OFICINA DE POSGRADOS

Tema:

MODELO PARA ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID

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

Línea de investigación:

SEGURIDAD DE LA INFORMACIÓN

Autor:

KLEVER WASHINGTON BELTRÁN TAPIA

Director:

MSC. ING. EDGAR FERNANDO SOLÍS ACOSTA

Ambato – Ecuador

Septiembre 2021

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

MODELO PARA ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID

Línea de investigación:

SEGURIDAD DE LA INFORMACIÓN

Autor:

KLEVER WASHINGTON BELTRÁN TAPIA

Edgar Fernando Solís Acosta . Ing. MSc. f.
CALIFICADOR

Firmado electrónicamente por:
EDGAR FERNANDO SOLIS ACOSTA

Diego Fernando Avila Pesántez. Ing. MSc f.
CALIFICADOR

Firmado electrónicamente por:
DIEGO FERNANDO AVILA PESANTEZ

Darío Javier Robayo Jácome. Ing. MSc. f.
CALIFICADOR

Darío Robayo Jácome

Firmado digitalmente por Darío Robayo Jácome.
DN: C=EC, O=Pontificia Universidad Católica del Ecuador Sede Ambato, CN=Darío Robayo Jácome, E=drobayo@pucesa.edu.ec
Razón: He revisado este documento
Ubicación: la ubicación de su firma aquí
Fecha: 2021.09.20 12:03:44-05'00'
Foxit PDF Reader Versión: 11.0.1

Juan Carlos Acosta, Padre, MSc f.
DIRECTOR UNIDAD ACADÉMICA

Hugo Rogelio Altamirano Villaroel, Dr.
SECRETARIO GENERAL PUCESA

Ambato - Ecuador

Septiembre 2021

DECLARACIÓN DE AUTENCIDAD Y RESPONSABILIDAD

Yo: **KLEVER WASHINGTON BELTRÁN TAPIA**, con CC. **050232435-3**, autor del trabajo de graduación intitulado: "MODELO PARA ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID", previa a la obtención del título profesional de **MAGISTER EN CIBERSEGURIDAD**, en 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, septiembre 2021

Firmado electrónicamente por:
KLEVER WASHINGTON BELTRAN TAPIA

AGRADECIMIENTO

Al culminar una etapa más de mi vida estudiantil agradezco de todo corazón a las personas que me apoyaron de forma incondicional para concluir este trabajo de investigación.

Infinitas gracias a mis padres por cuidarme, guiar mis pasos y por concederme la sabiduría suficiente para lograr mis metas.

A la Pontificia Universidad Católica del Ecuador y a los docentes de la maestría por darme la oportunidad de crecer profesionalmente.

Klever Washington Beltrán Tapia

DEDICATORIA

A mis padres quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo y valentía, A los docentes de esta prestigiosa universidad porque con sus consejos, guía y palabras de aliento hicieron de mí un mejor profesional y por extender su mano en momentos difíciles.

Klever Washington Beltrán Tapia

RESUMEN

En los últimos años se ha evidenciado un gran aumento de la comunicación global y el uso de equipos móviles con sistema operativo Android, el que, se ha convertido en líder indiscutible del mercado a nivel mundial al ser la plataforma más utilizada; el presente proyecto tiene como objetivo diseñar un modelo para análisis forense en dispositivos móviles con sistema operativo Android, debido a que en la actualidad no existe un procedimiento establecido basado en los requerimientos nacionales que guíe el análisis forense de estos dispositivos. La metodología que se aplica para el trabajo es una investigación bibliográfica de modelos y normas nacionales e internacionales que permitan: asegurar la escena motivo de investigación, identificar evidencias, adquirir datos, analizar datos y presentar informes. Aplicado el diseño, se comprueba que mediante la documentación realizada en cada una de las fases facilita al perito la realización del informe final, a la vez que, estar apegado a la normativa legal vigente disminuye los riesgos de caer en infracción, por tanto, se verifica la factibilidad del modelo propuesto basado en análisis forense dentro del laboratorio de la Universidad de las Fuerzas Armadas ESPE, apoyado en múltiples pruebas con lo que se determina la validez del presente trabajo.

PALABRAS CLAVE

Android, modelo forense, dispositivos móviles, metodología, comandos, sistema operativo.

ABSTRACT

In recent years, there has been a great increase in global communication and the use of mobile devices with Android operating system, which has become the undisputed market leader worldwide, as it is the most widely used platform. The objective of this research project is to design a forensic analysis model on mobile devices with Android operating system, since there is currently no established procedure based on national requirements to guide the forensic analysis of these devices. The applied methodology is the bibliographic investigation of national and international models and standards that allow to secure the research motif, identify evidence, acquire data, analyze data and present reports. Once the design has been applied, it is verified that the documentation in each of the phases makes it easier for the expert to produce the final report. At the same time, it allows you to comply with current legal regulations and reduces the risks of committing infractions. Therefore, the feasibility of the proposed model based on forensic analysis supported by multiple tests within the laboratory of the University of the Armed Forces ESPE is verified, thereby determining the validity of this work.

Keywords: Android, forensic model, mobile devices, methodology, commands, operating system.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

En la conferencia de desarrolladores del año 2019 se señala que, existe 2.500 millones de usuarios que, utilizan dispositivos móviles con sistema operativo Android (Nts solutios, 2020), esta cifra refleja cuanto ha crecido el mismo, se considera que, Android fue desarrollado y presentado hace poco más de una década por lo que, se evidencia su evolución en la comunicación global, esto se atribuye a que, la mayor parte de fabricantes de dispositivos han optado por usar este sistema operativo, por lo que, se ha convertido en líder indiscutible del mercado a nivel mundial, por esta razón podemos decir que, un gran número de delitos informáticos tanto en el presente como en el futuro están enfocados en este tipo de sistemas, lo que, ha permitido el desarrollo de nuevas ciencias como la Informática Forense.

Según (Torres, 2020) la definición instituida por el F.B.I., quienes describieron a la informática forense como: la ciencia que se encarga de aplicar técnicas informáticas en el proceso de adquirir, preservar, obtener y presentar datos que, han sido procesados y/o almacenados de forma electrónica y que, son relevantes en el ámbito judicial. Es necesario un análisis detallado para comprender su efectivo significado, se estudia los elementos de la descripción:

La adquisición: habla de la recolección efectiva del objeto de estudio o elemento de análisis.

La preservación: mantiene dicho elemento a peritar en su estado original, evita su alteración en lo más mínimo con el fin de, excluir resultados erróneos.

La obtención: es la observación en sí, determina que, la información es efectivamente la que se desea indagar. Los casos más normales, para ejemplificar son, el chequeo de historial de navegación, recuperación de archivos de texto o imágenes borrados de forma poco segura, entre otros procedimientos. Y finalmente;

La presentación: la cual, hace referencia a la exposición de un informe se utiliza un lenguaje acorde a quienes sean los destinatarios del análisis. Dado que, tanto las partes como el juez son los principales interesados de los resultados de esta actividad pericial.

En tanto, al referirse que "han sido procesados y/o almacenados de forma electrónica", hace referencia a dispositivos físicos de retención de información y a los transmitidos en una red de datos.

Se argumenta que la Informática Forense no está limitada solo al sector público donde se da un juicio de valor a las evidencias encontradas determinadas por una sentencia, sino que, va más allá y se extiende a investigaciones de carácter privado, sin la necesidad de llevar estos hechos a un espacio jurídico.

El Ecuador no ha sido la excepción frente al posicionamiento y crecimiento significativo en el uso de equipos móviles, lo que, permite estar comunicados acorde al avance tecnológico; sin embargo, la comunicación no ha sido utilizada solamente en el desarrollo de actividades lícitas, por el contrario, muchas personas han encontrado una oportunidad para cometer actos ilícitos, por lo que, surge la necesidad de realizar investigaciones periciales. Estos sucesos dan paso a la Informática Forense, que aplica conocimientos y herramientas conjuntas del Derecho y la Informática para realizar análisis de datos en dispositivos con sistemas operativos Android, como resultado se obtiene pruebas que sirven como evidencia dentro de un proceso judicial.

La gran popularidad del sistema operativo Android ha provocado que, los hackers estén tentados en desarrollar herramientas sofisticadas para realizar ataques cibernéticos que, ponen en riesgo a todos los usuarios, de esta manera se genera que, a mayor demanda de este sistema, hay más posibilidades de ataque, por lo que, en la actualidad los agresores prefieren vulnerar las seguridades de los dispositivos móviles, además, los incidentes en cuanto a delitos informáticos se presenta, no solo a nivel de personas especializadas, sino que, también, a nivel de usuarios comunes. Existen múltiples guías que, pretenden encaminar en el procedimiento forense, pero, debido a la diversidad de fuentes el investigador podría confundirse en la aplicación de estas y llegar incluso a obviar ciertos lineamientos.

A nivel mundial se utiliza modelos para análisis forense de dispositivos móviles, especialmente, con sistemas Android que, es el más utilizado a nivel nacional e internacional, en nuestro medio se utilizan procesos no adecuados para realizar el análisis forense de equipos móviles, convirtiéndose en un problema porque, no se apega a la realidad de los procedimientos legales establecidos para la investigación de estas causas, además,

estos procedimientos no se los tiene a disposición o necesitan ser adquiridos para ser utilizados.

La falta de aplicación de la normativa legal vigente de los modelos en el Ecuador ha ocasionado que en muchas de las investigaciones no se aplique el proceso como corresponde, lo que conlleva a que, no se obtenga resultados satisfactorios en las investigaciones. Por lo expuesto anteriormente el problema se enuncia de la siguiente forma: ¿Cómo se puede solucionar la inaplicabilidad de los procesos legales vigentes en el análisis forense de los dispositivos móviles con sistema operativo Android?, con el diseño del modelo se propone el análisis forense a dispositivos móviles con sistema operativo Android con el que, se obtiene resultados acordes a los procesos legales vigentes.

El presente trabajo de investigación tiene por objeto diseñar un Modelo para Análisis Forense en Dispositivos Móviles con Sistema Operativo Android, denominado Modelo Basado en Dispositivos Móviles Android (MBDMA).

El modelo desarrollado tiene como objetivos específicos lo siguiente:

1. Identificar la base teórica para implementar procedimientos de análisis forense.
2. Determinar una metodología adecuada a los procesos legales vigentes para implementar el modelo propuesto.
3. Generar pruebas sobre el modelo planteado que permitan determinar procesos legales.
4. Comparar resultados obtenidos de la implementación del modelo.

La propuesta actual se basa en una metodología inductiva, puesto que, es flexible y permite el razonamiento para ser validado a través de pruebas. Al tratarse de un diseño de Modelo de Análisis Forense donde es necesario la interpretación de los resultados, por tanto, se recurre a la investigación cualitativa a través de los métodos; Bibliográfico que recopila investigaciones elaboradas anteriormente para realizar un análisis comparativo y Merise que, aporta con recursos como; estudio preliminar, análisis, diseño y puesta en marcha.

El (MBDMA), concede la aplicación de una guía apropiada en la investigación al permitir; asegurar la escena, identificar evidencias, adquirir datos, analizar datos y presentar informes apegados a las leyes penales y civiles del Ecuador. Esto contribuye al Sistema Judicial, constituyéndose en un factor decisivo dentro de un proceso penal. El modelo resulta

útil para los peritos informáticos que laboran en el sector público, también, para aquellos que apoyan de manera particular, con la investigación de procesos legales forenses, al aplicar principios de buena práctica. Con lo que, se justifica el desarrollo del presente trabajo.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Informática Forense

La Informática Forense es una disciplina que, permite identificar, adquirir, preservar y analizar evidencias mediante investigación al utilizar modelos y técnicas forenses en áreas específicas de casos penales y civiles, ésta permite que, se resuelvan disputas judiciales ante los tribunales, debido a esto, es necesario que investigadores y peritos posean un conocimiento en áreas técnicas. La Informática Forense permite detectar y recuperar datos e información digital y utilizar la misma como evidencia en el restablecimiento de un hecho y por tanto, ser utilizados como un valor demostrativo (Iorio, y otros, 2017)

Debido al desarrollo tecnológico al que, se está expuesto en los últimos tiempos, la petición de pericias informáticas 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 pericial.

Es necesario contar con personal técnico poseedor de conocimientos sólidos que permita actuar ordenada, sistemáticamente y apliquen métodos con el fin de, “identificar, adquirir, recuperar y analizar la información ya sea que, ésta se encuentre visible u oculta” (Iorio, y otros, 2017).

La Informática Forense aparece como necesidad para la investigación de los diferentes delitos que, afectan día a día a la sociedad, 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 las diferentes técnicas.

Es importante que, la información no sea modificada de ninguna manera, para lo cual, es necesario mantener la integridad de la evidencia, por lo que, es necesario seguir una metodología, la norma ISO/IEC 27037:2012 *Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence*, provee modelos para la identificación, sistematización, recolección, adquisición, y preservación de la información, esta norma se basa en tres elementos: relevancia, confiabilidad y suficiencia.

1.2. Informática Forense en dispositivos móviles

El incremento del uso de dispositivos móviles, debido al fácil acceso para adquirirlos y a su portabilidad, hace que, se convierta en una herramienta de comunicación necesaria en la vida de la sociedad actual, las personas realizan actividades económicas mediante este dispositivo, como por ejemplo, transacciones bancarias, compras en línea, contratos de comercio internacional solo para mencionar algunas de las actividades que realizan los usuarios a diario.

La utilización de este medio de comunicación ha generado algunos problemas de vulnerabilidad, un gran número de crímenes cibernéticos aparecen, en el medio local e internacional hay una deficiencia de organismos que, normalicen y vigilen el uso adecuado de los dispositivos móviles, además, que, el desconocimiento de las personas en cuanto a riesgos de actividades ilícitas en la información digital genera más inseguridad para que, esta sea vulnerada.

Esta Disciplina Forense surge como necesidad de generar un aporte significativo en las investigaciones, al cumplir fases y etapas definidas con la finalidad de detectar; hallazgos, delimitar debilidades, acciones no consentidas y determinar las principales causas de las diferentes infracciones realizadas en un dispositivo móvil. En consecuencia, se garantiza la accesibilidad, legalidad, responsabilidad, principios de transparencia según la Carta Iberoamericana de Gobierno Electrónico.

El avance de la tecnología de hardware - software en la telecomunicación ha establecido una nueva subdivisión dentro de las TIC, nace una nueva generación de herramientas tecnológicas de impacto en el sector empresarial. Las soluciones basadas en tecnologías móviles portables, tendencia que, hoy es sinónimo de producción (Gómez, Herrera, Moscoso, & Guamán, s. f.).

Los dispositivos móviles poseen grandes ventajas como: portabilidad, uso relativamente fácil y la posibilidad de mantener en contacto a los usuarios, esto permite a las personas encontrar varias maneras de permanecer comunicadas, pero, también, se ha proliferado el uso de esta tecnología en actividades ilícitas, de ahí que, una prueba digital podría o no, requerirse en un proceso legal, esto depende de lo que, considere el juez y la formalidad con la que, se presente las evidencias.

Para realizar un análisis forense digital se considerará lo siguiente: “Extracción y gestión de las evidencias, la extracción constituye un factor importante porque, depende de estas el resultado que, se halle, el manejo es cuidadoso con el fin de, precautelar la integridad” (Figueroa, Lara, Lesca, Viaña, & Binda, 2018).

1.2.1. Informática Forense en dispositivos móviles Android

El sistema más utilizado en dispositivos móviles es Android. Las empresas desarrolladoras de sistemas operativos envían actualizaciones constantes con la finalidad de, corregir vulnerabilidades existentes, 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 investigación forense pasa a formar parte fundamental para esclarecer estos hechos delictivos.

La investigación forense procede a realizar un análisis íntegro de los registros almacenados en un sistema. Es importante revisar bibliografía que permita la gestión de una causa pericial, con la finalidad de, proporcionar un informe detallado, los investigadores tienen a disposición; estándares, guías, y metodologías como:

ISO/IEC 27037: Directrices para la identificación, recopilación, adquisición y preservación de la evidencia digital. Es un documento que, publicó la Organización Internacional para la estandarización (ISO).

RFC 3227: Guía para recolectar y archivar evidencia. Proporciona sistemas, directrices para la recopilación y archivo de las pruebas en un incidente de seguridad.

UNE 71505: Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales. Proporcionan la información sobre los sucesos en un sistema de información.

UNE 71506: Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas. Define los procesos del análisis forense dentro del ciclo de gestión de evidencias electrónicas.

El seguimiento de métodos adecuados y las buenas prácticas hace que, el trabajo de los Magistrados en los procesos judiciales sea más eficiente, puesto que, la interpretación de los resultados será fácil de comprender, de esta manera se evita que cometan errores relacionados al análisis de detalles tecnológicos. (Álvares, 2016).

1.3. Modelos de análisis forense en dispositivos móviles

Los peritos informáticos necesitan modelos eficientes que, ayuden a mejorar los procedimientos a ejecutarse dentro del análisis forense, es necesario que, estas operaciones se sujeten a la normativa legal vigente, en la extracción de datos no se altera su estructura original para luego ser analizada y emitir el informe pericial. Se analiza los modelos existentes de diversos autores con el fin de, optar por los más eficientes, que, permitan obtener resultados óptimos en el análisis forense (Jaya, 2017).

1.3.1. Modelo Digital Forensic Research Workshops (DFRWS)

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

Figura 1. Fases (DFRWS)
Fuente: (Jaya, 2017).

- **Identificación.-** Esta etapa permite ejecutar el reconocimiento y determinar el tipo de suceso.
- **Preservación.-** Esta etapa contiene la cadena de custodia, para que, los datos no sean manipulados.
- **Recolección.-** Los datos son recolectados mediante la utilización de herramientas tecnológicas tanto de software como de hardware.
- **Inspección.-** Se analizan los datos recogidos los que, permitirán la reconstrucción de los hechos.
- **Análisis.-** Mediante el resultado del análisis de los datos se realiza la reconstrucción de los hechos.
- **Presentación.-** Se emite el informe pericial documentado con sus respectivas conclusiones.
- **Decisión.-** La información obtenida se constituye en un factor decisivo en el dictamen de la sentencia (Jaya, 2017)

1.3.2. Modelo *The Computer Forensics Field Triage Process Model* (CFFTPM).

El modelo (CFFTPM) se utiliza en investigaciones que, requieren resultados de manera inmediata porque, se estudia los datos en el lugar de los hechos, por lo que, no se realiza un análisis detallado, la aplicación de este dependerá del caso que, vaya a ser analizado, por el perito en los sistemas informáticos en cuestión (Rogers, Goldman, Mislan, Wedge, & Debrota, 2016).

Es muy importante tomar en cuenta que, el primer contacto con el sospechoso es un factor decisivo, porque, en ese momento son más colaborativos y francos en responder más interrogantes.

Este modelo tiene las siguientes guías:

- Indagar y recopilar pruebas inmediatamente.
- Identificar víctimas en riesgo.
- Guía de la investigación.
- Reconocer posibles implicados.
- Valorar la amenaza del infractor para las personas.

La integridad de los datos es un factor primordial para el desarrollo de un análisis anexo.

Las etapas del modelo CFFTPM, se muestran en la figura 2:

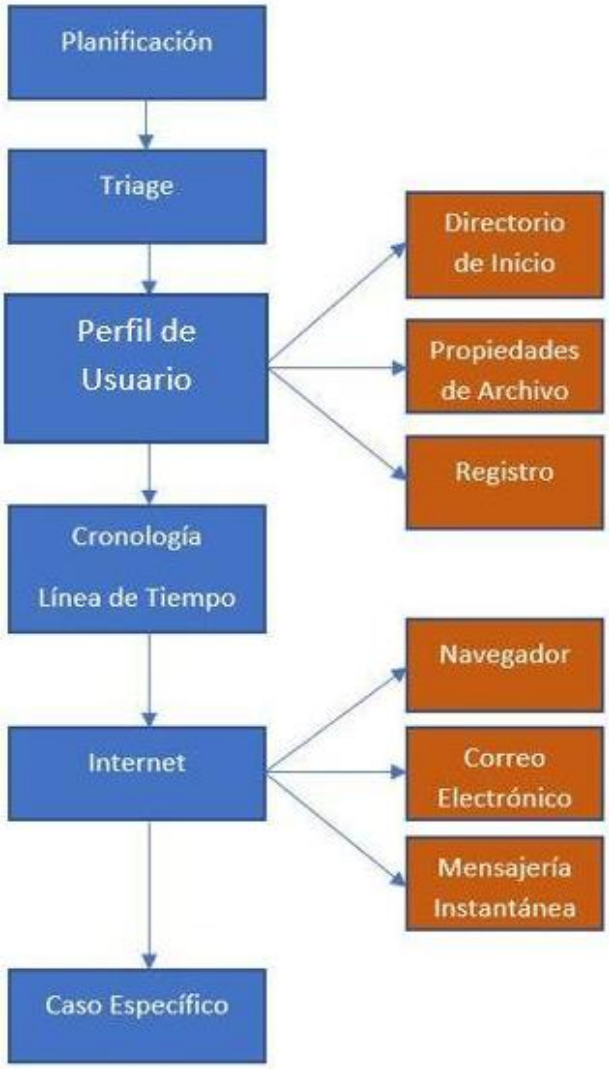

Figura 2. Fases (CFFTPM)
Fuente: (Rogers, Goldman, Mislan, Wedge, & Debrota, 2016)

- **Planificación.-** Al ser esta la primera etapa se realiza una matriz de cuantificación de los elementos del acontecimiento, que, permita precisar lo conocido y desconocido. Esta matriz contendrá los sucesos, los infractores, evidencia digital.
- **Triage.-** A partir de esta etapa se cimientan el resto de las etapas del modelo CFTTPM. Esta etapa tiene estrecha relación con el acontecimiento puesto que, enfatiza la evidencia física, digital y sospechoso. Es importante tener en cuenta que, cierta evidencia digital podría tener un periodo corto de duración como, por ejemplo,

los datos almacenados en una memoria *random access memory* (RAM). El investigador forense contará con las herramientas necesarias como un bloqueador de escritura con el fin de, precautelar la integridad de la información, además, del software necesario para el análisis de los datos en el lugar de los hechos. Los datos obtenidos en esta etapa serán ordenados según el nivel de importancia y procesados de acuerdo con el mismo.

- **Perfil de usuario.-** Con las evidencias de las etapas anteriores se realiza la reconstrucción de los sucesos y se crea un vínculo con el presunto infractor, lo cual, abre la posibilidad que, el sospechoso confiese el delito cometido. Es importante analizar que, el uso de los equipos informáticos no siempre es personal, un equipo podría usarse con varias cuentas e incluso una cuenta por varios usuarios, por lo que, es necesario realizar un a análisis de los perfiles de cada uno de ellos.
- **Directorio de inicio.-** En los sistemas operativos *Microsoft Windows* el directorio de inicio contiene varias carpetas como, por ejemplo; documentos, escritorio, imágenes, música, etc., para un usuario en específico. Esto sirve como medio probatorio del acto ilícito cometido por el o los sospechosos, cada usuario cuanta con una estructura de subdirectorios y solamente aquel que inicie sesión tendrá acceso a los archivos.
- **Propiedades de archivo.-** Estas resultan muy útiles porque revelan información del usuario que, lo creó, es decir, cada archivo que, se genere se guarda con los datos del usuario que inicio sesión, y no se modifica a menos que, tenga derechos administrativos.
- **Registro.-** El registro de Windows aloja información importante de todos los archivos utilizados, sin embargo, para esto el analista cuenta con conocimientos sólidos que, permitan obtener la información veraz.
- **Línea de tiempo.-** En una investigación forense digital la evidencia se valora por los tiempos de: modificación, acceso y creación (MAC). En el sistema operativo Windows los tiempos MAC se delimitan en los sistemas de archivos FAT32 y NTFS. Se considera como modificación a un archivo que, cambia su contenido, acceso es el momento en que, un archivo fue abierto, creación es el instante en que, un archivo fue creado.

