos móviles mediante herramientas *open-source.* Es así que, se siguió para el desarrollo del presente proyecto el proceso de extracción de evidencia en dispositivos móvil revisado de trabajos relacionados.

Para la extracción de información de dispositivos móviles existe una metodología propuesta por (Cajías, 2018), de, la cual, para el presente proyecto de desarrollo, se va adoptar solo las fases necesarias para la presente investigación. En la figura 4, se proporciona una descripción general del proceso a considerar para la extracción de evidencia en dispositivos móviles con sistema operativo Android.

Figura 4: Proceso extracción de información en dispositivo móviles



Fuente: adaptado de (Cajías, 2018).

Como, se muestra en la figura anterior, para la extracción de información en un dispositivo móvil para este caso, se considera las siguientes fases: identificación y preservación y adquisición. Para la ejecución del proyecto, se ha definido trabajar sobre dos escenarios: un escenario con simuladores y otro escenario con equipos reales, en, los cuales, se van utilizar las mismas herramientas y modelos seleccionados para la extracción de información; con el objetivo de contar con más evidencias y en diferentes escenarios. Además, se siguió los métodos de extracción ya mencionado en el capítulo 1 junto con la utilización de herramientas basadas en la pirámide de clasificación de herramientas de análisis forense para dispositivos móviles.

En la siguiente tabla, se detalla las características de cada uno de los equipos donde, se va a realizar la adquisición de información definido para cada escenario.

Tabla 1. Características de equipos en cada escenario

Tipo de Escenario	Equipo	Marca	Modelo	Sistema Operativo	Memoria Ram	Procesador	CPU	Almacenamiento interno
Real	1	Samsung Galaxy J5	SM-J500M	Android 5.1.1	1388 MB	Qualcomm Snapdragon 1.19 GHz	4 Cores 4x ARM Cortex-A53	8 GB
Emulado	1	Samsung Galaxy S7	vbox86p	Android 6.0	4 GB	Intel Core I7	4 Cores X86	16 GB

Fuente: elaboración propia

De acuerdo a las fases indicadas anteriormente, a continuación, se detalla el proceso a seguirse en cada una de ellas para llevar a cabo el desarrollo.

Fase de identificación y preservación

Del proceso mencionado anteriormente de esta fase puntualmente, se va a realizar la documentación relevante de la información del dispositivo a analizar, a fin de tener un detalle de las pruebas a realizar en cada dispositivo que nos sirvió en el capítulo posterior para evaluar los resultados. La información que, se va a registrar es marca, modelo, serie, versión de sistema operativo, memoria RAM, capacidad de almacenamiento interno, entre otros.

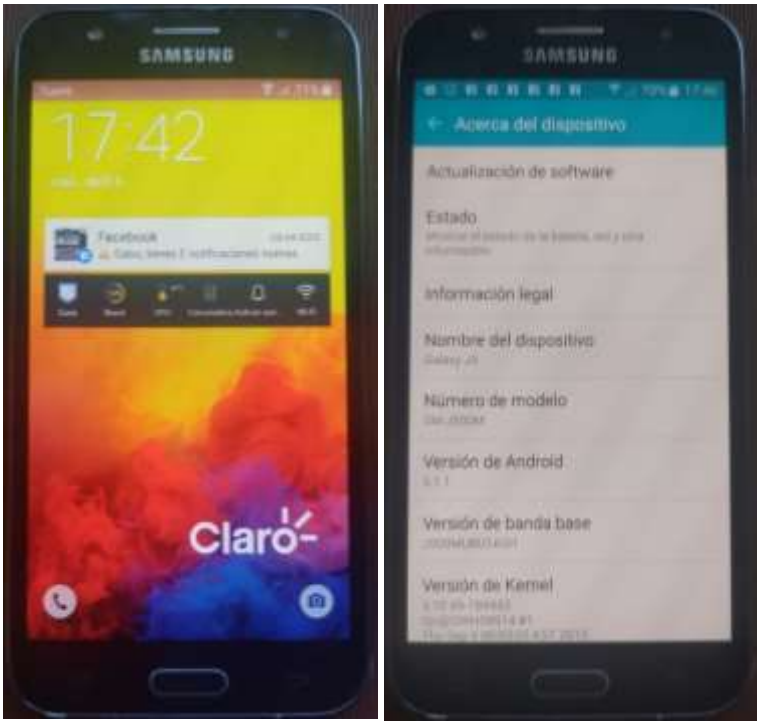
Al seguir el modelo propuesto, se procede con el registro de información del equipo para el caso de estudio. Las actividades a realizar en esta fase son:

1. Evidenciar imagen del equipo a analizar
2. Registrar información del equipo en una ficha

Escenario con dispositivos real

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 y, se procede a registrar en la ficha como, se ve en la figura 5 y tabla 2.

Figura 5. Equipo real a analizar



Fuente: elaboración propia

Tabla 2. Ficha de registro de información del dispositivo móvil real

Ficha técnica de dispositivos móviles	
Perito	Darwin Chimbo

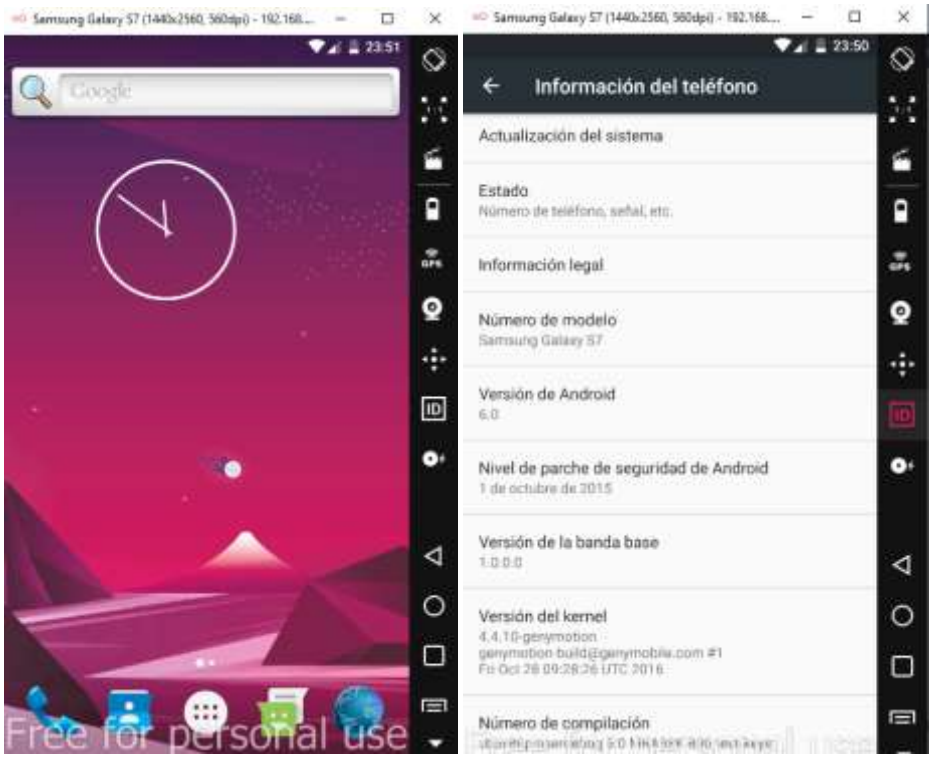
Numero de caso	001					
Fecha	16 de diciembre de 2021					
Hora	10:00					
Item	**Tipo**	**Marca**	**Serie**	**Modelo**	**Estado**	**Observaciones**
1	Celular	Samsung Galaxy J5	RV8H10X3AXE	SM-J500M	Bueno	Encendido

Fuente: elaboración propia

Escenario con simuladores

Se procede con la identificación y el registro del equipo a analizar en el entorno simulado con la ejecución de las mismas actividades realizadas para el escenario del equipo real, ver figura 6 y tabla 3.

Figura 6. Equipo emulado a analizar



Fuente: elaboración propia

Tabla 3. Ficha de registro de información del dispositivo móvil emulado

Ficha técnica de dispositivos móviles

Perito	Darwin Chimbo					
Numero de caso	002					
Fecha	17 de diciembre de 2021					
Hora	10:00					
Item	**Tipo**	**Marca**	**Serie**	**Modelo**	**Estado**	**Observaciones**
1	Celular	Samsung Galaxy S7	N/A	vbox86p	Bueno	Encendido

Fuente: elaboración propia

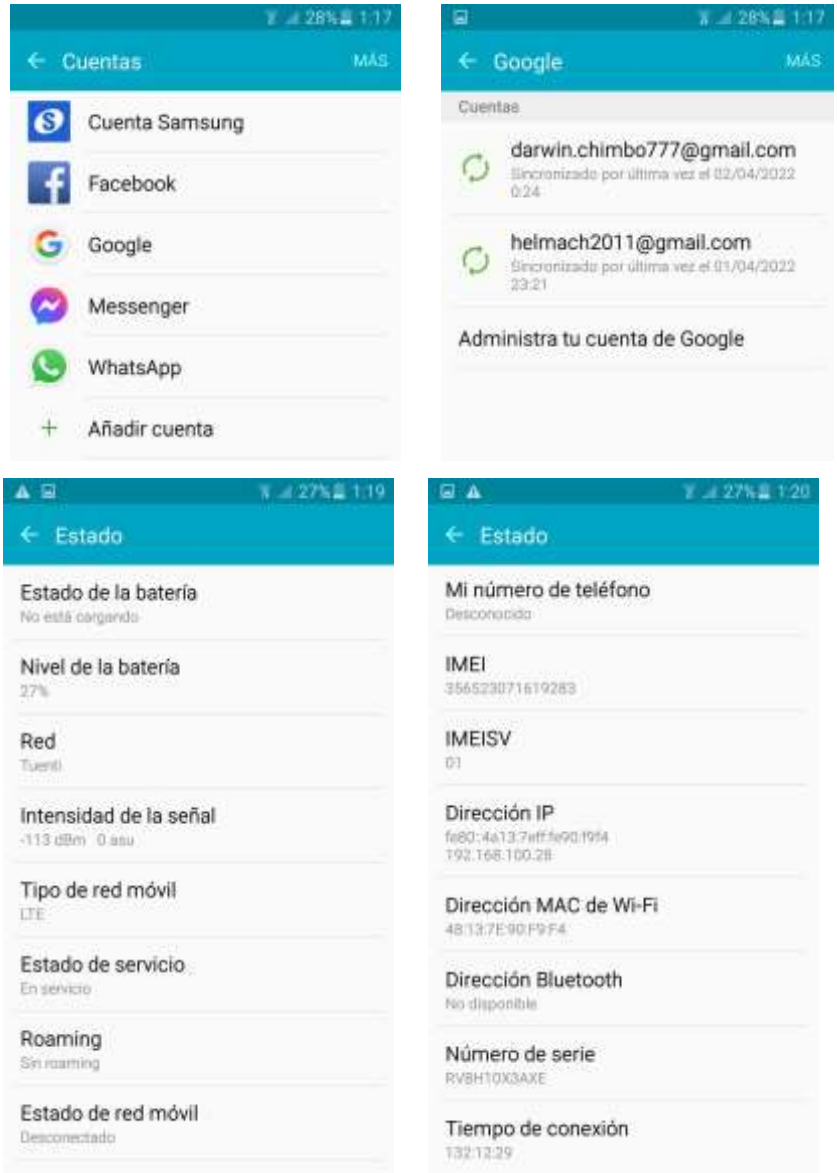
Fase de adquisición

En esta fase, se realizó la extracción manual, lógica (recuperación de archivos según arquitectura del sistema operativo), física (recuperación de archivos de unidades físicas), este último contempla la ejecución de un respaldo bit a bit del dispositivo móvil.

Escenario con dispositivo real

Al continuar con la fase de adquisición, se procedió con la extracción manual de los datos, en donde, se busca información relacionada a contactos, mensajes SMS y chat, cuentas de Gmail y redes sociales. Información a detalle sobre el dispositivo móvil (sistema operativo, marca, modelo, serial), información de las conexiones Wifi y de Bluetooth, detalle de la tarjeta SIM, número IMEI, operadora de red, serial SIM, tiempo de actividad del dispositivo, tipo de red móvil (GSM, CDMA, LTE), ver figura 7.

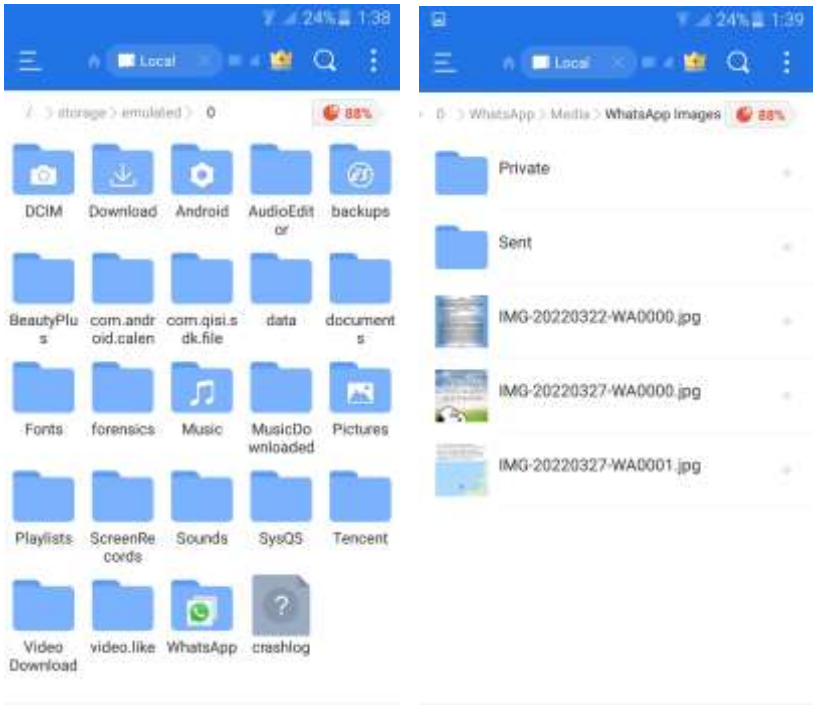
Figura 7. Extracción manual



Fuente: elaboración propia

Además, si el dispositivo ya tiene instalado o, se le instala un explorador de archivos (como *ES File Explorer*), se facilita la búsqueda y la visualización de información sobre el dispositivo, ver figura 8.

Figura 8. Navegador de archivos



Fuente: elaboración propia

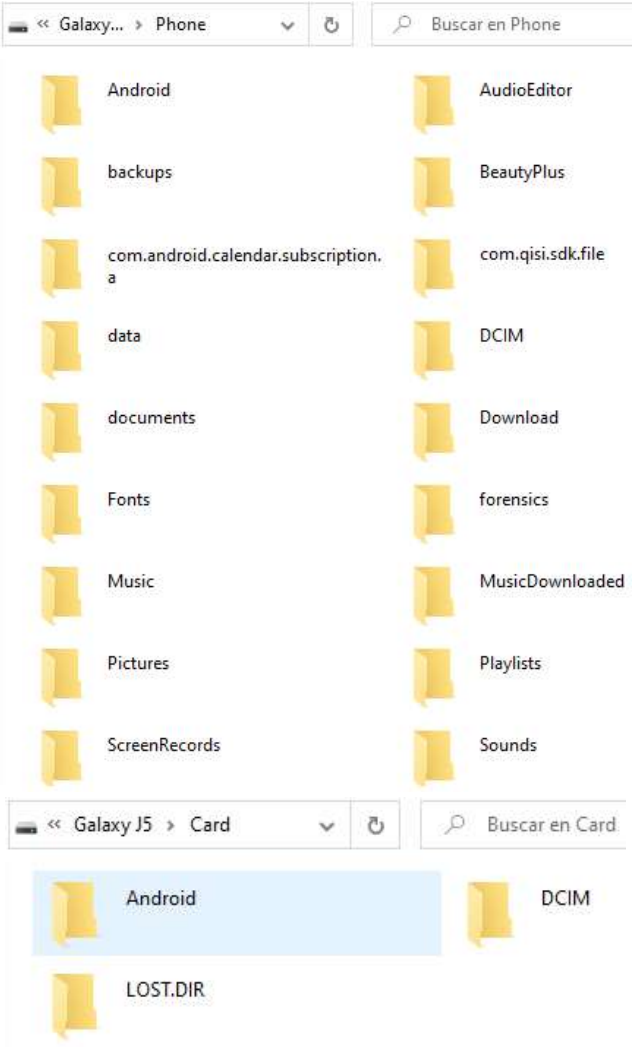
La extracción lógica mediante *Media Transfer Protocol* (MTP) ayudó a extraer información almacenada en una ubicación lógica del dispositivo, para, lo cual, es necesario tener conectado el dispositivo a la computadora, ver figura 9.

Figura 9. Conexión dispositivo móvil a la computadora

Fuente: elaboración propia

Una vez conectado el dispositivo móvil, se visualizó en el computador una o dos unidades de almacenamiento a, las cuales, se logró acceder a ver la información, ver figura 10.

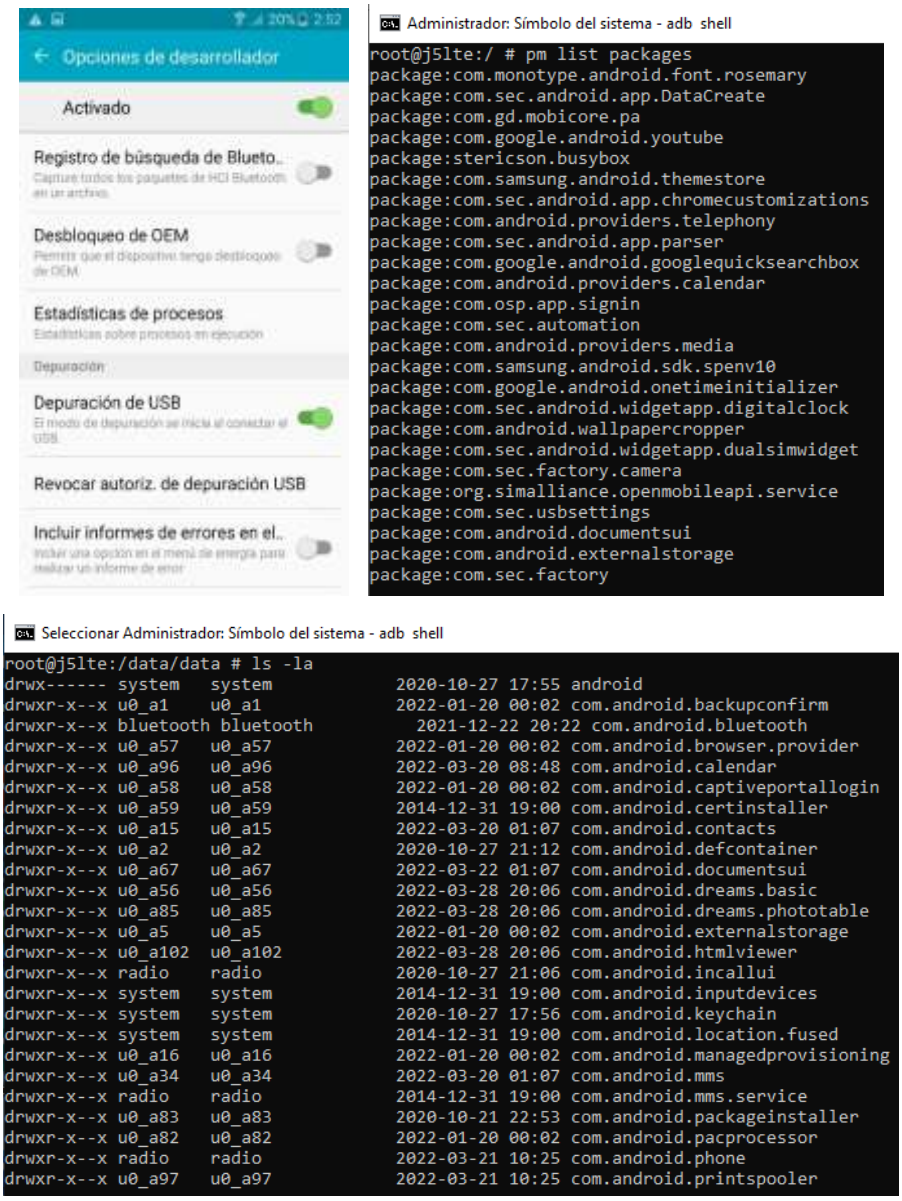
Figura 10. Acceso al dispositivo móvil mediante MTP



Fuente: elaboración propia

La extracción lógica mediante ADB ayuda a obtener datos almacenados en la carpeta /data/data que permanecen inaccesibles vía MTP, para acceder a esta utilidad es necesario tener activado la opción depuración por *usb,* ver figura 11. Es posible ver información como, por ejemplo, las aplicaciones instaladas.

