UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: **RPC-SO-02-No.053-2021**

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
Propuesta de una metodología forense para dispositivos móviles con sistema operativo Android
Línea de Investigación:
Seguridad Informática
Campo amplio de conocimiento:
Tecnologías de la Información y Comunicación
Autora:
Jhoana Carolina Villacis Peralvo
Tutor:
Mg. Recalde Varela Pablo Marcel

Quito – Ecuador

2022

APROBACIÓN DEL TUTOR

Yo, PABLO MARCEL RECALDE VARELA con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado PROPUESTA DE UNA METODOLOGÍA FORENSE PARA DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID.

Elaborado por: JHOANA CAROLINA VILLACIS PERALVO, de C.I: 0502824154, estudiante de la Maestría: SEGURIDAD INFORMÁTICA, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2022

Firma

ORCID: 0000-0003-4710-1178

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, JHOANA CAROLINA VILLACIS PERALVO con C.I: 0502824154, autora del proyecto de titulación denominado: PROPUESTA DE UNA METODOLOGÍA FORENSE PARA DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID. Previo a la obtención del título de Magister en SEGURIDAD INFORMÁTICA.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación 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. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2022

Firma

ORCID: 0000-0001-8354-4465

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

Según (Revista_Líderes_EC, 2018), en la actualidad los dispositivos móviles para las personas se han vuelto una necesidad, el incremento de los mismos crece desde la llegada de la evolución digital a la vida humana que al querer comunicarse con otras personas hizo cambios tecnológicos beneficiosos que permitieron optimizar recursos y tiempo. Sin embargo, todo este avance tecnológico trae desafíos a nivel de seguridad de la información y grandes oportunidades para los ciberdelincuentes. Con el aumento de dispositivos móviles crece el riesgo de delitos informáticos con programas maliciosos que son específicamente diseñados para este tipo de teléfonos inteligentes con tecnología Android este sistema operativo ha ocupado el primer lugar en el mercado debido a su cantidad de aplicaciones siendo el más usado en comparación con el sistema de Apple IOS y la facilidad de usarlas ya sean están gratuitas o de pago.

Durante la última década, los dispositivos móviles se han convertido en la herramienta informática fundamental para el acceso a sistemas de información, aplicaciones y a Internet, por lo que son ampliamente utilizados en todo tipo de escenarios y para aplicaciones tales como redes sociales, comercio, banca, educación, telecomunicaciones, etc. Lo cual ha sido un gran atractivo para los ciberdelincuentes, siendo necesario contar con una investigación forense cuando se ha visto involucrado un dispositivo para delinquir, y en base a una herramienta se podría determinar o recopilar pruebas para abrir una investigación judicial en contra de quien cometió el delito.

Conforme al avance tecnológico y el descubrimiento de riesgos que implica la seguridad de la información, se han desarrollado diversas metodologías para las buenas prácticas en gestión de la información, estas estrategias han sido adoptadas por organizaciones para salvaguardar la confidencialidad, integridad y disponibilidad de la información aplicando técnicas analíticas y científicas.

Problema de investigación

Según (Lockheimer, 2019), dice que los avances tecnológicos expresan la evolución del hombre, avances que han cambiado en el transcurso del tiempo, en las que cada día existe una mayor conexión a los dispositivos digitales, generando dependencia de los mismos, provocando que manejen y almacenen información en dispositivos más pequeños y portátiles.

En la actualidad el uso del Sistema Operativo Android se ha incrementado con rapidez, esto parte por su fácil manejo y no complicaciones al momento de utilizar app, en la actualidad no existen normas vigentes que permitan realizar análisis forense de los mismos, es por ello que se han incrementado los famosos ataques informáticos realizados por ciberdelincuentes obteniendo información de empresas públicas, privadas y usuarios, desconociendo el uso de herramientas que se necesitan para realizar dichos ataques informáticos. Sin embargo, para extraer información de este tipo de dispositivos, existen muchas técnicas o métodos, pero el más común es el de recuperación de información mediante el sistema de archivos del sistema operativo, que incluso tiene la capacidad de encontrar información que ha sido previamente eliminada. El problema existente surge cuando durante el análisis forense no existe una guía que brinde los lineamientos necesarios a utilizar en dispositivos móviles con sistema operativo Android que permitan obtener información del mismo.