  En esta etapa de la investigación se realizan mediciones con el fin de, clasificar los archivos mediante el análisis de las MAC, en primera instancia se analizan los

tiempos en que, usan la computadora o dispositivo tanto el sospechoso y demás usuarios, con lo que, determina que, usuario y que, actividades pudo realizar durante un determinado tiempo. También, el determinar las aplicaciones y archivos que, fueron usados durante este periodo de tiempo. Además, se debe, tomar en cuenta, el analizar la línea de tiempo no solo en las MAC sino en el archivo inex.dat, cookies de navegación y caché, considerar que los tiempos registrados varían según las diferentes zonas horarias.

- **Internet.-** En la mayor parte de casos será necesario ejecutar un análisis a los equipos para evaluar la utilización relacionada con el uso del internet como la mensajería, navegación web y correo electrónico, con el fin de, evaluar si estas actividades tienen relación con el caso de estudio.
- **Navegador.-** Es importante analizar la información contenida en el navegar como por ejemplo, las cookies que, muestran el localizador uniforme de recursos (URL) del sitio visitado el cual, indica la fecha y hora de acceso. También, se encuentra evidencia en la cache de navegación, donde se descarga información como las imágenes de páginas visitadas. El archivo index.dat igualmente, contiene información relevante como; sitios visitados y correo electrónico basado en web.
- **Correo electrónico.-** Este medio probatorio contiene una gran cantidad de información que, resulta útil en la investigación, para el análisis de este se requiere algunas horas de revisión lo que, implicará mayor inversión. Si el correo es basado en la web no existe almacenamiento local.
- **Mensajería instantánea.-** Las aplicaciones de mensajería generalmente guardan la información en sus servidores, por lo que, dificultan el acceso directo a los datos, lo que, complica la extracción de estos, en ciertas aplicaciones se mantiene registros de información que, son analizados por el investigador.
- **Caso específico.-** La destreza del investigador juega un papel importante en cada una de las investigaciones puesto que, existe una variedad de casos a ser tratados y analizados de manera personalizada, el tiempo es uno de los factores primordiales en la investigación. El investigador forense deberá, con anticipación planificar estrategias para ser utilizadas en el momento de analizar la escena (Rogers, Goldman, Mislan, Wedge, & Debrota, 2016).

1.3.3. Modelo Generic Computer Forensic Investigation Model (GCFIM)

El modelo (GCFIM), propuesto por Yunus Yusoff y sus colaboradores, esta investigación fue analizada a partir de modelos forenses creados entre el año 1985 hasta el año 2011, el trabajo dio como resultado cinco etapas genéricas de los modelos que, le anteceden, de esta manera se da inicio a este nuevo modelo (Satti & Jafari, 2015), como se observa en la figura 3.

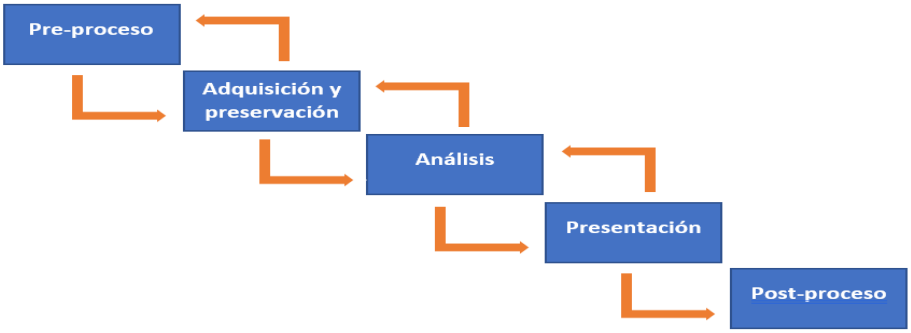

Figura 3. Fases (GCFIM)
Fuente: (Satti & Jafari, 2015)

- **Pre-proceso.-** Esta etapa se constituye en el pilar para las siguientes fases, se verificará el cumplimiento del uso adecuado de las herramientas a emplearse que, el grupo forense se encuentre capacitado, además, se diligenciará los procesos necesarios para la aplicación en el análisis como; permisos, preferencias y consentimientos.
- **Adquisición y preservación.-** A esta etapa se le atribuye subprocesos como el reconocimiento y recopilación de la prueba en el lugar de los hechos, la integridad de los datos será esencial en esta etapa, por lo que, se proporcionará seguridad en el transporte y almacenamiento para impedir cambios de la información obtenida que, será utilizada en la siguiente etapa.
- **Análisis.-** Se realizará una exploración a profundidad de los datos obtenidos en la etapa anterior y se ordena de acuerdo con la importancia con la que, se le considere para el análisis, además, se excluye información que, no sea relevante en el proceso.
- **Presentación.-** Se elabora la documentación; informes y reportes con respecto al análisis de los datos obtenidos en la etapa anterior.

- **Post-proceso.-** Etapa en la que, se presenta el informe pericial ante la función judicial. Lo que, ayudará a determinar si existe culpabilidad de él, o los implicados en la investigación (Satti & Jafari, 2015).

  Se enuncia tres modelos de Análisis Forense con la finalidad de realizar un estudio comparativo que, permita desarrollar un nuevo modelo acorde a las necesidades actuales de los peritos informáticos. El DFRWS se enfoca en preservar la integridad de la información mediante una cadena de custodia, este es útil al momento de manejar información en proporciones considerables. Por otro lado, el CFFTPM hace énfasis en la recopilación de la información en el lugar de los hechos, al proporcionar resultados de la pericia en el menor tiempo posible, lo que, elimina la necesidad del uso de un laboratorio forense fuera del sitio. Mientras que el GCFIM es flexible y se adapta a diversos escenarios, sin embargo, al proponer fases con un concepto general no permite ser implementado en casos reales, por lo que, se le considera como una directriz dentro del Análisis Forense.

1.4. Marco legal

Al tratarse del diseño de un modelo para Análisis Forense surge la necesidad de considerar la normativa legal vigente del Ecuador y cómo se aplica en las diferentes fases propuestas. Se describe algunos artículos y reglamentos importantes relacionados con el presente trabajo de investigación.

1.4.1. Código Orgánico Integral Penal (COIP)

(Código Integral Penal).- Establece una serie de sanciones relacionadas con los delitos informáticos y de telecomunicaciones en el Ecuador, en algunos de ellos:

Artículo 69 (2a)

2. Comiso penal, procede en todos los casos de delitos dolosos y recae sobre los bienes, cuando estos son instrumentos, productos o réditos en la comisión del delito. No habrá comiso en los tipos penales culposos. En la sentencia condenatoria, la o el juzgador competente dispondrá el comiso de:

a) Los bienes, fondos o activos, o instrumentos equipos y dispositivos informáticos utilizados para financiar o cometer la infracción penal o la actividad preparatoria punible (Código Orgánico Integral Penal, COIP, 2018).

Artículo 103.- Pornografía con utilización de niñas, niño o adolescentes.- La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual; será sancionada con pena privativa de libertad de trece a dieciséis años (Código Orgánico Integral Penal, COIP, 2018).

Si la víctima, además, sufre algún tipo de discapacidad o enfermedad grave o incurable, se sancionará con pena privativa de libertad de dieciséis a diecinueve años (Código Orgánico Integral Penal, COIP, 2018).

Cuando la persona infractora sea el padre, la madre, pariente hasta el cuarto grado de consanguinidad o segundo de afinidad, tutor, representante legal, curador o pertenezca al entorno íntimo de la familia; ministro de culto, profesor, maestro, o persona que por su profesión o actividad haya abusado de la víctima, será sancionada con pena privativa de libertad de veintidós a veintiséis años (Código Orgánico Integral Penal, COIP, 2018).

Artículo 173.- Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos. – La persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno a tres años (Código Orgánico Integral Penal, COIP, 2018).

Cuando el acercamiento se obtenga mediante coacción o intimidación, será sancionada con pena privativa de libertad de tres a cinco años (Código Orgánico Integral Penal, COIP, 2018).

La persona que suplantando la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad, será sancionada con la pena privativa de libertad de tres a cinco años (Código Orgánico Integral Penal, COIP, 2018).

Artículo 174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos.- La persona, que utilice o facilite el correo electrónico, chat,

mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad, será sancionada con pena privativa de libertad de siete a diez años (Código Orgánico Integral Penal, COIP, 2018).

Artículo 178.- Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años (Código Orgánico General de Procesos, COGEP, 2010).

No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley (Código Orgánico Integral Penal, COIP, 2018).

La retractación no constituye una forma de aceptación de culpabilidad.

Artículo 190.- Apropiación fraudulenta por medios electrónicos. - La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años (Código Orgánico Integral Penal, COIP, 2018).

La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes (Código Orgánico Integral Penal, COIP, 2018).

Artículo 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, será sancionada con pena privativa de libertad de uno a tres años (Código Orgánico Integral Penal, COIP, 2018).

Artículo 192.- Intercambio, comercialización o compra de información de equipos terminales móviles.- La persona que intercambie, comercialice o compre bases de datos que contengan información de identificación de equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años (Código Orgánico Integral Penal, COIP, 2018).

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

Artículo 194.- Comercialización ilícita de terminales móviles.- La persona que comercialice terminales móviles con violación de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años (Código Orgánico Integral Penal, COIP, 2018).

Artículo 195.- Infraestructura ilícita.- La persona que posea infraestructura, programas, equipos, bases de datos o etiquetas que permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil, será sancionada con pena privativa de libertad de uno a tres años (Código Orgánico Integral Penal, COIP, 2018).

No constituye delito, la apertura de bandas para operación de los equipos terminales móviles (Código Orgánico Integral Penal, COIP, 2018).

Artículo 229.- Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años (Código Orgánico Integral Penal, COIP, 2018).

Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen

intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años (Código Orgánico Integral Penal, COIP, 2018).

Artículo 230.- Interceptación ilegal de datos.- Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible (Código Orgánico Integral Penal, COIP, 2018).

2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder (Código Orgánico Integral Penal, COIP, 2018).

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares (Código Orgánico Integral Penal, COIP, 2018).

Artículo 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, será sancionada con pena privativa de libertad de tres a cinco años (Código Orgánico Integral Penal, COIP, 2018).

Con igual pena será 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 (Código Orgánico Integral Penal, COIP, 2018).

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general (Código Orgánico Integral Penal, COIP, 2018).

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad (Código Orgánico Integral Penal, COIP, 2018).

Artículo 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, será sancionada con la pena privativa de la libertad de tres a cinco años (Código Orgánico Integral Penal, COIP, 2018).

Artículo 354.- Espionaje.- La o el servidor militar, policial o de servicios de inteligencia que en tiempo de paz realice uno de estos actos, será sancionado con pena privativa de libertad de siete a diez años, cuando:

1. Obtenga, difunda, falsee o inutilice información clasificada legalmente y que su uso o empleo por país extranjero atente contra la seguridad y la soberanía del Estado (Código Orgánico Integral Penal, COIP, 2018).

2. Intercepte, sustraiga, copie información, archivos, fotografías, filmaciones, grabaciones u otros sobre tropas, equipos, operaciones o misiones de carácter militar o policial (Código Orgánico Integral Penal, COIP, 2018).

3. Envíe documentos, informes, gráficos u objetos que pongan en riesgo la seguridad o la soberanía del Estado, sin estar obligado a hacerlo o al haber sido forzado no informe inmediatamente del hecho a las autoridades competentes (Código Orgánico Integral Penal, COIP, 2018).

4. Oculte información relevante a los mandos militares o policiales nacionales (Código Orgánico Integral Penal, COIP, 2018).

5. Altere, suprima, destruya, desvíe, incluso temporalmente, información u objetos de naturaleza militar relevantes para la seguridad, la soberanía o la integridad territorial (Código Orgánico Integral Penal, COIP, 2018).

Si la o el servidor público realiza alguno o varios de estos actos en tiempo de conflicto armado, será sancionado con pena privativa de libertad de diez a trece años (Código Orgánico Integral Penal, COIP, 2018).

Artículo 456.- Cadena de custodia. - Se aplicará cadena de custodia a los elementos físicos o contenido digital materia de prueba, para garantizar su autenticidad, acreditando su identidad y estado original; las condiciones, las personas que intervienen en la recolección, envío, manejo, análisis y conservación de estos elementos y se incluirán los cambios hechos en ellos por cada custodio (Código Orgánico Integral Penal, COIP, 2018).

La cadena inicia en el lugar donde se obtiene, encuentra o recauda el elemento de prueba y finaliza por orden de la autoridad competente. Son responsables de su aplicación, el personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, el personal competente en materia de tránsito y todos los servidores públicos y particulares que tengan relación con estos elementos, incluyendo el personal de servicios de salud que tengan contacto con elementos físicos que puedan ser de utilidad en la investigación (Código Orgánico Integral Penal, COIP, 2018).

Artículo 471.- Registros relacionados a un hecho constitutivo de infracción.- No requieren autorización judicial las grabaciones de audio, imágenes de video o fotografía relacionadas a un hecho constitutivo de infracción, registradas de modo espontáneo al momento mismo de su ejecución, por los medios de comunicación social, por cámaras de vigilancia o seguridad, por cualquier medio tecnológico, por particulares en lugares públicos y de libre circulación o en los casos en que se divulguen grabaciones de audio o video obtenidas por uno de los intervinientes, en cuyo caso se requerirá la preservación de la integralidad del registro de datos para que la grabación tenga valor probatorio (Código Orgánico Integral Penal, COIP, 2018).

En estos casos, las grabaciones se pondrán inmediatamente a órdenes de la o el fiscal en soporte original y servirán para incorporar a la investigación e introducirlas al proceso y de ser necesario, la o el fiscal dispondrá la transcripción de la parte pertinente o su reproducción en la audiencia de juicio (Código Orgánico Integral Penal, COIP, 2018).

Artículo 475.- Retención de correspondencia. – La retención, apertura y examen de la correspondencia y otros documentos se regirá por las siguientes disposiciones:

1. La correspondencia física, electrónica o cualquier otro tipo o forma de comunicación, es inviolable, salvo los casos expresamente autorizados en la Constitución y en este Código (Código Orgánico Integral Penal, COIP, 2018).

2. La o el juzgador podrá autorizar a la o al fiscal, previa solicitud motivada, el retener, abrir y examinar la correspondencia, cuando haya suficiente evidencia para presumir que la misma tiene alguna información útil para la investigación (Código Orgánico Integral Penal, COIP, 2018).

3. Para proceder a la apertura y examen de la correspondencia y otros documentos que puedan tener relación con los hechos y circunstancias de la infracción y sus participantes, se notificará previamente al interesado y con su concurrencia o no, se leerá la correspondencia o el documento en forma reservada, informando del particular a la víctima y al procesado o su defensor público o privado. A falta de los sujetos procesales la diligencia se hará ante dos testigos. Todos los intervinientes jurarán guardar reserva (Código Orgánico Integral Penal, COIP, 2018).

4. Si la correspondencia u otros documentos están relacionados con la infracción que se investiga, se los agregará al expediente fiscal después de rubricados; caso contrario, se los devolverá al lugar de donde son tomados o al interesado (Código Orgánico Integral Penal, COIP, 2018).

5. Si se trata de escritura en clave o en otro idioma, inmediatamente se ordenará el desciframiento por peritos en criptografía o su traducción (Código Orgánico Integral Penal, COIP, 2018).

Artículo 476.- Interceptación de las comunicaciones o datos informáticos. - La o el juzgador ordenará la interceptación de las comunicaciones o datos informáticos previa solicitud fundamentada de la o el fiscal cuando existan indicios que resulten relevantes a los fines de la investigación, de conformidad con las siguientes reglas:

1. La o el juzgador determinará la comunicación interceptada y el tiempo de intercepción, que no podrá ser mayor a un plazo de noventa días. Transcurrido el tiempo autorizado se

podrá solicitar motivadamente por una sola vez una prórroga hasta por un plazo de noventa días (Código Orgánico Integral Penal, COIP, 2018).

Cuando sean investigaciones de delincuencia organizada y sus delitos relacionados, la interceptación podrá realizarse hasta por un plazo de seis meses. Transcurrido el tiempo autorizado se podrá solicitar motivadamente por una sola vez una prórroga hasta por un plazo de seis meses (Código Orgánico Integral Penal, COIP, 2018).

2. La información relacionada con la infracción que se obtenga de las comunicaciones que se intercepten durante la investigación serán utilizadas en el proceso para el cual, se las autoriza y con la obligación de guardar secreto de los asuntos ajenos al hecho que motive su examen (Código Orgánico Integral Penal, COIP, 2018).

3. Cuando, en el transcurso de una interceptación se conozca del cometimiento de otra infracción, se comunicará inmediatamente a la o al fiscal para el inicio de la investigación correspondiente. En el caso de delitos flagrantes, se procederá conforme con lo establecido en este Código (Código Orgánico Integral Penal, COIP, 2018).

4. Previa autorización de la o el juzgador, la o el fiscal, realizará la interceptación y registro de los datos informáticos en transmisión a través de los servicios de telecomunicaciones como: telefonía fija, satelital, móvil e inalámbrica, con sus servicios de llamadas de voz, mensajes SMS, mensajes MMS, transmisión de datos y voz sobre IP, correo electrónico, redes sociales, videoconferencias, multimedia, entre otros, cuando la o el fiscal lo considere indispensable para comprobar la existencia de una infracción o la responsabilidad de los partícipes (Código Orgánico Integral Penal, COIP, 2018).

5. Está prohibida la interceptación de cualquier comunicación protegida por el derecho a preservar el secreto profesional y religioso. Las actuaciones procesales que violenten esta garantía carecen de eficacia probatoria, sin perjuicio de las respectivas sanciones (Código Orgánico Integral Penal, COIP, 2018).

6. Al proceso solo se introducirá de manera textual la transcripción de aquellas conversaciones o parte de ellas que se estimen útiles o relevantes para los fines de la investigación. No obstante, la persona procesada podrá solicitar la audición de todas sus grabaciones, cuando lo considere apropiado para su defensa (Código Orgánico Integral Penal, COIP, 2018).

7. El personal de las prestadoras de servicios de telecomunicaciones, así como las personas encargadas de interceptar, grabar y transcribir las comunicaciones o datos informáticos tendrán la obligación de guardar reserva sobre su contenido, salvo cuando se las llame a declarar en juicio (Código Orgánico Integral Penal, COIP, 2018).

8. El medio de almacenamiento de la información obtenida durante la interceptación deberá ser conservado por la o el fiscal en un centro de acopio especializado para el efecto, hasta que sea presentado en juicio (Código Orgánico Integral Penal, COIP, 2018).

9. Quedan prohibidas la interceptación, grabación y transcripción de comunicaciones que vulneren los derechos de los niños, niñas y adolescentes, especialmente en aquellos casos que generen la revictimización en infracciones de violencia contra la mujer o miembros del núcleo familiar, sexual, física, sicológica y otros (Código Orgánico Integral Penal, COIP, 2018).

Artículo 477.- Reconocimiento de grabaciones. - La o el juzgador autorizará a la o al fiscal el reconocimiento de las grabaciones mencionadas en el artículo anterior, así como de vídeos, datos informáticos, fotografías, discos u otros medios análogos o digitales. Para este efecto, con la intervención de dos peritos que juren guardar reserva, la o el fiscal, en audiencia privada, procederá a la exhibición de la película o a escuchar el disco o la grabación y a examinar el contenido de los registros informáticos. Las partes podrán asistir con el mismo juramento (Código Orgánico Integral Penal, COIP, 2018).

La o el fiscal podrá ordenar la identificación de voces grabadas, por parte de personas que afirmen poder reconocerlas, sin perjuicio de ordenar el reconocimiento por medios técnicos (Código Orgánico Integral Penal, COIP, 2018).

Artículo 498.- Medios de prueba. - Los medios de prueba son:

1. El documento

2. El testimonio

3. La pericia (Código Orgánico Integral Penal, COIP, 2018)

Artículo 500.- Contenido digital. - El contenido digital es todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático,

incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí (Código Orgánico Integral Penal, COIP, 2018).

En la investigación se seguirán las siguientes reglas:

1. El análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de técnicas digitales forenses (Código Orgánico Integral Penal, COIP, 2018).

2. Cuando el contenido digital se encuentre almacenado en sistemas y memorias volátiles o equipos tecnológicos que formen parte de la infraestructura critica del sector público o privado, se realizará su recolección, en el lugar y en tiempo real, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido (Código Orgánico Integral Penal, COIP, 2018).

3. Cuando el contenido digital se encuentre almacenado en medios no volátiles, se realizará su recolección, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido (Código Orgánico Integral Penal, COIP, 2018).

4. Cuando se recolecte cualquier medio físico que almacene, procese o transmita contenido digital durante una investigación, registro o allanamiento, se deberá identificar e inventariar cada objeto individualmente, fijará su ubicación física con fotografías y un plano del lugar, se protegerá a través de técnicas digitales forenses y se trasladará mediante cadena de custodia a un centro de acopio especializado para este efecto (Código Orgánico Integral Penal, COIP, 2018).

1.4.2. Ley de comercio electrónico, firmas y mensajes de datos

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

Art. 5.- Confidencialidad y reserva. - Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada

conforme a lo dispuesto en esta ley y demás normas que rigen la materia (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

Art. 8.- Conservación de los mensajes de datos. - Toda información sometida a esta ley, podrá ser conservada; este requisito quedará cumplido mediante el archivo del mensaje de datos, siempre que se reúnan las siguientes condiciones:

a. Que la información que contenga sea accesible para su posterior consulta;

b. Que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida;

c. Que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado; y,

d. Que se garantice su integridad por el tiempo que se establezca en el reglamento a esta ley (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

La información que tenga por única finalidad facilitar el envío o recepción del mensaje de datos, no será obligatorio el cumplimiento de lo establecido en los literales anteriores (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

Art. 9.- Protección de datos. - Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales, podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo (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 entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe, para actuar conforme al contenido del mismo, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica, excepto en los siguiente 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 hará antes de que la persona que lo recibe actúe conforme a dicho mensaje (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

En caso contrario, quien conste como emisor deberá justificar plenamente que el mensaje de datos no se inició por orden suya o que el mismo fue alterado; y,

b) Si el destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o hizo caso omiso de su resultado (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

Art. 52.- Medios de prueba.- Los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta ley, cualquiera sea su procedencia o generación, serán considerados medios de prueba. Para su valoración y efectos legales se observará lo dispuesto en el Código de Procedimiento Civil (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

Art. 55.- Valoración de la prueba. - La prueba será valorada bajo los principios determinados en la ley y tomando en cuenta la seguridad y fiabilidad de los medios con los cuales se la envió, recibió, verificó, almacenó o comprobó si fuese el caso, sin perjuicio de que dicha valoración se efectúe con el empleo de otros métodos que aconsejen la técnica y

la tecnología. En todo caso la valoración de la prueba se someterá al libre criterio judicial, según las circunstancias en que hayan sido producidos (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

Para la valoración de las pruebas, el juez o árbitro competente que conozca el caso deberá designar los peritos que considere necesarios para el análisis y estudio técnico y tecnológico de las pruebas presentadas (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

Art. 57.- Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

Reformas al Código Penal

Art. 58.- A continuación del artículo 202, inclúyanse los siguientes artículos enumerados: "Art...- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica (Código Orgánico Integral Penal, COIP, 2018).