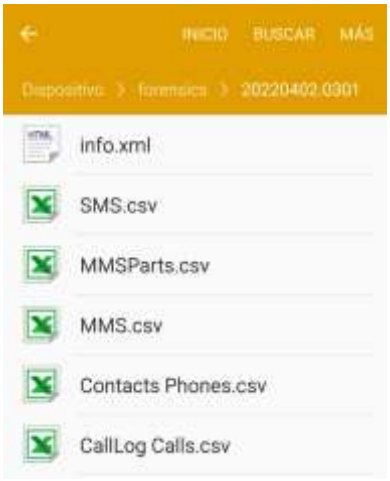
Figura 11. Lista paquetes instaladas en el dispositivo móvil y modo de depuración



Fuente: elaboración propia

Con la extracción mediante AFLogical nos permitió obtener datos como registros de llamadas, contactos telefónicos almacenados, mensajes multimedia, mensajes SMS, además, un archivo con todas las características del dispositivo móvil, ver figura 12.

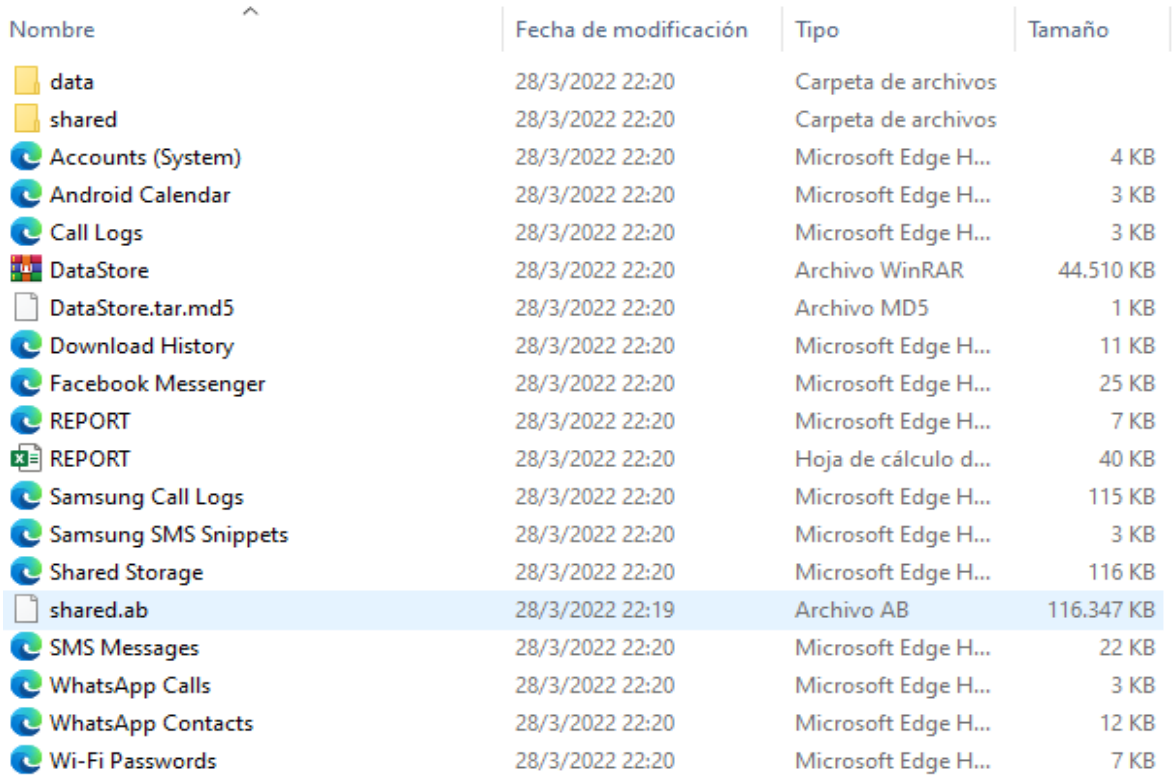
Figura 12. Información obtenida mediante AFLogical



Fuente: elaboración propia

La extracción lógica al utilizar la herramienta Andriller permite realizar *backup* del dispositivo móvil, obtener logs de llamadas, cuentas creadas, mensajes de *Facebook*, mensajes de *WhatsApp*, contactos de *WhatsApp*, llamadas de *WhatsApp*, mensajes SMS, claves de wifi e informes en formato html y en excel. Para utilizar es necesario que el móvil, se conecte mediante un cable *usb* y que tenga habilitado la depuración *usb*, ver figura 13.

Figura 13. Información obtenida mediante Andriller



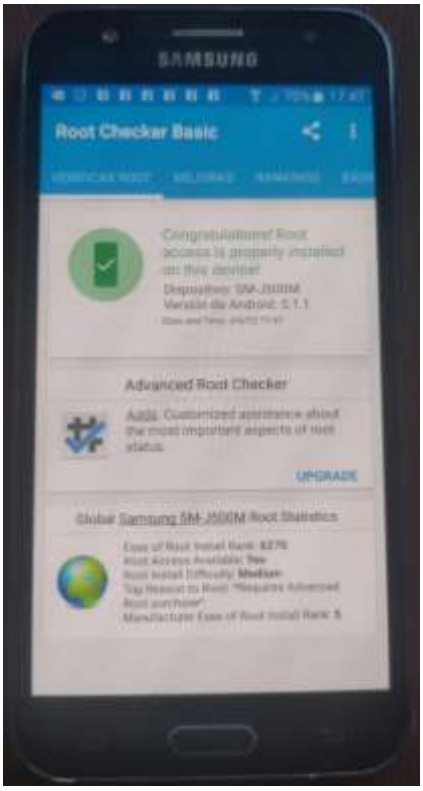
Nombre	Fecha de modificación	Tipo	Tamaño
data	28/3/2022 22:20	Carpeta de archivos	
shared	28/3/2022 22:20	Carpeta de archivos	
Accounts (System)	28/3/2022 22:20	Microsoft Edge H...	4 KB
Android Calendar	28/3/2022 22:20	Microsoft Edge H...	3 KB
Call Logs	28/3/2022 22:20	Microsoft Edge H...	3 KB
DataStore	28/3/2022 22:20	Archivo WinRAR	44.510 KB
DataStore.tar.md5	28/3/2022 22:20	Archivo MD5	1 KB
Download History	28/3/2022 22:20	Microsoft Edge H...	11 KB
Facebook Messenger	28/3/2022 22:20	Microsoft Edge H...	25 KB
REPORT	28/3/2022 22:20	Microsoft Edge H...	7 KB
REPORT	28/3/2022 22:20	Hoja de cálculo d...	40 KB
Samsung Call Logs	28/3/2022 22:20	Microsoft Edge H...	115 KB
Samsung SMS Snippets	28/3/2022 22:20	Microsoft Edge H...	3 KB
Shared Storage	28/3/2022 22:20	Microsoft Edge H...	116 KB
shared.ab	28/3/2022 22:19	Archivo AB	116.347 KB
SMS Messages	28/3/2022 22:20	Microsoft Edge H...	22 KB
WhatsApp Calls	28/3/2022 22:20	Microsoft Edge H...	3 KB
WhatsApp Contacts	28/3/2022 22:20	Microsoft Edge H...	12 KB
Wi-Fi Passwords	28/3/2022 22:20	Microsoft Edge H...	7 KB

Fuente: elaboración propia

Para realizar la extracción física, se utilizó el comando **“DD”** (*Dataset Definition*) mediante, el cual, se obtuvo imagen forense o una copia bit a bit de la partición que contiene información de interés del dispositivo móvil. El sistema operativo con el que, se trabajó es el **Santoku,** el cual, es una distribución *open-source* basada en Linux, en donde es posible la ejecución de herramientas para adquisición y análisis de datos de manera forense. Para gestionar la comunicación entre el dispositivo móvil con sistema operativo Android y el equipo con sistema operativo Santoku, es necesario tener habilitado previamente la depuración por *USB* dentro de la configuración del dispositivo móvil luego de ingresar al modo de desarrollador.

Otro aspecto a tener en cuenta es, que el dispositivo móvil cuente con privilegios de superusuario (*root)* ver figura 14, a través del cual sea posible el acceso sin restricciones a la información. De esta manera, se utiliza la herramienta **adb** y **dd** para investigar y crear la imagen forense del dispositivo móvil.

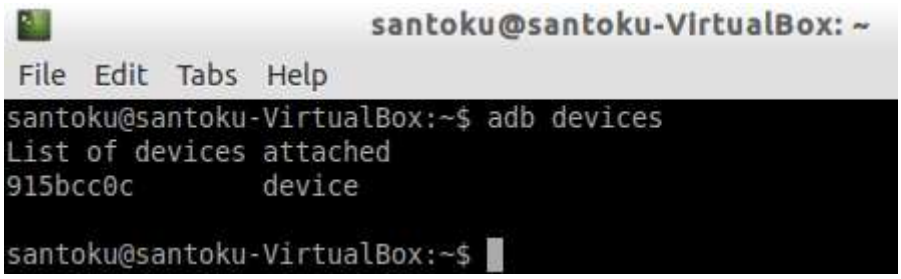
Figura 14. Teléfono con privilegios de root



Fuente: elaboración propia

Al utilizar el sistema operativo Santoku, se realizó la imagen forense del dispositivo móvil, el mismo que sirvió para un posterior análisis. Para verificar que existe comunicación del dispositivo móvil y el computador, se conecta el móvil mediante el puerto USB, seguidamente, se abre una terminal y, se ejecuta el comando *adb devices*, ver figura 15.

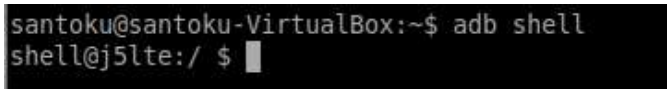
Figura 15. Revisión de dispositivos conectados



Fuente: elaboración propia

Una vez establecida la conexión con el móvil, se procede a ejecutar el comando *adb Shell*, el cual, permite ingresar a la *Shell* del dispositivo y ejecutar cualquier actividad mediante línea de comandos, ver figura 16.

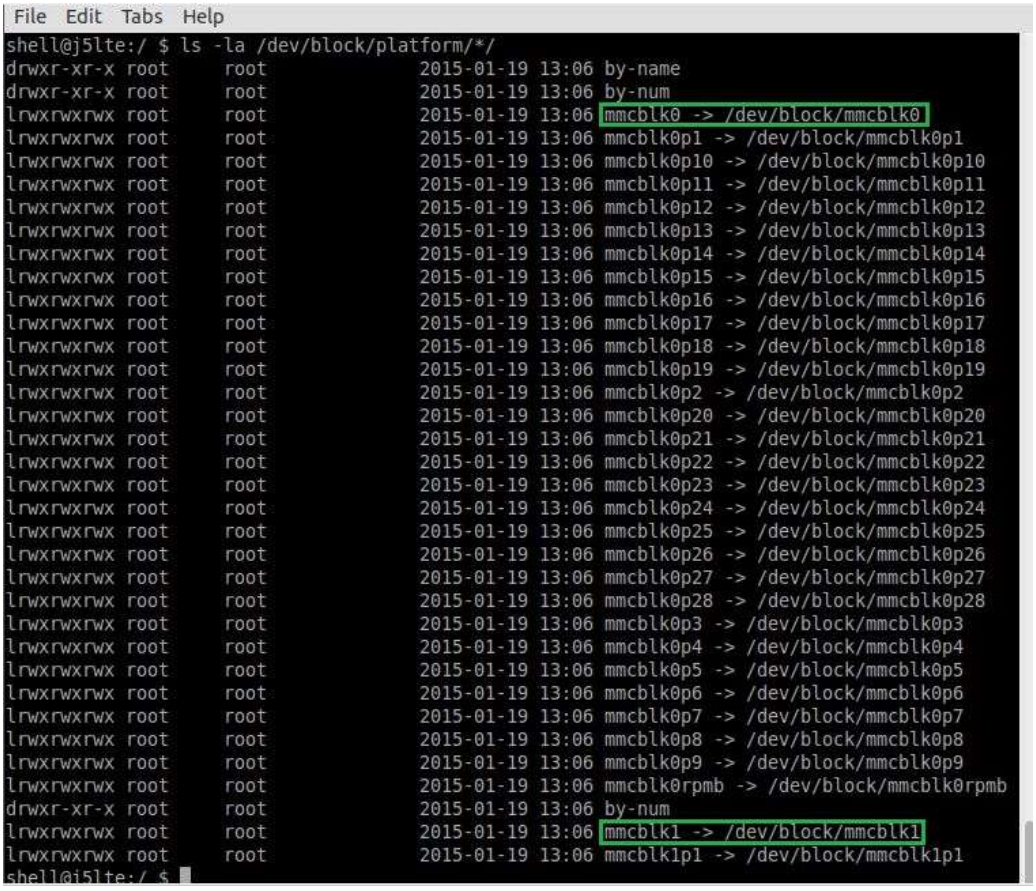
Figura 16. Ejecución del comando adb Shell



Fuente: elaboración propia

Depende de la marca, modelo del dispositivo para seleccionar la partición de, la cual, se requiere crear la imagen forense. Para este caso, se trabajó sobre la partición interna (mmcblk0) debido a que esta contiene toda la información relacionada al dispositivo móvil y el usuario; y la partición externa (mmcblk1) que almacena, también, información importante, contiene datos importantes para una investigación, en este último, se guardan la mayoría de imágenes y archivos de gran capacidad relacionados con multimedia. Para ver las particiones existentes, se utiliza el comando: ls -la /dev/block/platform/*/, ver figura 17.

Figura 17. Ejecución del comando ls -la /dev/block/platform//*



Fuente: elaboración propia

La imagen forense, se realiza en un equipo diferente, para realizar el copiado hacia el equipo externo, se utiliza la herramienta *netcat*, como esta herramienta no viene preinstalada en el dispositivo móvil, se lo consigue mediante la instalación de la aplicación *BusyBox*. Para realizar el reenvío de puertos desde el equipo al utilizar el *adb,* se abre una terminal como usuario *root* y ejecuta el comando *adb forward* tcp:8888 tcp:8888, ver figura 18.

Figura 18. Reenvío de puertos mediante adb

Fuente: elaboración propia

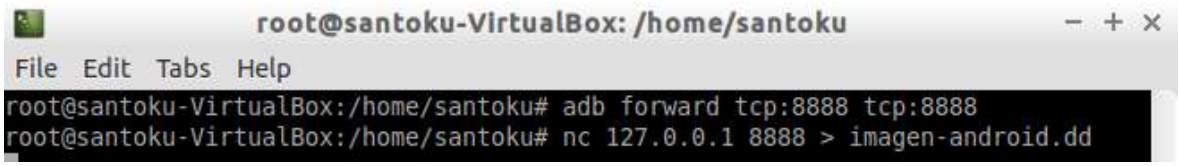
Para proceder con la creación de la imagen forense una vez ya identificada, para este caso la partición (mmcblk0), la cual, contiene información interesante del dispositivo móvil, se lo realizó mediante la herramienta dd, en esta, se digitó el comando dd if=/dev/block/mmcblk0 | busybox nc -l -p 8888, a través del cual, también, se activa la conexión de *netcat* del móvil y pone el puerto 8888 en modo escucha, ver figura 19.

Figura 19. Creación de la imagen forense

Fuente: elaboración propia

Para guardar la imagen forense en el equipo externo, se crea una conexión con el dispositivo móvil mediante el *netcat* y el puerto 8888 en este caso, y, por último, ejecutar el comando: nc 172.0.0.1 8888 > imagen-android, ver figura 20.

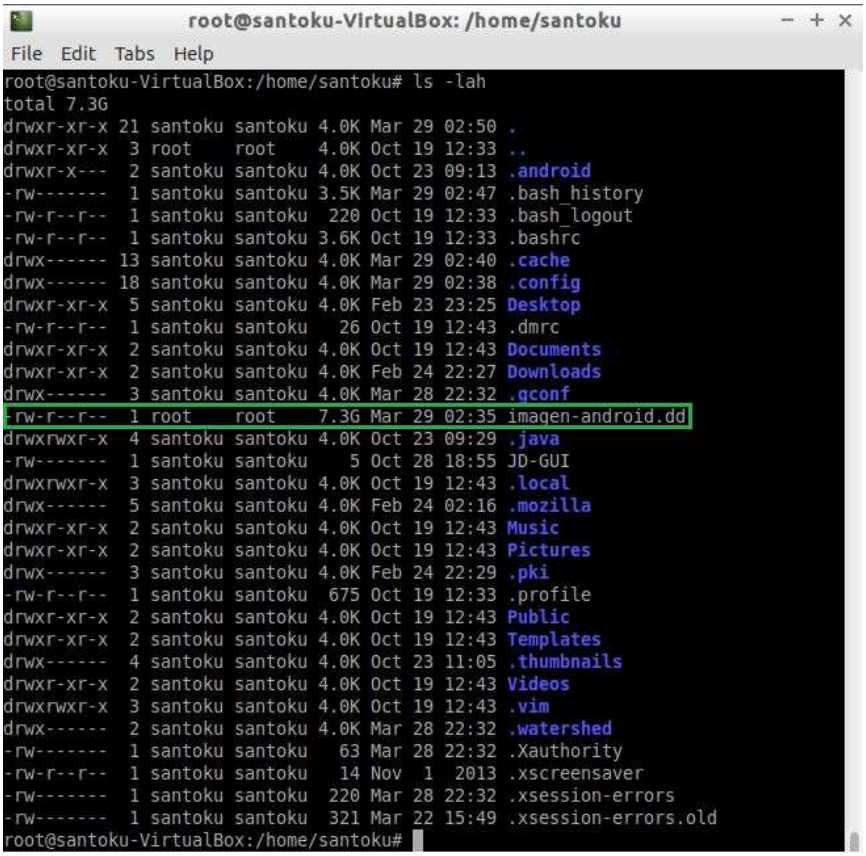
Figura 20. Conexión de netcat para guardar la imagen forense



Fuente: elaboración propia

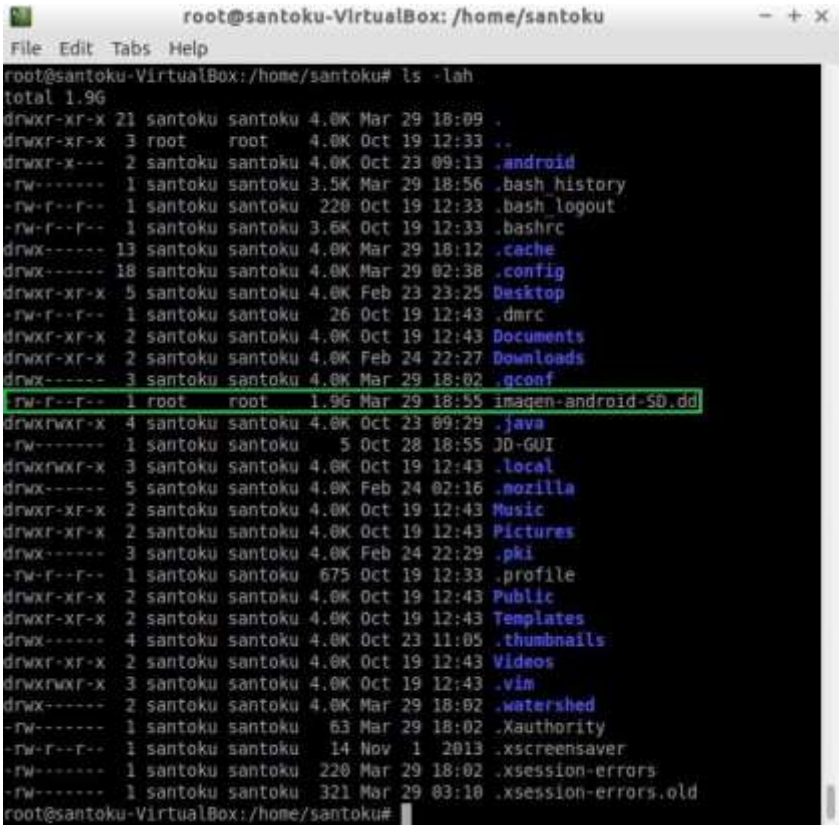
Finalmente, después de un tiempo, se ve que la imagen, se ha creado, ver figura 21 y 22.