Según (INDICIOS, 2018), en el transcurso de los años se ha evidenciado a varias entidades públicas, privadas y usuarios comunes, hacer uso de herramientas tecnológicas (laptops, Tablet, Smartphone). En la actualidad las tecnologías más utilizadas son teléfonos móviles con sistema Android, estos dispositivos se caracterizan por el fácil manejo y la prestación de servicios, es por ello que hoy en día la dependencia de la tecnología ha conllevado a que se almacene y administre información personal en dichos dispositivos tecnológicos. La información de entidades o usuarios comunes se ha convertido en el activo más valioso, esto debido a que varias empresas han realizado la implementación de sistemas de información que tiene como finalidad de mejorar de prestación de servicios, de esta manera surge la informática forense, el cual proyecta objetivos preventivos para la protección de información y evitar infiltración en el sistema.

El diseñar una metodología forense permitirá el desarrollo de actividades a las autoridades judiciales mediante conocimiento basado en estudio forense hacia terminales móviles que utilicen sistema Android con la finalidad de obtener resultados significativos en las investigaciones judiciales.

La aplicación de una metodología forense permite buscar, encontrar y extraer información clave que proporcionará los dispositivos móviles investigados, dicha información podrá ser utilizada como pruebas relevantes en las investigaciones forenses, de esta manera los procesos judiciales serán esclarecidos involucrado dicha herramienta tecnológica.

¿Qué método forense se puede aplicar a dispositivos móviles con sistema operativo Android?

Objetivo general

Diseñar una metodología forense para dispositivos móviles con Sistema Operativo Android, con el propósito de analizar la evidencia de un caso de delito informático.

Objetivos específicos

Contextualizar sobre términos de análisis forense y herramientas que se utilizan.

Analizar el uso de herramientas forenses, en dispositivos móviles con sistema Android.

Diseñar una metodología para análisis forense en dispositivos móviles con sistema Android.

Validar el uso de la metodología forense propuesta para dispositivos con sistema Android.

Vinculación con la sociedad y beneficiarios directos:

La propuesta de una metodología forense para dispositivos móviles con Sistema Operativo Android, permitirá tener las pautas necesarias para proceder con el peritaje en un acto de delito en el que está inmerso un dispositivo móvil, con la finalidad de obtener información pertinente que puede ser objeto de uso en un acto judicial.

Beneficiarios directos: entre los beneficiarios se encuentran autoridades y usuarios que están involucrados en un proceso de un delito. Se pretende aportar y cumplir con las metas de los Objetivos de Desarrollo Sostenible (ODS) nueve y dieciséis con la finalidad de generar conciencia e impacto en la sociedad para un bien común.

El presente proyecto tiene como meta modernizar y aumentar de manera relevante el acceso a la tecnología de la información y las comunicaciones aquellos países que están en desarrollo cumpliendo con el objetivo de industria, innovación e infraestructura. Así, también considerar la reducción en todas sus formas de corrupción y soborno principalmente en el sector público; siendo la meta principal el acceso público a la información en leyes nacionales y acuerdos internacionales cumpliendo con el objetivo, justicia e instituciones sólidas.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

Hoy en día, la mayoría de las personas tiene un teléfono móvil para uso personal o profesional, el uso de estos dispositivos ha sido importante en todo ámbito convirtiéndose para los usuarios en una herramienta indispensable. Por esta razón, durante la última década, los dispositivos móviles se han incrementado dramáticamente debido a los servicios que ofrecen para mantener comunicadas a las personas (Román, 2017).