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica (Código Orgánico Integral Penal, COIP, 2018).

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, serán sancionadas con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica (Código Orgánico Integral Penal, COIP, 2018).

Si la divulgación o la utilización fraudulenta se realizan por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica (Código Orgánico Integral Penal, COIP, 2018).

Art...- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica (Código Orgánico Integral Penal, COIP, 2018).

Art. 59.- Sustitúyase el artículo 262 por el siguiente:

"Art. ...- 262.- Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados sin razón de su cargo (Código Orgánico Integral Penal, COIP, 2018).

Art. 60.- A continuación del artículo 353, agréguese el siguiente artículo innumerado:

"Art. ...- Falsificación electrónica. - Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio; alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;

2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;

3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho (Código Orgánico Integral Penal, COIP, 2018).

El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo.

Art. 61.-A continuación del artículo 415 del Código Penal, inclúyanse los siguientes artículos innumerados:

"Art. ...- Daños informáticos. - El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculado con la defensa nacional (Código Orgánico Integral Penal, COIP, 2018).

Art....- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimido con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica (Código Orgánico Integral Penal, COIP, 2018).

Art. 63.- Añádase como segundo inciso del artículo 563 del Código Penal, el siguiente:

"Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos (Código Orgánico Integral Penal, COIP, 2018).

1.4.3. Reglamento del Sistema Pericial Integral de la Función Judicial

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 tendrá 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 podrán presentar 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, tendrá 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 podrán solicitar plazos adicionales al antes establecido de forma excepcional y tomando en consideración las dificultades para la presentación del informe (Reglamento del Sistema Permicial Integral de la Función Judicial, 2014).

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; (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 Permicial 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 subirá sin los anexos al sistema informático que administra el proceso correspondiente, dejando constancia e incluyendo 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 Permicial Integral de la Función Judicial, 2014).

1.4.4. Código orgánico General de Procesos (COGEP)

Art. 176.- Objeciones a los testimonios. Las partes podrán objetar de manera motivada cualquier pregunta, en particular las que acarreen responsabilidad penal a la o el declarante, sean capciosas, sugestivas, compuestas, vagas, confusas, impertinentes o hipotéticas por opiniones o conclusiones. Se exceptúan las preguntas hipotéticas en el caso de los peritos dentro de su área de experticia. Podrán objetarse las respuestas de las o los declarantes que van más allá, no tienen relación con las preguntas formuladas o son parcializadas. Una vez realizada la objeción, la o el juzgador se pronunciará aceptándola o negándola (Código Orgánico General de Procesos, COGEP, 2010).

PRUEBA PERICIAL

SECCIÓN I

PERITO

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

acreditarse como peritos para ese proceso en particular (Código Orgánico General de Procesos, COGEP, 2010).

Concordancias: CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, Arts. 76

CÓDIGO CIVIL (LIBRO I), Arts. 41, 564.

Art. 222.- Declaración de peritos. La o el perito será notificado en su dirección electrónica con el señalamiento de día y hora para la audiencia de juicio o única, dentro de la cual sustentará su informe. Su comparecencia es obligatoria. En caso de no comparecer por caso fortuito o fuerza mayor, debidamente comprobado y por una sola vez, se suspenderá la audiencia, después de haber practicado las demás pruebas y se determinará el término para su reanudación. En caso de inasistencia injustificada, su informe no tendrá eficacia probatoria y perderá su acreditación en el registro del Consejo de la Judicatura. En la audiencia las partes podrán interrogarlo bajo juramento, acerca de su idoneidad e imparcialidad y sobre el contenido del informe, siguiendo las normas previstas para los testigos. Las partes tendrán derecho, si lo consideran necesario, a interrogar nuevamente al perito, en el orden determinado para el testimonio. En ningún caso habrá lugar a procedimiento especial de objeción del informe por error esencial, que únicamente podrá alegarse y probarse en la audiencia. Concluido el contrainterrogatorio y si existe divergencia con otro peritaje, la o el juzgador podrá abrir el debate entre peritos de acuerdo con lo previsto en este Código. Finalizado el debate entre las o los peritos, la o el juzgador, abrirá un interrogatorio y contrainterrogatorio de las partes, exclusivamente relacionado con las conclusiones divergentes de los informes. La o el juzgador conducirá el debate. Nota: Inciso primero reformado por artículo 30 de Ley No. 0, publicada en Registro Oficial Suplemento 517 de 26 de Junio del 2019 (Código Orgánico General de Procesos, COGEP, 2010).

Concordancias:

CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, Arts. 76, 179, 181

CÓDIGO ORGÁNICO GENERAL DE PROCESOS, COGEP, Arts. 222

CÓDIGO ORGÁNICO INTEGRAL PENAL, COIP, Arts. 505, 507, 533

Art. 223.- Imparcialidad del perito. La o el perito desempeñará su labor con objetividad e imparcialidad. Durante la audiencia de juicio o única podrán dirigirse a la o al perito, preguntas y presentar pruebas no anunciadas oportunamente orientadas a determinar su

parcialidad y no idoneidad, a desvirtuar el rigor técnico o científico de sus conclusiones así como cualquier otra destinada a solventar o impugnar su credibilidad. Nota: Inciso segundo reformado por artículo 30 de Ley No. 0, publicada en Registro Oficial Suplemento 517 de 26 de Junio del 2019 (Código Orgánico General de Procesos, COGEP, 2010).

Concordancias:

CÓDIGO ORGÁNICO GENERAL DE PROCESOS, COGEP, Arts. 222

SECCIÓN II

INFORME PERICIAL

Art. 224.- Contenido del informe pericial. Todo informe pericial deberá contener, al menos, los siguientes elementos: 1. Nombres y apellidos completos, número de cédula de ciudadanía o identidad, dirección domiciliaria, número de teléfono, correo electrónico y los demás datos que faciliten la localización del perito. 2. La profesión, oficio, arte o actividad especial ejercida por quien rinde el informe. 3. El número de acreditación otorgado por el Consejo de la Judicatura y la declaración de la o del perito de que la misma se encuentra vigente. 4. La explicación de los hechos u objetos sometidos a análisis. 5. El detalle de los exámenes, métodos, prácticas e investigaciones a las cuales ha sometido dichos hechos u objetos. 6. Los razonamientos y deducciones efectuadas para llegar a las conclusiones que presenta ante la o el juzgador. Las conclusiones deben ser claras, únicas y precisas (Código Orgánico General de Procesos, COGEP, 2010).

Art. 225.- Solicitud de pericia. Cuando alguna de las partes justifique no tener acceso al objeto de la pericia, solicitará en la demanda o contestación, reconvención o contestación a la reconvención, que la o el juzgador ordene su práctica y designe el perito correspondiente. El informe pericial será notificado a las partes con el término de por lo menos diez días antes de la audiencia, término que podrá ser ampliado a criterio de la o del juzgador y de acuerdo con la complejidad del informe (Código Orgánico General de Procesos, COGEP, 2010).

Concordancias:

CÓDIGO ORGÁNICO GENERAL DE PROCESOS, COGEP, Arts. 226, 227

Art. 226.- Informe pericial para mejor resolver. En caso de que los informes periciales presentados por las partes sean recíprocamente contradictorios o esencialmente divergentes sobre un mismo hecho, la o el juzgador podrá ordenar el debate entre sí de acuerdo con lo

dispuesto en el presente Código. Si luego del debate entre las o los peritos, la o el juzgador mantiene dudas sobre las conclusiones de los peritajes presentados, ordenará en la misma audiencia un nuevo peritaje, para cuya realización sorteará a una o un perito de entre los acreditados por el Consejo de la Judicatura, precisando el objeto de la pericia y el término para la presentación de su informe, el mismo que inmediatamente será puesto a conocimiento de las partes. En aquellos casos en que una de las partes sea representada por una o un defensor público o demuestre tener escasos recursos económicos, los honorarios y gastos del peritaje, podrán ser cubiertos por el Consejo de la Judicatura, a petición de esta (Código Orgánico General de Procesos, COGEP, 2010).

Concordancias:

CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, Arts. 75, 179, 181, 191, 192

CÓDIGO ORGÁNICO INTEGRAL PENAL, COIP, Arts. 505

Art. 227.- Finalidad y contenido de la prueba pericial. La prueba pericial tiene como propósito que expertos debidamente acreditados puedan verificar los hechos y objetos que son materia del proceso. Las partes procesales, podrán sobre un mismo hecho o materia, presentar un informe elaborado por una o un perito acreditado (Código Orgánico General de Procesos, COGEP, 2010).

PRUEBA PERICIAL SECCIÓN I

PERITO

Art. 221.- Perito. Es la persona natural o jurídica que por razón de sus conocimientos científicos, técnicos, artísticos, prácticos o profesionales está en condiciones de informar a la o al juzgador sobre algún hecho o circunstancia relacionado con la materia de la controversia. Aquellas personas debidamente acreditadas por el Consejo de la Judicatura estarán autorizadas para emitir informes periciales, intervenir y declarar en el proceso. En el caso de personas jurídicas, la declaración en el proceso será realizada por el perito acreditado que realice la pericia. En caso de que no existan expertos acreditados en una materia específica, la o el juzgador solicitará al Consejo de la Judicatura que requiera a la institución pública, universidad o colegio profesional, de acuerdo con la naturaleza de los conocimientos necesarios para la causa, el envío de una terna de profesionales que puedan acreditarse como peritos para ese proceso en particular (Código Orgánico General de Procesos, COGEP, 2010).

Concordancias:

CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, Arts. 76

CÓDIGO CIVIL (LIBRO I), Arts. 41, 564

Art. 222.- Declaración de peritos. La o el perito será notificado en su dirección electrónica con el señalamiento de día y hora para la audiencia de juicio o única, dentro de la cual sustentará su informe. Su comparecencia es obligatoria. En caso de no comparecer por caso fortuito o fuerza mayor, debidamente comprobado y por una sola vez, se suspenderá la audiencia, después de haber practicado las demás pruebas y se determinará el término para su reanudación. En caso de inasistencia injustificada, su informe no tendrá eficacia probatoria y perderá su acreditación en el registro del Consejo de la Judicatura. En la audiencia las partes podrán interrogarlo bajo juramento, acerca de su idoneidad e imparcialidad y sobre el contenido del informe, siguiendo las normas previstas para los testigos. Las partes tendrán derecho, si lo consideran necesario, a interrogar nuevamente al perito, en el orden determinado para el testimonio. En ningún caso habrá lugar a procedimiento especial de objeción del informe por error esencial, que únicamente podrá alegarse y probarse en la audiencia. Concluido el contrainterrogatorio y si existe divergencia con otro peritaje, la o el juzgador podrá abrir el debate entre peritos de acuerdo con lo previsto en este Código. Finalizado el debate entre las o los peritos, la o el juzgador, abrirá un interrogatorio y contrainterrogatorio de las partes, exclusivamente relacionado con las conclusiones divergentes de los informes. La o el juzgador conducirá el debate. Nota: Inciso primero reformado por artículo 30 de Ley No. 0, publicada en Registro Oficial Suplemento 517 de 26 de Junio del 2019 (Código Orgánico General de Procesos, COGEP, 2010).

Concordancias:

CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, Arts. 76, 179, 181

CÓDIGO ORGÁNICO GENERAL DE PROCESOS, COGEP, Arts. 223

CÓDIGO ORGÁNICO INTEGRAL PENAL, COIP, Arts. 505, 507, 533

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

reformado por artículo 30 de Ley No. 0, publicada en Registro Oficial Suplemento 517 de 26 de Junio del 2019 (Código Orgánico General de Procesos, COGEP, 2010).

Concordancias:

CÓDIGO ORGÁNICO GENERAL DE PROCESOS, COGEP, Arts. 224

SECCIÓN II

INFORME PERICIAL

Art. 224.- Contenido del informe pericial. Todo informe pericial deberá contener, al menos, los siguientes elementos: 1. Nombres y apellidos completos, número de cédula de ciudadanía o identidad, dirección domiciliaria, número de teléfono, correo electrónico y los demás datos que faciliten la localización del perito. 2. La profesión, oficio, arte o actividad especial ejercida por quien rinde el informe. 3. El número de acreditación otorgado por el Consejo de la Judicatura y la declaración de la o del perito de que la misma se encuentra vigente. 4. La explicación de los hechos u objetos sometidos a análisis. 5. El detalle de los exámenes, métodos, prácticas e investigaciones a las cuales ha sometido dichos hechos u objetos. 6. Los razonamientos y deducciones efectuadas para llegar a las conclusiones que presenta ante la o el juzgador. Las conclusiones deben ser claras, únicas y precisas (Código Orgánico General de Procesos, COGEP, 2010).

Art. 225.- Solicitud de pericia. Cuando alguna de las partes justifique no tener acceso al objeto de la pericia, solicitará en la demanda o contestación, reconvención o contestación a la reconvención, que la o el juzgador ordene su práctica y designe el perito correspondiente. El informe pericial será notificado a las partes con el término de por lo menos diez días antes de la audiencia, término que podrá ser ampliado a criterio de la o del juzgador y de acuerdo con la complejidad del informe (Código Orgánico General de Procesos, COGEP, 2010).

Concordancias:

CÓDIGO ORGÁNICO GENERAL DE PROCESOS, COGEP, Arts. 226, 227

Art. 226.- Informe pericial para mejor resolver. En caso de que los informes periciales presentados por las partes sean recíprocamente contradictorios o esencialmente divergentes sobre un mismo hecho, la o el juzgador podrá ordenar el debate entre sí de acuerdo con lo dispuesto en el presente Código. Si luego del debate entre las o los peritos, la o el juzgador mantiene dudas sobre las conclusiones de los peritajes presentados, ordenará en la misma

audiencia un nuevo peritaje, para cuya realización sorteará a una o un perito de entre los acreditados por el Consejo de la Judicatura, precisando el objeto de la pericia y el término para la presentación de su informe, el mismo que inmediatamente será puesto a conocimiento de las partes. En aquellos casos en que una de las partes sea representada por una o un defensor público o demuestre tener escasos recursos económicos, los honorarios y gastos del peritaje, podrán ser cubiertos por el Consejo de la Judicatura, a petición de esta (Código Orgánico General de Procesos, COGEP, 2010).

Concordancias:

CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, Arts. 75, 179, 181, 191, 192

CÓDIGO ORGÁNICO INTEGRAL PENAL, COIP, Arts. 505

Art. 227.- Finalidad y contenido de la prueba pericial. La prueba pericial tiene como propósito que expertos debidamente acreditados puedan verificar los hechos y objetos que son materia del proceso. Las partes procesales, podrán sobre un mismo hecho o materia, presentar un informe elaborado por una o un perito acreditado (Constitución de la Republica del Ecuador, 2008).

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Caracterización de la institución

Con más de 90 años de historia, la Universidad de las Fuerzas Armadas ESPE es considerada una de las más emblemáticas del país por su constante innovación y aporte al desarrollo productivo del Ecuador. Fundada en 1922, la Universidad se distingue por entregar soluciones prácticas a las necesidades y preocupaciones de la sociedad ecuatoriana, contribuyendo a la generación de nuevos conocimientos a través de la docencia, la investigación y la vinculación con la sociedad. En el 2014, fue cataloga por el prestigioso Ranking Mundial de Universidades QS entre las 250 mejores de América Latina y la cuarta mejor del Ecuador. Actualmente, nuestra universidad preside la REDU (Red de Universidades y Escuelas Politécnicas para la Investigación y Posgrados) conformada por más de 20 universidades ecuatorianas. La Universidad es parte del Sistema de Educación Superior del Ecuador, integrada por el campus matriz en Sangolquí, las sedes Latacunga y Santo Domingo de los Tsáchilas, así como las Unidades Académicas Especiales y el Instituto de Idiomas; cuenta con más de 13.000 estudiantes, entre civiles y militares, de ellos 8.309 son hombres y 5.606 son mujeres. Es un centro de educación superior público regulado por la Constitución de la República del Ecuador y la Ley Orgánica de Educación Superior. Luego de la firma del Estatuto de creación, el 26 de junio del 2013, y aprobado por el Consejo de Educación Superior (CES) (Universidad de las Fuerzas Armadas, 2018).

Misión

Formar profesionales e investigadores de excelencia, creativos, humanistas, con capacidad de liderazgo, pensamiento crítico y alto conciencia ciudadana; generar y aplicar el conocimiento científico; y transferir tecnología, en el ámbito de sus dominios académicos, para contribuir con el desarrollo nacional y atender las necesidades de la sociedad y de las Fuerzas Armadas (Universidad de las Fuerzas Armadas, 2018).

Visión

La Universidad de las Fuerzas Armadas- ESPE es reconocida, como un referente a nivel nacional y regional por su contribución en el ámbito de sus dominios académicos, al fortalecimiento de la Seguridad y la Defensa, bajo un marco de valores éticos, cívicos y de

servicio a la comunidad (https://www.espe.edu.ec/filosofia/) (Universidad de las Fuerzas Armadas, 2018).

En el Ecuador él uso de dispositivos móviles con sistema operativo Android se ha popularizado, esto conlleva a la posibilidad de ser involucrados en actos que, requieran de un análisis forense. Por esta razón se opta realizar el presente trabajo de investigación y se centra en el diseño del (MBDMA). Las pruebas de validez del modelo se ejecutan en el laboratorio forense de la Universidad de las Fuerzas Armadas (ESPE), este cuenta con el software y hardware necesario para la puesta en marcha.

2.2. Metodología de la investigación

Mediante la selección de una correcta metodología en el desarrollo del modelo (MBDMA), la recopilación, análisis e interpretación de los datos se convierte en una tarea sencilla, a fin de, establecer conclusiones. Para el presente trabajo, se ha seleccionado el siguiente tipo de investigación:

2.2.1. Investigación cualitativa

Para el modelo propuesto se establece la utilización de la investigación cualitativa que, permitió la obtención de información y datos de distintos modelos, para el análisis forense en dispositivos móviles con sistema operativo Android, las características del entorno donde se desarrolló los modelos, ventajas y desventajas del uso de modelos propuestos.

2.2.2. Método bibliográfico

Se usa este método porque, constituye el análisis de bibliografías, 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 nuestro país.

El constante avance tecnológico junto al crecimiento y desarrollo de la sociedad generan la necesidad de actualizar los modelos de análisis forense existentes. Para la aplicación se procede a la identificación de la información y recursos, se utiliza una metodología basada en la investigación bibliográfica de modelos y normas 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, contribuirá al esclarecimiento de crímenes digitales.

2.2.3. Técnicas e instrumentos de investigación

Se emplea la técnica de la observación mediante la revisión de modelos existentes para el análisis forense en dispositivos móviles con sistema operativo Android, con el objetivo de determinar la importancia de cada uno de los modelos y el aporte que estos han realizado a los profesionales de la investigación 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*.

A continuación, se muestra el cuadro comparativo de los modelos y sus fases citadas para análisis forense en dispositivos móviles con sistema operativo Android, tabla 1.

Tabla 1. Modelos para análisis forense

Fases		
DFRWS	CFFTPM	GCFIM
Identificación	Planificación	Pre-proceso
Preservación	Triage	Adquisición y preservación
Recolección	Perfil de usuario	Análisis
Inspección	Cronología de línea de tiempo	Presentación
Análisis	Internet	Post-proceso
Presentación	Caso específico	
Decisión		

Fuente: elaboración propia

Cuadro de ventajas y desventajas de los modelos citados para análisis forense en dispositivos móviles con sistema operativo Android, tabla 2.

Tabla 2. Ventajas y desventajas

Modelos de análisis forense					
DFRWS		CFFTPM		GCFIM	
Ventajas	Desventajas	Ventajas	Desventajas	Ventajas	Desventajas
Enfocado a cubrir todas las partes esenciales de la investigación forense.	No tiene procedimiento concreto.	Investigación en el lugar de los hechos.	El análisis forense depende de la destreza del investigador.	Flexibilidad en el estudio de los diferentes tipos de casos.	El grupo forense será capacitado constantemente.
Mantiene la cadena de custodio e integridad de los datos.	Modelo levemente estricto.	Optimización del tiempo para el peritaje.	Su uso es limitado puesto que la mayor parte de investigaciones requieren de un análisis detallado.	Obtención de las evidencias en el lugar de los hechos.	Requieren gastos adicionales, se necesita seguridad en el transporte y almacenamiento de los datos
Utiliza métodos para obtener datos escondidos.		Trato personalizado en cada caso.		Clasifica los datos más relevantes, y desecha aquellos que no son útiles.	
Actualizaciones periódicas.		Flexibilidad en el análisis de las evidencias, en caso de ser necesario un análisis de laboratorio.			

Fuente: elaboración propia

Como instrumento de investigación se usa la ficha de observación que, sirve para recolectar información relevante acerca de los modelos de análisis forense en dispositivos móviles con sistema operativo Android, estas fichas están representadas a través de cuadros informativos como se observa en la tabla 3 y comparativos como indica la tabla 4.

Tabla 3. Ficha de observación

Modelos para análisis forense			
Descripción	Modelos		
	DFRWS	CFFTPM	GCFIM
Se adapta a cualquier tipo de caso			
Minimiza el tiempo de respuesta			
Optimiza recursos			
Aplica la cadena de custodia			
Almacenamiento seguro de evidencia			
Análisis forense en el lugar de los hechos			
Inspecciona elementos a ser analizados			
Usa técnicas para la extracción de la información			
Aplica procedimientos de copias de seguridad			
Transporte seguro de posible evidencia			
Emite informes de resultados del análisis			

Fuente: elaboración propia

Tabla 4. Cuadro comparativo de fases y actividades - modelos estudiados

Cuadro comparativo de fases y actividades - modelos estudiados

DFRWS		CFFTPM		GCFIM	
Fases	Actividades	Fases	Actividades	Fases	Actividades
Identificación	Reconocimiento Tipo de suceso	Planificación	Matriz de evidencia digital	Pre-proceso	Selección de herramientas, personal capacitado, permisos, preferencias y consentimientos
Preservación	Cadena de custodia	Triage	Precautelar la integridad de la información y realiza el análisis de los datos en el lugar de los hechos	Adquisición y preservación	Reconocimiento, recopilación de pruebas, integridad de los datos
Recolección	Herramientas para recolectar datos	Perfil de usuario	Reconstrucción de los hechos, análisis de perfiles de usuario y registro del sistema operativo	Análisis	Ordena los datos según la importancia

Inspección	Análisis de datos	Línea de tiempo	Análisis y clasificación, modificación, acceso, creación de archivos, cookies, navegación y caché	Presentación	Elaboración de informes y reportes
Análisis	Reconstrucción de los hechos	Internet	Indagación del uso de: navegador, correo electrónico y mensajería instantánea	Post proceso	Presentación de informe ante la Función Judicial
Presentación	Informe pericial	Caso específico	Estudio de casos de manera personalizada		
Decisión	Dictamen de la sentencia				

Fuente: elaboración propia

2.3. Método Merise

Propone procedimientos como; análisis, concepción y gestión de proyectos, esto dentro del campo informático, al tratarse de un diseño de Modelo para Análisis Forense en Dispositivos Móviles con Sistema Operativo Android se toma como base en su desarrollo, en el medio no existe una metodología específica. Las fases con las que cuenta favorecen el avance de la presente investigación, estas se, describen a continuación.