Figura 21. Creación de la imagen forense memoria interna



Fuente: elaboración propia

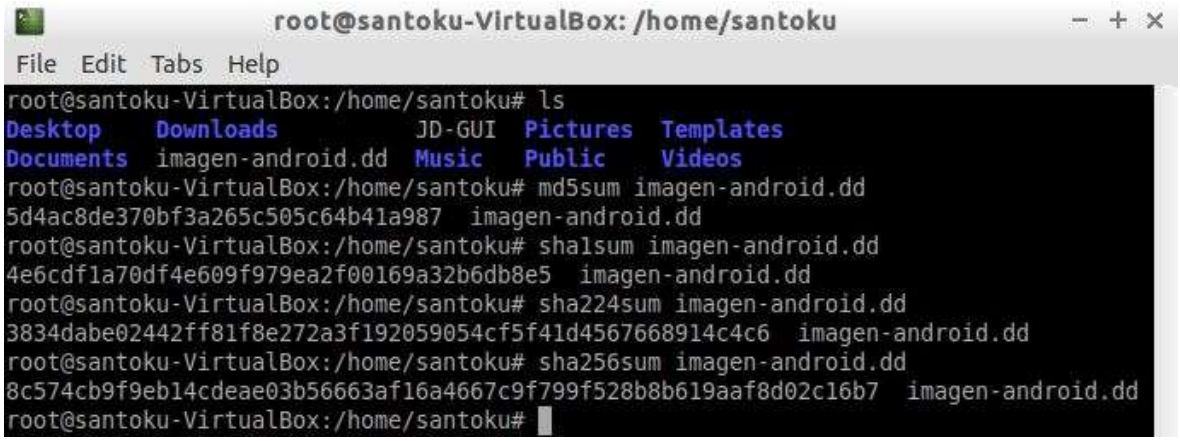
Figura 22. Creación de la imagen forense memoria externa



Fuente: elaboración propia

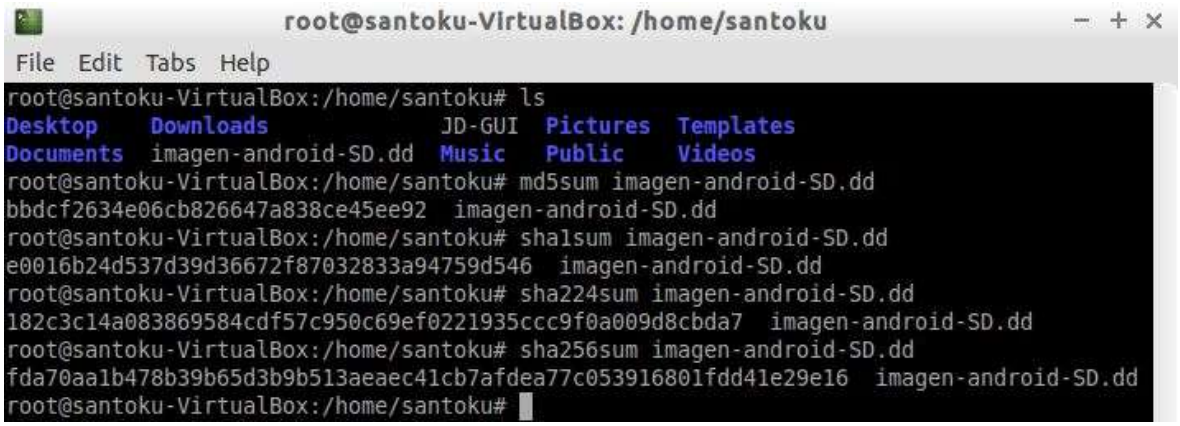
Con el fin de mantener la integridad de la imagen forense es necesario generar los hashes (md5, sha1, sha224, sha256), mediante esto, se verifica si realizaron alguna modificación sobre la imagen, ver figura 23 y 24.

Figura 23. Hash de la imagen forense memoria interna



Fuente: elaboración propia

Figura 24. Hash de la imagen forense memoria externa



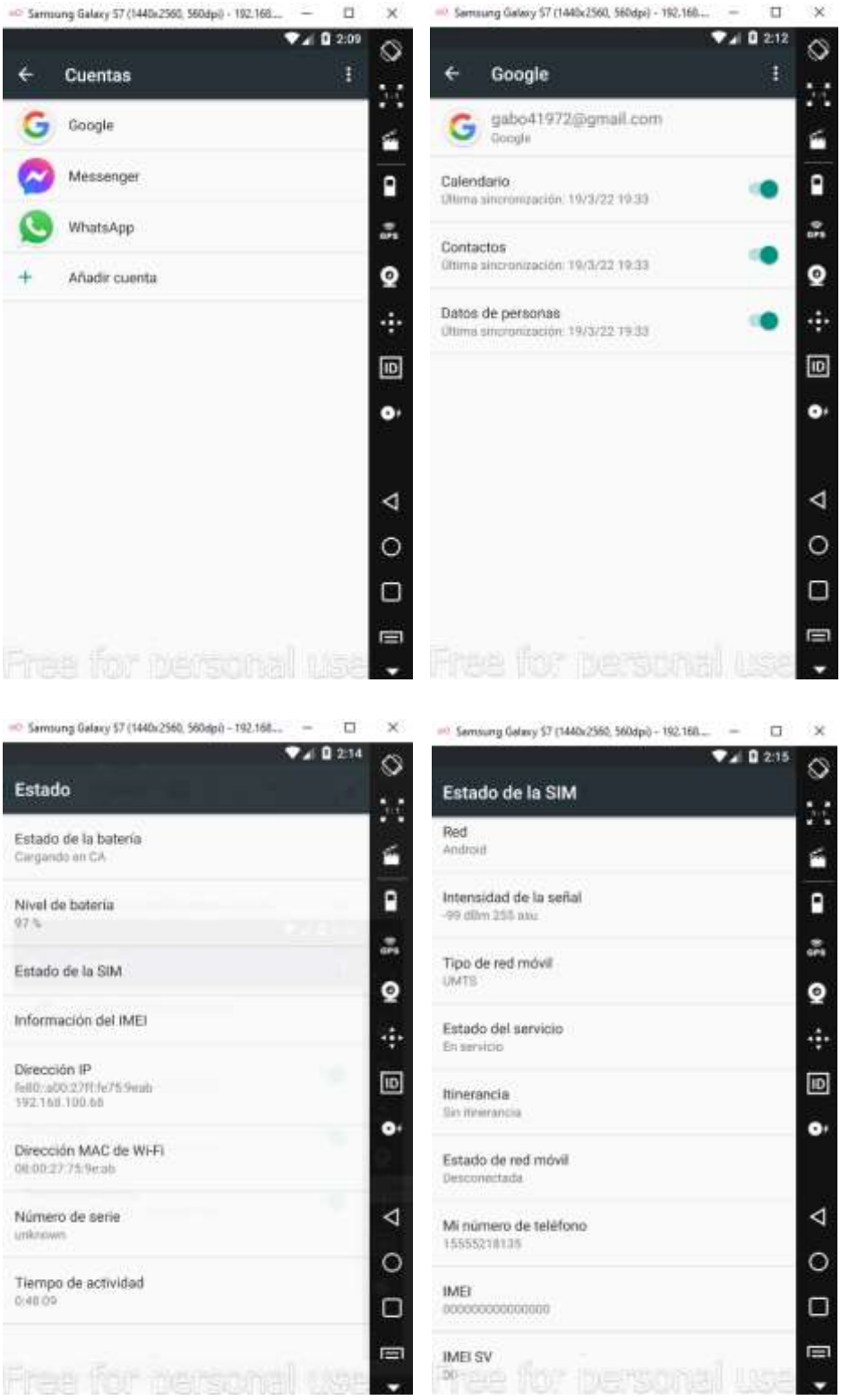
Fuente: elaboración propia

Una vez generada los *hashes,* se realiza las copias necesarias de la imagen forense para su posterior análisis con las herramientas adecuadas existentes.

Escenario con simuladores

Similarmente como, se realiza las actividades para el equipo real, se procede con las tareas para equipo emulado. Se procedió con la extracción manual de los datos, ver en la figura 25.

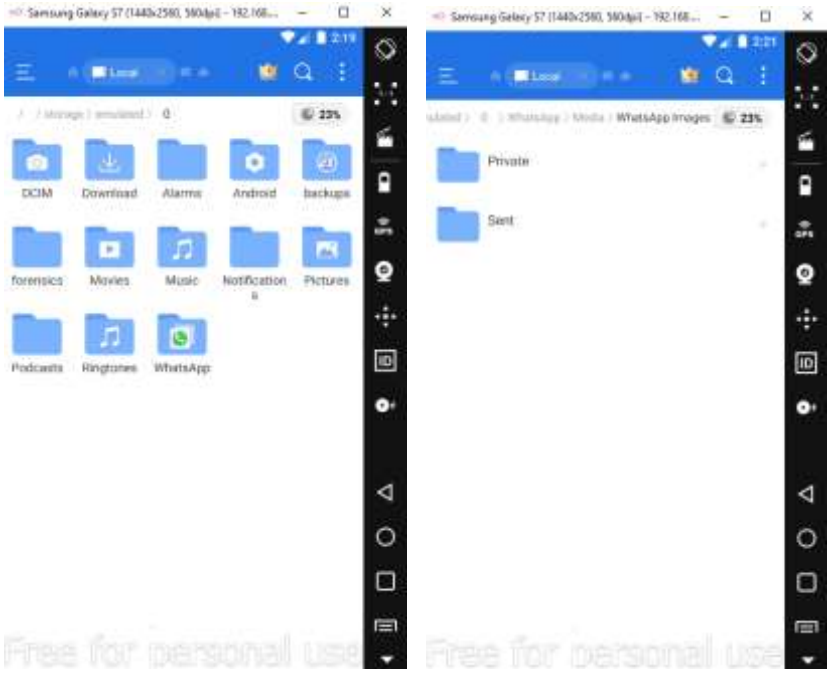
Figura 25. Extracción manual equipo emulado



Fuente: elaboración propia

Con un explorador de archivos, se obtiene información del dispositivo de una manera más fácil como, se ve en la figura 26.

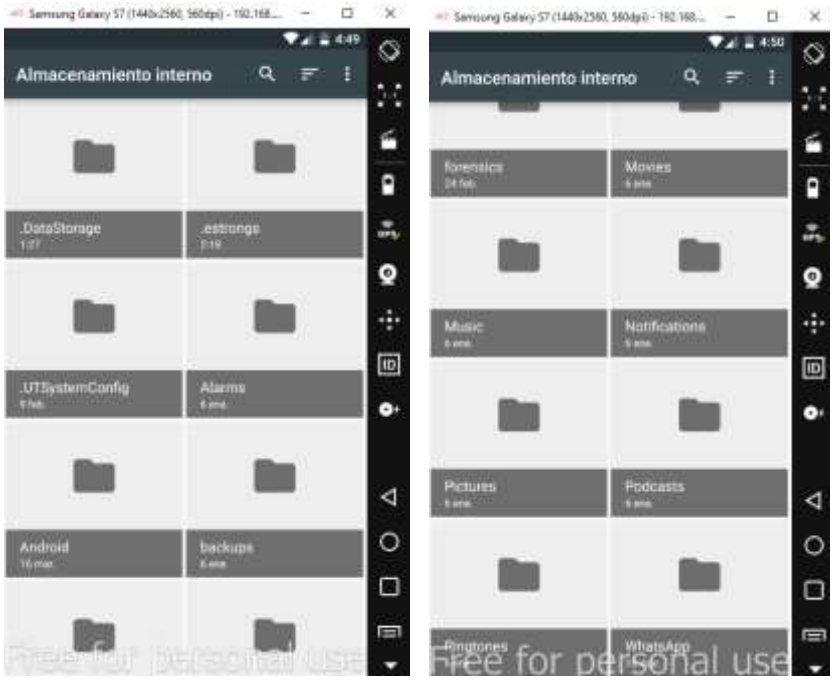
Figura 26. Explorador de archivos en equipo emulado



Fuente: elaboración propia

Al utilizar el protocolo MTP ya mencionado en el escenario con el equipo real y el cumplimiento de los prerrequisitos, se procedió a extraer información de la ubicación lógica del dispositivo ver figura 27.

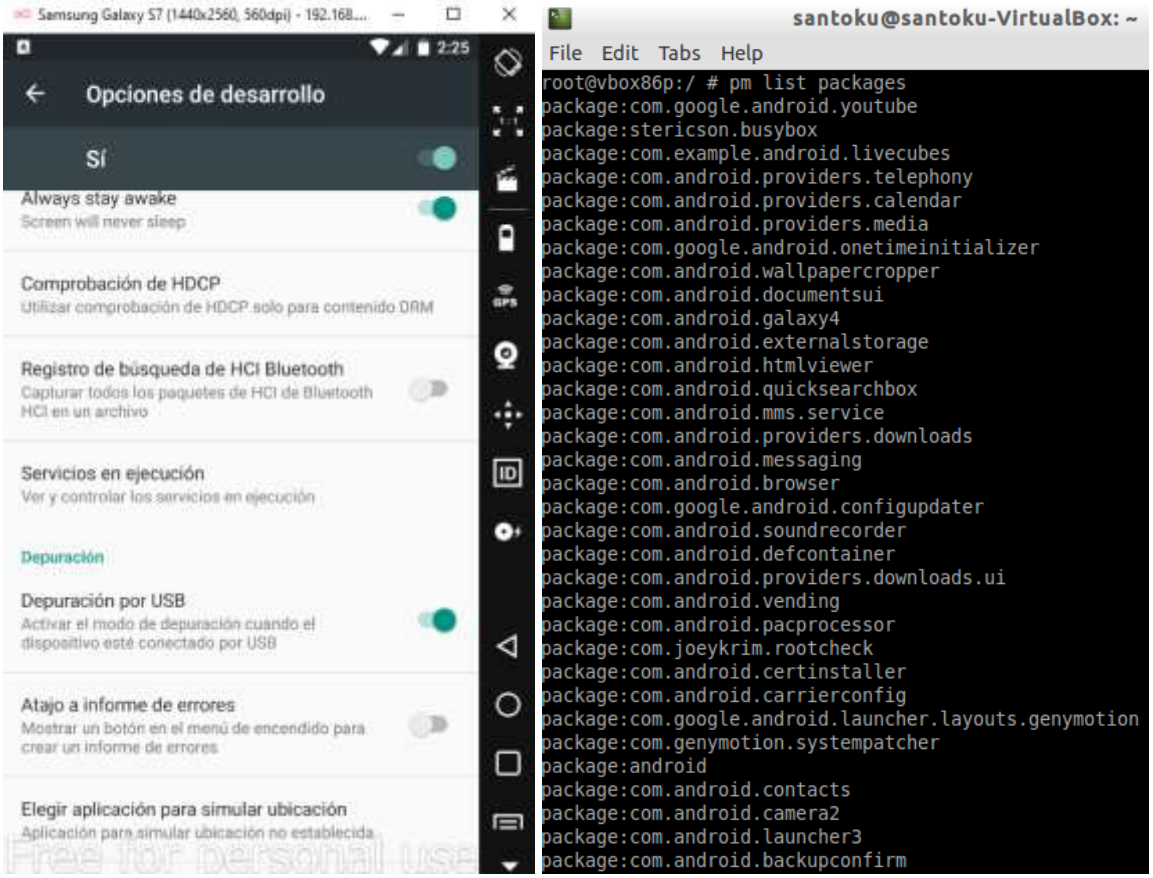
Figura 27. Acceso al dispositivo móvil emulado mediante MTP



Fuente: elaboración propia

A continuar con la extracción lógica de la información del dispositivo móvil para acceder a datos inaccesible por el protocolo MTP, se realiza mediante el ADB ya mencionado en la extracción del equipo real ver figura 28.

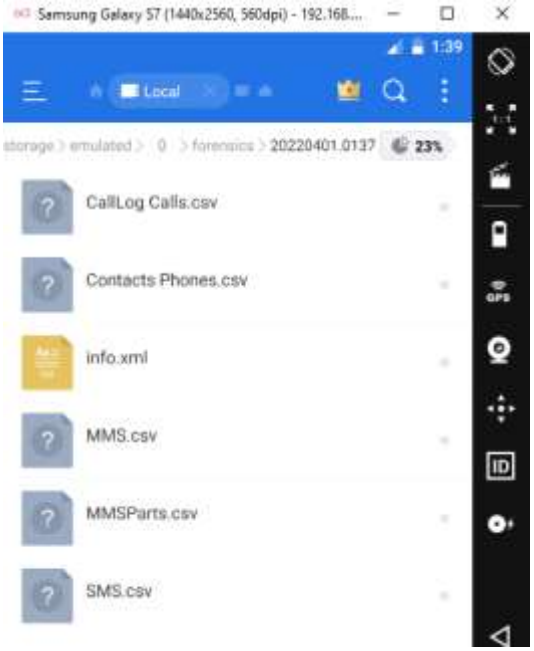
Figura 28. Paquetes instalados en el dispositivo emulado y modo de depuración



Fuente: elaboración propia

Adicionalmente, se obtiene más información lógica del dispositivo móvil mediante AFLogical de manera similar realizada en el equipo real ver figura 29.

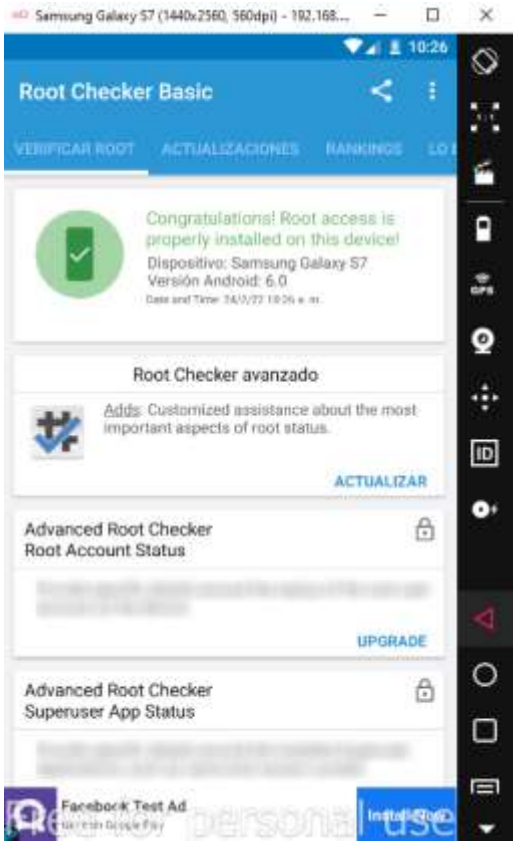
Figura 29. Información obtenida mediante AFLogical en el dispositivo emulado



Fuente: elaboración propia

Para ejecutar la extracción física, se va a realizar mediante DD, a través del sistema operativo Santoku con el mismo proceso que, se realizó con el equipo real previo al cumplimiento de los prerrequisitos ver figura 30.

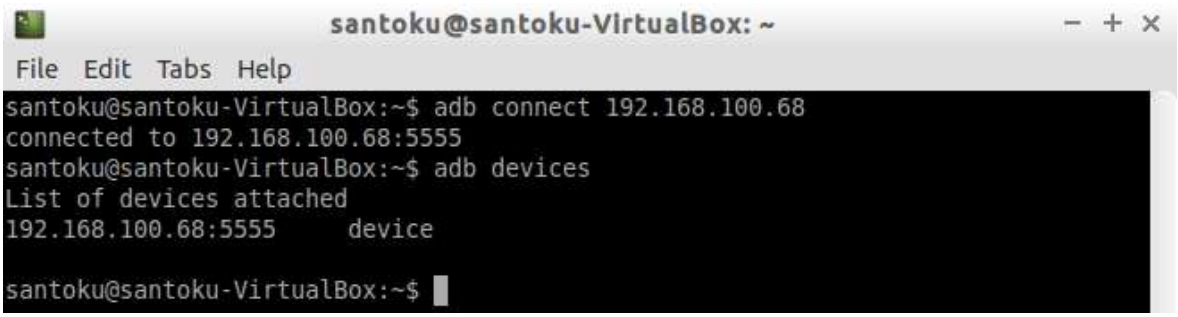
Figura 30. Permisos de root para el dispositivo emulado



Fuente: elaboración propia

Para realizar una imagen forense, se conecta el móvil mediante red, se abre la terminal y, se lanza el comando *adb devices* para verificar que, hay comunicación con el móvil, ver figura 31.

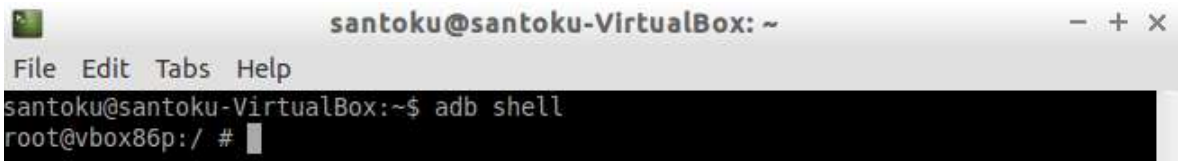
Figura 31. Revisión de dispositivo emulado conectado



Fuente: elaboración propia

Al tener la conexión con el dispositivo móvil, se realiza la ejecución del comando *adb Shell* para acceder a la Shell del equipo ver figura 32.

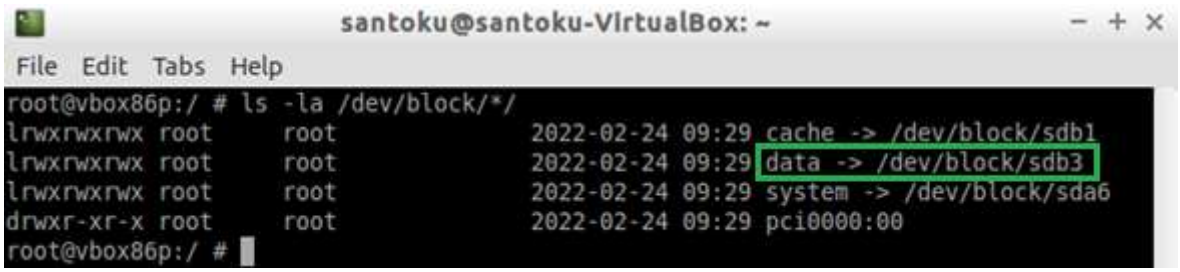
Figura 32. Ejecución del comando adb Shell del equipo emulado



Fuente: elaboración propia

Para identificar la partición a realizar la imagen forense, la cual, contiene toda la información relevante del dispositivo móvil, se utiliza el comando: ls -la /dev/block/*/, ver figura 33.