Según (Tapia & Washington, 2021), el Ecuador no es la excepción con su posicionamiento y crecimiento significativo en el uso de dispositivos móviles, permiten comunicarse de acuerdo con los avances tecnológicos; la comunicación no solo ha sido utilizada en el desarrollo de actividades lícitas, por el contrario, muchas personas han encontrado la oportunidad de cometer actos ilícitos, de ahí surgió la necesidad de hacer lo correcto. Estos hechos dan paso a la Informática Forense, que aplica los conocimientos y herramientas generales del Derecho y la Informática para realizar el análisis de datos en dispositivos con sistema operativo Android, por lo que las pruebas recabadas se utilizan como prueba durante el juicio.

La comunicación global es obvia, hay millones de usuarios que utilizan dispositivos móviles con sistema operativo Android, según la empresa (New Technology Systems Solutions, 2020), esto se atribuye a que la mayoría de fabricantes de dispositivos han optado por utilizar este sistema, por lo que se ha convertido en un líder indiscutible en el mercado mundial, por tal motivo, podemos decir que un gran número de delitos informáticos actuales y futuros tienen lugar en este tipo de sistema, lo que ha permitido el desarrollo de nuevas ciencias como la informática forense.

Informática Forense

La gran variedad de formas de perder información sea estás involuntarias han provocado una serie de inconvenientes en la integridad de la información, el valor de la información en la sociedad y en las organizaciones cada vez se hace importante ya que contribuye al desarrollo de las Instituciones. La informática forense se compone de metodologías que se han utilizado como guía para investigaciones y procesos de búsqueda de pruebas, para garantizar que la información no se altere o se dañe durante el proceso durante la investigación (Arias, 2016).

Sistema Operativo

Según (Monterrubio, 2019), la mayoría de los equipos electrónicos que se usan hoy en día, como computadoras, teléfonos celulares y otros equipos, con algunos microchips en como procesadores, están en sistemas de operación, los sistemas operativos son fundamentales pues permiten la interacción con los usuarios, brindando práctica.

En el ambiente, estos sistemas operativos son básicos, activos, lo que permite que los programas y aplicaciones funcionen correctamente, esto requiere actualizaciones constantes necesarias para que los sistemas operativos funcionen correctamente en los servicios requeridos, realizando cambios en la versión del sistema operativo gráfico para el entorno y así facilitar su uso mediante la satisfacción de las necesidades del usuario, otros servicios que proveen, los hacen cada vez más eficientes. Además, es necesario saber en qué se consideran estos productos como free y se puede decir que el software libre es gratuito e indica que usted puede usarlos, por lo que el usuario tiene derecho a copiarlos y modificarlos.

Dispositivo móvil

Según (Ascheri et al., 2017), dicen que, en el primer trimestre del año 2011, más de 156 millones de teléfonos inteligentes Android se adquirieron, lo que representa el total global, en cambio el periodo del año anterior fue el 56,9%. En este tiempo Samsung se toma como el mayor fabricante de dispositivos Android, y su mercado continuo está en liderazgo, con cuota de mercado de 30,80% frente al 27,6% anual. Las aplicaciones para los dispositivos móviles y los contenidos digitales representan un gran potencial dentro de la cadena de valor del sector de las telecomunicaciones, con una proyección de que los próximos cinco años habrá un incremento promedio de 23,6% en contenido móvil y adquisición en América Latina.

Dispositivo Android

Se los conoce a los terminales que disponen de un sistema operativo especializado para dispositivos móviles, se considera como el software de base capaz de administrar todos los recursos del dispositivo para su uso de manera eficiente, para que el usuario pueda mantenerlo funcionando sin problemas con cualquier recurso que tenga. El sistema operativo Android es un sistema operativo que se deriva de Linux de plataforma abierta para terminales móviles, fue adquirida por la empresa de Google y también por Open Handset, el principal objetivo es satisfacer las necesidades de los usuarios y fabricantes de dispositivos que integran dicho sistema, para promover el uso de aplicaciones, con calidad que cualquier otro sistema operativo pueda incluir en sus conceptos (Polanco & Taibo, 2017).