2.3.1. Estudio preliminar

Proporciona un plan de trabajo, que, permite establecer cuáles son los recursos para utilizarse, los costos y el tiempo a emplearse, con la finalidad de optimizar cada uno de ellos, con este estudio se comprende las necesidades a la que se enfrenta los peritos informáticos. En esta fase se toma en cuenta los siguientes pasos:

- La observación.
- Análisis del modelo.
- Descripción del escenario presente.
- Diagnóstico.

El estudio preliminar considera la tabla 5 de observación, con base al análisis comparativo de los modelos citados anteriormente.

Tabla 5. Ficha de observación

Modelos para análisis forense			
Descripción	Modelos		
	DFRWS	CFFTPM	GCFIM
Se adapta a cualquier tipo de caso	✓	✓	✓
Minimiza el tiempo de respuesta		✓	
Optimiza recursos		✓	
Aplica la cadena de custodia	✓	✓	✓
Almacenamiento seguro de evidencia	✓		✓
Análisis forense en el lugar de los hechos		✓	
Inspecciona elementos a ser analizados	✓	✓	✓
Usa técnicas para la extracción de la información	✓	✓	✓
Aplica procedimientos de copias de seguridad	✓	✓	✓
Transporte seguro de posible evidencia	✓		✓
Emite informes de resultados del análisis	✓	✓	✓

Fuente: elaboración propia

2.3.2. Análisis

Se realiza un estudio de los modelos citados para Análisis Forense en Dispositivos Móviles con Sistema Operativo Android, se observa ciertas falencias que, se describe a continuación:

- Se identifica que, en el medio no existe modelos adecuados para el Análisis Forense en Dispositivos Móviles con Sistema Operativo Android, ninguno considera la documentación como respaldo en la pericia en cada una de las fases.
- Los modelos existentes no se apegan a la normativa legal vigente, por tanto, la creación de un nuevo modelo es factible.

2.3.3. Diseño

Una vez realizado el análisis de los modelos anteriores e identificado ciertos vacíos, se procede a diseñar el (MBDMA), usa técnicas nuevas que, permite un manejo adecuado de la investigación, hace énfasis en la importancia de la documentación como respaldo en cada una de las fases y la aplicación de la normativa legal vigente en el Ecuador, el diseño expuesto a continuación, ver figura 4.

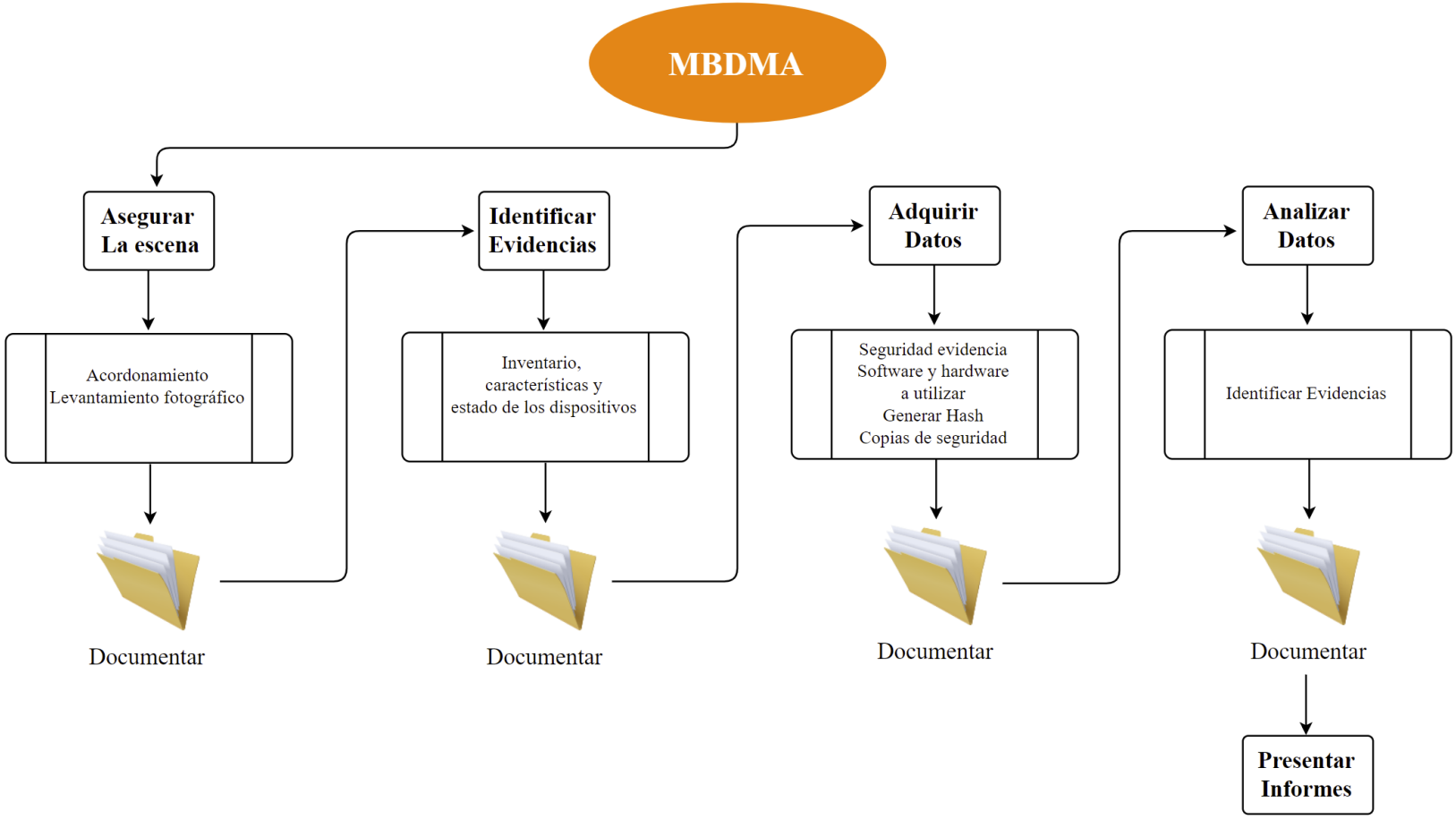

Figura 4. Fases (MBDMA)
Fuente: elaboración propia

- **Asegurar la escena.-** Esta actividad es coordinada con las personas encargadas de brindar seguridad del área donde se suscitó el evento motivo de investigación, con el objeto de asegurar las posibles evidencias, se procede con el acordonamiento del sitio, posteriormente se realiza un levantamiento fotográfico de la escena acordonada con el fin de, que, ésta quede documentada, de esta manera se inicia con la ejecución del modelo sugerido, para una correcta aplicación de la normativa legal vigente del Ecuador en esta fase se considera el art. 69 del COIP, artículos: 176, 221 y 227 del COGEP
- **Identificar evidencias.-** Se realiza una indagación de los equipos móviles que, se encuentre en el lugar de los hechos, los que, podrían contener información valiosa que contribuya en el proceso de investigación, en esta fase el perito informático realiza una valoración de las posibles evidencias motivo de análisis, verifica de esta manera que, los equipos no hayan sido manipulados, para salvaguardar la integridad de la información contenida en ellos, se procede a realizar el inventario de los dispositivos móviles identificados en la escena, queda documentado las características técnicas y el estado de el o los equipos identificados en la escena sujetos a investigación, para lo cual, se apoya en el uso de la ficha técnica ver tabla 6, en esta fase se considera los siguientes artículos del COIP 103, 173, 174, 178, 190, 192, 193, 194, 195 y 471, Ley de Comercio Electrónico artículos: 52, 55 y 58.

Tabla 6. Ficha de observación

Ficha técnica de dispositivos móviles						
Perito:						
Número de caso:						
Fecha:						
Hora:						
Item	Tipo	Marca	Serie	Modelo	Estado	Observaciones

Fuente: elaboración propia

- **Adquirir datos.-** En esta etapa es importante aplicar la cadena de custodia que, garantice; la protección de la información para que, esta sea la misma al inicio, durante y al final de la investigación. El objetivo de esta fase es la extracción de datos para posteriormente ser analizados, se toma en cuenta los siguientes aspectos:

- **Seguridad de la posible evidencia.-** El buen manejo de la evidencia en el sitio, transporte y almacenamiento garantiza la autenticidad y veracidad de los datos a ser analizados en la siguiente fase.
- **Determinar software y o hardware a utilizar.-** Es importante seleccionar herramientas que, ofrezcan garantías al momento de realizar imágenes de los dispositivos de almacenamiento y memoria en dispositivos móviles con sistema operativo Android. Para lo citado se describe algunas herramientas que, ayudan en la ejecución de este proceso:
  - MOBILedit Forensic Express
  - FTK (Forensic Toolkit)
  - Caine GNU/Linux (Computer Aided Investigative Environment)
  - DEFT Linux (Digital Evidence Forensic Toolkit)
  - EnCase
  - Lime (Linux memory extractor)
  - Santoku.
- **Generar *Hash*.-** La integridad de la información es esencial en los procesos de análisis forense informático, el *Hash* permite comprobar si los datos originales fueron alterados, esto es, posible mediante la generación de un código único que, muestra la identidad de la información, el mismo que, cambia si los datos han sido manipulados por agentes externos.
- **Realizar copias de seguridad.-** Crear las copias de seguridad es uno de los procesos más importantes que, se aplica en el análisis forense informático, ayuda a evitar pérdida de información en el proceso pericial. Se utiliza herramientas de hardware o software que, empleen bloqueadores de escritura, con el objeto de garantizar un respaldo correcto bit a bit de los dispositivos móviles con sistema operativo Android, de los cuales, se realizará copias de seguridad del almacenamiento y memoria. La eficacia de las copias de seguridad se constituye en un factor decisivo en el proceso de investigación.

Para documentar la fase de adquisición de datos se empleará la siguiente ficha de registro, ver tabla 7. Los artículos del COIP a considerar en esta etapa son: 229, 230, 232, 234, 456, 470, 475, 476 y 500, Ley de Comercio Electrónico artículos: 5, 8, 9 y 10.

Tabla 7. Ficha para el registro de imagen forense

Ficha: para el registro de imagen forense				
Perito:		Dispo		
Número de caso:		Marca:		
Fecha:		Serie:		
Hora:		Modelo:		
Ítem	Has	Estado del respaldo	Herramienta utilizada	Observaciones

Fuente: elaboración propia

- **Analizar datos. -** Una vez realizadas las copias de seguridad en la etapa anterior, se procede a una revisión exhaustiva de los mismos con el fin de, identificar evidencias, para aportar en la toma de decisiones dentro de un proceso judicial. Es importante seleccionar la o las herramientas adecuadas en el análisis de datos, con el propósito de obtener resultados satisfactorios, para ello, se cita algunas herramientas comerciales y libres que, se podrían usar en el análisis de datos:
  - Caine GNU/Linux.
  - Forensic Explorer.
  - Autopsy.
  - DiskDigger.
  - Bulk Extractor.
  - EnCase.
  - Santoku.

Las evidencias encontradas en esta fase se documenta en una guía ilustrativa con las capturas realizadas del proceso de análisis de datos, en esta fase se toma valora el artículo 500 del COIP, articulo 52, 55, 59 y 61 de la Ley de Comercio Electrónico.

- **Presentar informes.-** De acuerdo con las evidencias extraídas se procede a realizar el informe pericial, este será explícito de tal manera que, la información facilite el trabajo de los funcionarios judiciales, entidad, órgano o persona natural que, requiera este tipo de investigación, el informe contendrá anexos de las evidencias encontradas que, servirá como respaldo de la investigación realizada por el perito.

En Ecuador, existe un modelo de informe pericial definido por el Consejo de la Judicatura, este será utilizado para procesos de investigación forense solicitadas por parte de

la Función Judicial, como lo dictamina el artículo 19 y 20 del Reglamento. Este aporta en la toma de decisiones en el momento de ejecutar la sentencia y ayuda a determinar la culpabilidad o inocencia del posible implicado.

Para la elaboración del informe pericial se sugiere los siguientes pasos:

- Datos informativos.
- Objeto de la investigación pericial.
- Descripción del análisis forense digital.
- Documentación de evidencias encontradas.
- Conclusiones.
- Firmas de responsabilidad.
- Anexos.

Es importante tener en cuenta los artículos: 222, 223, 224, 225 y 227 del COGEP.

2.3.4. Puesta en marcha

En necesario verificar la factibilidad del modelo propuesto basado en análisis forense en dispositivos móviles con sistema operativo Android, en el laboratorio forense de la Universidad de las Fuerzas Armadas ESPE, apoyado en múltiples pruebas a través de los cuales, se determine la validez. En esta etapa se utiliza herramientas de hardware y software, técnicas y experticia del perito informático con el fin de, evaluar la eficacia del modelo citado.

CAPÍTULO III. APLICACIÓN DEL MODELO PROPUESTO Y ANÁLISIS DE RESULTADOS

3.1. Aplicación del modelo

Este capítulo se enfoca en realizar pruebas de validación para la propuesta del modelo de análisis forense, de modo que, se pondrá en práctica las técnicas mencionadas, en un escenario de prueba, el que, permitirá realizar un análisis de resultados del dispositivo móvil sujeto de estudio. Seguido se inicia con la comprobación del modelo para análisis forense en dispositivos móviles con sistema operativo Android (MBDMA).

3.1.1. Espacio y herramientas

Para la aplicación del modelo se determina como lugar de investigación el laboratorio forense de la Universidad de las Fuerzas Armadas (sede Sangolquí), este espacio se encuentra diseñado con equipos y herramientas que, facilitan el trabajo del perito informático. Para proceder con el ensayo se dispone de los siguientes recursos: Computador, programa *Autopsy*, Sistema Operativo *Santoku* y *Caine*.

3.2. Primer ensayo

Como elemento probatorio para la factibilidad del modelo (MBDMA), se analiza el siguiente caso experimental, en un escenario en el que, los nombres de las personas y empresa han sido creados con motivo de estudio, sin mencionar identidades reales.

La empresa Ecucargo mediante oficio OF-07032021 se pone en contacto con el Ing. Klever Beltrán con el objeto de solicitar una investigación pericial en la que, se le involucra a María Cortez quien mantuvo relaciones comerciales con la empresa mencionada para realizar compras en el exterior, quien utiliza una tarjeta de crédito posiblemente sustraída. Para coordinar estas acciones se mantuvo una conversación con Sofía Pérez asistente de compras de la empresa Ecucargo mediante el aplicativo WhatsApp. La empresa solicita la pericia al ser demandada por parte del señor José Sánchez propietario de la tarjeta de crédito quién afirma realizaron compras sin su autorización.

Ecucargo provee de dispositivos móviles a sus trabajadores para mantener conversaciones vía chat con sus clientes, al confirmar la demanda la dirección administrativa de la empresa procede a incautar el dispositivo móvil de Sofía Sánchez con el objeto de verificar la

conversación con María Cortez, sin embargo, una vez realizada la indagación observa que algunos mensajes fueron eliminados de la conversación, por tanto, solicita se recupere los mensajes suprimidos.

Descripción de las características del equipo incautado:

- Teléfono celular marca Samsung j2 core.
- Modelo SM-J260M
- Sistema operativo Android
- Versión del Android 8.1.0
- Parche de seguridad Android 1 de diciembre de 2020
- Memoria Ram 879 Mb.
- Procesador ARM Cortex-A53
- CPU 4 cores 1.43GHz.
- Almacenamiento interno de 16 Gb.

3.3. Modelo propuesto (MBDMA)

A continuación, se desarrolla el modelo propuesto una vez que se identificó el dispositivo móvil motivo de investigación.

3.3.1. Asegurar la escena

En esta fase al tratarse de un ambiente de prueba se procede a colocar el dispositivo móvil en un espacio adecuado que brinde las comodidades necesarias que, amerita el caso, posteriormente se documenta la escena mediante un archivo fotográfico, ver figura 5.

Figura 5. Dispositivo móvil
Fuente: elaboración propia

3.3.2. Identificar evidencias

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, este factor es importante puesto que, esto permitirá el acceso a las bases de datos de la aplicación WhatsApp, se procede a documentar como se muestra a continuación, ver figura 6 y tabla 8.

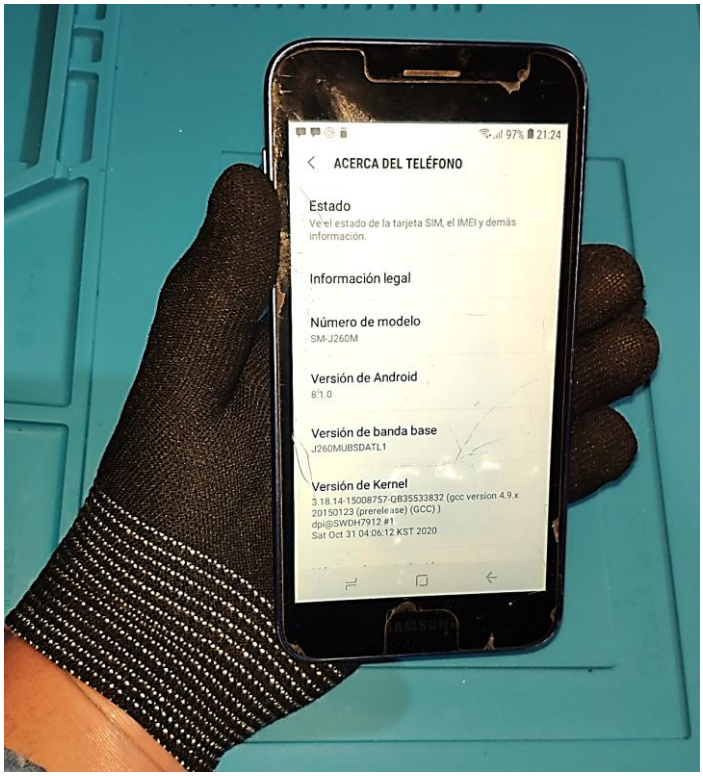

Figura 6. Documentación del equipo
Fuente: elaboración propia

Tabla 8. Ficha de observación dispositivos móviles

Ficha técnica de dispositivos móviles

Perito: Klever Beltrán

Número de caso: 001

Fecha: 9-marzo-2021

Hora: 14:00

Item	Tipo	Marca	Serie	Modelo	Estado	Observaciones
1	Celula	Samsung	89bee74a	SM-J260M	Bueno	Encendido

Fuente: elaboración propia

3.3.3. Adquisición de datos

Se garantiza la seguridad de la evidencia al aplicar la cadena de custodia en el área de trabajo designada del laboratorio forense de la ESPE, se toma como muestra las bases de datos de WhatsApp instalado en el dispositivo móvil con sistema operativo Android, de dónde se borró mensajes que, contenía información como: cuentas de usuario, claves de acceso y números de tarjeas de crédito, correspondientes a transacciones comerciales realizadas en tiendas virtuales en el exterior, ver figura 7.

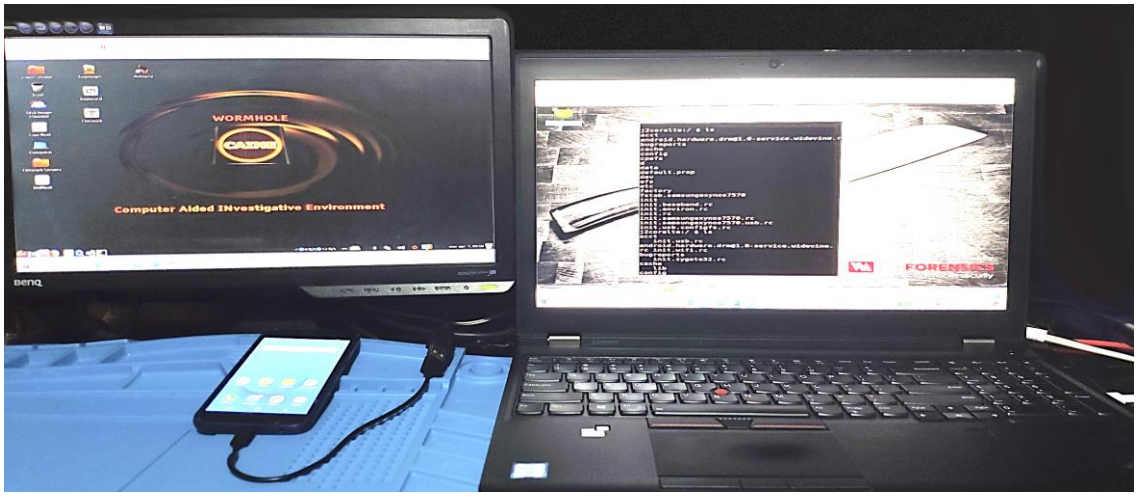

Figura 7. Adquisición de datos
Fuente: elaboración propia

Con el fin de, obtener los datos de la evidencia se utiliza el sistema operativo *Santoku* que, es una distribución libre basada en Linux, permite la ejecución de herramientas para adquirir y analizar datos de forma forense.

Para la administración de la comunicación entre el dispositivo móvil con sistema operativo Android y el sistema operativo *Santoku*, se debe previamente habilitar en la configuración del móvil la depuración por USB dentro del modo desarrollador, ver figura 8.

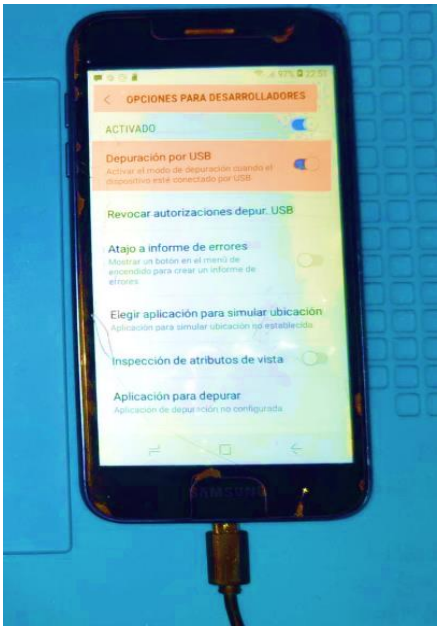

Figura 8. Depuración por USB
Fuente: elaboración propia

El dispositivo móvil tendrá privilegios *root*, el cual, permita acceder a la información sin restricciones de tal manera que se admita utilizar la herramienta adb y dd para explorar y obtener la imagen forense del dispositivo, ver figura 9.

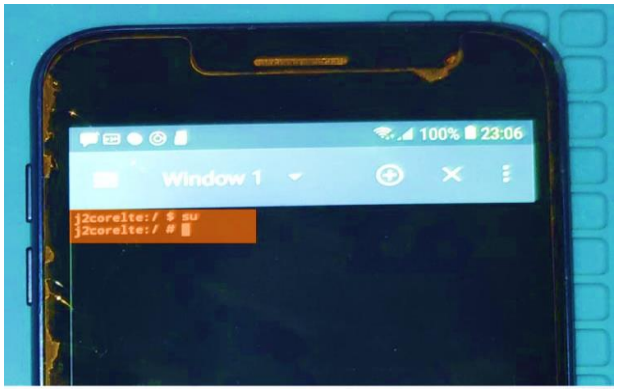

Figura 9. Privilegios *root*
Fuente: elaboración propia

Para precautelar la integridad de la información, se procede a realizar la copia forense del dispositivo móvil, mediante el uso del sistema operativo *Santoku*, para lo cual, se conecta el móvil mediante el puerto USB, se abre la terminal y se lanza el comando adb *devices* para verificar que, hay comunicación con el móvil, ver figura 10.