Figura 33. Partición a realizar imagen forense del equipo emulado



Fuente: elaboración propia

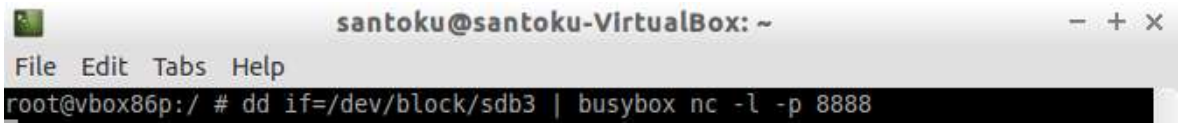
Para realizar la comunicación entre el equipo y el dispositivo móvil, en este último una vez instalado el *netcat,* se ejecutó el comando para reenvío de puertos, ver figura 34.

Figura 34. Reenvío de puertos equipo emulado

Fuente: elaboración propia

Una vez identificado la partición que contiene información importante para el caso de estudio, se procedió a crear la imagen forense del dispositivo móvil, ver figura 35.

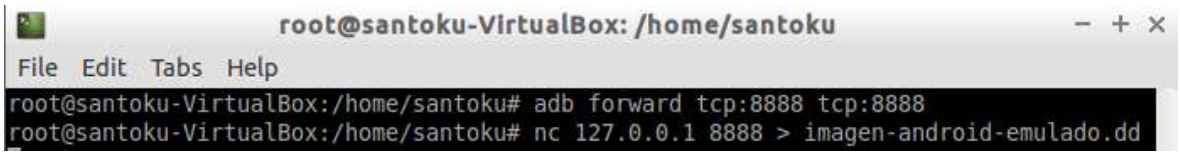
Figura 35. Creación de imagen forense equipo emulado



Fuente: elaboración propia

Para copiar la imagen forense hacia un equipo externo, se inició una conexión mediante *netcat* hacia el equipo en donde, se guardará, ver figura 36.

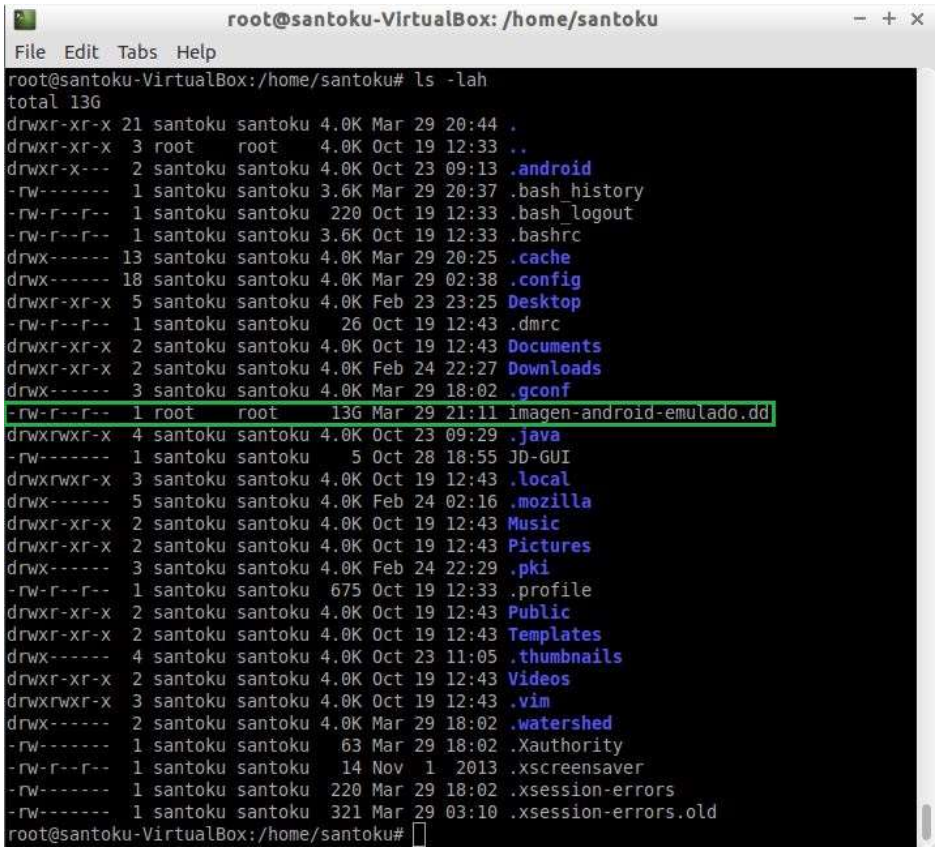
Figura 36. Comando para guardar imagen en equipo externo



Fuente: elaboración propia

Al final, se obtiene la imagen forense creada como, se ve en la figura 37.

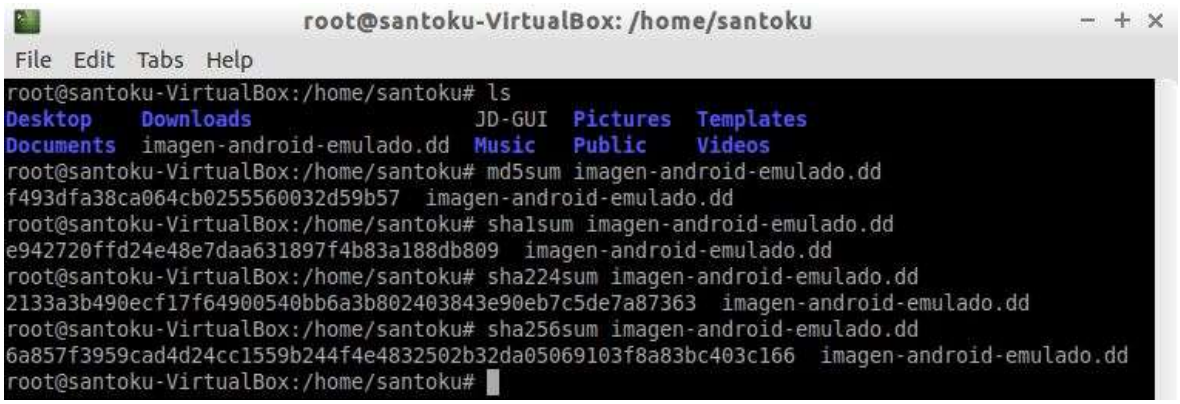
Figura 37. Ruta de creación de imagen forense equipo emulado



Fuente: elaboración propia

Con el objetivo de garantizar la integridad de la imagen forense, se obtuvo los *hashes* (md5, sha1, sha224, sha256), ver figura 38.

Figura 38. Validación de integridad de la imagen forense equipo emulado



Fuente: elaboración propia

Una vez obtenido los hashes de la imagen forense, se realiza una copia y empezar a realizar el análisis con las herramientas existentes para el caso.

Hallazgos encontrados en los escenarios propuestos

Para los escenarios propuestos: extracción de información en equipo real y extracción en equipo emulado con las diferentes herramientas *open-source* mencionadas en capítulos anteriores, se pudo evidenciar que es posible en los dos escenarios utilizar la mayoría de las herramientas, ver tabla 4.

Tabla 4. Herramientas utilizadas en equipo real y emulado

Herramienta Forense	Equipo Real	Equipo Emulado
Extracción Manual		
ES File Explorer	SI	SI
Extracción Lógica		
MTP	SI	SI
ADB	SI	SI
AFLogical	SI	SI
Andriller	SI	NO
Extracción Física		
DD	SI	SI

Fuente: elaboración propia

En la extracción de información del equipo emulado mediante el software Andriller fue imposible realizar esa actividad, debido a que uno de los requisitos es tener una conexión a través del cable USB entre en dispositivo móvil y el equipo dónde, se ejecuta la herramienta.

Para realizar la extracción de información en su totalidad con las herramientas ya citadas es necesario que el equipo sea rooteado, para así explorar en el dispositivo con privilegios de *root*. Además, se pudo identificar que para los dispositivos analizados no influye si, se utiliza el cable USB original o genérico, se obtiene los mismos resultados y en el mismo tiempo.

CAPÍTULO III. EVALUACIÓN Y ANÁLISIS DE RESULTADOS

3.1. Comparación de resultados obtenidos en los escenarios

De la extracción de datos realizados en el equipo real y en el equipo emulado mediante métodos manuales, lógicos y físicos; cada una con sus respectivas herramientas/software y con el cumplimiento de los requisitos necesarios para su correcto funcionamiento, se logró extraer información interesante que tranquilamente sirve en la investigación de un caso, ver tabla 5.

Tabla 5. Datos extraídos del equipo real y emulado

Herramienta Forense	Datos Extraídos Equipo Real	Datos Extraídos Equipo Emulado
Extracción Manual		
ES File Explorer	Mensajes SMS y chat, cuentas de Gmail y redes sociales. Información a detalle sobre el dispositivo móvil (sistema operativo, marca, modelo, serial), información de las conexiones Wifi y de Bluetooth, detalle de la tarjeta SIM, número IMEI, operadora de red, serial SIM, tiempo de actividad del dispositivo, tipo de red móvil	Cuentas de Gmail y redes sociales. Información a detalle sobre el dispositivo móvil (sistema operativo, marca, modelo), información de las conexiones Wifi, tiempo de actividad del dispositivo
Extracción Lógica		
MTP	Información almacenada en la memoria interna y tarjeta SD	Información almacenada en la memoria interna
ADB	Aplicaciones instaladas en la memoria interna y externa	Aplicaciones instaladas en la memoria interna
AFLogical	Registros de llamadas, contactos telefónicos, mensajes multimedia, mensajes SMS, archivo con todas las características del móvil	Registros de llamadas, contactos telefónicos, archivo con todas las características del móvil
Andriller	Accounts (System), Android Calendar, Call Logs, Download History, Facebook Messenger, REPORT, Samsung Call Logs, Shared Storage, SMS Messages, WhatsApp Calls, WhatsApp Contacts, Wi-Fi Passwords, WhatsApp Messages, backup	No es posible aplicar esta herramienta sin tener conexión por USB
Extracción Física		
DD	Imagen forense de la partición /dev/block/mmcblk0 y /dev/block/mmcblk1	Imagen forense del dispositivo móvil de la partición /dev/block/sdb3

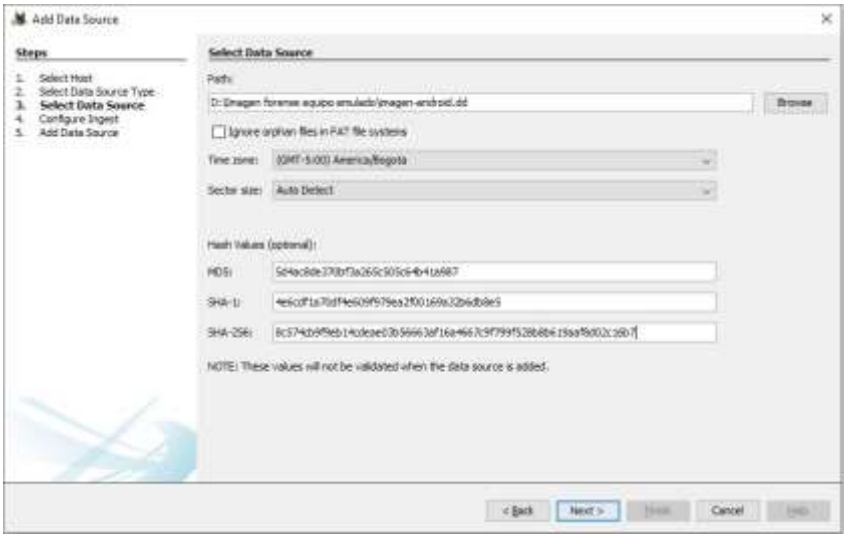
Fuente: elaboración propia

En la extracción física para visualizar el contenido de la imagen forense del dispositivo móvil real y el emulado, se necesita de herramientas de análisis forense, para el presente caso, se va a utilizar el Autopsy.

Análisis de la imagen forense del dispositivo real

Para realizar el análisis de la imagen forense primeramente, se monta la imagen forense en la herramienta Autopsy, ver figura 39.

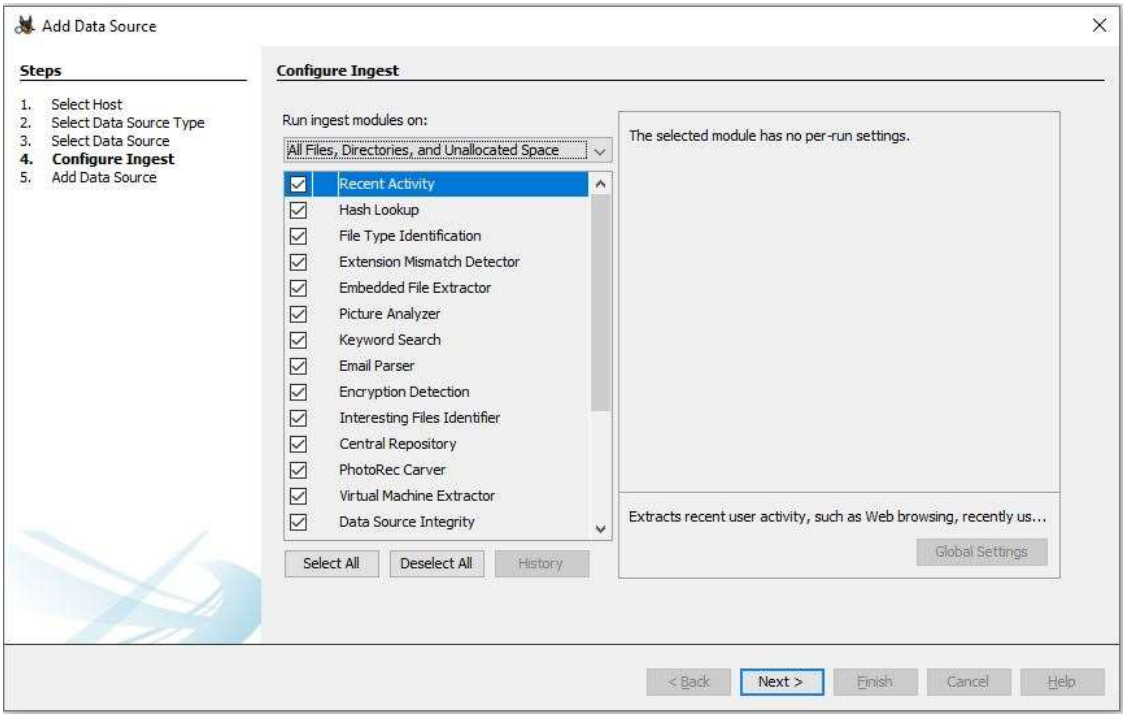
Figura 39. Carga de imagen forense equipo real



Fuente: elaboración propia

Una vez cargado la copia forense, se procedió con la configuración de los módulos necesarios para realizar el análisis forense con Autopsy, ver figura 40.

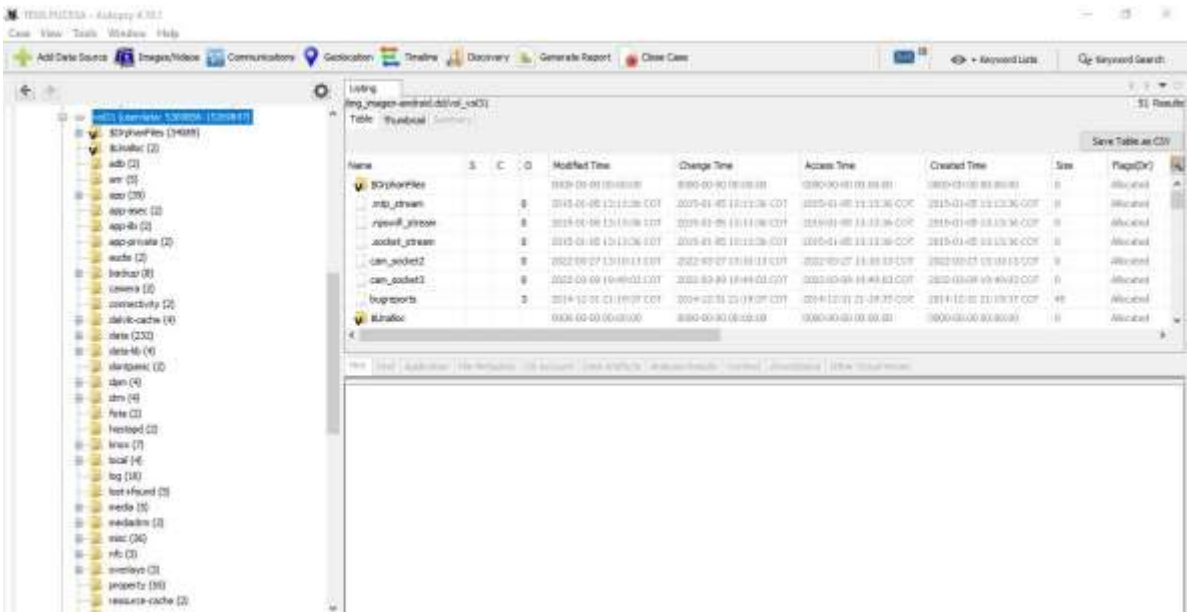
Figura 40. Configuración de módulos imagen forense equipo real



Fuente: elaboración propia

Luego de seleccionar los módulos empezó a cargar los datos, los cuales, una vez terminado el proceso, se visualizó en la herramienta, ver figura 41. Con la imagen forense ya cargada y procesada, se inicia el análisis a fin de encontrar información relevante que aporte en la investigación de algún caso.

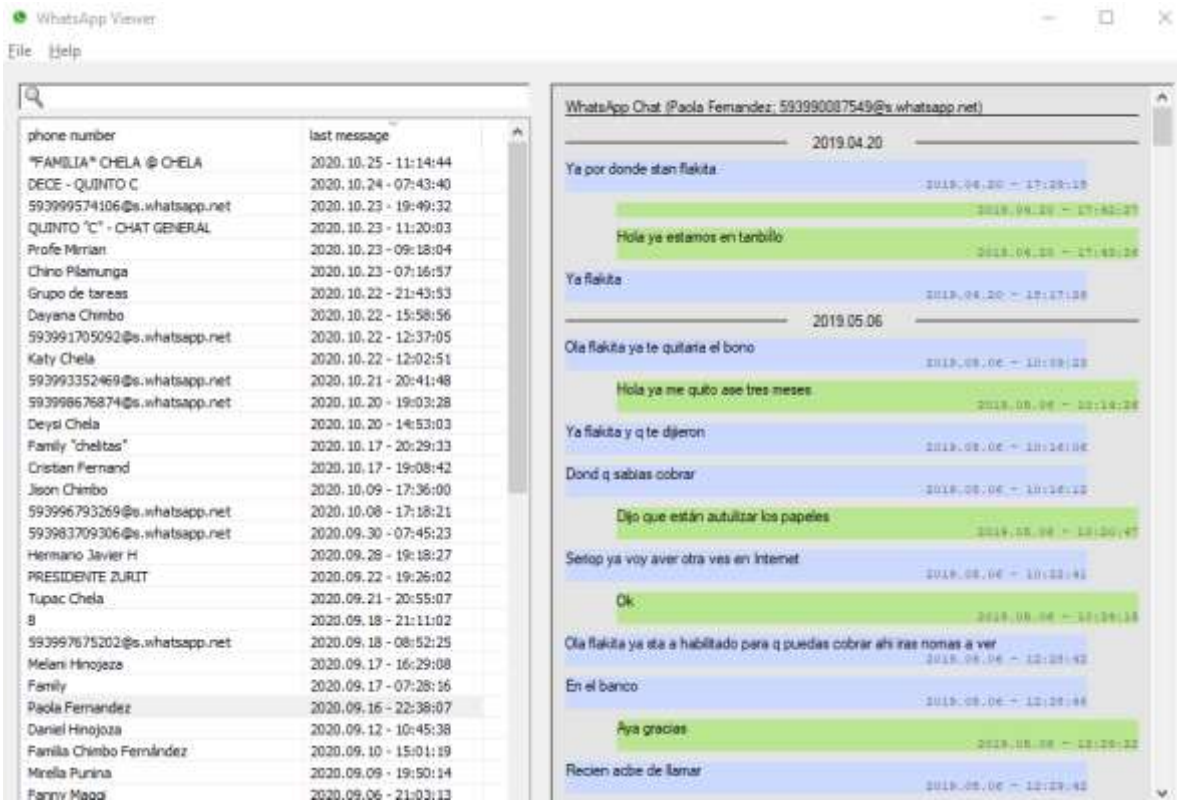
Figura 41. Visualización información imagen forense equipo real



Fuente: elaboración propia

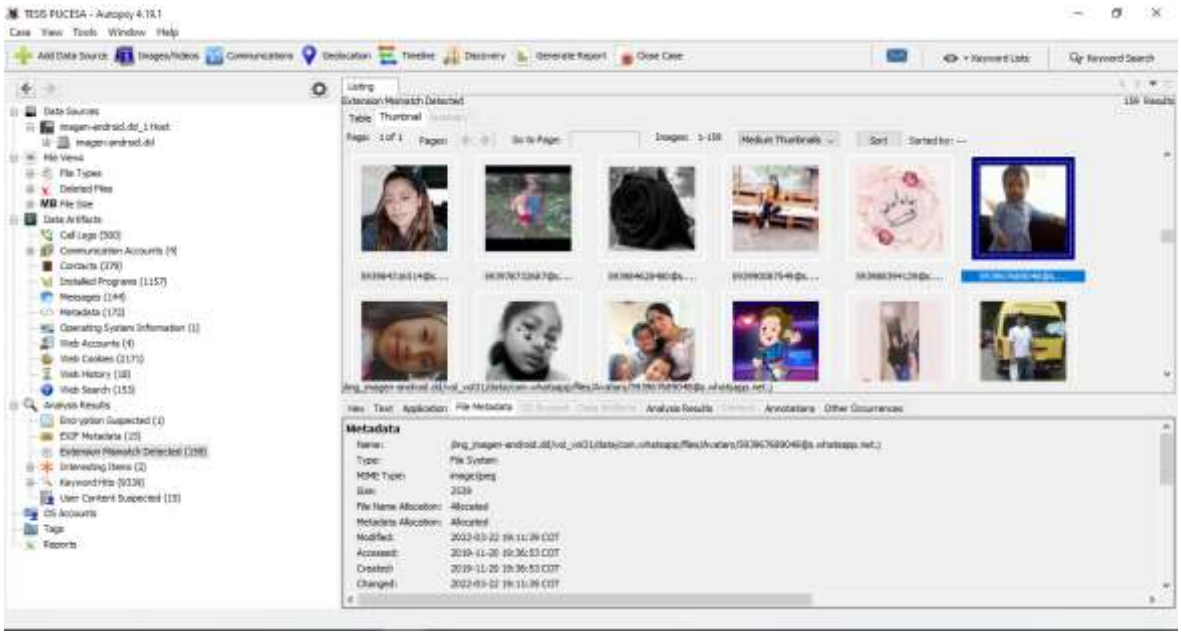
Al tener la información de la imagen forense en la herramienta Autopsy, se obtiene acceso a la base de datos del aplicativo *WhatsApp* y mediante el software *WhatsApp Viewer* visualizar las posibles conversaciones que tuvo el propietario, ver figura 42. Además, se obtiene fotografías, logs de llamadas, contactos del teléfono, mensajes SMS, chats de *Facebook Messenger*, programas instalados, información del sistema operativo, *web accounts, web cookies, web history, web search, email addresses, communications accounts,* metadatos, archivos almacenados, archivos borrados, entre otros, ver figura 43, 44, 45 y 46.