Herramientas Tecnológicas

Según (Herrera et al., 2019), las herramientas tecnológicas tienen la facilidad de ayudar al experto que está realizando la investigación a obtener mejores pruebas, proporcionando medios y pautas para una recopilación de información más precisa que sirvan como prueba clara para delincuentes comunes sin miedo a los errores. De esta forma, se puede decir que las herramientas informáticas son la columna vertebral, así como el soporte para colaborar en el análisis de las pruebas obtenidas en un forense. A continuación, en la Tabla 1 se presenta una serie de herramientas que se usan para extraer información de un dispositivo móvil.

Tabla 1

Herramientas tecnológicas de extracción

Herramienta	**Siglas**	**Descripción**
AFLogical OSE	Android Framework Forensics Logical	Esta aplicación debe ser previamente instalada en el dispositivo móvil mediante una serie de comandos.
Andriller CE	Community Edition Andriller	Aplicación para el sistema operativo Windows y Linux.
FTK Imager Lite	Imager Lite Forensic Toolkit	Opera en los volcados de la memoria del dispositivo móvil para posterior análisis y recopilación de pruebas.
NowSecure _Forensics	NowSecure_Forensics Extract_Community_Edition	Se distribuye como una imagen virtual que reúne una serie de herramientas para realizar análisis forense.
LIME	Linux_Memory_Extractor	Opera en la memoria de volcado volátil de dispositivos al ejecutar el sistema operativo Linux, como un teléfono móvil Android.

Nota. Fuente: Herrera et al., 2019

Herramientas para aplicaciones específicas

A continuación, se muestra en la Tabla 2 las aplicaciones específicas para la extracción de información en dispositivos Android.

Tabla 2

Aplicaciones específicas de extracción

Herramienta	Descripción
Android Data Extractor Lite	Herramienta desarrollada en Python que permite extraer diagramas de flujo forenses de bases de datos de dispositivos móviles.
WhatsApp Xtract	Herramienta que permite ver las conversaciones de WhatsApp en su computadora de manera simple y sencilla.
Skype Xtractor	Herramienta compatible con Windows y Linux, permite ver información en el archivo main.db de Skype proporciona una amplia variedad de información como la agenda telefónica, chats, mensajes, llamadas, archivos, etc.

Nota. Fuente: Herrera et al. 2019

Herramientas comerciales de pago

En la Tabla 3 se da a conocer las aplicaciones comerciales para la extracción de información en dispositivos móviles con sistema Android.

Tabla 3

Aplicaciones comerciales de extracción

Herramienta	Descripción
Cellebrite Touch	Opera con aproximadamente 6300 dispositivos de varias marcas entre los principales sistemas operativos.
Encase Forensics	Su amplia gama de funciones incluye la identificación de archivos cifrados y el intento de descifrarlos utilizando Passware_Kit_Forensic, esta herramienta contiene algoritmos especiales para el descifrado.

Oxygen_Forensic_Suite	Su funcionamiento es capaz de extraer información de aproximadamente 10000 dispositivos de diferentes marcas, como también puede extraer información de servicios de la nube, con la particularidad de hacer copias de seguridad.
MobileEdit_Forensic	Capaz de obtener información del sistema del dispositivo y puede realizar operaciones avanzadas, como obtener el volcado de memoria del dispositivo, saltarse seguridades de bloque en dispositivos y generar informes de la investigación.
Elcomsoft_Forensic_Toolkit	Permite la adquisición física de información en dispositivos Apple y Android. También, incluye otras funciones de descifrar llaveros que almacena el dispositivo, conjuntamente permite registrar cada operación realizada durante el proceso.

Nota. Fuente: Herrera et al. 2019

1.2. Proceso investigativo metodológico

En el proceso de investigación se utiliza la metodología aplicada debido que se recolecta información cuantitativa y cualitativa, convirtiéndose en una investigación de tipo no experimental. Al analizar los contenidos de las diferentes características que componen los procedimientos permite sintetizarlos eficientemente para la redundancia del contenido e inclusión de información irrelevante. Se aplica métodos de investigación como el de inducción y también la deducción para la optimización de procesamiento de evidencias digitales parte de premisas obtenidas del análisis jurídico con la finalidad de que el procedimiento sea considerado, evidente y demostrable a partir de la evidencia obtenida, la base del procedimiento tiene un esquema de adquisición que cumple con etapas esenciales para prácticas informáticas forenses.