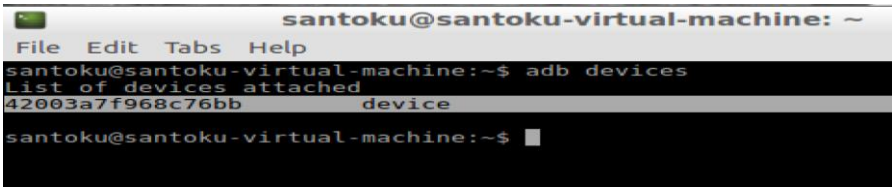

Figura 10. Comando adb *devices*
Fuente: elaboración propia

Una vez verificada la conexión con el móvil, se procede a ejecutar el comando adb shell el cual, permite controlar el dispositivo en modo texto, ver figura 11.

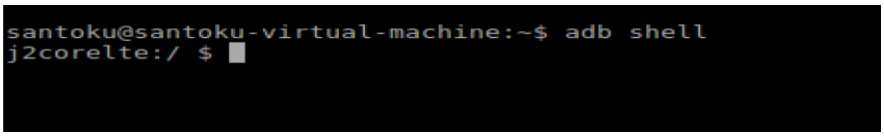

Figura 11. Comando adb shell
Fuente: elaboración propia

La identificación de la partición (mmcblk0), en donde se creará la imagen forense, esta contiene toda la información del dispositivo móvil, se utiliza el comando: ls -la /dev/block/platform/*/, ver figura 12.

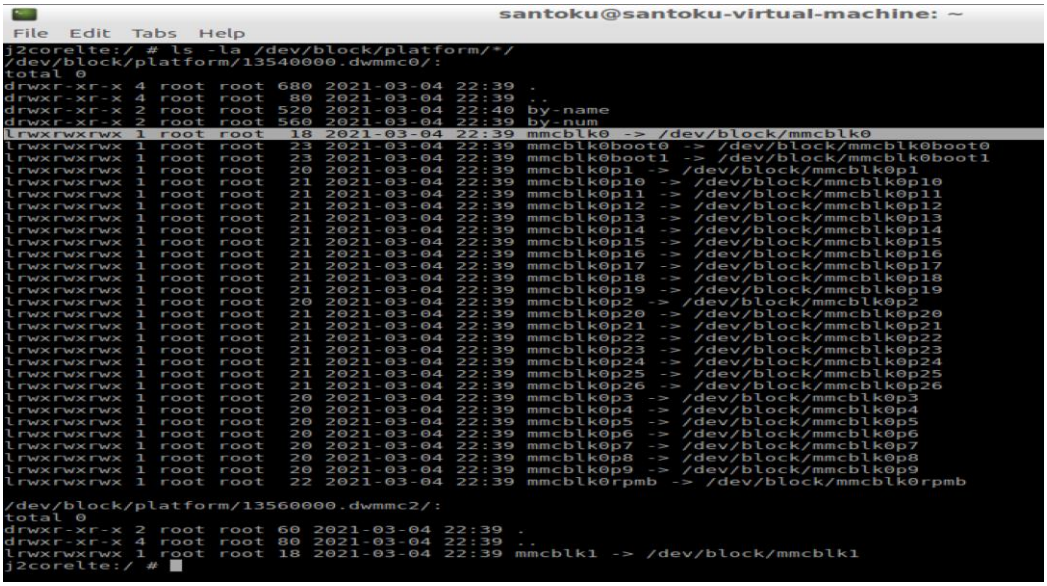

Figura 12. Comando ls -la /dev/block/platform/*/
Fuente: elaboración propia

Para obtener la imagen forense se utiliza la herramienta netcat que, se instala en el dispositivo móvil, esta se consigue a través de la aplicación *BusyBox*, el procedimiento se lo realiza para transferir la imagen desde el móvil hacia el ordenador, evita así errores

producidos por falta de espacio en el dispositivo señalado, una vez realizada esta acción abrir una terminal como usuario *root* y ejecutar: adb *forward* tcp:8888 tcp:8888 que permite reenviar los puertos del ordenador a través del adb, ver figura 13.

Figura 13. Creación de la imagen forense
Fuente: elaboración propia

Creación de una imagen de la partición (mmcblk0) motivo de estudio, la que, contiene toda la información del dispositivo móvil a través de la herramienta dd: dd if=/dev/block/mmcblk0 | busybox nc -l -p 8888, este a la vez activa la conexión de netcat y coloca el puerto 8888 en modo escucha, ver figura 14.

Figura 14. Creación de la imagen forense
Fuente: elaboración propia

Creación de una conexión con la maquina a través del netcat y el puerto 8888 y se guarda la imagen con un nombre y extensión (imagen-android.dd), ver figura 15.

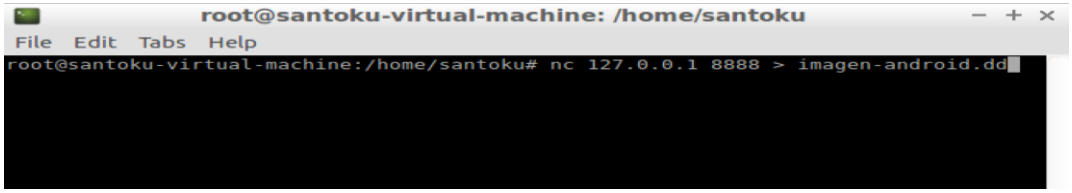

Figura 15. Conexión netcat
Fuente: elaboración propia

Finalmente, se observa la imagen creada, como indica la figura 16.

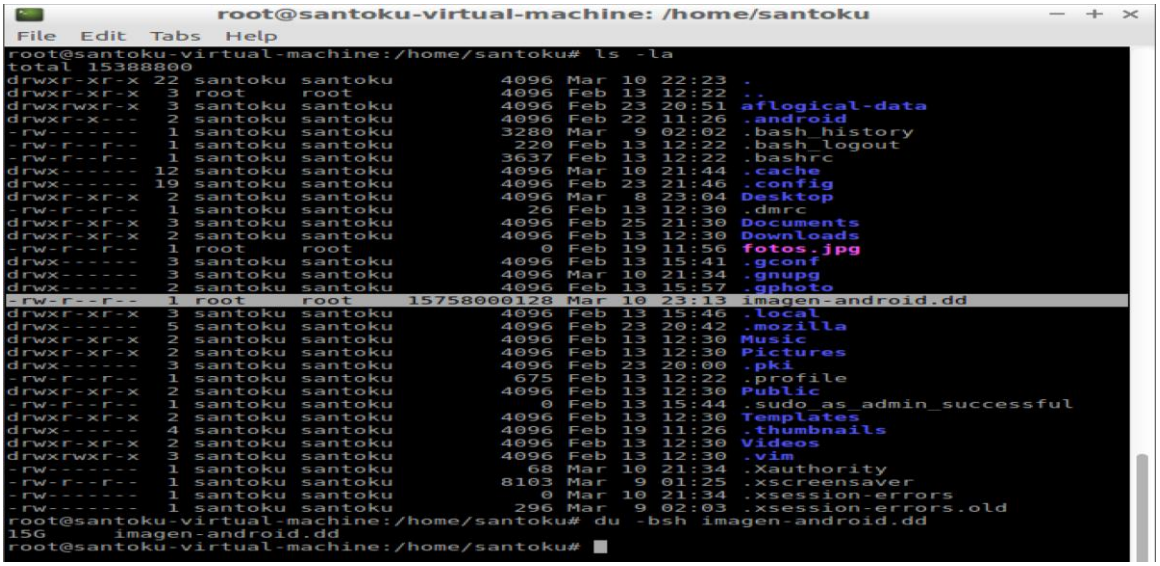

Figura 16. Imagen forense
Fuente: elaboración propia

Con la finalidad de, precautelar la integridad de la información se procede a generar los hashes (md5, sha224, sha256) de la imagen, esto se utiliza como medio probatorio en caso de que sea modificada en el transcurso del análisis forense, ver imagen 17.

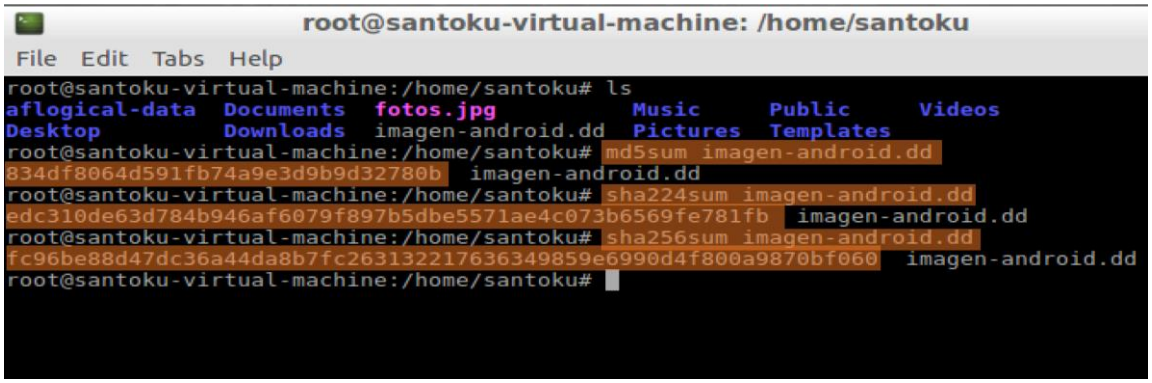

Figura 17. Hashes
Fuente: elaboración propia

En esta fase se adquiere la imagen forense para posteriormente analizarla, con el fin de, obtener la evidencia necesaria y emitir el informe final, se documenta los hashes que, garantiza la integridad de la imagen forense como se muestra en la tabla 9.

Tabla 9. Ficha para el registro de imagen forense

Ficha: para el registro de imagen forense

Perito: Klever Beltrán	Dispositivo: Celular
Número de caso: 001	Marca: Samsung
Fecha: 10 de marzo del 2021	Serie: 89bee74a
Hora: 23:13	Modelo: m1807e8a

Item	Hash	Estado del respaldo	Herramienta utilizada	Observaciones
1	MD5 834df8064d591fb74a9e3d9b9d32780b	Satisfactorio	dd(Linux)	Ninguna
	SHA224 edc310de63d784b946af6079f897b5dbdbe5571ae4c073b6569fe781fb	Satisfactorio	dd(Linux)	Ninguna
	SHA256 fc96be88d47dc36a44da8b7fc2631322176363498 59e6990d4f800a9870bf060	Satisfactorio	dd(Linux)	Ninguna

Fuente: elaboración propia

3.3.4. Analizar datos

En esta fase se explica el proceso para realizar el análisis de los datos que, permita identificar la información motivo de estudio. Una vez calculado los hashes (md5, sha224, sha256), copiar la imagen forense a un dispositivo externo para proceder a analizarla, se utiliza la distribución GNU/Linux *CAINE* (Entorno de investigación asistido por computadora)

Se procede a realizar una copia de la imagen forense desde el dispositivo externo hacia el *CAINE*, antes de realizar el análisis, para verificar los hashes con el propósito de comprobar que, la información no haya sido modificada, ver figura 18.

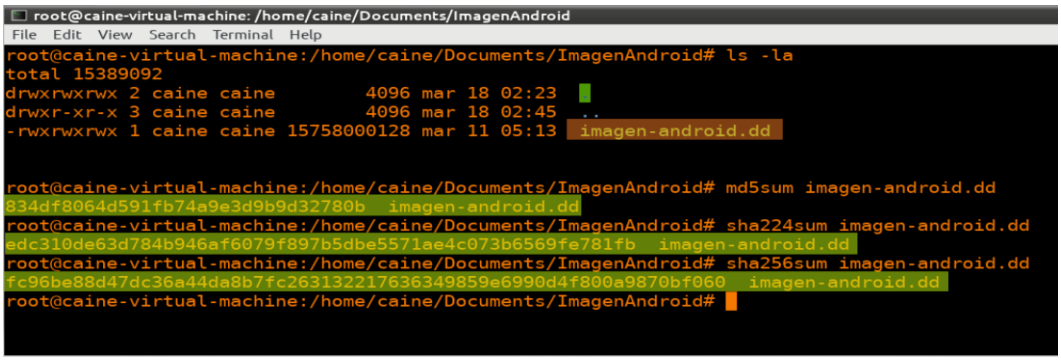

Figura 18. Verificación de Hashes
Fuente: elaboración propia

Al observar los diferentes hashes y poder verificar que, no han cambiado, se certifica la integridad de los datos, para continuar con el análisis se monta la imagen forense con la herramienta *Disk Image Mounter*, ver figura 19.

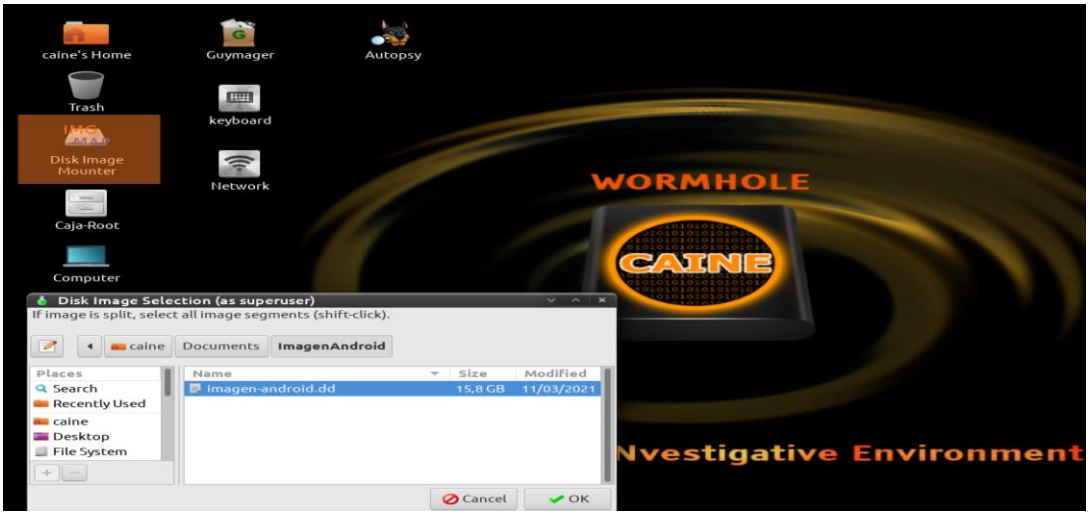

Figura 19. *Disk Image Mounter*.
Fuente: elaboración propia

El siguiente paso es abrir la terminal, con la finalidad de, verificar que, las particiones de la imagen forense se haya montado de manera exitosa, para esto hay que, ubicarse en el directorio /media y ejecutar el comando: ls -la para observar las particiones montadas como se indica en la figura 20.

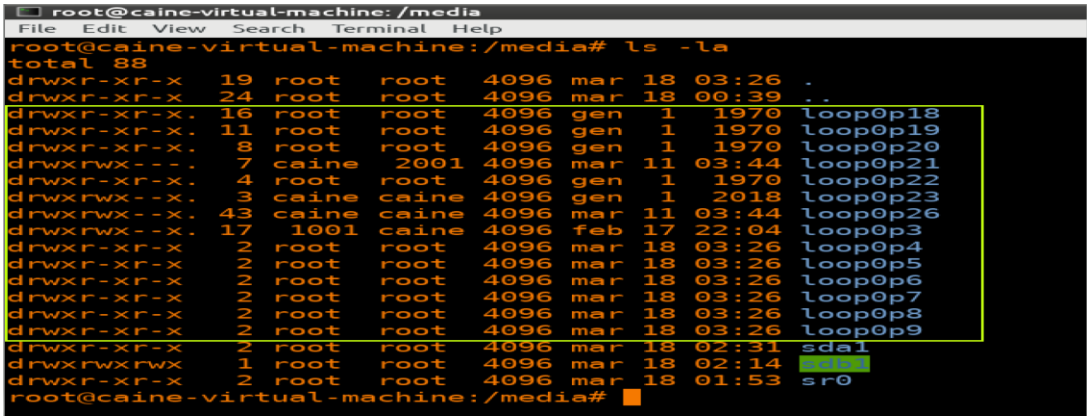

Figura 20. Particiones de la imagen forense
Fuente: elaboración propia

El tener claro la partición que contiene los datos que, proporcionará la información indagada, en este caso el contenido de los mensajes eliminados del aplicativo WhatsApp se encuentra en la partición loop0p26, para llegar al archivo (msgstore.db-wal), que, contiene

la información y se dirige a la ruta: /media/loop0p26/data/com.whatsapp/ en dónde se ejecuta el comando ls -la como se muestra en la figura 21.

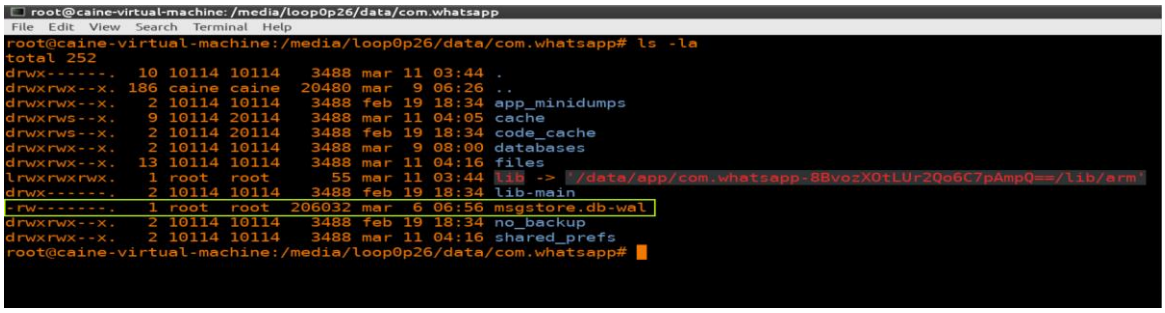

Figura 21. Base de datos de mensajes eliminados
Fuente: elaboración propia

Es importante analizar la conversación establecida en la aplicación WhatsApp del dispositivo móvil con sistema operativo Android, con el objeto de identificar los mensajes eliminados, facilita la búsqueda de la información suprimida. En el dialogo se visualiza claramente que, existe un mensaje borrado, por tanto, se deduce que, pertenece a la cuenta y clave de usuario que, se desea recuperar como se muestra en la figura 22.

Figura 22. Evidencia de mensaje eliminado
Fuente: elaboración propia

El tener un grado de conocimiento, destreza, técnicas y herramientas facilita la identificación de la información requerida. En este caso se procede analizar la base de datos (msgstore.db-wal) que, contiene los mensajes suprimidos, para esto, abrimos una terminal en *CAINE* y ubicarse en la ruta donde se encuentra la base de datos, digitar el comando *strings* de Linux seguido del nombre de la base datos (/strings msgstore.db-wal), donde se observa su contenido como se muestra en la figura 23.

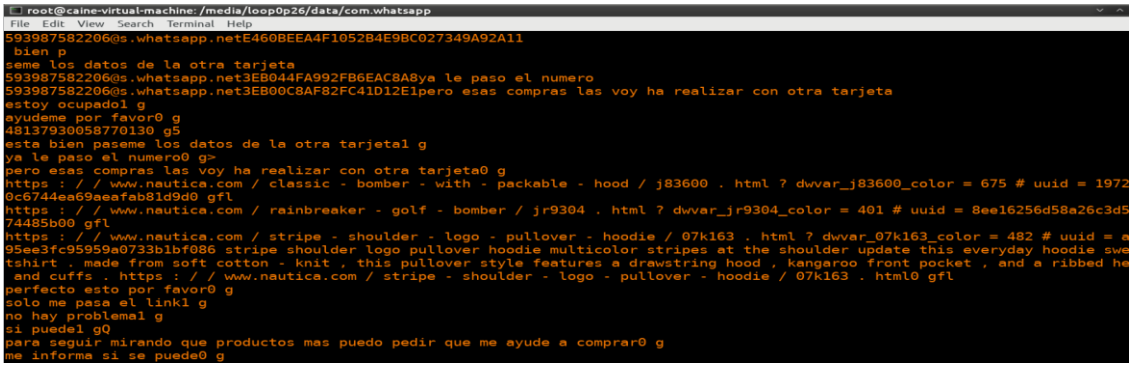

Figura 23. Comando *strings*
Fuente: elaboración propia

Luego de realizar un análisis profundo y la aplicación de técnicas y herramientas al contenido de la base de datos se logró identificar la información que fue eliminada con respecto al usuario y clave de acceso como se muestra en la figura 24.

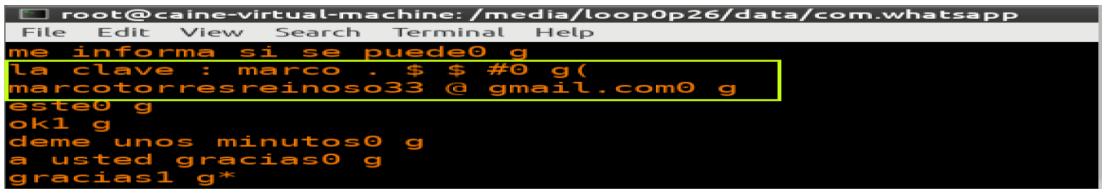

Figura 24. Evidencias encontradas
Fuente: elaboración propia

Se continúa con el análisis para recuperar el número de tarjeta de crédito, código CVC y nombre, se aplica el protocolo mencionado anteriormente, identifica referencias del mensaje borrado como se muestra en la figura 25.

Figura 25. Evidencia de mensaje eliminado
Fuente: elaboración propia

Posteriormente se realiza una vez más el análisis de la base de datos y se localiza la información borrada correspondiente a los números y código CVC de la tarjeta de crédito como se muestra en la figura 26.

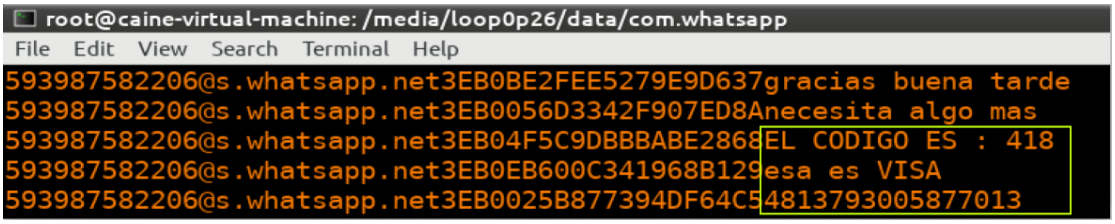

Figura 26. Evidencias encontradas.
Fuente: elaboración propia

3.3.5. Elaboración y presentación de informe pericial

Una vez obtenida la información requerida para el caso forense se procede a elaborar y presentar el informe final, como referencia se toma el formato propuesto por el Consejo de la Judicatura según el Reglamento del Sistema Pericial Integral de la Función Judicial, como establece en los artículos 19 y 20, ver anexo 1. Para los casos formulados con número de causa por parte de la Función Judicial se emitirá el informe en el formato establecido por la entidad, su uso será obligatorio, ver anexo 3.