Figura 42. Mensajes WhatsApp del equipo real



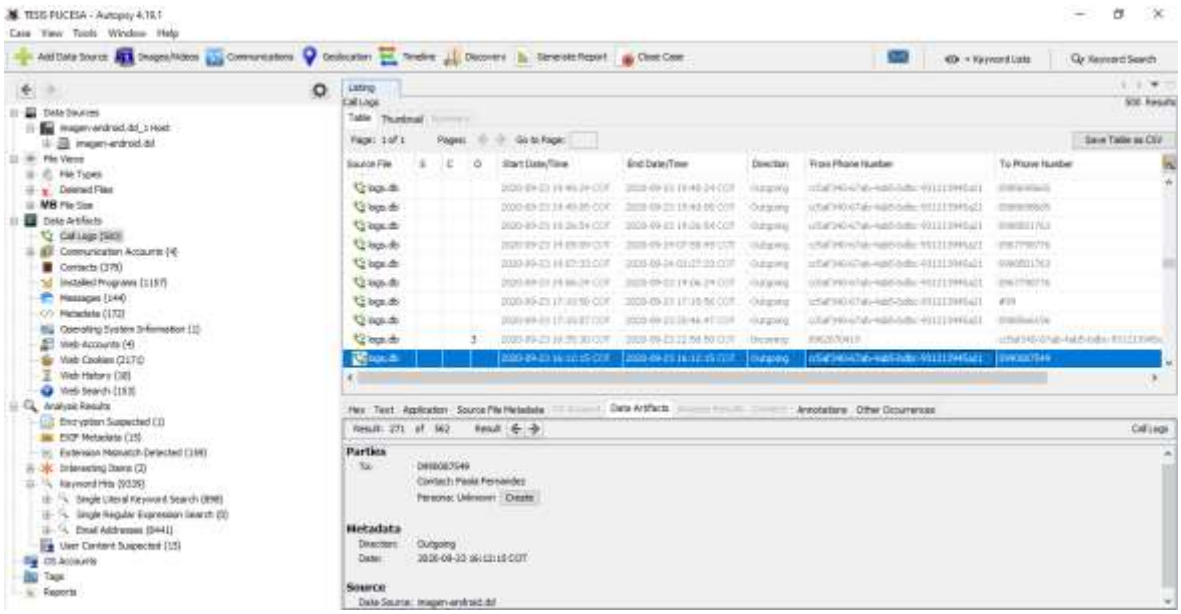
Fuente: elaboración propia

Figura 43. Fotografías almacenadas en el dispositivo real



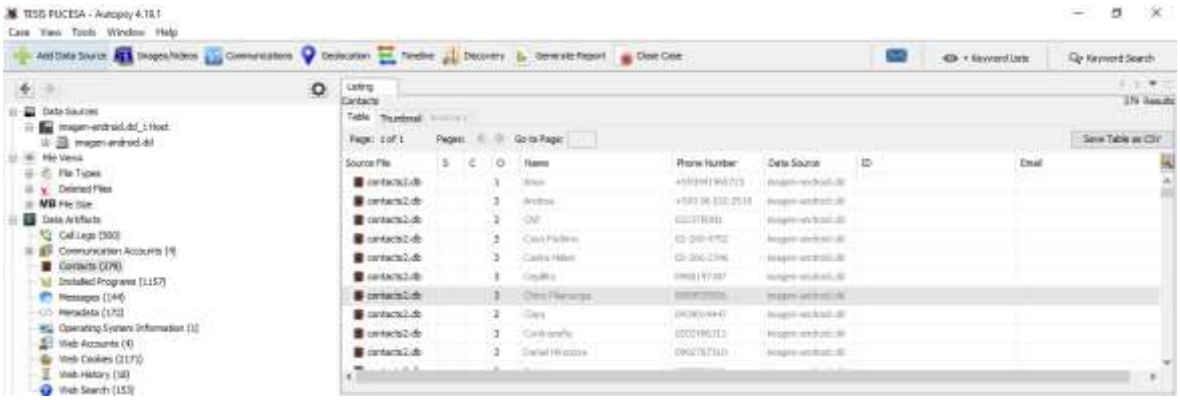
Fuente: elaboración propia

Figura 44. Logs de llamadas del dispositivo real



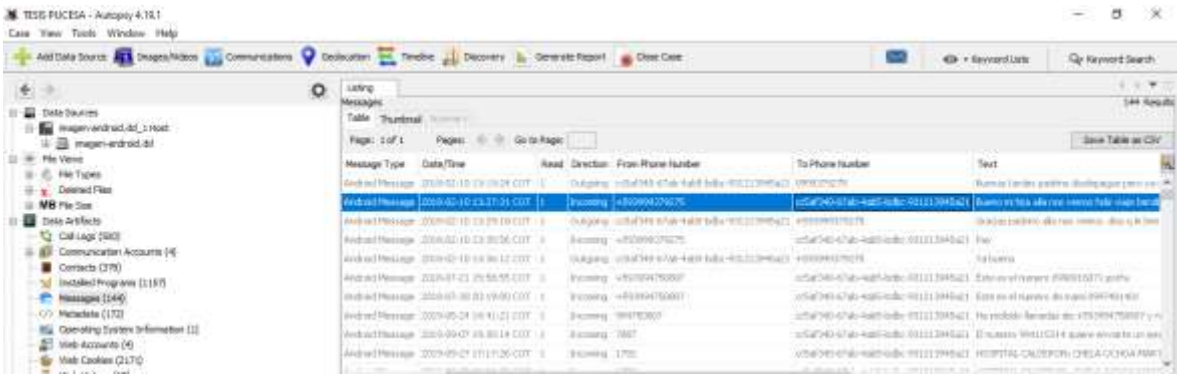
Fuente: elaboración propia

Figura 45. Contactos almacenados en el dispositivo



Fuente: elaboración propia

Figura 46. Mensajes SMS



Fuente: elaboración propia

3.2. Análisis de resultados de la prueba de concepto

Para obtener información necesaria que sirva como evidencia en la investigación de algún caso relacionado con dispositivos móviles, es necesario realizar la extracción a través de la aplicación de cada tipo de método ya mencionado con sus respectivas herramientas. La información que, se pudo extraer varía según las facilidades que provee cada una de las herramientas, pero que luego de realizar la extracción con todas, se consolida tener toda la información completa del dispositivo. Por otra parte, para visualizar la información recopilada no, se necesita de algún software de análisis extra.

Mientras que al extraer la información del dispositivo móvil con el método físico realiza una imagen forense del almacenamiento interno y externo; es posible tener toda la información consolidada en uno solo. Además, para visualizar la información extraída del móvil, se necesita de un software de análisis de la imagen forense, para este caso, se utilizó el Autopsy.

La utilización de uno u otro método con su herramienta depende del investigador forense, del tipo de caso y de que información necesite extraer del dispositivo móvil en una investigación.

3.3. Informe de los resultados obtenidos

Con la información recopilada tanto del dispositivo móvil real como del dispositivo móvil emulado, se realiza un informe forense que contiene datos relevantes encontrados en la investigación que, se hay realizado, ver anexo 1 y anexo 2. Para este caso, se va a utilizar el formato de informe pericial proporcionado por el Consejo de la Judicatura, ver anexo 3, de acuerdo a lo mencionado en el Reglamento del Sistema Pericial Integral de la Función Judicial detallados en los artículos 19 y 20.

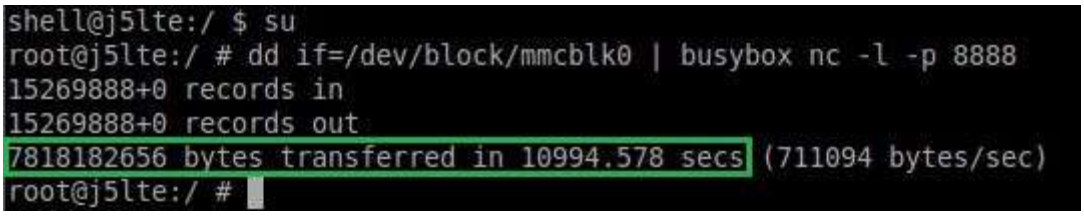
3.4 Demostración de hipótesis

Para saber la eficiencia de las actividades realizadas y respuesta de las herramientas utilizadas en la extracción de datos, para este proyecto, se los controló a través de los indicadores de desempeño (KPI). En este caso los indicadores de desempeño que, se utilizó son: el tiempo que tarda en hacer la imagen forense, el tiempo que tarda en calcular el hash de la imagen forense, velocidad de transferencia de datos, el tiempo que tarda en cargar la imagen forense en el Autopsy.

Según lo expuesto, a continuación, se presenta cada indicador de desempeño con su valor:

- El tiempo que tarda en hacer la imagen forense en la herramienta Santoku fue 183 minutos, ver figura 47.

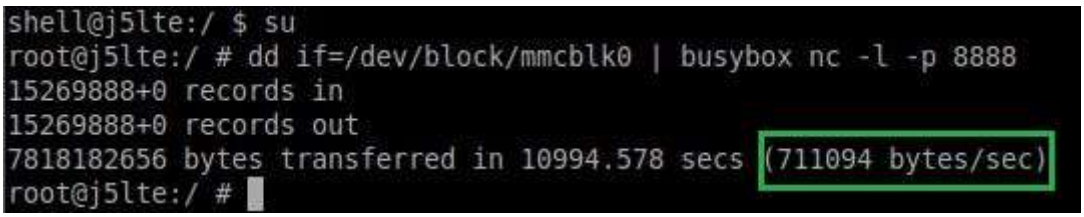
Figura 47. Tiempo para realizar imagen forense



Fuente: elaboración propia

- La velocidad de transferencia de los datos de la imagen forense hacia el equipo donde, se va almacenar fue de 711094 bytes/sec, ver figura 42.

Figura 48. Velocidad de transferencia de datos



Fuente: elaboración propia

- El tiempo que tarda en calcular el *hash* (md5, sha1, sha224, sha256) de la imagen forense fue 5 minutos.
- El tiempo que tarda en cargar la imagen forense en el Autopsy para ya tener la información lista para ser analizada fue de 120 minutos.

Los KPI mencionados variaran de acuerdo a la cantidad de información que tenga almacenado el dispositivo móvil y a la capacidad de almacenamiento.

Mediante la utilización de las herramientas/software *open-source* cada una con su tipo de extracción y herramientas para análisis forense de imágenes forenses, se obtuvo información interesante del dispositivo móvil analizado que es utilizado para

esclarecer algún delito informático. De acuerdo a lo mencionado, se comprueba que es posible extraer información importante con herramientas open-source en dispositivos móviles con sistema operativo Android, el cual, es utilizado por el perito informático en la investigación de algún caso.

Nota de Descargo de Procedimientos: Esta tesis fue realizada únicamente para fines educativos y de investigación, bajo ningún concepto para obtener información de forma no ética y sin las debidas autorizaciones.

CONCLUSIONES

- La documentación del estado del arte para el análisis informático forense en dispositivos con la utilización de software libre, permitió la conformación de la base teórica identificada de los tipos de extracción de datos en dispositivos móviles con sistema operativo Android tuvo un gran aporte para el desarrollo de la prueba de concepto planteado, se logró extraer de una manera eficaz y eficiente la información mediante herramientas open-source en los escenarios tanto con equipo real como con el emulado.

- El análisis del proceso existente aplicable al ámbito forense en dispositivos móviles según la normativa ecuatoriana de software libre, confirma la validez de los tipos de extracción de información en dispositivos móviles aplicable según las normativas ecuatorianas vigentes, se evidencia a través del estudio del Código Integral Penal (COIP), Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Reglamento del Sistema Pericial Integral de la Función Judicial, necesarios para este tipo de procedimientos.

- La identificación de los KPI técnicos más importantes, para la comparación de las herramientas de extracción de información a ejecutarse en las pruebas de concepto, evidencia los indicadores de desempeño (KPI), y permite conocer aspectos importantes en la extracción física de información de un dispositivo móvil como: el tiempo que tarda en realizar la imagen forense, el tiempo que tarda en calcular el hash de la imagen forense, velocidad de transferencia de datos hacia la ruta de almacenamiento, el tiempo que tarda en cargar la imagen forense en la herramienta de análisis forense autopsy.

- Con el diseño de las pruebas de concepto en entorno real y simulado sobre extracción de información en dispositivos móviles usando software libre, se concluye que la ejecución de la prueba de concepto para extraer información con herramientas de software libre tanto en el escenario con el dispositivo móvil real y con el dispositivo móvil emulado permitió obtener información relevante que aporta en la investigación de algún caso, así como, también, saber qué

herramienta utilizar de acuerdo al tipo de extracción que esté en ejecución y, con esta herramienta, qué datos, se adquiere.

- La consolidación de la información recopilada en un informe pericial de acuerdo con lo establecido en los artículos 19 y 20 del REGLAMENTO QUE REGULA EL SISTEMA PERICIAL INTEGRAL DE LA FUNCIÓN JUDICIAL, ratificó que sí es posible extraer información necesaria e importante de un dispositivo móvil con sistema operativo Android mediante la utilización de herramientas *open-source*, y esta información es utilizado por el perito informático para argumentar algún caso relacionado con delitos informáticos de dispositivos móviles.

- Es posible concluir que la extracción de información mediante las herramientas ADB, AFlogical, Andriller y DD, se realiza previa activación del modo de depuración en el dispositivo móvil, caso contrario no es posible acceder.

- La extracción de información con herramientas *open-source* requiere que el dispositivo móvil, se encuentre desbloqueado, a excepción del ADB y DD que requieren que tenga el modo de depuración activado y, además, el equipo este roteado. Para el caso que el equipo móvil, se encuentre cifrado la imagen forense realizada es necesario descifrarlo con software adicionales. Existen algunas herramientas comerciales como Encase Forensics que permiten desencriptar imágenes forenses encriptadas mediante el Passware Kit Forensic, así, también, el MOBILedit Forensic que permiten realizar el desbloqueo de equipos y de esta manera evadir las protecciones.

RECOMENDACIONES

- Para extraer la información del dispositivo móvil, se realiza con privilegios de super usuario, en este caso con permisos de *root*, a fin de explorar, acceder a cualquier directorio sin restricción y así obtener todos los datos en su totalidad. Además, para la herramienta ADB, AFlogical y DD es necesario que este activado el modo de depuración.

- Realizar el estudio teórico practico para extraer información de dispositivos móviles que tengan sistemas operativos diferentes a Android, mediante herramientas de software libre, y así proseguir con aportes a los peritos informáticos en la ejecución de sus investigaciones forenses.

- Continuar la investigación de métodos para la extracción de información en dispositivo móviles con sistema operativo Android que tengan diferentes versiones a las realizadas en este proyecto de desarrollo.

- Realizar estudios de herramientas de software libre que permitan extraer información en dispositivo móviles que estén dañados o hayan sufrido algún golpe que ocasionó su daño físico, pero que su chip de almacenamiento de datos interno está en perfecto estado.

- Desarrollar herramientas de software libre que permitan realizar todo el proceso que engloba un análisis forense en dispositivos móviles con sistema operativo Android y, además, emita un informe acorde a las normativas vigentes en el país.

- Investigar herramientas de software libre que permitan realizar la extracción de información en dispositivos que, se encuentren bloqueados y que sus unidades de almacenamiento estén cifradas.

BIBLIOGRAFÍA

Aji, M. P., Hariyadi, D., & Rochmadi, T. (2020). *Logical Acquisition in the Forensic Investigation Process of Android Smartphones based on Agent using Open Source Software.*IOP Conference Series: Materials Science and Engineering,771(1),012024.https://doi.org/10.1088/1757-899X/771/1/012024

Álvarez Murillo, M. (2016). *Análisis forense en dispositivos móviles iOS y Android.*

Andrade-Salinas, G., Salazar-Chacon, G., & Vintimilla, L.-M. (2019). *Integration of IoT Equipment as Transactional Endorsing Peers over a Hyperledger-Fabric Blockchain Network*: Feasibility Study. International Conference on Applied Technologies, 95-109.

Araujo-Costa-Silva, L. (2019). *Herramientas de análisis forense para android*.

Autopsy | Digital Forensics. (s. f.). *Autopsy*. Recuperado 17 de septiembre de 2022, de https://www.autopsy.com/

Ayers, R., Brothers, S., & Jansen, W. (2014). *Guidelines on mobile device forensics* (NIST SP 800-101r1; p. NIST SP 800-101r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-101r1

Barmpatsalou, K., Cruz, T., Monteiro, E., & Simoes, P. (2018). *Mobile Forensic Data Analysis*: Suspicious Pattern Detection in Mobile Evidence. IEEE Access, 6, 59705-59727. https://doi.org/10.1109/ACCESS.2018.2875068

Cajías, P. (2018). *Metodología de análisis forense para dispositivos móviles alineado a leyes del Ecuador*. 103.

Calderón, F. A. C., & Martínez, M. R. A. (2020). *Guía integral de empleo de la informática forense en el proceso penal de Ecuador*. Universidad y Sociedad, 12(S (1)), 182-190.

Chaves, M. A. (s. f.). *Panorama general de la Informática Forense y de los delitos informáticos en Costa Rica*. . . ISSN, 15.

Código Orgánico Integral Penal, COIP. (2021). *Código Orgánico Integral Penal*, COIP. https://www.defensa.gob.ec/wp-conte nt/up load s/do wnlo ads/ 2021 /03/COIP_act_feb-2021.pdf

Computer Security Division, I. T. L. (2016, junio 8). *Mobile Forensics—Mobile Security and Forensics* | CSRC | CSRC. CSRC | NIST. https://csrc.nist.gov/projects/mobile-security-and-forensics/mobile-forensics

Cristian, P.-C., Hernan, T.-C., Rene, G.-Q., Francisco, A.-P., & Cristian, N.-G. (2020). *Methodologies and Forensic Analysis Tools on Android Mobile Devices*: A Systematic Literature Review. 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), 1-7. https:// doi.org /10.23 919/CISTI49556.2020.9140852

Di Iorio, A. H., Castellote, M. A., Constanzo, B., Curti, H., Waimann, J., Lamperti, S. B., Giaccaglia, M. F., Cistoldi, P. A., Podestá, A., & Iturriaga, J. I. (2017). *El rastro digital del delito*: Aspectos técnicos, legales y estratégicos de la informática forense.

Díaz Muñoz, D. S. (2015). *Análisis forense desde una perspectiva práctica*. Universidad Piloto de Colombia.

Fénnema, M. C., Figueroa, L. M., Viaña, G., Lesca, N., & Lara, C. (2017). *Trat ami ento de evidencias digitales forenses en dispositivos móviles*. XIX Workshop

de Investigadores en Ciencias de la Computación (WICC 2017, ITBA, Buenos Aires).

Figueroa, L. M., Lara, C., Lesca, N., Viaña, G., & Binda, A. (2018). *Tratamiento de evidencias digitales forenses en dispositivos móviles*. XX Workshop de Investigadores en Ciencias de la Computación (WICC 2018, Universidad Nacional del Nordeste).

Gómez, D. A. M., & Bejarano, M. H. (2020). *Análisis forense para Móviles*. Revista Avenir, 4(2), 1-8.