Los materiales de uso para la investigación son de diversas fuentes bibliográficas, reseñas, artículos y revistas científicas que sustentan el proyecto. En el desarrollo de la investigación se utiliza métodos científicos, también el teórico, prevaleciendo el método histórico, para definir

los contextos de la investigación referente a los análisis forenses desde los inicios hasta la actualidad; en donde el análisis y la síntesis se usa para esquematizar algunas opiniones de diferentes fuentes de investigación. Las técnicas científicas y analíticas especializadas se usan para facilitar la recuperación y procesamiento de la información la cual consta de las siguientes etapas: identificar, preservar, analizar y presentar informe con resultados.

1.3. Análisis de resultados

En los resultados se muestra los fundamentos sobre la investigación recolectada los cuales sirven para determinar términos referentes a lo forense y son la parte fundamental para el desarrollo del presente proyecto para poder determinar una guía forense para dispositivos móviles con sistema operativo Android, lo cual permitió obtener datos para establecer un informe pericial.

CAPÍTULO II: PROPUESTA

1.1. Fundamentos teóricos aplicados

Informática forense en dispositivos Android

Es una de las disciplinas de la ciencia forense que se encarga de la identificación, preservación, recuperación y documentación e interpretación de evidencias de diferentes fuentes digitales mediante la aplicación de metodologías científicas. En el proceso de recolectar la evidencia digital es fundamental facilitar la redención de hechos y el posterior uso de esa evidencia como prueba en los tribunales (Tiffany, 2019).

Evidencia Digital

Se considera como una forma de evidencia física que está compuesta por campos magnéticos o pulsos electrónicos, los mismos que se recolectan para analizarlos mediante herramientas especializadas de análisis forense. La evidencia digital se denomina medio de alta validez porque puede ser utilizada como prueba en la legislación informática de cualquier país donde se aplica a cualquier tipo de datos extraídos del hardware (Villacres et al., 2021).

Informática forense en dispositivos móviles Android

El uso de diferentes softwares en computadoras y móviles promueve la obtención de información no solo de gran importancia, también el poder hacer una copia exacta de llamadas, documentos, videos, fotos e incluso información eliminada. Dentro de la informática forense en dispositivos móviles con tecnología Android da origen a etapas de proceso como son; incautación, adquisición forense, análisis y producción de datos recopilados; así como adquisición lógica, física de sistemas en computadoras y dispositivos móviles (Revista Ingenio, 2017).

Tipos de adquisición de datos en dispositivos

Manual: se requiere manipular el dispositivo buscando evidencias en los archivos del dispositivo móvil.

Lógica: en este tipo de adquisición de datos se emplea cables, software y hardware, para extraer los datos del dispositivo móvil.

Física: esta forma de adquisición es mediante un proceso de obtención de la copia de los datos de bit a bit del chip de almacenamiento de datos conocida como Jtag, la cual se conectan un conjunto de cables a la memoria del dispositivo para ser extraído, esta forma es la técnica más compleja de extracción.

Procedimiento forense en dispositivos Android

Consiste en aplicar algunas técnicas científicas para posterior análisis especializado con diferentes herramientas para facilitar el la recuperación y el procesamiento de la información luego de la ocurrencia de un determinado tipo de incidente. El procedimiento forense se da en fases las cuales ayudan a recopilar información, autenticación, revisión de datos; pero es necesario saber cuáles son los que deben examinarse y cuáles son las pruebas a aplicar en el marco de una investigación. El análisis forense es una disciplina que utiliza la tecnología más avanzada para preservar la integridad de los datos con los procedimientos adecuados. No solo ayuda a comprobar y ataques informáticos, sino también a recuperar y eliminar información, lo que requiere un conocimiento profundo de software (Estrada, 2017).