3.4. Análisis de resultados

Al concluir el ensayo se evidencia que, la información solicitada por la empresa Ecucargo fue recuperada de manera satisfactoria, esto gracias al correcto uso del modelo (MBDMA) propuesto y la utilización de herramientas de software libre. Finalmente, se logra determinar que, este es aplicable en dispositivos móviles con sistema operativo Android. La ejecución de todas sus etapas en el ensayo realizado anteriormente permitió visualizar y documentar la información que se buscaba, por lo que, se comprueba su eficacia. El aporte es significativo para el conocimiento del perito forense al convertirse en un modelo que, ayudará a resolver los diferentes escenarios que, se le presente a lo largo de su carrera.

3.5. Segundo ensayo

Como segundo caso evidenciable para la comprobación de factibilidad del modelo (MBDMA), se estudia otro caso práctico, en un escenario en el que, los nombres de las personas y empresa han sido creados con motivo de estudio, sin mencionar identidades reales.

El jueves 15 de julio del año 2021 se recibe la visita del Sr. Juan Ramos propietario de la empresa Lacoor S.A. a fin de, mantener una reunión con el Ing. Klever Beltrán, para solicitar se realice un análisis Forense al dispositivo móvil de uno de los empleados de la empresa.

El objetivo de la pericia es buscar indicios de responsabilidad por la pérdida de dos paquetes que, contenía mercadería con un alto valor económico, la misma que, debía ser retirada por el mensajero de la empresa el que, informa que los paquetes ya fueron retirados el 14 de julio de 2021 en horas de la tarde según informe verbal por parte del servicio al cliente de las empresas mencionadas. Quien dirige Lacoor S.A. procede a incautar el celular de propiedad de la empresa a uno de los empleados del cual, sospecha que, retiró las encomiendas que, se encontraba bajo custodia de una empresa de servicio de courier y otra de transporte terrestre, se solicita extraer posible información de evidencias que, permita determinar si mencionado empleado participo o no en el caso mencionado.

Características del equipo motivo de investigación.

- Teléfono celular marca Samsung Galaxy J1 ace.
- Modelo SM-J111M.
- Sistema operativo Android.
- Versión del Android 5.1.1.
- Memoria Ram 919 Mb.
- Procesador ARM Cortex-A7.
- CPU 4 cores 1.5GHz.
- Almacenamiento interno de 4.71 Gb.

3.6. Modelo propuesto (MBDMA)

Para identificar las posibles evidencias se aplica el MBDMA al dispositivo incautado propiedad de la empresa Lacoor S.A. con las características mencionadas anteriormente.

3.6.1. Asegurar la escena

Se recibe el dispositivo móvil, el que, se lo ubica en un espacio apropiado y seguro, para realizar la documentación mediante archivo fotográfico, ver figura 27.

Figura 27. Dispositivo móvil
Fuente: elaboración propia

3.6.2. Identificar evidencias

Para estar al tanto del funcionamiento y estado del equipo móvil se inicia con un proceso de examen visual y documentación de las características del equipo apoyados en una ficha de observación como se muestra en la figura 28 y tabla 10.

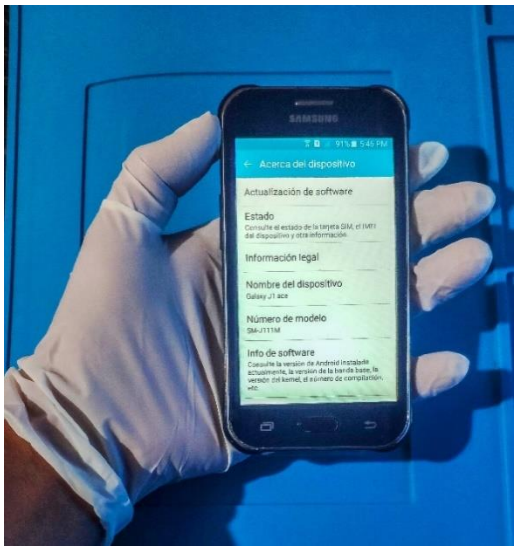

Figura 28. Documentación del equipo
Fuente: elaboración propia

Tabla 10. Ficha de observación dispositivos móviles

Ficha técnica de dispositivos móviles
Perito: Klever Beltrán
Número de caso: 002
Fecha: 15-julio-2021
Hora: 17:00

Item	Tipo	Marca	Serie	Modelo	Estado	Observaciones
1	Celular	Samsung	J111M/DSGH	SMJ11M	Bueno	Operativo

Fuente: elaboración propia

3.6.3. Adquisición de datos

Se aplica la cadena de custodia la que genera un ambiente seguro de trabajo en el laboratorio forense de la ESPE, para obtener los datos evidenciables se utiliza la herramienta adb del sistema operativo *Santoku*, previo a esto el dispositivo móvil contará con privilegios *root* y estar activado la depuración usb, lo que, permite acceder a la información total con el fin, de crear una imagen forense de la partición userdata, ver figura 29.

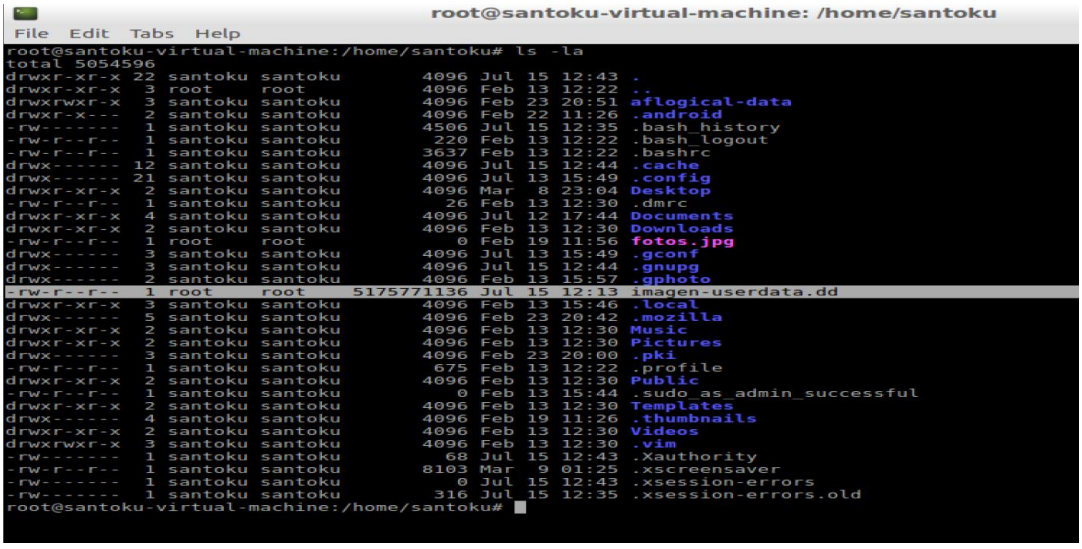

Figura 29. Imagen forense
Fuente: Elaboración propia

Para preservar la integridad de la imagen forense (imagen-userdata.dd) se genera los hashes (md5, sha1, sha256), de esta manera se valida si se realizó alguna modificación de la imagen en el transcurso del proceso, ver imagen 30, además, se documenta los datos obtenidos, ver tabla 11.

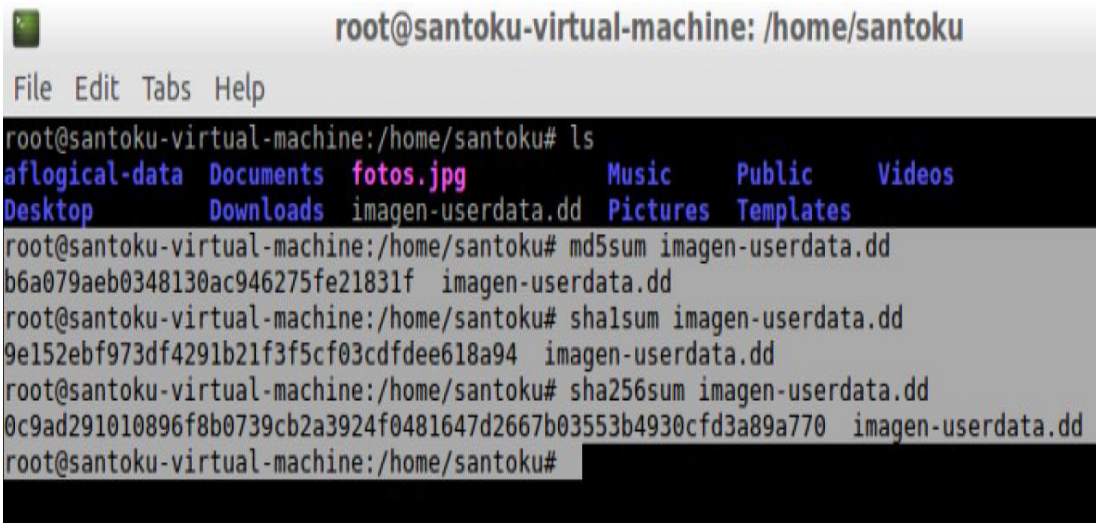

Figura 30. Hashes
Fuente: elaboración propia

Tabla 11. Ficha para el registro de imagen forense

Ficha: para el registro de imagen forense

Perito: Klever Beltrán	Dispositivo: Celular
Número de caso: 002	Marca: Samsung
Fecha: 15 de julio del 2021	Serie: J111M/DSGSMH
Hora: 20:13	Modelo: SM-J111M

Item	Hash	Estado del respaldo	Herramienta utilizada	Observaciones
1	MD5 b6a079aeb0348130ac946275fe21831f	Satisfactorio	dd(Linux)	Ninguna
	SHA1 9e152ebf973df4291b21f3f5cf03cdfdee618a94	Satisfactorio	dd(Linux)	Ninguna
	SHA256 0c9ad291010896f8b0739cb2a3924f0481647d2667b03553b4930cfd3a89a770	Satisfactorio	dd(Linux)	Ninguna

Fuente: elaboración propia

3.6.4. Analizar datos

Se procede a copiar la imagen forense desde el sistema operativo *Santoku* hacia un medio externo, esta será analizada con el programa *Autopsy* en este caso bajo Windows, por lo que, realizamos el cálculo de los hashes (md5, hsa1, sha256) con el propósito de verificar la integridad de la información como se muestra en la figura 31.

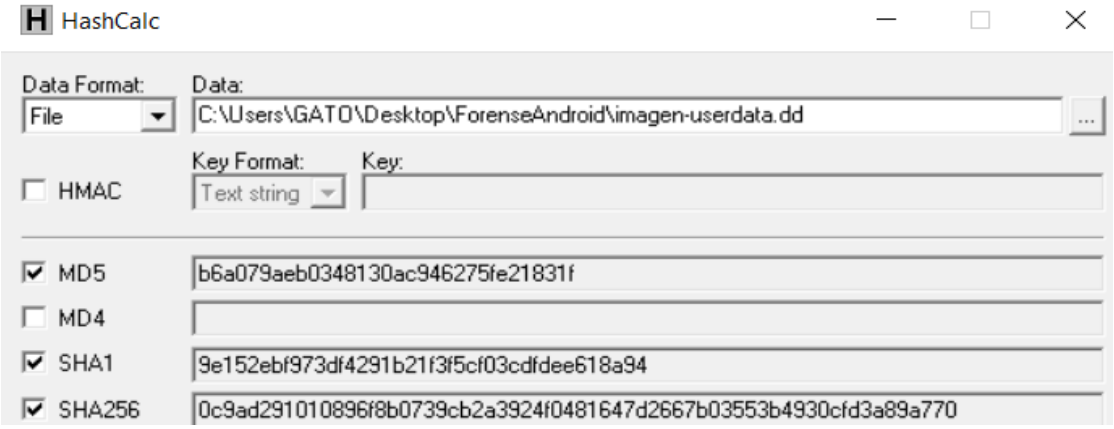

Figura 31. Verificación de hashes
Fuente: Elaboración propia

Una vez verificado los hashes y constatar que, no existe inconsistencia, se procede a montar la imagen forense, ver figura 34 y configurar los módulos a ejecutarse en el proceso de análisis con el programa *Autopsy*, ver figura 32.

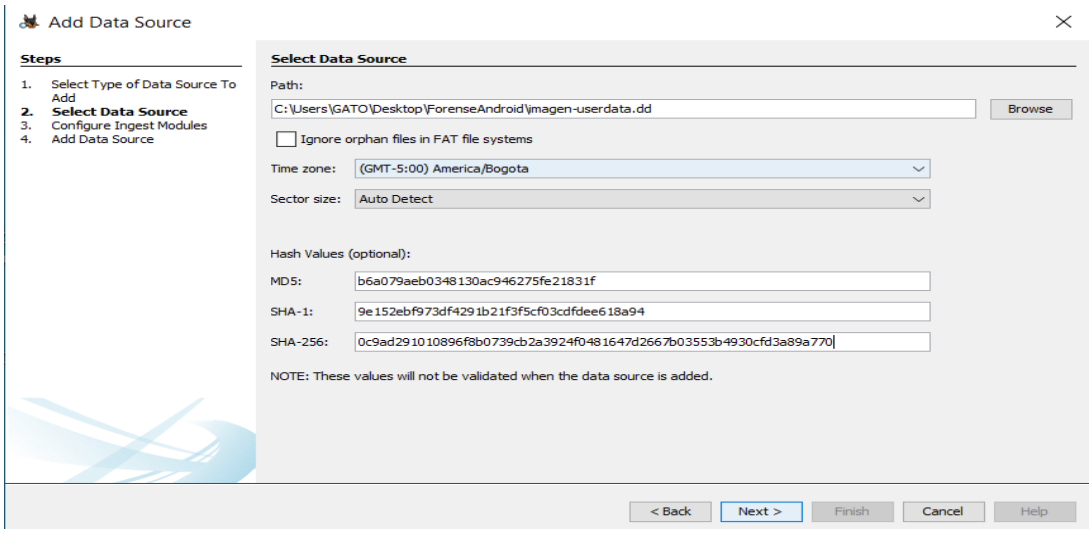

Figura 32. Montar imagen forense
Fuente: Elaboración propia

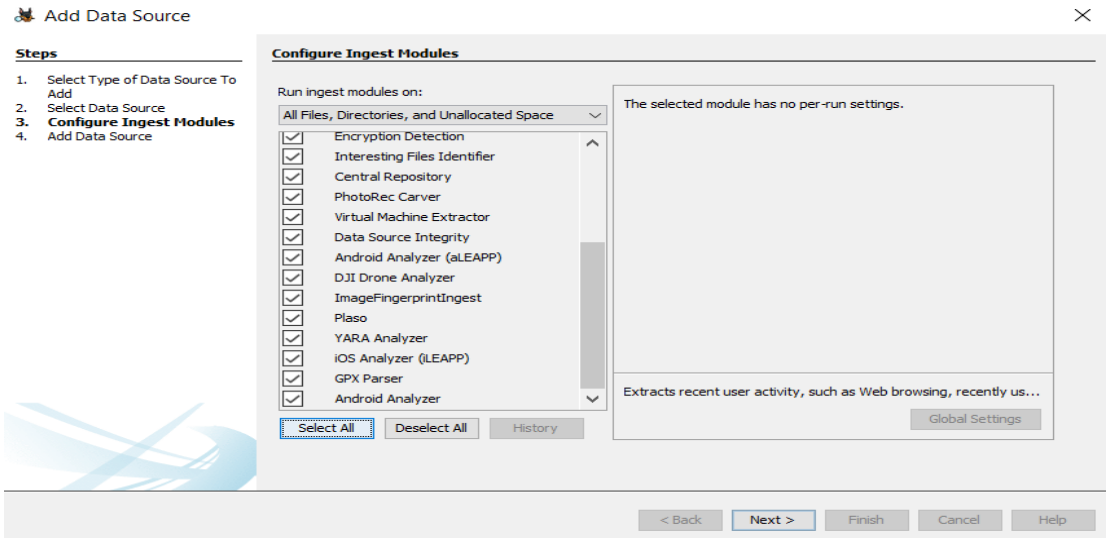

Figura 33. Configuración de módulos
Fuente: elaboración propia

Se procede con la ejecución del análisis a la imagen forense a través de los diferentes módulos que brinda *Autopsy*, una vez terminado el proceso se muestra los datos del análisis como se ilustra en la figura 34, estos están preparados para ser examinados con el fin de, encontrar evidencias en torno al caso motivo de estudio.

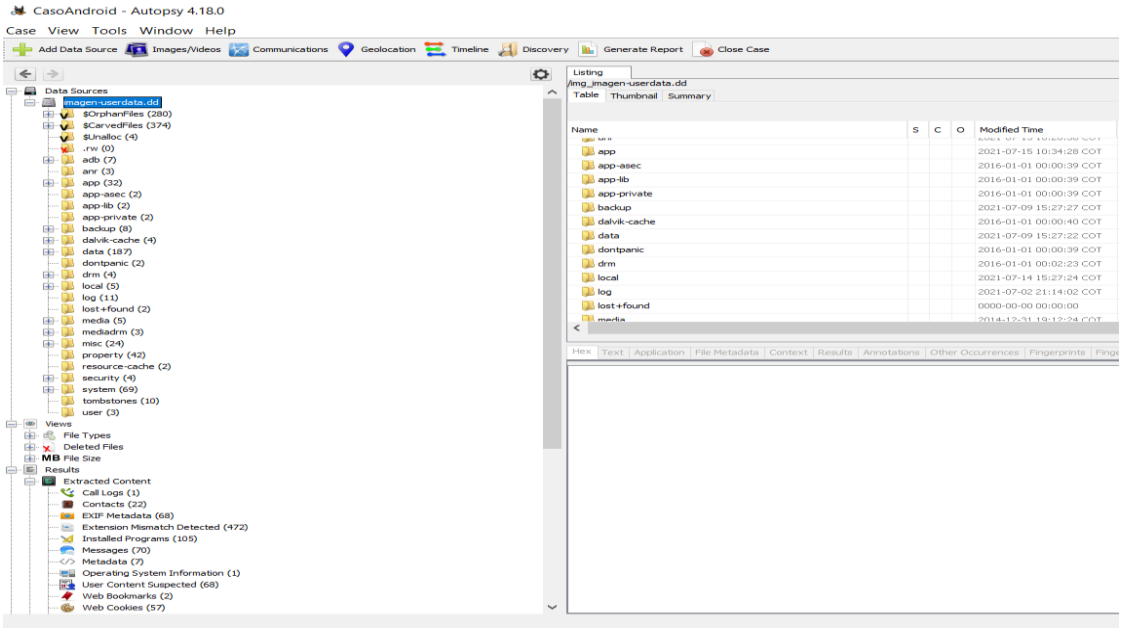

Figura 34. Análisis de imagen forense
Fuente: elaboración propia

Una vez que, se obtiene los datos de la imagen forense, se da inicio al proceso de indagación de posibles evidencias relacionadas al asunto en estudio, se procede con el análisis de las bases de datos del aplicativo *WhatsApp*, ver figura 37, con el fin de, determinar

si existe alguna conversación relacionada al caso en análisis, luego de analizar, las bases de datos se determina que existe una conversación en la que, se hace mención a unos paquetes, estos mensajes sirven como posible evidencia en el proceso investigativo, ver figura 35 y 36.

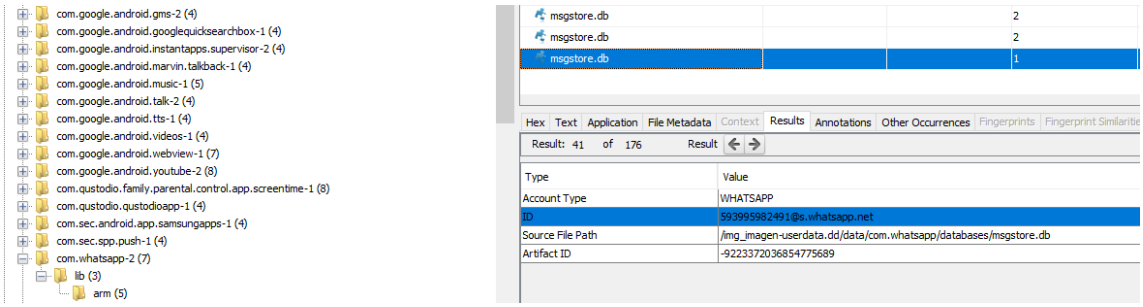

Figura 35. Bases de datos de aplicativo WhatsApp
Fuente: elaboración propia

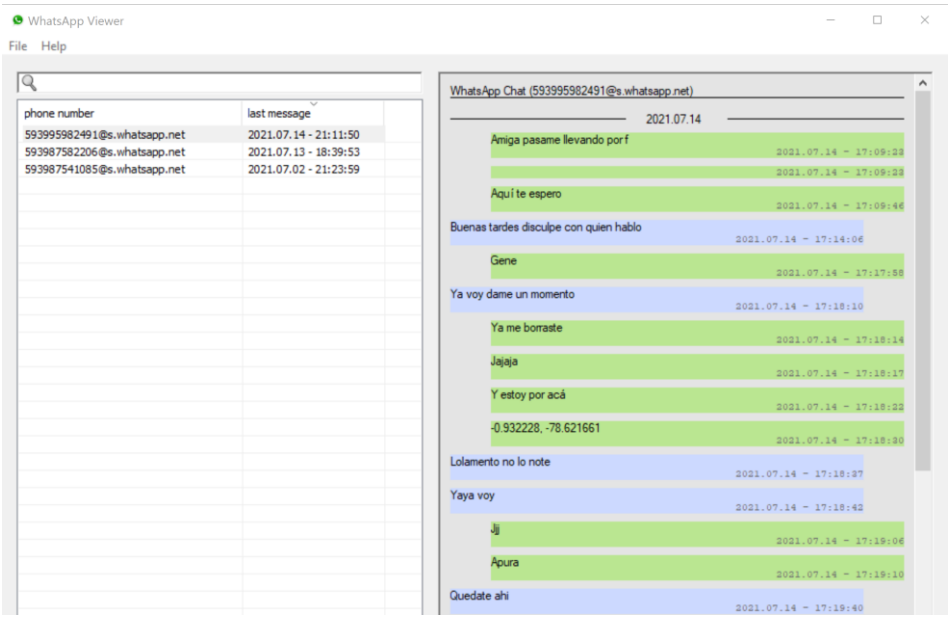

Figura 36. Mensajes de WhatsApp parte 1
Fuente: elaboración propia

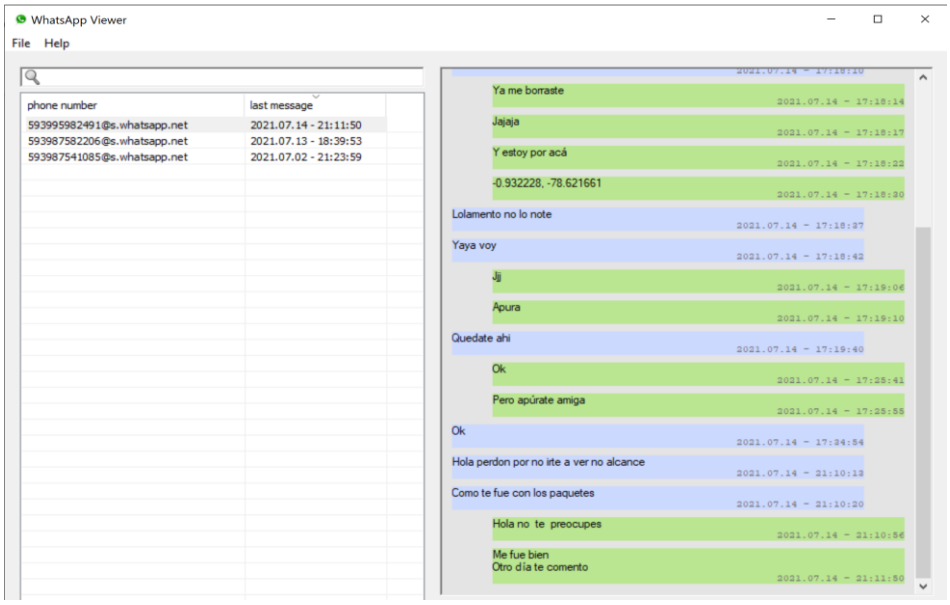

Figura 37. Mensajes de WhatsApp parte 2
Fuente: elaboración propia

Seguidamente se realiza un análisis a las imágenes captadas con el dispositivo incautado y se determina que, existe cuatro de ellas que, se tomó en lugares muy cercanos a las empresas donde se encontraba los paquetes mencionados en el caso, por lo que, se realiza un análisis más detallado de las fotos, se obtiene datos precisos e incluso coordenadas del sitio donde estas fueron tomadas, ver figuras 38, 39, 40 y 41.