Gómez, E., Herrera, N., Moscoso, O., & Guaman, P. (s. f.). *Propuesta de Análisis Forense para Dispostivos Móviles con Sistema Operativo Android*.

Hachem, M., Sharma, B. K., El Naggar, A., Pilankar, I., & Anwar, N. (2020). *Systematic Approaches For Soil Analysis in Forensic Investigation*. 2020 Advances in Science and Engineering Technology International Conferences (ASET), 1-5. https://doi.org/10.1109/ASET48392.2020.9118299

Hernández, R. S., Ramírez, W. L., Piña, D. L., & Jasso, C. P. (2018). *Laboratorio didáctico del análisis forense en dispositivos móviles*. Actas de las Jornadas Virtuales de Colaboración y Formación Virtual USATIC 2018, Ubicuo y Social: Aprendizaje con TIC, 125.

Investigación forense de dispositivos móviles: Metodología y herramientas. (2020, octubre 21). Redseguridad. https://www.redseguridad.com/especialidades-tic/activos-de-informacion/investigacion-forense-de-dispositivos-moviles-metodologias-y-herramientas_20201021.html

Jadhav, M., & Joshi, K. K. (2016). *Forensic investigation procedure for data acquisition and analysis of Firefox OS based mobile devices*. 2016

International Conference on Computing, Analytics and Security Trends (CAST), 456-461. https://doi.org/10.1109/CAST.2016.7915012

Kruse II, W. G., & Heiser, J. G. (2001). *Computer forensics*: Incident response essentials. Pearson Education.

Ley de Comercio Electrónico, Firmas y Mensajes de Datos. (2002). *Ley de Comercio Electrónico, Firmas y Mensajes de Datos*. https:// www.te lecomu nicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf

Li, S., Sun, Q., & Xu, X. (2018). *Forensic Analysis of Digital Images over Smart Devices and Online Social Networks*. 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 1015-1021. https://doi.org/10.1109/HPCC/SmartCity/DSS.2018.00168

Loarte Cajamarca, B. G. (2018). *Desarrollo de una guía metodológica para el análisis forense digital en equipos de cómputo con sistema operativo mac os x e el ecuador*. http://localhost:8080/xmlui/handle/123456789/2758

López, M. (2007). *Análisis Forense Digital. Universidad Nacional de Educación a Distancia*. Recuperado de http://www. gnu. org/copyleft/fdl. html.

Martínez Ródenas, C. (2020). *Análisis forense en dispositivos móviles: Un caso práctico*.

Martinez, A. (2016, febrero 23). *Herramientas para realizar análisis forenses a dispositivos móviles*. Incibe-cert. https://www.incibe-ce rt. es / /herramientas-forense-moviles

Mendillo, V. (2018). *Análisis forense de dispositivos móviles*. XX Workshop de Investigadores en Ciencias de la Computación (WICC 2018, Universidad Nacional del Nordeste).

Moreno, J., Leguias, I., & Vargas-Lombardo, M. (2018). *Revisión sobre la forensía digital en dispositivos móvil con sistemas operativos Android*. I+ D Tecnológico, 14(2), 74-83.

Mushcab, R. A., & Gladyshev, P. (2015). *Forensic analysis of instagram and path on an iPhone 5s mobile device*. 2015 IEEE Symposium on Computers and Communication (ISCC), 146-151. https://doi. org/10.110 9/ISCC.20 15.7405508

Padmanabhan, R., Lobo, K., Ghelani, M., Sujan, D., & Shirole, M. (2016). *Comparative analysis of commercial and open source mobile device forensic tools*. 2016 Ninth International Conference on Contemporary Computing (IC3), 1-6. https://doi.org/10.1109/IC3.2016.7880238

Palacios, G., Nicolás, P., Colazo, D., José, Ing, M., Solinas, M., & Angel. (2020). *Prototipo de aplicación para extracción de información de dispositivos móviles Android para uso forense*.

Parrales, C. A. V., Calle, J. E. C., Castillo, V. A. F., & Pin, J. X. B. (2021). *Aplicación informática forense para el análisis de dispositivos tecnológicos*: UNESUM-Ciencias. Revista Científica Multidisciplinaria. ISSN 2602-8166, 5(4), 9-22. https://doi.org/10.47230/unesum-ciencias.v5.n4.2021.390

Pérez Salvador, J. A. (s. f.). *Elaboración de una metodología para la realización del análisis forense en dispositivos móviles basados en Android*.

Practical Mobile Forensics | Satish Bommisetty, Rohit Tamma, Heather Mahalik | download. (s. f.). Recuperado 1 de diciembre de 2021, de https://b-ok.lat/book/2604505/90bab9?dsource=recommend

Practical Mobile Forensics—Third Edition. (s. f.). Packt. Recuperado 29 de noviembre de 2021, de https://www.packtpub.com/product/practical-mobile-forensics-third-edition/9781788839198

Quintana, M., Uribe, S., Sánchez, F., & Álvarez, F. (2015). *Recommendation techniques in forensic data analysis*: A new approach. 6th International Conference on Imaging for Crime Prevention and Detection (ICDP-15), 1-5. https://doi.org/10.1049/ic.2015.0113

Rahman, R., & Riadi, I. (2019). *Framework Analysis of IDFIF V2 in WhatsApp Investigation Process on Android Smartphones*. International Journal of Cyber-Security and Digital Forensics, 8, 213-222. https://d oi.org/1 0.17781 /P002610

Ramon, P. (2006). *Introducción a la informática forense*.

Reglamento del Sistema Pericial Integral de la Función Judicial. (2014). 16.

Repositorio PUCESA: *Modelo para análisis forense en dispositivos móviles con sistema operativo Android*. (s. f.-b). Recuperado 13 de abril de 2022, de https://repositorio.pucesa.edu.ec/handle/123456789/3293

Riadi, I., Umar, R., & Firdonsyah, A. (2017). *Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method*. International Journal of Computer Science and Information Security, 15, 155-160.

Rico-Bautista, D., & Rueda-Rueda, J. S. (2016). *La informática forense en dispositivos Android*. Revista Ingenio, 9(1), 21-34.

Rivera, P. J. A. (s. f.). *Mobile Digital Forensic Tool using Santoku Linux. 9*.

Rodríguez, Á. M. G., & López, M. C. (s. f.). *Investigación forense, a incidentes en dispositivos móviles. 4*.

Rohit Tamma, O. S., & Heather Mahalik, S. B. (s. f.). *Practical Mobile Forensics Third Edition*. Recuperado 29 de noviembre de 2021, de htt ps ://l ea rning.oreilly.com/library/view/practical-mobile-forensics/978178 8 83 91 98/7c9df1a 4-32c8-44ea-ab82-7bb6dbcc5448.xhtml

Rueda, R. J. S., & Dewar Wilmer Rico, B. (2016). *Defining of a practical model for digital forensic analysis on Android device using a methodology post-mortem*. 2016 8th Euro American Conference on Telematics and Information Systems (EATIS), 1-5. https://doi.org/10.1109/EATIS.2016.7520109

Rueda-Rueda, J. S., Rico-Bautista, D., & Florez-Solano, E. (2019). *Guía práctica abierta para el análisis forense digital en dispositivos Android*. RISTI (Revista Ibérica de Sistemas y Tecnologías de La Información), 18, 442-457.

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

Rueda-Rueda, J., Rico-Bautista, D., & Guerrero, C. (2019). *Open Practice Guide for Digital Forensics on Android Devices*. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao, 442-457.

Saavedra, L. F. C., & Jaime, J. A. B. (2015). *Informática Forense en Colombia*. Ciencia, innovación y tecnología, 2, 83-94.

Soto, É. N. (2020). *Investigación forense de dispositivos móviles*: Metodologías y herramientas. Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones, 90, 58-59.

Soto, É. N. (2021). *Investigación forense de dispositivos móviles: Metodologías y herramientas*. Seguritecnia, 482, 52-54.

Tapia, B., & Washington, K. (2021). *Modelo para análisis forense en dispositivos móviles con sistema operativo Android*. Pontificia Universidad Católica del Ecuador.

Yuliani, V., & Riadi, I. (2019). *Forensic Analysis WhatsApp Mobile Application On Android-Based Smartphones Using National Institute of Standard and Technology (NIST) Framework*. International Journal of Cyber-Security and Digital Forensics, 8, 223-231. https://doi.org/10.17781/P002615

Yunia Pasa, I., & Hariyadi, D. (2020). *Analisis Forensik Untuk Mendeteksi Pesan yang Disembunyikan pada Short Message Service Menggunakan Aplikasi Berlisensi Open Source* | SMARTICS Journal. https://e journal. unikam a.ac.id/index.php/jst/article/view/4703

Zhang, H., Chen, L., & Liu, Q. (2018). *Digital Forensic Analysis of Instant Messaging Applications on Android Smartphones*. 2018 International Conference on Computing, Networking and Communications (ICNC), 647-651. https://doi.org/10.1109/ICCNC.2018.8390330

ANEXOS

Anexo 1. Informe pericial equipo real

Informe pericial

Datos generales:

Empresa contratante: No aplica

Nombre y apellido del perito: Darwin Chimbo

Profesión: Ing. En Electrónica Telecomunicaciones y Redes

Dirección de contacto: E-14 y Jorge Enrique Adoum

Teléfono fijo de contacto: 023662346

Teléfono celular de contacto: 0999574106

Correo electrónico de contacto: drchimbo@pucesa.edu.ec

Antecedentes:

En la ciudad de Quito a los 10 días del mes de enero del 2022, se procede a extraer datos de un dispositivo móvil con sistema operativo Android del cual, se requiere obtener información necesaria e importante mediante la utilización de herramientas open-source, y que sea considerado como evidencia valida en la investigación de algún caso.

Consideraciones técnicas:

El lunes 10 de enero del presente año a las 19:00, se inicia con la extracción de datos del dispositivo móvil de marca Samsung Galaxy J5*,* el cual, es el motivo de esta investigación.

- Se realiza la identificación e inspección del dispositivo móvil, con la finalidad de validar el estado y las características, en donde, se verifica que el móvil trabaja bajo el sistema operativo Android versión 5.1.1. Seguidamente, se procede a documentar las características a través de fotografías y de una ficha técnica; ver figura 1, tabla 1.

Figura 1: identificación del dispositivo móvil real

Tabla 1: Ficha de registro de información del dispositivo móvil real

Ficha técnica de dispositivos móviles						
Perito	Darwin Chimbo					
Numero de caso	001					
Fecha	10 de enero de 2022					
Hora	19:00					
Item	**Tipo**	**Marca**	**Serie**	**Modelo**	**Estado**	**Observaciones**
1	Celular	Samsung Galaxy J5	RV8H10X3AXE	SM-J500M	Bueno	Encendido

- Una vez que, se adquirió los datos del dispositivo móvil con el uso de herramientas open-source en los diferentes tipos de extracción; y luego de garantizar la integridad y analizar la imagen forense con herramientas de análisis forense, se pudo obtener información interesante como: mensajes del aplicativo WhatsApp, fotografías, logs de llamadas, contactos del teléfono, mensajes SMS, chats de Facebook Messenger, programas instalados, información del sistema operativo, web accounts, web cookies, web history, web search, email addresses, communications accounts, metadatos, archivos almacenados, archivos borrados, claves de redes wifi,

los mismos que, se documenta por medio de capturas de imágenes, ver figura 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 y 17.

Figura 2: mensajes de WhatsApp

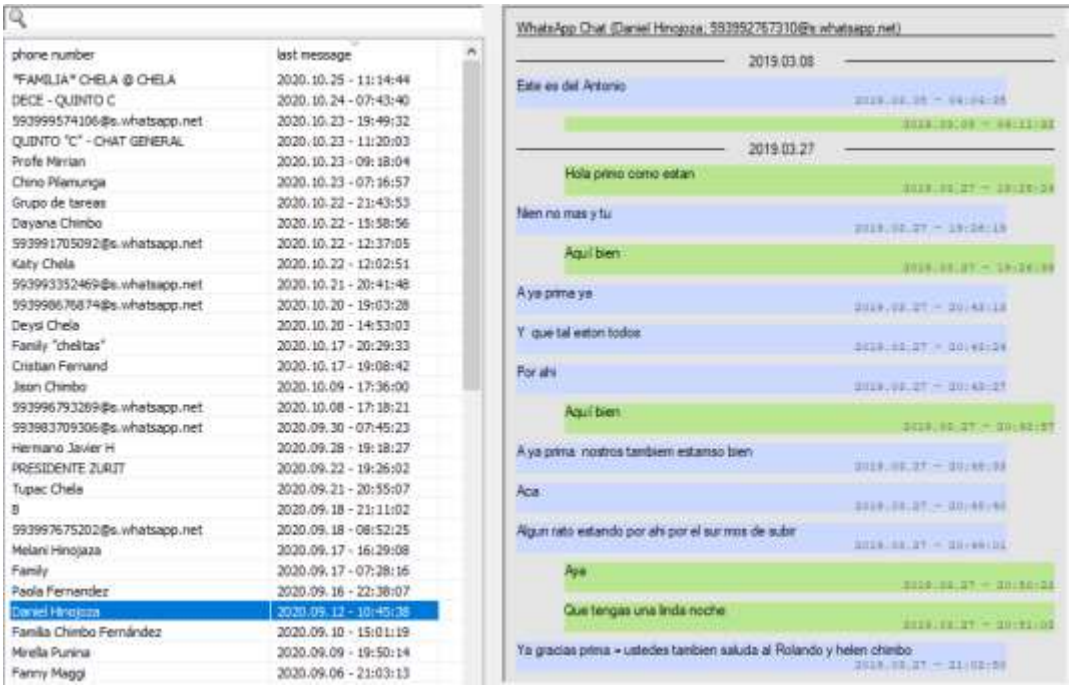
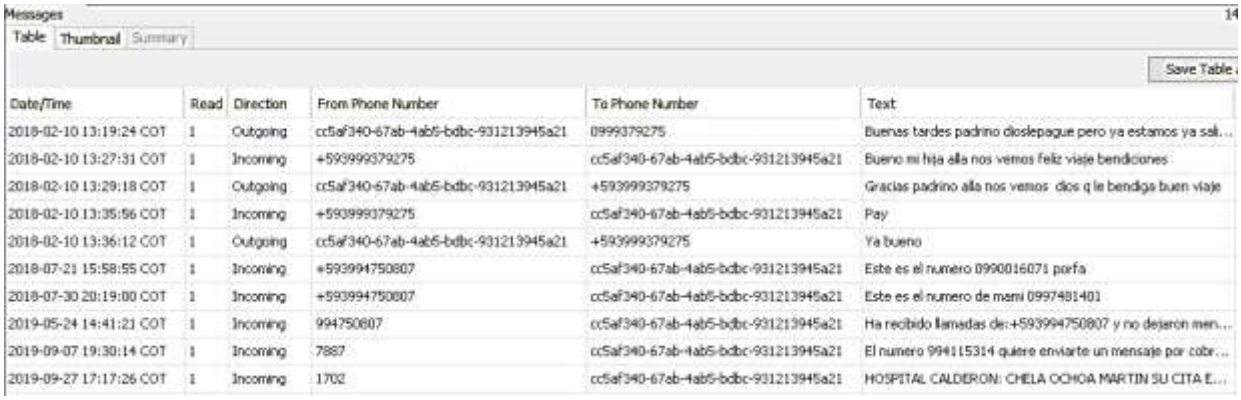


Figura 3: chats de Facebook Messenger

Sender	Sender Account	Message	Recipients	Time
	Darwin Siño	Seguro???	Ga Bo	2022-03-19 23:21:04 UTC
	Ga Bo	No creo	Darwin Siño	2022-03-19 23:17:13 UTC
	Ga Bo	Hablé bien	Darwin Siño	2022-03-19 23:17:04 UTC
	Ga Bo	no tengo idea	Darwin Siño	2022-03-19 23:15:26 UTC
	Ga Bo	con quien tengo el gusto	Darwin Siño	2022-03-19 23:15:07 UTC
	Darwin Siño	Cómo está	Ga Bo	2022-03-19 23:14:16 UTC
	Darwin Siño	Saludos	Ga Bo	2022-03-19 23:14:03 UTC
	Ga Bo	confirme	TelNet Cia	2022-03-19 22:50:50 UTC
	Ga Bo	Para que ciudad es	TelNet Cia	2022-03-19 22:40:02 UTC
	Ga Bo	Ayudeme su contacto para comunucarme	TelNet Cia	2022-03-19 22:39:38 UTC
	TelNet Cia	De dónde se comunica	Ga Bo	2022-03-19 22:28:08 UTC
	TelNet Cia	Ya le envío	Ga Bo	2022-03-19 22:27:56 UTC
	Ga Bo	Algún número de contacto para comunicsrme	TelNet Cia	2022-03-19 22:20:26 UTC
	Ga Bo	Buenas tardes	TelNet Cia	2022-03-19 22:20:01 UTC
	Ga Bo	Saludos	Darwin Siño	2022-03-19 22:10:29 UTC

Figura 4: mensajes SMS



Messages

Table | Thumbnail | Summary

Save Table

Date/Time	Read	Direction	From Phone Number	To Phone Number	Text
2018-02-10 13:19:24 COT	1	Outgoing	cc5af340-67ab-4ab5-bdbc-931213945a21	0999379275	Buenas tardes padrino dioslepague pero ya estamos ya sal...
2018-02-10 13:27:31 COT	1	Incoming	+593999379275	cc5af340-67ab-4ab5-bdbc-931213945a21	Bueno mi hija alla nos vemos feliz viaje bendiciones
2018-02-10 13:29:18 COT	1	Outgoing	cc5af340-67ab-4ab5-bdbc-931213945a21	+593999379275	Gracias padrino alla nos vemos dios q le bendiga buen viaje
2018-02-10 13:35:56 COT	1	Incoming	+593999379275	cc5af340-67ab-4ab5-bdbc-931213945a21	Pay
2018-02-10 13:36:12 COT	1	Outgoing	cc5af340-67ab-4ab5-bdbc-931213945a21	+593999379275	Ya bueno
2018-07-21 15:58:55 COT	1	Incoming	+593994750807	cc5af340-67ab-4ab5-bdbc-931213945a21	Este es el numero 0990016071 porfa
2018-07-30 20:19:00 COT	1	Incoming	+593994750807	cc5af340-67ab-4ab5-bdbc-931213945a21	Este es el numero de mami 0997481401
2019-05-24 14:41:21 COT	1	Incoming	994750807	cc5af340-67ab-4ab5-bdbc-931213945a21	Ha recibido llamadas de:+593994750807 y no dejaron men...
2019-09-07 19:30:14 COT	1	Incoming	7887	cc5af340-67ab-4ab5-bdbc-931213945a21	El numero 994115314 quiere enviarte un mensaje por cobr...
2019-09-27 17:17:26 COT	1	Incoming	1702	cc5af340-67ab-4ab5-bdbc-931213945a21	HOSPITAL CALDERON: CHELA OCHOA MARTIN SU CITA E...