Código Orgánico Integral Penal (COIP)

Determina una serie de sanciones relacionadas a delitos informáticos y de telecomunicaciones, en la Tabla 4 se describen los artículos.

Tabla 4

Artículos en delitos informáticos

Artículo	Descripción
6	Comiso penal, deriva en casos de delitos dolosos y recae en los bienes cuando son instrumentos, productos o réditos de comisión de delito.
174	Ofertar servicios sexuales con menores de edad por medios electrónicos.
190	Apropiarse de forma fraudulenta por medios electrónicos.
191	Reprogramación o alteración de la información de terminales móviles.
192	Intercambiar, comercializar o importe de información de terminales móviles.
193	Reemplazar la identificación de terminales móviles.

194	Comercializar de forma ilícita terminales móviles.
195	Infraestructura de forma ilícita.
229	Revelar ilegalmente base de datos.
230	Interceptar ilegalmente datos.
232	Atacar la integridad de sistemas de información.
234	Acceso no autorizado a sistema informático, telemático o telecomunicaciones.
354	Espionaje.

Nota. Fuente: Código Orgánico Integral Penal

La Ley de Comercio Electrónico, Firmas y Mensajes de Datos

La ley establece regular y sancionar las infracciones que se atribuyen a lo relacionado con los sistemas de información, redes electrónicas e internet como se muestra en la Tabla 5.

Tabla 5

Artículos de la Ley de Comercio Electrónico

Artículo	**Descripción**
5	Confidencial y reserva.
8	Conserva de mensajes de datos.
9	Protección de datos.
10	Procedencia e identidad de un mensaje de datos.

52	Medios de prueba
55	Valoración de la prueba
57	Infracciones informáticas.

Nota. Fuente: Ley de Comercio Electrónico, Firmas y Mensajes de Datos

Reglamento del Sistema Pericial Integral de Función Judicial

En la Tabla 6 se describen los artículos de las obligaciones de los peritos.

Tabla 6

Artículos de obligaciones de los peritos

Artículo	Descripción
19	Obligaciones Específicas
20	Formato

Nota. Fuente: Sistema Pericial Integral 2014

Métodos para el análisis forense

En la Tabla 7 se detalla el análisis forense el cual consta de un conjunto de etapas

Tabla 7

Método de análisis forense

Técnica	Descripción
Acceso	Solicita autorización para que no entre en conflicto con las políticas y leyes, luego de la autorización comenzaremos a evaluar cuáles son los principales datos a extraer.
Obtención	Inicia la investigación y el acceso a los datos para que puedan ser extraídos y almacenados.
Análisis	Analiza toda la información recolectada, dependiendo del tipo de datos el análisis es diferente ya que se encuentra varios tipos de archivos.

Reporte	Organiza toda la información que ha sido analizada y evaluada para su presentación en un informe.

Nota. Fuente: Elaboración propia

Sistema operativo Linux Distribución Santoku

Es un sistema operativo basado en la distribución de Lubuntu el cual permite experimentar en terminales móviles en busca de errores o alguna vulnerabilidad que pueda invadir la privacidad mientras se usa uno de estos dispositivos móviles (Velasco, 2018).

Sistema operativo Linux Distribución CAINE

Es un sistema operativo de basado en Ubuntu y es utilizado en modo especializado para realizar análisis forense, buscar datos ocultos y eliminados en discos e identificar información residual para restaurar un sistema (Velasco, 2018).

Herramienta HashCalc

Es una herramienta libre que permite HashCalc es una calculadora gratuita que permite la detección de descargas y cargas corruptas. Usando tres formatos de datos de entrada: cadena hexadecimal, cadena de texto y archivos, uno puede comparar rápidamente imágenes, audio, películas y verificar archivos de CD y disco duro (SlavaSoft Inc, 2022).