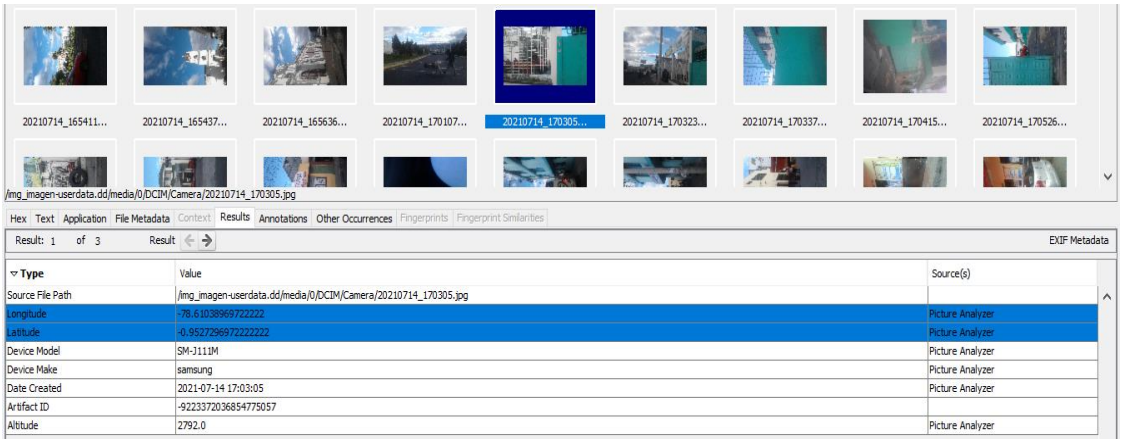

Figura 38. Fotografía 1
Fuente: elaboración propia

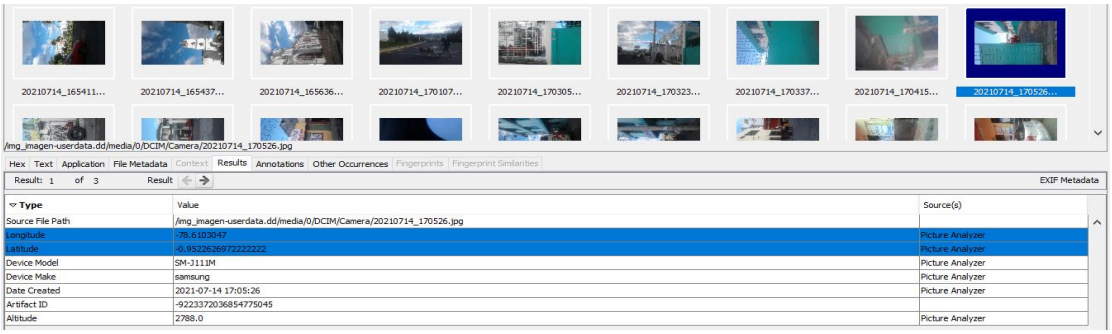

Figura 39. Fotografía 2
Fuente: elaboración propia

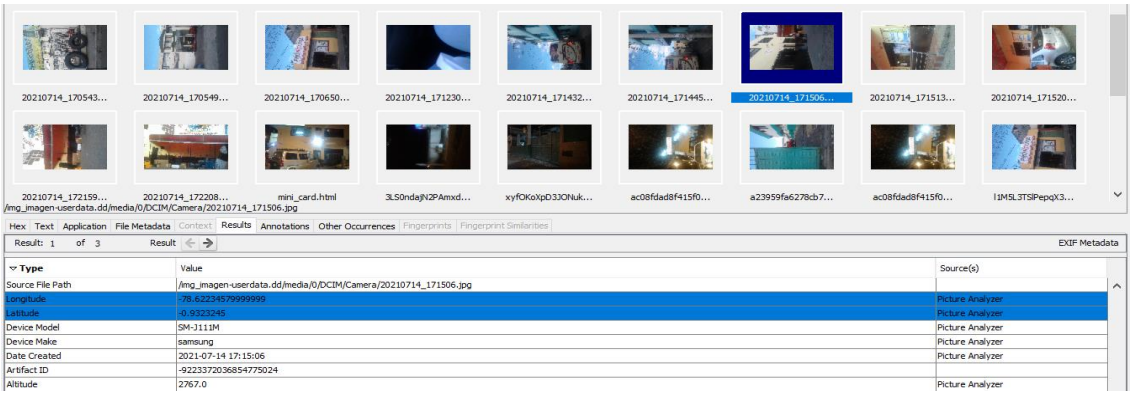

Figura 40. Fotografía 3
Fuente: elaboración propia

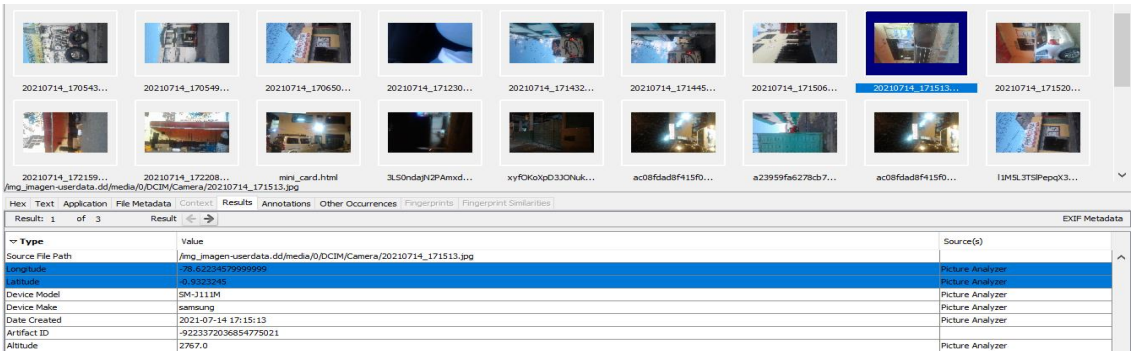

Figura 41. Fotografía 4
Fuente: elaboración propia

Al continuar con la investigación se realiza un rastreo, se aplica geolocalización para determinar los puntos, con el fin de, determinar si los resultados obtenidos concuerda con las coordenadas descritas en las imágenes que, anteceden, ver figura 42.

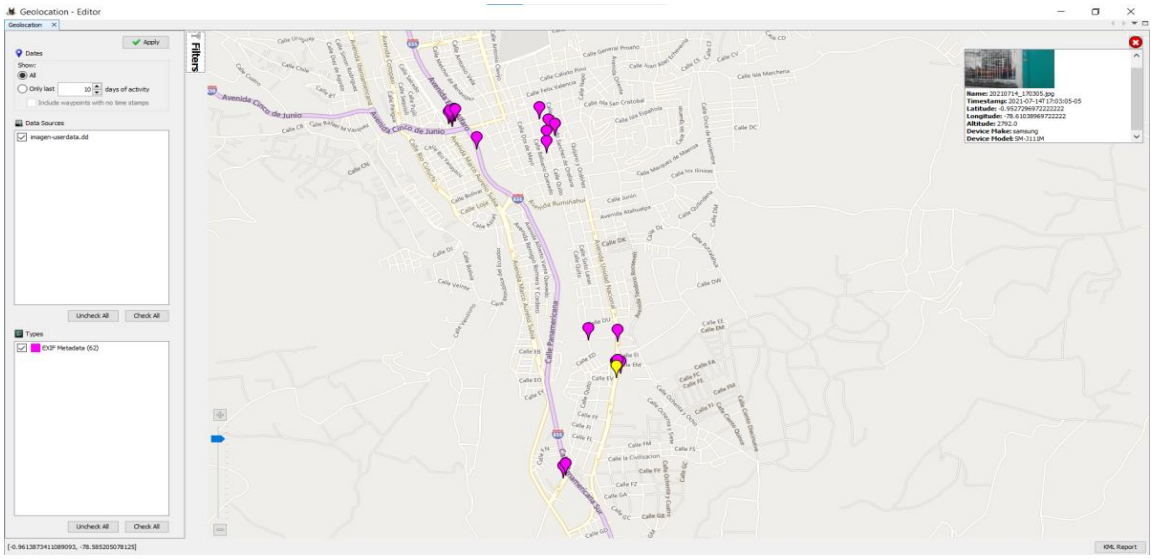

Figura 42. Geolocalización
Fuente: elaboración propia

3.6.5. Elaboración y presentación de informe pericial

Con los datos obtenidos en el análisis forense se procede a la elaboración del informe pericial, ver anexo 2, para lo cual, se toma como referencia el formato expuesto por el Consejo de la Judicatura según el Reglamento del Sistema Pericial Integral de la Función Judicial, como lo instaura en los artículos 19 y 20.

3.7. Análisis de resultados

Mediante la aplicación del MBDMA, experticia, y la utilización de herramientas de análisis forense se obtuvo información relevante con relación al caso de peritaje solicitado por la empresa Lacoor S.A., la administración de esta procederá hacer uso de la información emitida en el informe pericial como creyere conveniente. Con lo expuesto se comprueba la validez del modelo desarrollado este es flexible en los diversos casos de investigación y aplicable en dispositivos móviles con sistema operativo Android.

CONCLUSIONES

- La identificación de la base teórica para implementar procedimientos de análisis forense fue de gran importancia en la investigación y desarrollo del proyecto denominado (MBDMA), al conseguir una implementación eficaz y eficiente en las distintas fases del análisis forense, mediante la aplicación en los casos detallados.

- La determinación de una metodología adecuada a los procesos legales vigentes permite implementar el modelo propuesto mediante el análisis del Código Integral Penal (COIP), Constitución de la República del Ecuador, Código Orgánico General de Procesos (COGEP), Reglamento del Sistema Pericial Integral de la Función Judicial, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

- La generación de las pruebas sobre el modelo planteado en el ensayo determinó hallazgos de información válida que, contribuyen con evidencias que, aportarán al fallo dentro de un proceso investigativo legal.

- La comparación de los resultados obtenidos de la implementación del modelo (MBDMA) propuesto dio como resultado un proceso minucioso en cada una de las fases, no permite avanzar a la siguiente etapa si esta no es documentada, se lleva un registro de la información en fichas técnicas para cada una de sus etapas, lo que, permite al investigador tener a disposición los elementos evidenciables en todo momento, optimizando el tiempo en la elaboración del informe final.

RECOMENDACIONES

- Adaptar el modelo según las necesidades que implica el paso del tiempo y los cambios tecnológicos en los dispositivos móviles con sistema operativo Android ampliamente usados por las personas a nivel mundial.

- Profundizar el estudio teórico práctico para extender la lista de procedimientos, herramientas de software y hardware con el fin de, contribuir al uso apropiado de las mismas, que, faciliten el soporte para la recolección e indagación de la información en un proceso investigativo.

- Revisar constantemente las actualizaciones a las reformas legales, normas y reglamentos, para asegurar la validez del informe pericial al momento de su presentación. La constante actualización de conocimientos en materia judicial evitará que, el investigador incurra en errores legales, además, que los profesionales forenses mantendrán la línea de investigación basada en el objetivo de lo solicitado, con el fin de, generar seguridad y confianza que, permita dictar un fallo conveniente sin perjuicio de las partes actoras.

- Adaptar o crear nuevos instrumentos de registro documental fundamentados en el modelo planteado que, sirva de sustento en el proceso investigativo, que, apoye al perfeccionamiento del informe pericial.

BIBLIOGRAFÍA

Alcívar Trejo, C., Blanc Pihuave, G., & Calderón Cisneros, J. (2018). Application of forensic science in cybercrime in Ecuador and its punishability. Espacios, 39(42). Scopus. Recuperado de https://www.scopus.com/inward/record.uri?eid=2-s2.0-85055020389&partnerID=40&md5=4507f0a32544e2511e52cc36276d317e

Álvares, M. (2016). Análisis forense en dispositivos móviles iOS y Android.

Báez, M., Borrego, Á., Cordero, J., Cruz, L., González, M., Hernández, F., … Saucedo, M. (2019). Introducción a android.

Briz Ponce, L., Juanes Méndez, J. A., & García Peñalvo, F. J. (2015). Dispositivos móviles y apps: Características y uso actual en educación médica.

Cajamarca, L., & Gustavo, B. (2018). DESARROLLO DE UNA GUÍA METODOLÓGICA PARA EL ANÁLISIS FORENSE DIGITAL EN EQUIPOS DE CÓMPUTO CON SISTEMA OPERATIVO MAC OS XE EL ECUADOR.

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.

Código Orgánico General de Procesos, COGEP. (2010). Prueba pericial. Quito: Ministerio de Telecomunicaciones.

Código Orgánico Integral Penal, COIP. (2018). Concordancias, Código Civil. Quito: Ministerio del Interior.

Código Orgánico Integral Penal, COIP. (2018). Delitos de la propiedad inteclectual. Quito: Ministerio del Interior.

Código Orgánico Integral Penal, COIP. (2018). Medios de Prueba. Quito: MInisterio del Interior.

Constitución de la República del Ecuador. (2008). Acreditación. Monte Cristi: Asamblea Nacional.

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. En Rocha A., Perez B.E., Penalvo F.G., del Mar Miras M., & Goncalves R. (Eds.), Iberian Conf. Inf. Syst. Technol., CISTI (Vol. 2020-June). IEEE Computer Society. Scopus.

https://doi.org/10.23919/CISTI49556.2020.9140852

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: Universidad Nacional de Noreste.

Filosofía. (s. f.). Recuperado 3 de diciembre de 2020, de ESPE website: https://www.espe.edu.ec/filosofia/

Gómez, E., Herrera, N., Moscoso, O., & Guamán, P. (s. f.). Propuesta de Análisis forense para Dispositivos Móviles con Sistema Operativo Android.

Google. (s. f.). Recuperado 10 de noviembre de 2020, de https://www.google.com/

Grijalva Lima, J. S., & Loarte Cajamarca, B. (2017). Modelo para el análisis forense y la legalización de evidencia digital atípica en procesos judiciales en Ecuador.

Hitchcock, B., Le-Khac, N.-A., & Scanlon, M. (2016). Tiered forensic methodology model for Digital Field Triage by non-digital evidence specialists. Digital Investigation, 16, S75-S85. https://doi.org/10.1016/j.diin.2016.01.010

Iorio, D., H., A., Castellote, M. A., B., C., H., C., J., W., . . . I., I. J. (2017). El rastro digital del delito: Aspectos ténicos , legales y estratégicos de la Informática Forence.

Jaya, C. A. (2017). Desarrollo de una guía de procedimientos en base al estudio de modelos de análisis forense de datos, aplicada en análisis a dispositivos móviles. Quito: PUCE.

Ley de Comercio Electrónico, Firmas y Mensajes de Datos. (2002). Prueba y Notificaciones Electrónicas. Quito: Ministerio del Interior.

Mateus, J. C., Aran-Ramspott, S., & Masanet, M.-J. (2017). Análisis de la literatura sobre dispositivos móviles en la universidad española. RIED. Revista Iberoamericana de Educación a Distancia, 20(2), 49-72.

Murcia, A. F. H., García, P. C., & Betancur, C. D. A. (s. f.). Sistemas Operativos. Obtenido de Sistemas Operativos: http://dis. um. es/~ jfernand/docencia/si ….

Nineteenth Annual DFRWS Conference. (2019). Digital Investigation, 29, S1-S2. Scopus. https://doi.org/10.1016/j.diin.2019.05.003

Peñaloza Reinoso, L. E. (2016). Estrategia de informática forense para dispositivos móviles bajo tecnología android en la Universidad Regional Autónoma de Los Andes (B.S. thesis).

Pineda Vaca, A. E. (2016). Diseño de un modelo de análisis forense informático en el Honorable Gobierno Provincial de Tungurahua (B.S. thesis). Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas.

Reglamento del Sistema Permicial Integral de la Función Judicial. (2014). Obligación de Peritos. Quito: Evolución Jurídico.

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

Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2016). Paper Session II: Computer Forensics Field Triage Process Model.

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.

Santoyo, G. J. (2015). El mercado de los dispositivos móviles. Obtenido de El mercado de dipositivos moviles: http://www. northware. mx ….

Satti, R. S., & Jafari, F. (2015). Domain specific cyber forensic investigation process model. Journal of Advances in Computer Networks, 3(1), 75-81.

Scopus—Detalles del documento. (s. f.).

https://doi.org/10.23919/CISTI49556.2020.9140852

Scopus—Metric Details. (s. f.). Recuperado 10 de noviembre de 2020, de https://scopus.puce.elogim.com/record/pubmetrics.uri?eid=2-s2.0-85066034621&origin=recordpage

Universidad de las Fuerzas Armadas. (2018). Lineamientos generales. Latacunga: Universidad de las Fuerzas Armadas.

Urbina, G. B. (2016). Introducción a la seguridad informática. Grupo editorial PATRIA.

ANEXOS

Anexo 1. Informe pericial

Informe pericial

Datos generales:

Empresa contratante: Ecucargo

Nombre y apellido del perito: Klever Beltrán

Profesión: Ing. En Informática y Sistemas Computacionales

Dirección de contacto: Calle las Gaviotas y Puerto Ayora (s/n)

Teléfono fijo de contacto: 032259009

Teléfono celular de contacto: 0987541085

Correo electrónico de contacto: kleverwbeltran@gmail.com

Antecedentes:

En la ciudad de Latacunga a los 8 días del mes de marzo del 2021, la empresa Ecucargo mediante oficio OF-07032021, solicita realizar una pericia a un dispositivo móvil con sistema operativo Android del que, se eliminaron mensajes del aplicativo Whatsapp, la finalidad es recuperar la información descrita en el oficio anexado al final del informe, ver anexo 1.1.

Consideraciones técnicas:

El jueves 9 de marzo del presente año a las 14:00, en el laboratorio forense se da inicio al peritaje del dispositivo móvil de marca Samsung modelo j2core motivo de investigación;

- Se procede a identificar el dispositivo móvil y se lo coloca en un área adecuada, destinada exclusivamente para el análisis forense, con el fin de, proteger el equipo para que, este no sea manipulado; ver figura 1.

Asegurar la escena

Figura 1. Asegura la escena

- Se inspecciona el dispositivo con el fin de, verificar su estado y características propias, se verifica que, el móvil funciona bajo el sistema operativo Android versión 8.1.0, posteriormente se documenta las particularidades mediante ficha técnica y fotografía; ver figura 2, tabla 1.

Identificar evidencias

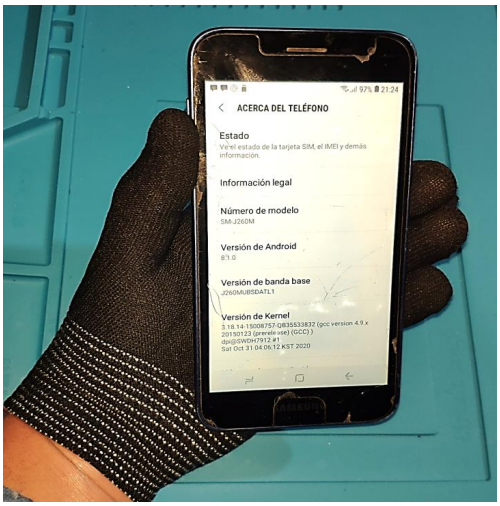

Figura 2. Identificar evidencias

Tabla 1. Ficha técnica de dispositivos móviles

Ficha técnica de dispositivos móviles

Perito: Klever Beltrán

Número de caso: 001

Fecha: 9-marzo-2021

Hora: 14:00

Item	Tipo	Marca	Serie	Modelo	Estado	Observaciones
1	Celular	Samsung	89bee74a	SM-J260M	Bueno	Encendido

- Se procede aplicar la cadena de custodia mediante el cálculo de los hashes (md5, sha224, sha256), con la finalidad de, salvaguardar la integridad de la información, se documenta mediante imagen y ficha técnica; ver figura 3, tabla 2.

Cadena de custodia

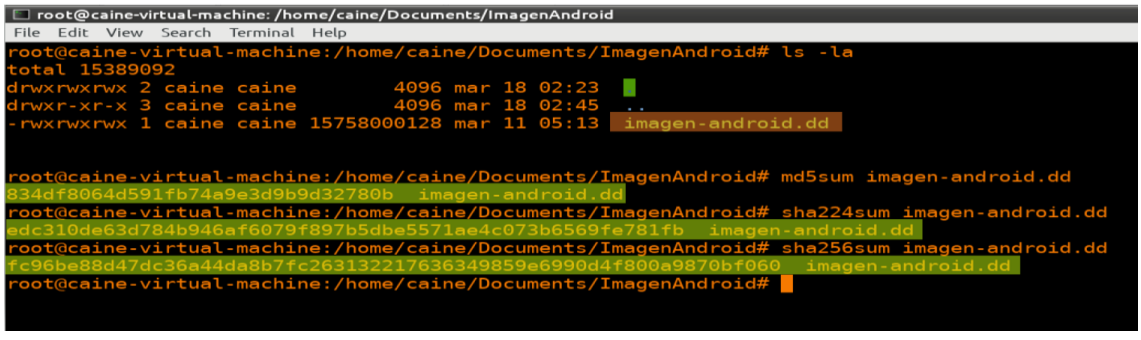

Figura 3. Cadena de custodia

Tabla 2. Ficha: para el registro de imagen forense

Ficha: para el registro de imagen forense

Perito: Klever Beltrán
Número de caso: 001
Fecha: 10 de marzo del 2021
Hora: 23:13

Dispositivo: celular
Marca: Samsung
Serie: 89bee74a
Modelo: m1807e8a

Ítem	Hash		Estado del respaldo	Herramienta utilizada	Observaciones
1	MD5	834df8064d591fb74a9e3d9b9d32780b	Satisfactorio	DD(Linux)	Ninguna
	SHA224	edc310de63d784b946af6079f897b5db dbe5571ae4c073b6569fe781fb			
	SHA256	fc96be88d47dc36a44da8b7fc26313221 7636349859e6990d4f800a9870bf060			

- Luego de la aplicación de la cadena de custodia, mediante el uso de herramientas informáticas y experticia se logra obtener la información solicitada por la parte contratante (mensajes eliminados del aplicativo WhatsApp), lo cual, se documenta mediante capturas de imágenes obtenidas durante el proceso de análisis forense; ver imagen 4 y 5.