Figura 5: logs de llamadas

Index	Type	Number	Name	Time	Duration
14714	Dialled	911		2022-01-20 21:50:55 UTC	00:00:00
14713	Dialled	0997481401		2020-10-22 20:33:49 UTC	00:00:09
14712	Missed	0999574106		2020-10-21 12:45:43 UTC	00:00:00
14711	Missed	0999574106		2020-10-21 12:45:03 UTC	00:00:00
14710	Received	0999574106		2020-10-21 12:16:52 UTC	00:00:21
14704	Dialled	0993352469		2020-10-18 01:54:12 UTC	00:00:07
14703	Missed	0993352469		2020-10-18 01:27:15 UTC	00:00:00
14702	Missed	0993352469		2020-10-18 01:26:19 UTC	00:00:00
14701	Dialled	0986098265		2020-10-17 18:55:30 UTC	00:00:16
14700	Dialled	0986098265		2020-10-17 18:49:55 UTC	00:00:08
14699	Missed	0985378669		2020-10-17 14:09:14 UTC	00:00:00
14698	Missed	0985378669		2020-10-17 13:58:38 UTC	00:00:00
14697	Missed	0985378669		2020-10-17 13:51:04 UTC	00:00:00

Figura 6: contactos del teléfono

Contacts

Table | Thumbnail | Summary

Source File	S	C	O	Name	Phone Number	Data Source
contacts2.db			1	Amor	+593991965723	imagen-android.dd
contacts2.db			3	Andrea	+593 98 020 2518	imagen-android.dd
contacts2.db			2	CNT	022370000	imagen-android.dd
contacts2.db			3	Casa Padrino	02-260-4752	imagen-android.dd
contacts2.db			3	Casita Helen	02-366-2346	imagen-android.dd
contacts2.db			3	Cepillito	0980197387	imagen-android.dd
contacts2.db			3	Chino Pilamunga	0989535856	imagen-android.dd
contacts2.db			2	Claro	0939014447	imagen-android.dd
contacts2.db			3	Contraseña	0202486312	imagen-android.dd
contacts2.db			3	Daniel Hinojoza	0992767310	imagen-android.dd
contacts2.db			5	Darwin	0999574106	imagen-android.dd

Figura 7: programas instalados

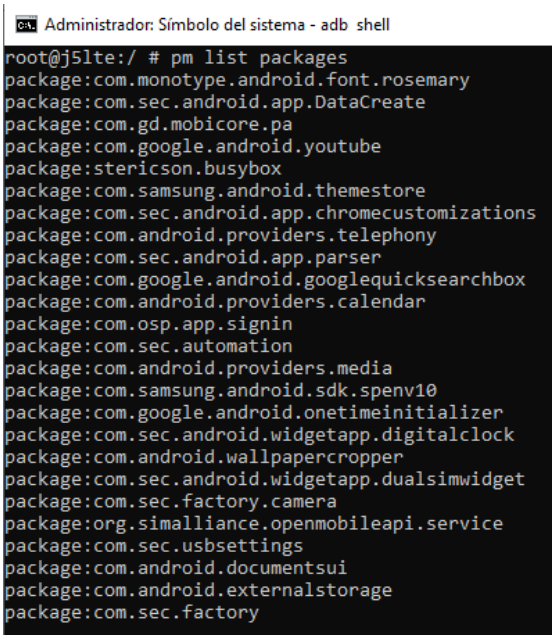


Figura 8: información del sistema operativo

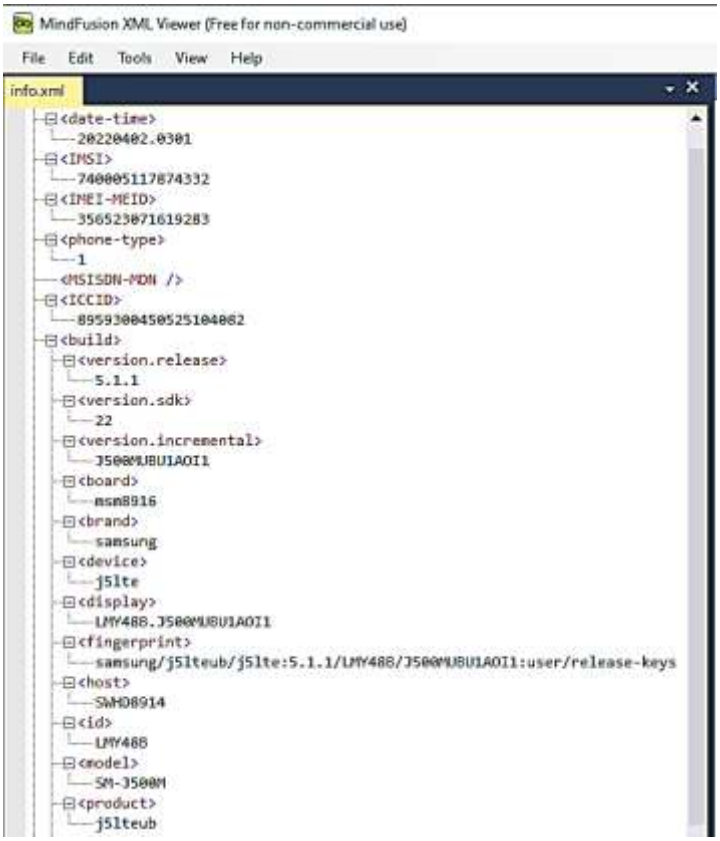


Figura 9: Cuentas de correo y redes sociales

Index	Account type	Username
1	com.google	darwin.chimbo777@gmail.com
2	com.osp.app.signin	darwin.chimbo777@gmail.com
13	com.whatsapp	WhatsApp
15	com.google	helmach2011@gmail.com
42	com.facebook.auth.login	Facebook
44	com.facebook.messenger	Messenger

Figura 10: web cookies

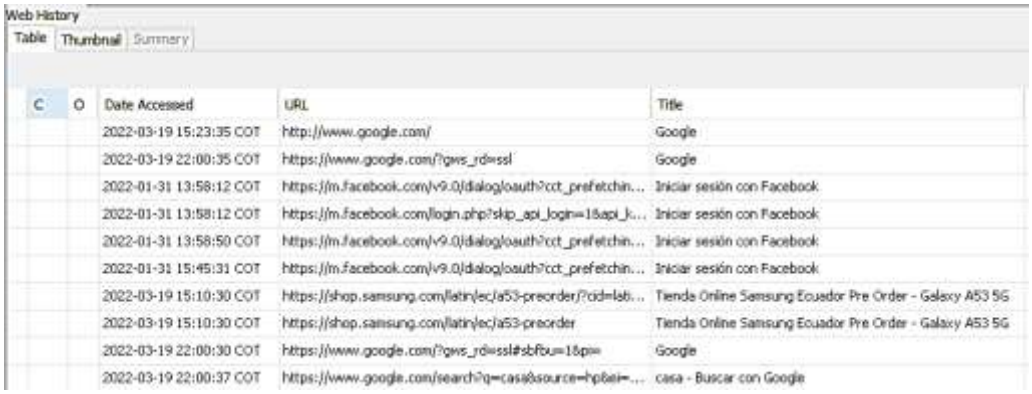
Web Cookies

Table | Thumbnail | Summary

Save Table

Date Accessed	URL	Name	Value	Date Created	End Date/Time
2020-07-24 03:35:38 COT	.guiainfantil.com	__cfduid	d3163d04d31b9694f4803f01a993827b31568935829	2019-09-19 23:30:28 COT	2020-09-18 23:30:28 COT
2020-07-24 03:35:38 COT	.guiainfantil.com	__gads	ID=bdf2a7f589109e23:T=1568935835:S=ALNI_MZP63Fdi...	2019-09-19 23:30:35 COT	2021-09-18 23:30:35 COT
2020-04-23 17:23:03 COT	.groovinads.com	__cfduid	db2a1908ff938ce4650666fb0a6fa4fb071568935838	2019-09-19 23:30:37 COT	2020-09-18 23:30:37 COT
2020-08-03 15:11:59 COT	.districtm.io	__cfduid	dfa23d6479e6a07093680b2509da931e71568935844	2019-09-19 23:30:43 COT	2020-09-18 23:30:43 COT
2020-07-20 19:14:56 COT	.srv.stackadapt.com	sa-user-id	s%3A0-95504b1f-6871-4b16-5e5b-7ed28d9e33eb.59dPag...	2019-09-19 23:30:46 COT	2024-09-17 23:30:46 COT
2020-04-23 17:23:03 COT	.retargetly.com	_ga	GA1.2.608406450.1568935863	2019-09-19 23:31:02 COT	2021-09-18 23:31:02 COT
2020-04-23 17:23:04 COT	.api.retargetly.com	_ga	GA1.3.608406450.1568935863	2019-09-19 23:31:02 COT	2021-09-18 23:31:02 COT
2020-04-23 17:23:04 COT	api.retargetly.com	_ga	GA1.1.608406450.1568935863	2019-09-19 23:31:02 COT	2021-09-18 23:31:02 COT
2020-03-05 00:03:33 COT	www.pinterest.es	csrftoken	7R2p0OqjvRYnEdEov4y6rNqNac8HVtHc	2019-09-19 23:31:09 COT	2020-09-17 23:31:09 COT
2019-09-19 23:32:37 COT	.uplynk.com	COMBOID	"comboid=UP809e7aa1-db35-11e9-88e5-023147cdd8bc|e...	2019-09-19 23:32:37 COT	2020-09-19 23:32:37 COT

Figura 11: Web History

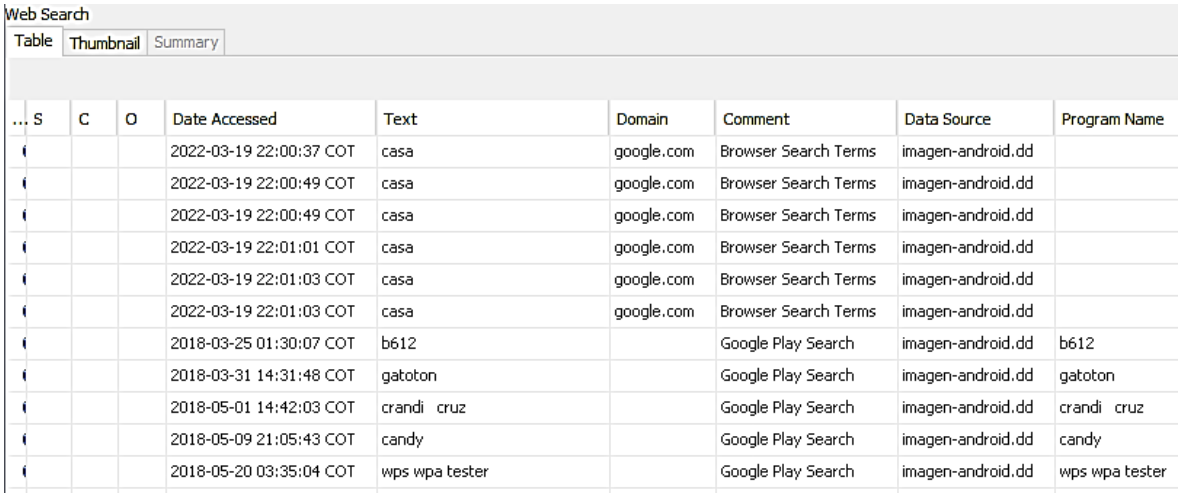


Web History

Table | Thumbnail | Summary

C	O	Date Accessed	URL	Title
		2022-03-19 15:23:35 COT	http://www.google.com/	Google
		2022-03-19 22:00:35 COT	https://www.google.com/?gws_rd=ssl	Google
		2022-01-31 13:58:12 COT	https://m.facebook.com/v9.0/dialog/oauth?cct_prefetchin...	Iniciar sesión con Facebook
		2022-01-31 13:58:12 COT	https://m.facebook.com/login.php?skip_api_login=1&api_k...	Iniciar sesión con Facebook
		2022-01-31 13:58:50 COT	https://m.facebook.com/v9.0/dialog/oauth?cct_prefetchin...	Iniciar sesión con Facebook
		2022-01-31 15:45:31 COT	https://m.facebook.com/v9.0/dialog/oauth?cct_prefetchin...	Iniciar sesión con Facebook
		2022-03-19 15:10:30 COT	https://shop.samsung.com/latin/ec/a53-preorder/?cid=lati...	Tienda Online Samsung Ecuador Pre Order - Galaxy A53 5G
		2022-03-19 15:10:30 COT	https://shop.samsung.com/latin/ec/a53-preorder	Tienda Online Samsung Ecuador Pre Order - Galaxy A53 5G
		2022-03-19 22:00:30 COT	https://www.google.com/?gws_rd=ssl#sbfbu=1&pi=	Google
		2022-03-19 22:00:37 COT	https://www.google.com/search?q=casa&source=hp&ei=...	casa - Buscar con Google

Figura 12: web search



Web Search

Table | Thumbnail | Summary

...	S	C	O	Date Accessed	Text	Domain	Comment	Data Source	Program Name
				2022-03-19 22:00:37 COT	casa	google.com	Browser Search Terms	imagen-android.dd	
				2022-03-19 22:00:49 COT	casa	google.com	Browser Search Terms	imagen-android.dd	
				2022-03-19 22:00:49 COT	casa	google.com	Browser Search Terms	imagen-android.dd	
				2022-03-19 22:01:01 COT	casa	google.com	Browser Search Terms	imagen-android.dd	
				2022-03-19 22:01:03 COT	casa	google.com	Browser Search Terms	imagen-android.dd	
				2022-03-19 22:01:03 COT	casa	google.com	Browser Search Terms	imagen-android.dd	
				2018-03-25 01:30:07 COT	b612		Google Play Search	imagen-android.dd	b612
				2018-03-31 14:31:48 COT	gatoton		Google Play Search	imagen-android.dd	gatoton
				2018-05-01 14:42:03 COT	crandi cruz		Google Play Search	imagen-android.dd	crandi cruz
				2018-05-09 21:05:43 COT	candy		Google Play Search	imagen-android.dd	candy
				2018-05-20 03:35:04 COT	wps wpa tester		Google Play Search	imagen-android.dd	wps wpa tester

Figura 13: metadatos

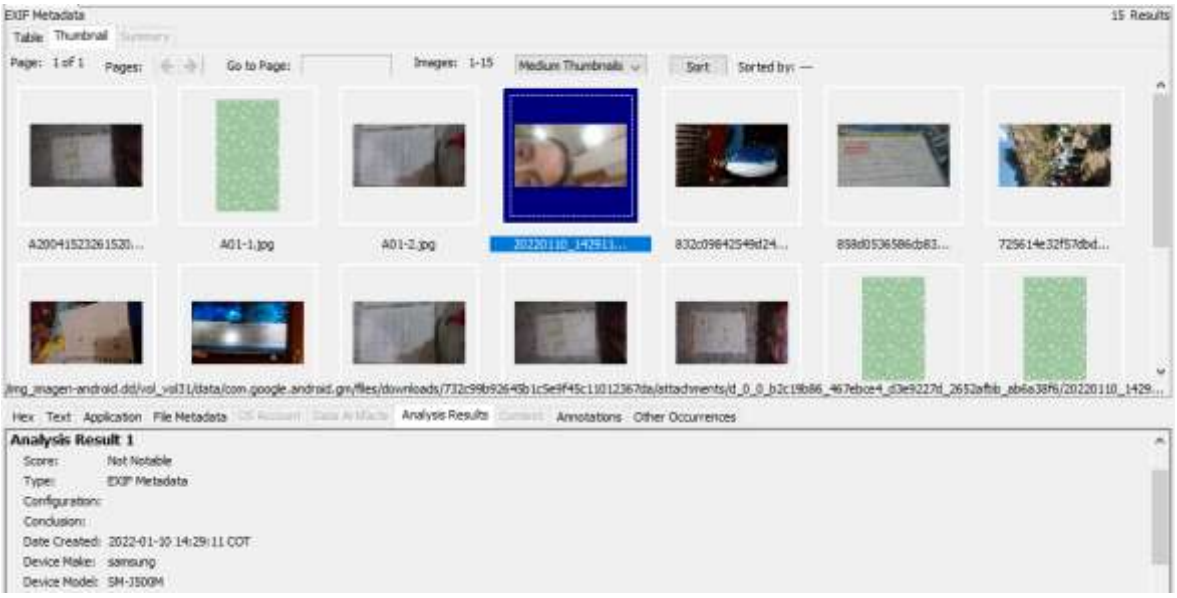


Figura 14: archivos almacenados

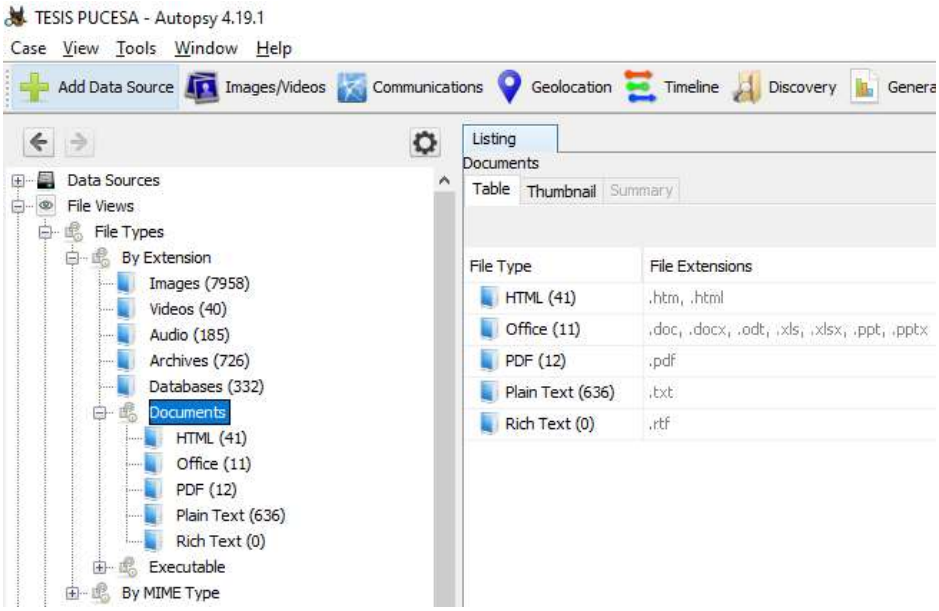


Figura 15: archivos borrados

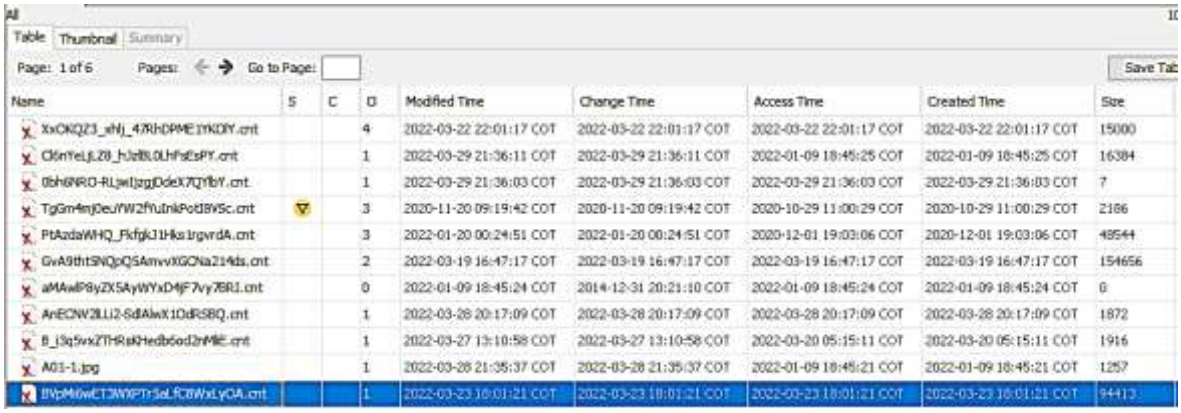


Figura 16: claves de redes wifi

Index	SSID	Password	Key Management	Priority
1	PUNTONET_CHIMBO	[redacted]	WPA-PSK	7
2	MARGOTH	[redacted]	WPA-PSK	2
3	FMAX:DARWIN	[redacted]	WPA-PSK	6
4	IPLANET_ESTUXNES	[redacted]	WPA-PSK	11
5	NETLIFE-CHELA	[redacted]	WPA-PSK	12
6	Stuxnes		NONE	13

Figura 17: fotografías

<u>Conclusiones del informe pericial</u>:

De acuerdo al informe presentado, se evidencia que al utilizar herramientas open-source, se extrae información relevante que es utilizada en la investigación de un delito informático, donde esté implicado un dispositivo móvil, se obtiene

conversaciones de la aplicación WhatsApp, fotografías, logs de llamadas, contactos del teléfono, mensajes SMS, chats de Facebook Messenger, programas instalados, información del sistema operativo, web accounts, web cookies, web history, web search, communications accounts, metadatos, archivos almacenados, archivos borrados, claves de redes wifi.

Atentamente,

Darwin Rolando Chimbo Fernandez

C.C # 0201683919

Anexo 2. Informe pericial equipo emulado

Informe pericial

Datos generales:

Empresa contratante: No aplica

Nombre y apellido del perito: Darwin Chimbo

Profesión: Ing. En Electrónica Telecomunicaciones y Redes

Dirección de contacto: E-14 y Jorge Enrique Adoum

Teléfono fijo de contacto: 023662346

Teléfono celular de contacto: 0999574106

Correo electrónico de contacto: drchimbo@pucesa.edu.ec

Antecedentes:

En la ciudad de Quito a los 21 días del mes de febrero del 2022, se procede con la extracción de datos de un dispositivo móvil emulado con sistema operativo Android del cual, se necesita recopilar información necesaria y relevante a través de herramientas de software libre, y que sea considerado como evidencia para la resolución de un delito informático.

Consideraciones técnicas:

El lunes 21 de febrero del presente año a las 19:00, se inicia con la extracción de datos del dispositivo móvil emulado de marca Samsung Galaxy S7, el cual, es el motivo de esta investigación.

- Se realiza la identificación e inspección del dispositivo móvil emulado, con la finalidad de validar el estado y las características, en donde, se verifica que el móvil trabaja bajo el sistema operativo Android versión 6.0. Seguidamente, se procede a documentar las características a través de fotografías y de una ficha técnica; ver figura 2, tabla 2.

Figura 1: identificación del dispositivo móvil emulado

Tabla 2: Ficha de registro de información del dispositivo móvil emulado

Ficha técnica de dispositivos móviles						
Perito	Darwin Chimbo					
Numero de caso	002					
Fecha	21 de febrero de 2021					
Hora	19:00					
Item	**Tipo**	**Marca**	**Serie**	**Modelo**	**Estado**	**Observaciones**
1	Celular	Samsung Galaxy S7	N/A	vbox86p	Bueno	Encendido

- Una vez que, se adquirió los datos del dispositivo móvil mediante herramientas open-source en los diferentes tipos de extracción; y luego de garantizar la integridad y analizar la imagen forense con herramientas de análisis forense, se pudo obtener información interesante como: fotografías, logs de llamadas, contactos del teléfono, mensajes SMS, chats de Facebook Messenger, programas instalados, información del sistema operativo, metadatos, archivos almacenados, archivos borrados, los mismos, que, se documenta por medio de capturas de imágenes, ver figura 2, 3, 4, 5, 6, 7, 8, 9, 10 y 11.