Análisis de datos

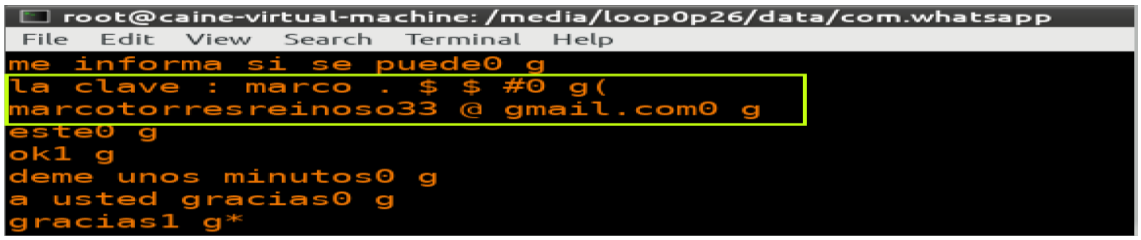

Figura 4. Análisis de datos

Análisis de datos

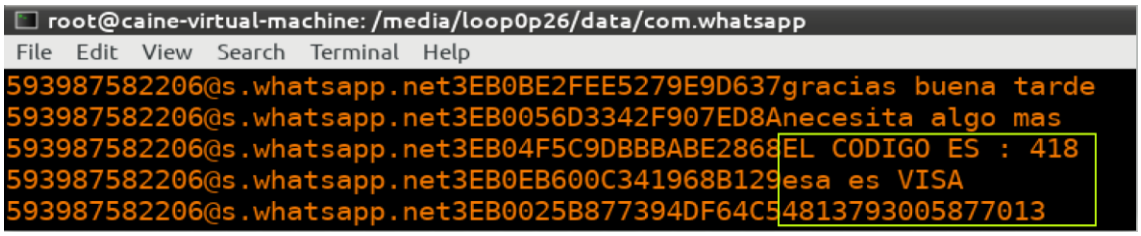

Figura 5. Análisis de datos

Conclusiones:

Con lo antes expuesto cabe mencionar que, se recuperó la información solicitada por la empresa Ecucargo, se visualiza la clave de usuario, correo electrónico, número de tarjeta de crédito, código CVC, que, contenían los mensajes eliminados en la conversación mantenida entre los actores mediante el aplicativo WhatsApp, por tanto, se remite el presente informe pericial y se pone en conocimiento de la parte solicitante para los fines pertinentes.

Declaración juramentada. - Juro evidenciar que, la información encontrada es real y no tiene ninguna alteración durante el proceso de recuperación, la misma fue encontrada mediante la utilización de herramientas informáticas.

Atentamente,

Firmado electrónicamente por:
KLEVER
WASHINGTON
BELTRAN TAPIA

.....
C.C # 0502324353

Anexo 1.1. Oficio peritaje

OF-07032021

Latacunga, 8 de marzo del 2021

Sr. Klever Beltrán

INGENIERO EN INFORMÁTICA Y SISTEMAS

De mi consideración:

La empresa Ecucargo a través del Ing. Raúl Cárdenas Gerente Administrativo, solicita a usted Ing. Klever Beltrán realizar un peritaje a un dispositivo móvil incautado por el área administrativa de nuestra empresa, con la finalidad de recuperar mensajes eliminados, que involucran a la cliente María Cortez quien mantuvo relaciones comerciales con nuestra empresa para realizar compras en el exterior, utilizando una tarjeta de crédito probablemente sustraída de manera ilegal, la antes mencionada mantuvo una conversación con Sofía Pérez asistente de compras de la empresa Ecucargo mediante el aplicativo WhatsApp.

A nombre de la empresa Ecucargo, como Gerente Administrativo mediante este oficio requiero contratar sus servicios profesionales para realizar una pericia con el objeto de recuperar los mensajes eliminados de la mencionada conversación como son: correo electrónico, clave de usuario, numero de tarjeta de crédito y código CVC.

Atentamente,

Ing. Raúl Cárdenas

GERENTE ADMINISTRATIVO

Anexo 2. Informe pericial

Informe pericial

Datos generales:

Empresa contratante: Lacoor S.A.

Nombre y apellido del perito: Klever Beltrán

Profesión: Ing. En Informática y Sistemas Computacionales

Dirección de contacto: Calle las Gaviotas y Puerto Ayora (s/n)

Teléfono fijo de contacto: 032259009

Teléfono celular de contacto: 0987541085

Correo electrónico de contacto: kleverwbeltran@gmail.com

Antecedentes:

En la ciudad de Latacunga a los 15 días del mes de julio del 2021, la empresa Lacoor S.A. mediante orden de trabajo OT-15072021, solicita realizar una pericia a un dispositivo móvil con sistema operativo Android del que, se requiere buscar indicios de responsabilidad por la pérdida de dos paquetes que, se encontraban bajo custodia de empresas de servicio de courier y transporte, ver anexo 2.1.

Consideraciones técnicas:

El jueves 15 de julio del presente año a las 14:00, en el laboratorio forense se da inicio al peritaje del dispositivo móvil de marca Samsung SM-J111M motivo de investigación;

- Se procede a identificar el dispositivo móvil y se lo coloca en un área adecuada, destinada exclusivamente para el análisis forense, con el fin de, proteger el equipo para que, este no sea manipulado; ver figura 1.

Asegurar la escena

Figura 1. Asegura la escena

- Se inspecciona el dispositivo con el fin de, verificar su estado y características propias, se verifica que, el móvil trabaja bajo el sistema operativo Android versión 5.1.1, posteriormente se documenta las particularidades mediante ficha técnica y fotografía; ver figura 2, tabla 1.

Identificar evidencias

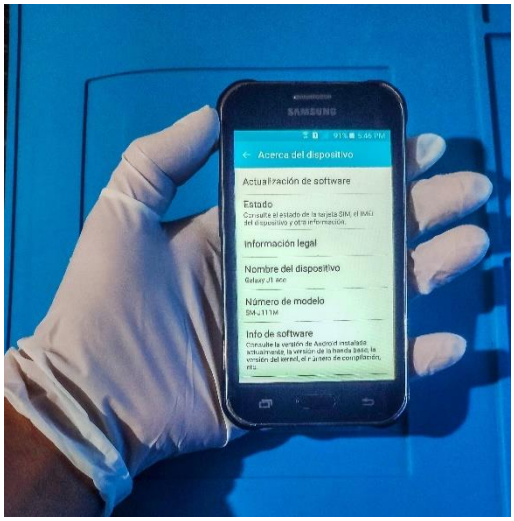

Figura 2. Identificar evidencias

.

Tabla 1. Ficha técnica de dispositivos móviles

Ficha técnica de dispositivos móviles

Perito: Klever Beltrán

Número de caso: 002

Fecha: 15-julio-2021

Hora: 14:30

Ítem	Tipo	Marca	Serie	Modelo	Estado	Observaciones
1	Celular	Samsung	J111M/DSGSMH	SM-J111M	Bueno	Operativo

- Se procede aplicar la cadena de custodia mediante el cálculo de los hashes (md5, sha1, sha256), con la finalidad de, salvaguardar la integridad de la información, se documenta mediante imagen y ficha técnica; ver figura 3, tabla 2.

Cadena de custodia

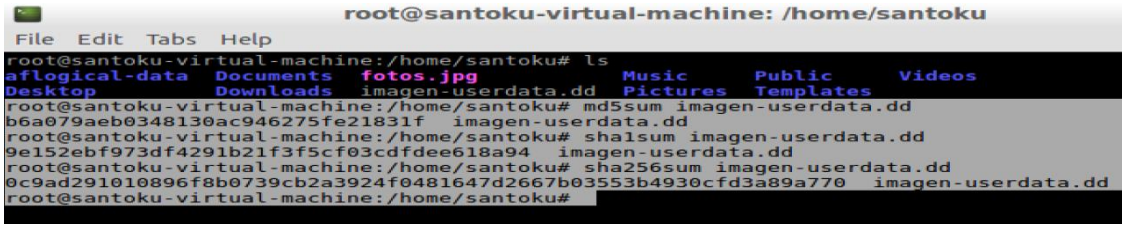

Figura 3. Cadena de custodia

Tabla 2. Ficha: para el registro de imagen forense

Ficha: para el registro de imagen forense

Perito: Klever Beltrán	Dispositivo: Celular
Número de caso: 002	Marca: Samsung
	Serie:
Fecha: 15 de julio del 2021	J111M/DSGSMH
	Modelo:
Hora: 15:00	SM-J111M

Ítem	Hash	Estado del respaldo	Herramienta utilizada	Observaciones
1	MD5 b6a079aeb0348130ac946275fe21831f	Satisfactorio	DD(Linux)	Ninguna
	SHA224 9e152ebf973df4291b21f3f5cf03cdfdee618a94			
	SHA256 0c9ad291010896f8b0739cb2a3924f0481647d2667b03553b4930cfd3a89a770			

- Luego de la aplicación de la cadena de custodia, mediante el uso de herramientas informáticas y experticia se logra obtener la información solicitada por la parte contratante (mensajes del aplicativo WhatsApp, fotografías y geolocalización), lo cual, se documenta mediante capturas de imágenes obtenidas durante el proceso de análisis forense; ver imagen 4,5,6,7,8,9 y 10.

Análisis de datos

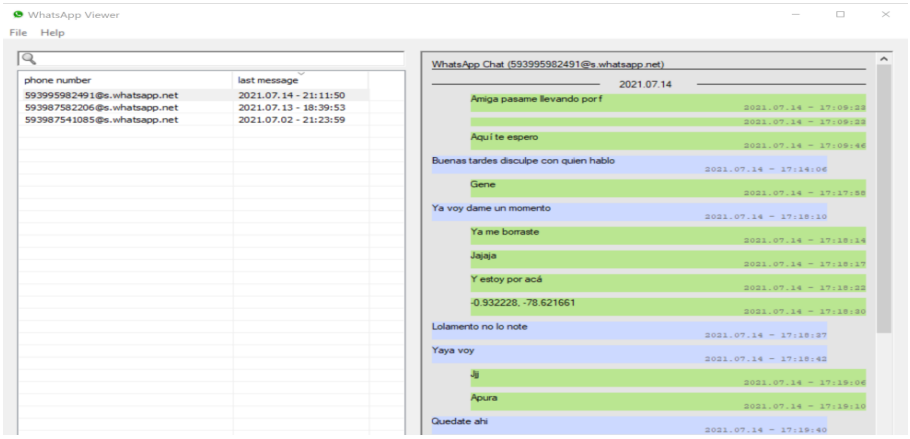

Figura 4. Análisis de datos

Análisis de datos

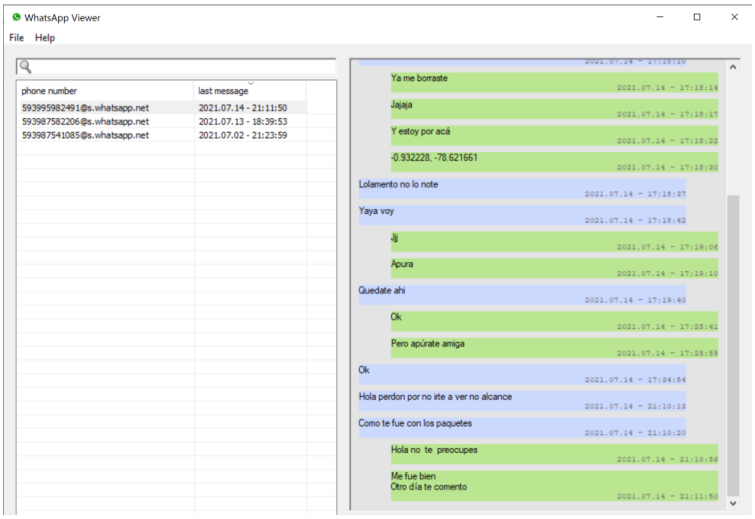

Figura 5. Análisis de datos

Análisis de datos

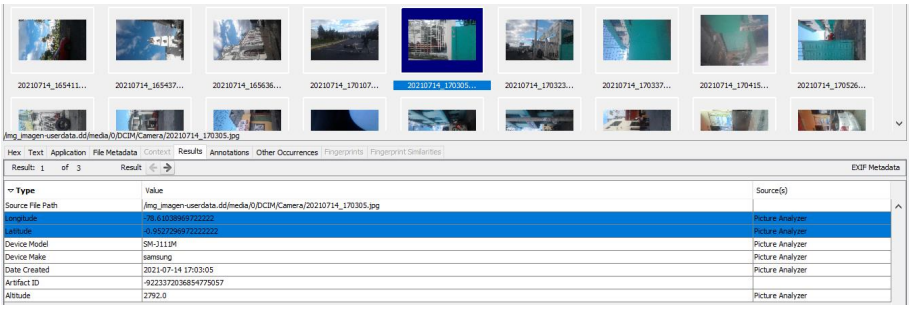

Figura 6. Análisis de datos

Análisis de datos

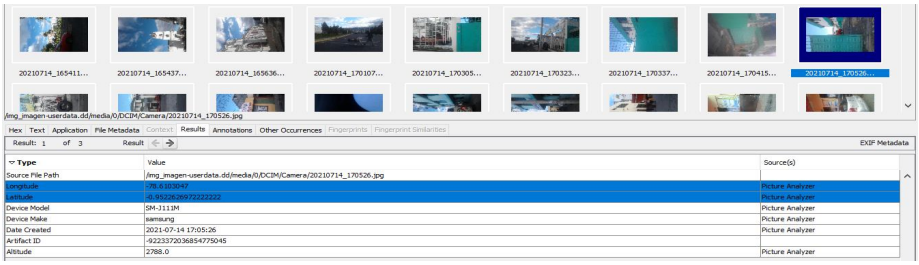

Figura 7. Análisis de datos

Análisis de datos

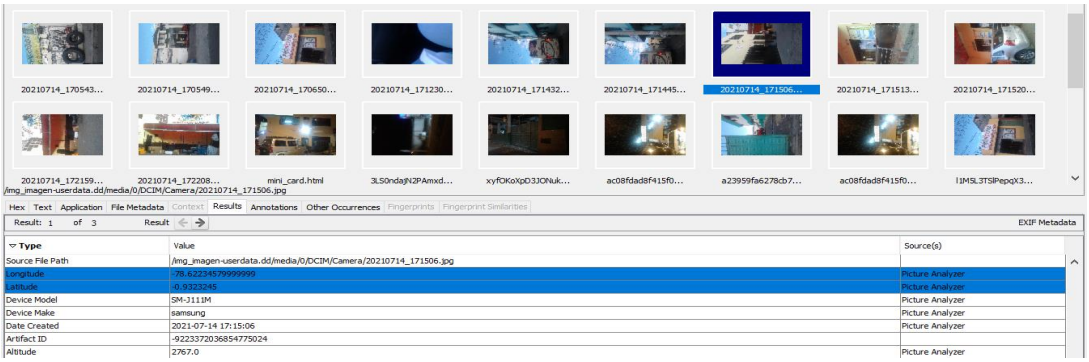

Figura 8. Análisis de datos

Análisis de datos

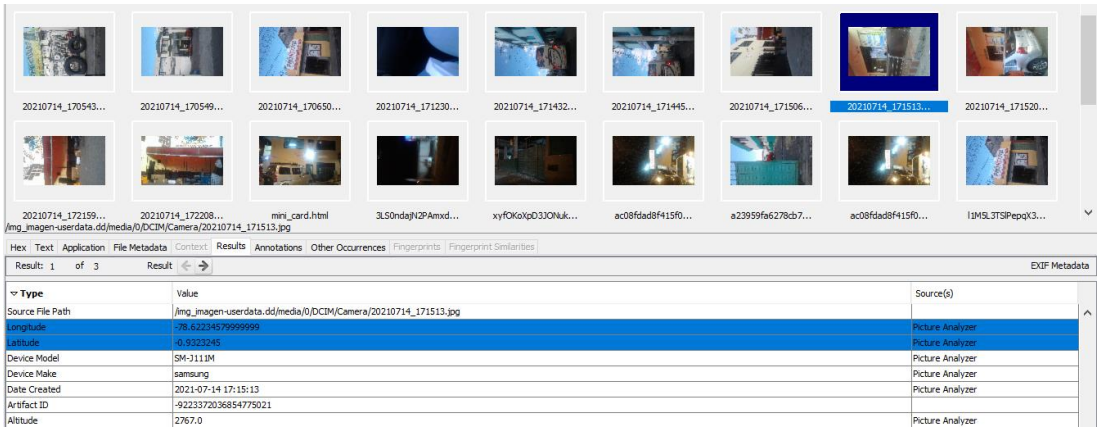

Figura 9. Análisis de datos

Análisis de datos

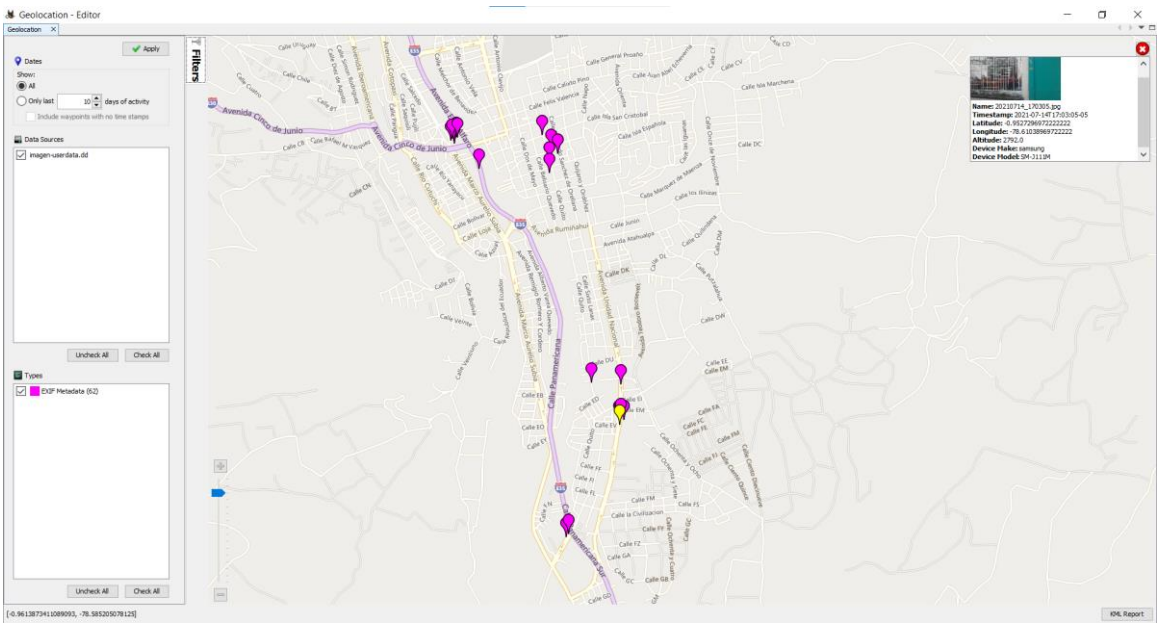

Figura 10. Análisis de datos

Conclusiones:

En base a la documentación presentada se determina que, se analiza y recupera información significativa solicitada por la empresa Lacoor S.A., se evidencia conversaciones del el aplicativo WhatsApp, fotografías realizadas con el dispositivo móvil y geolocalización de lugares visitados. Por tanto, se remite el presente informe pericial y se pone en conocimiento de la parte solicitante para los fines pertinentes.

Declaración juramentada. - Juro evidenciar que, la información encontrada es real y no tiene ninguna alteración durante el proceso de recuperación, la misma fue encontrada mediante la utilización de herramientas informáticas.

Atentamente,

Firmado electrónicamente por:
KLEVER
WASHINGTON
BELTRAN TAPIA

.....
C.C # 0502324353

Anexo 2.1. Orden de trabajo

ORDEN DE TRABAJO OT-15072021

Solicitante: Lacoor S.A.

Cedula de identidad/RUC: 0594603024001

Teléfono: 032602069

Dirección del Solicitante: Quito 16-45 y Padre Salcedo

Fecha: 15 de julio de 2021

Detalle de solicitud:

Lacoor S.A. solicita un peritaje total del dispositivo móvil:

Marca: Samsung.

Modelo: SM-J111M.

Serie: J111M/DSGSMH.

Estado: funcionando.

Se requiere obtener información del equipo mencionado que implique responsabilidad del retiro no autorizado de unos paquetes por parte de un empleado de la empresa, estos paquetes estaban bajo custodia de una empresa de servicio de courier y de transporte.

NOTA: La empresa Lacoor S.A. como titular del equipo mencionado autoriza al Ing. Klever Beltrán Tapia para que se realice el análisis forense al dispositivo móvil descrito anteriormente.

KLEVER WASHINGTON BELTRAN TAPIA

Solicitante	Recibe
Sr. Juan Ramos	Ing. Klever Beltrán
Lacoor S.A.	INvestigador

Anexo 3. Formato de informe pericial

FORMATO DE INFORME PERICIAL

Las y los peritos presentarán su informe de conformidad con lo establecido en los artículos 19 y 20 del REGLAMENTO DEL SISTEMA PERICIAL INTEGRAL DE LA FUNCION JUDICIAL. Por lo tanto, el presente formato puede ser considerado por los auxiliares de justicia para la presentación de los informes periciales, sin perjuicio a lo establecido en normas legales específicas.

"INFORME PERICIAL"

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

Nombre Judicatura o Fiscalía	
No. de Proceso	
Nombre y Apellido de la o el Perito	
Profesión y Especialidad acreditada	
No. de Calificación	
Fecha de caducidad de la acreditación	
Dirección de Contacto	
Teléfono fijo de contacto	

Teléfono celular de contacto	
Correo electrónico de contacto	

2. **PARTE DE ANTECEDENTES**, en donde se debe delimitar claramente el encargo realizado, esto es, se tiene que especificar claramente el tema sobre el que informará 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 debe explicar claramente, cómo aplican sus conocimientos especializados de su profesión, arte u oficio, al caso o encargo materia de la pericia. La o el perito deberá relacionar los contenidos de sus conocimientos especializados con el objeto de la pericia encargada. Analizará 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 procederá 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 versará sobre los hechos consultados y ordenados, establecidos en los antecedentes, y nada dirá 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 será tomado en cuenta al momento de resolver, y será 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**, deberá sustentar sus conclusiones ya sea con documentos y objetos de respaldo (fotos, copias certificadas de documentos, grabaciones, etc); y/o, con la explicación clara de cuál es el sustento técnico o científico para obtener un resultado o conclusión específica. Se debe exponer claramente las razones especializadas de la o el perito para llegar a la conclusión correspondiente. No se cumplirá 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 deberá razonar y motivar 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, será 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, la o el perito debe hacerlo constar necesariamente en su informe pericial de conformidad con dicha exigencia legal.
7. **INFORMACIÓN ADICIONAL,** la o el perito podrá incluir cualquier otro tipo de información adicional a los numerales anteriores, siempre y cuando la misma ayude a clarificar sus explicaciones y/o conclusiones; siempre y cuando esta información se encuentre dentro de los límites del objeto de la pericia.
8. **DECLARACIÓN JURAMENTADA,** la o el perito deberá 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 deberá hacer constar la firma y rúbrica de la o el perito, 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 deben considerar los auxiliares de justicia al momento de elaborar sus informes periciales.