Figura 2: chats de Facebook Messenger

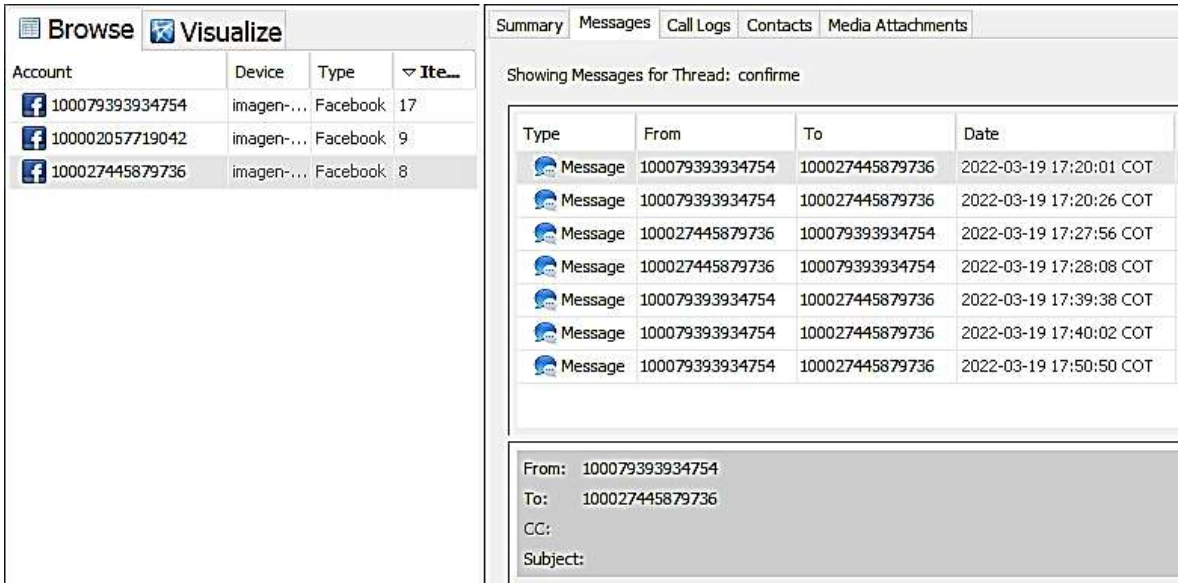


Figura 3: mensajes SMS

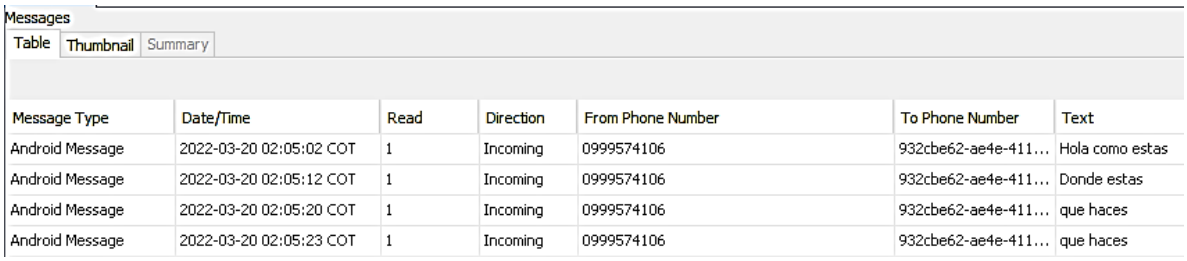


Figura 4: logs de llamadas

_id	number	date	duration	type	new	name	numbertype	numberlabel
1	0999574106	1647759868567	0	1	1			
2	0999574106	1647759804057	65	1	1			

Figura 5: contactos del teléfono

Contacts

Table | Thumbnail | Summary

Source File	S	C	O	Name	Phone Number	Data Source
contacts2.db			5	Darwin	0999574106	imagen-android-emulado.dd
contacts2.db			3	Flaca	0991965723	imagen-android-emulado.dd

Figura 6: programas instalados

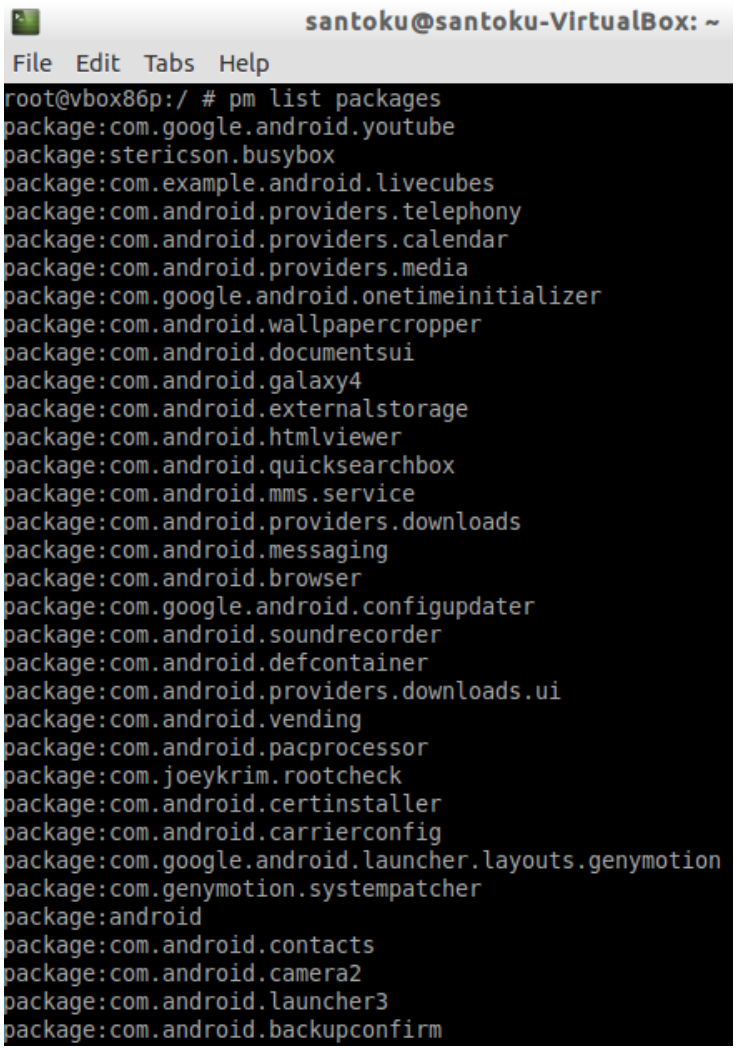


Figura 7: información del sistema operativo

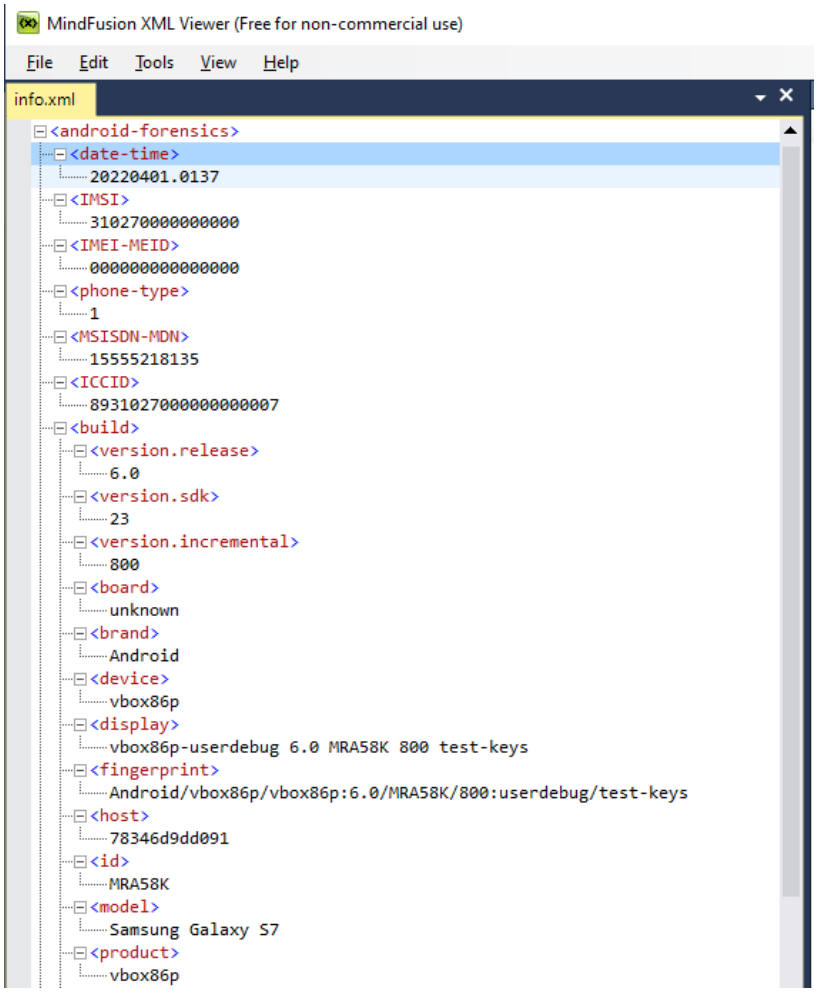


Figura 8: metadatos

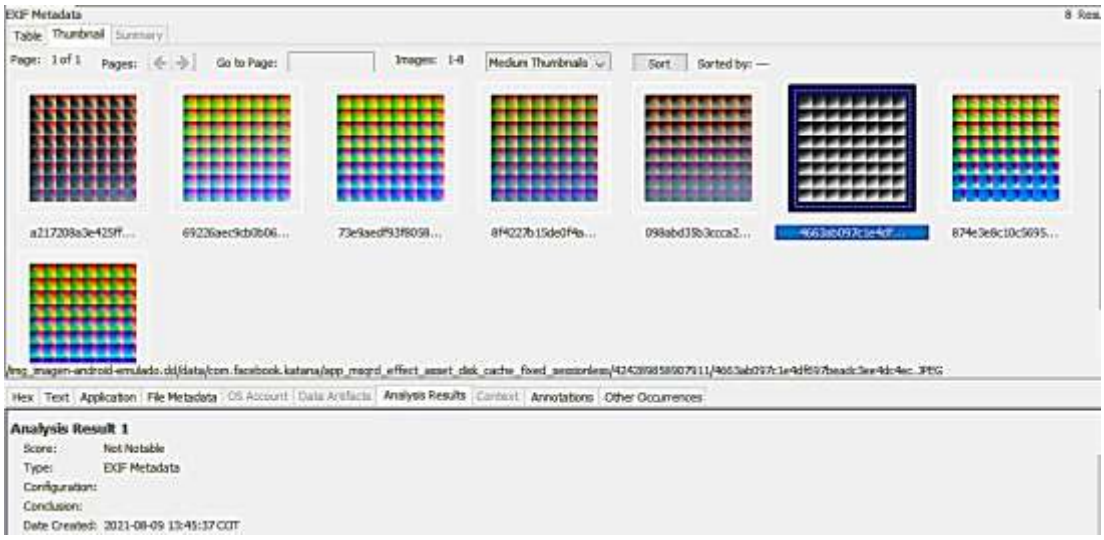


Figura 9: archivos almacenados

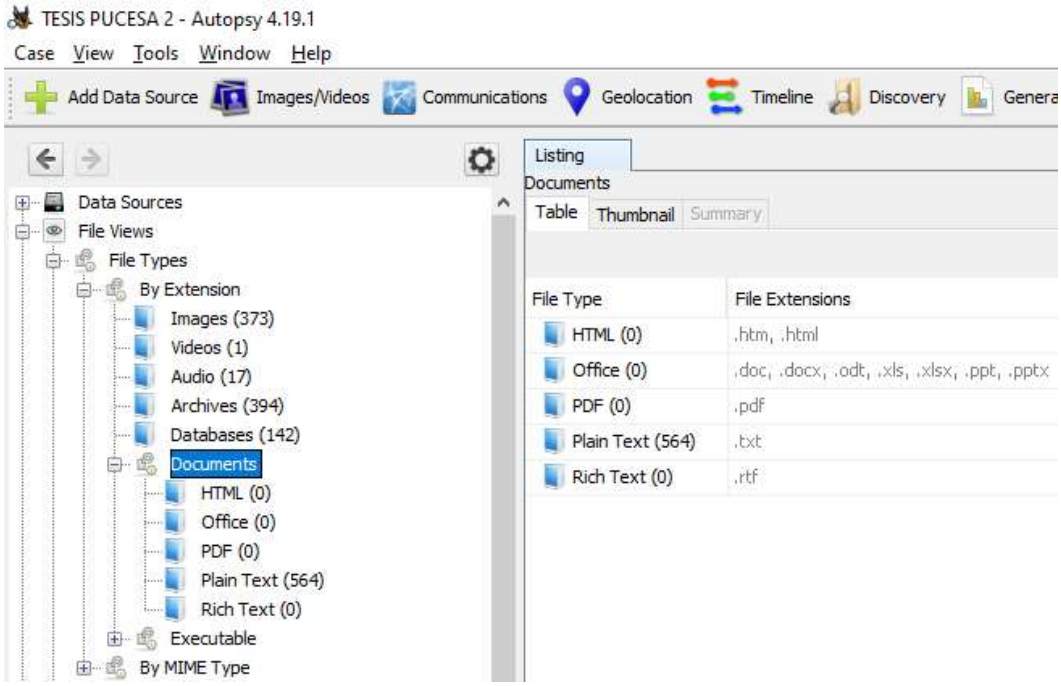


Figura 10: archivos borrados

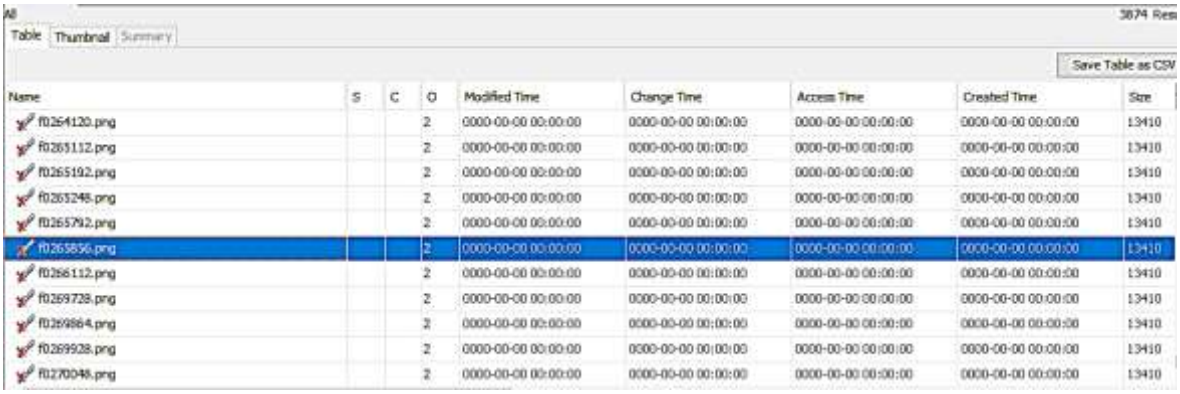
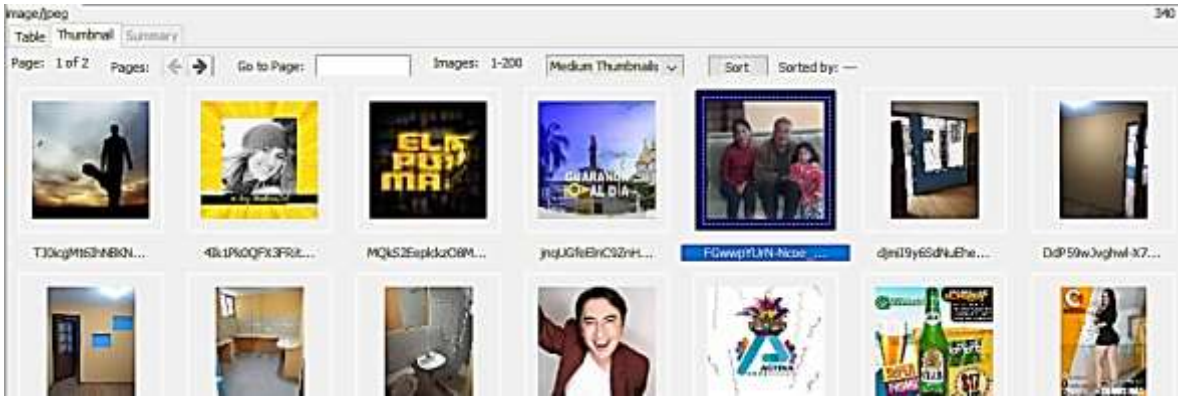


Figura 11: fotografías



Conclusiones de informe pericial:

De acuerdo al informe presentado, se evidencia que al utilizar herramientas open-source, se extrae información relevante que es utilizada en la investigación de un delito informático, donde esté implicado un dispositivo móvil, se obtiene fotografías, logs de llamadas, contactos del teléfono, mensajes SMS, chats de Facebook Messenger, programas instalados, información del sistema operativo, metadatos, archivos almacenados, archivos borrados.

Anexo 3. Formato de informe pericial

FORMATO DE INFORME PERICIAL

Las peritas y peritos presentarán su informe de conformidad con lo establecido en los artículos 19 y 20 del REGLAMENTO QUE REGULA EL SISTEMA PERICIAL INTEGRAL DE LA FUNCIÓN JUDICIAL. Por lo tanto, el presente formato es de uso obligatorio para la presentación de los informes periciales, sin perjuicio de lo establecido en normas legales específicas.

“INFORME PERICIAL”

1. DATOS GENERALES DEL JUICIO, O PROCESO DE INDAGACIÓN PREVIA

TRIBUNAL/JUZGADO/FISCALÍA
No. de Proceso/No. de Indagación Previa o Instrucción Fiscal
Nombre y Apellido del Perito/a
Profesión, Oficio, Arte, o Actividad calificada
No. de Calificación y Acreditación
Fecha de terminación de la calificación y acreditación
Dirección de contacto
Teléfono fijo de contacto
Teléfono celular de contacto
Correo electrónico de contacto

2. **PARTE DE ANTECEDENTES,** en donde, se delimita claramente el encargo realizado, esto es, se tiene que especificar claramente el tema sobre el que informa en base a lo ordenado por el juez, el fiscal y/o lo solicitado por las partes procesales.

3. **PARTE DE CONSIDERACIONES TÉCNICAS O METODOLOGÍA A APLICARSE,** en donde, se explica claramente, cómo aplican sus conocimientos especializados de su profesión, arte u oficio, al caso o encargo materia de la pericia. La o el perito relaciona los contenidos de sus conocimientos especializados con el objeto de la pericia encargada. Analizar si son pertinentes o no la aplicación de sus conocimientos especializados al caso concreto materia de su informe.

4. **PARTE DE CONCLUSIONES,** luego de las consideraciones técnicas, se procede a emitir la opinión técnica, o conclusión de la aplicación de los conocimientos especializados sobre el caso concreto analizado. Se prohíbe todo tipo de juicios de valor sobre la actuación de las partes en el informe técnico. El informe solamente versa sobre los hechos consultados y ordenados, establecidos en los antecedentes, y nada dice sobre el accionar

de las partes procesales en el caso en particular. Las conclusiones solamente, se referirán a los temas materia de la pericia debidamente delimitados y explicados en los antecedentes. Cualquier otro criterio adicional a la delimitación de la pericia no es tomado en cuenta al momento de resolver, y es tomado en consideración para la evaluación de la o el perito.

5. **PARTE DE INCLUSIÓN DE DOCUMENTOS DE RESPALDO, ANEXOS, O EXPLICACIÓN DE CRITERIO TÉCNICO,** sustenta sus conclusiones ya sea con documentos y objetos de respaldo (fotos, copias certificadas de documentos, grabaciones, entre otros); y/o, con la explicación clara de cuál es el sustento técnico o científico para obtener un resultado o conclusión específica. Se expone claramente las razones especializadas de la o el perito para llegar a la conclusión correspondiente. No, se cumple con este requisito si no, se sustenta la conclusión con documentos, objetos o con la explicación técnica y científica exigida en este numeral. La o el perito razona y motiva diáfanamente la razón de sus dichos, esto es, justificar desde todo punto de vista las conclusiones que incluya en el informe. En caso de que no fundamente sus conclusiones y esto sea informado por el juez, la jueza, o el/la fiscal, es considerado al momento de la evaluación de la o el perito.

6. **OTROS REQUISITOS,** si la ley procesal correspondiente determina la inclusión de requisitos adicionales a los establecidos por el reglamento, el perito debe hacerlo constar necesariamente en su informe pericial de conformidad con dicha exigencia legal.

7. **INFORMACIÓN ADICIONAL,** el perito o la perita incluye cualquier otro tipo de información adicional a los numerales anteriores, siempre y cuando la misma ayude a clarificar sus explicaciones y/o conclusiones; y, siempre y cuando esta información, se encuentre dentro de los límites del objeto de la pericia.

8. **DECLARACIÓN JURAMENTADA,** el perito o la perita debe en la parte final del informe, declarar bajo juramento que su informe es independiente y

corresponde a su real convicción profesional, así como, también, que toda la información que ha proporcionado es verdadera.

9. **FIRMA Y RÚBRICA**, al final del informe, se hace constar la firma y rúbrica del perito o perita, el número de su cédula de ciudadanía, y el número de su calificación y acreditación pericial.

Nota: El presente ejemplar es una guía de los ítems que al menos considerarán los auxiliares de justicia al momento de elaborar sus informes periciales.