Herramienta forense Autopsy

Es una plataforma digital forense de código abierto, escanee unidades de almacenamiento como discos duros, memorias, teléfonos y otros dispositivos que contengas datos. Esta herramienta se utiliza en todo tipo de casos de análisis forense digital: fraude, robo y robo de identidad, robo de datos de empleados o corporativos, pero es principalmente software que ha probado su utilidad en casos de pornografía infantil en donde se ha utilizado para detectar y ayudar a llevar a los culpables ante las autoridades. Se pueden ver sospechas de fotos, videos, archivos de texto, correos electrónicos, mensajes de WhatsApp y todos los archivos que han sido eliminados en un intento de evadir y la justicia (Tusclases, 2022).

1.2. Descripción de la propuesta

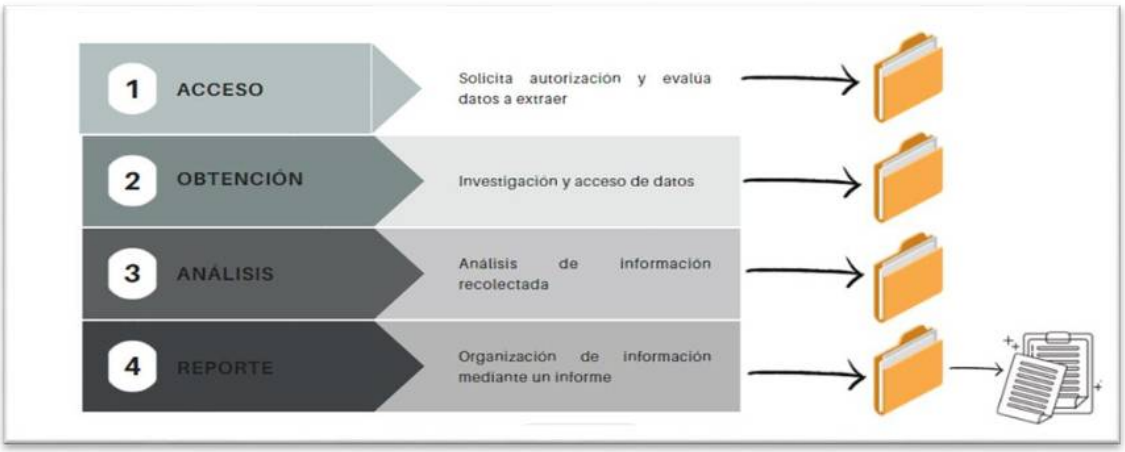
En el proyecto se propone una metodología forense para dispositivos con sistema operativo Android, tiene como propósito ser un referente para la investigación en delitos tecnológicos con dichos dispositivos, en donde se puede extraer información que podría ser de ayuda para aclarar el acto cometido, para complementar la guía se recurre al uso de la herramienta de investigación forense Autopsy en la que se obtendrá datos para un proceso de investigación judicial, al ser este proyecto una propuesta queda permitido su uso de forma libre para los usuarios.

a. Estructura general

Para el diseño de la propuesta se plantea un método que se lo denomina Modelo Basado en Dispositivos Móviles Android (MBDMA), el procedimiento a seguir está definido por etapas que sirven para proceder con la investigación forense en dispositivos móviles con sistema Android, se toma como base dicho modelo, para el efecto se definen cuatro etapas que se muestran en la Figura 1.

Figura 1

Modelo Basado en Dispositivos Móviles Android



Nota. Fuente: Elaboración propia

b. Aplicación del aporte

En el presente documento se da a conocer un modelo de procedimiento a seguir para análisis forense en dispositivos móviles con sistema operativo Android; a continuación, se explica las etapas a seguir para el desarrollo de dicha metodología:

Etapas

Una vez realizado el esquema de la propuesta se procede a enfatizar la importancia de cada etapa que permita una adecuada investigación usando técnicas que admita la aplicación de la normativa vigente, se presenta las siguientes etapas que se utilizan en un caso de análisis:

- Acceso a la escena: esta etapa es posible mediante la participación de personas encargadas de brindar seguridad en el lugar de los hechos con la finalidad de obtener datos para proceder con la normativa legal vigente del Ecuador, identificando la evidencia mediante la indagación de los equipos móviles a investigar.
- Obtener datos: Es necesario que se aplique la cadena de custodia la cual garantiza la protección de la información desde que inicia hasta que finaliza.
- Analizar datos: consiste en la revisión absoluta de los datos obtenidos que permite identificar evidencias que aporten con decisiones dentro de un proceso judicial.
- Reporte: En esta etapa final se procede al desarrollo del informe de tal forma que los hallazgos obtenidos proporcionen un panorama de los hechos del delito que se haya cometido.

c. Modelo propuesto

En base a las etapas anteriormente expuestas se propone un modelo a seguir, para lo cual se presenta a continuación una simulación con la guía forense para investigación de dispositivos móviles con sistema Android, la cual sirve para identificar las posibles evidencias que se puede encontrar en un dispositivo móvil.

Etapa de acceso

En esta etapa se cuenta con la participación de personas encargadas de brindar seguridad en el lugar de los hechos en donde se incauta las evidencias en este caso el dispositivo, luego se emite la orden en la que se designa a un perito para que haga la respectiva investigación, después de ello se facilita el dispositivo para continuar con la investigación.

Prerrequisitos

Para someter al equipo a investigación forense hay que tomar en cuenta ciertos requisitos que se describen a continuación:

- Dispositivo funcional
- Dispositivo sin bloqueos de pantalla
- Dispositivo con acceso a root o privilegios de administrador
- Dispositivo activado el modo depuración USB
- Dispositivo en modo Avión

En caso de no cumplir estos requisitos no será posible la investigación del dispositivo en el proceso de extracción de datos de forma lógica como se propone en este proyecto, de ser el caso se tendría que recurrir a métodos de extracción avanzada como la utilización de aparatología especializada mediante técnica de Jtag la cual consisten en extraer el chip de memoria donde se encuentra almacenado la información para posteriormente conectarlo mediante una serie de cables soldados a la memoria del dispositivo extraída para acceder a la información, en situaciones en las que los dispositivos su pantalla se encuentra rota o no este accesible se podría utilizar aplicaciones comerciales las cuales permiten obtener los datos del dispositivo. Después de revisar los requisitos que se cumplen, se procede a continuar con la investigación aplicando el modelo propuesto.

Asegurar la escena

Se recibe el dispositivo móvil que fue incautado, el mismo que se lo coloca en el espacio de trabajo del investigador, luego se procede a tomar fotos de cómo se recibe el dispositivo, para adjuntar al informe.

Figura 2

Dispositivo móvil simulación de caso

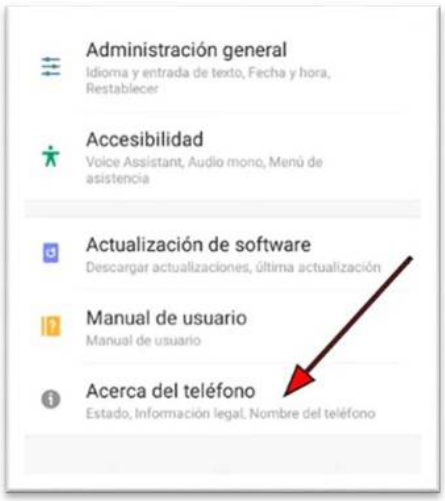
Nota. Fuente: Elaboración propia

Identificar evidencias

Para identificar la evidencia se procede a registrar las características del equipo, dichos datos se encuentran en la información del sistema del celular o parte de las características se encuentran en la aparte interna del dispositivo como se puede observar en la Figura 2. Para este caso se utiliza el siguiente equipo:

Figura 3

Información del dispositivo móvil simulación de caso



Nota. Fuente: Elaboración propia

Tabla 8

Características del dispositivo móvil

Detalle	Característica
Marca	Samsung
Modelo	J610m
Serie o IMEI	3,52234E+15
Sistema Operativo	Android 8
RAM	2 GB
Almacenamiento	32 GB
Procesador	Exynos 7780
CPU	4 cores 1.80 GHz

Nota. Fuente: Elaboración propia

Etapa de obtención

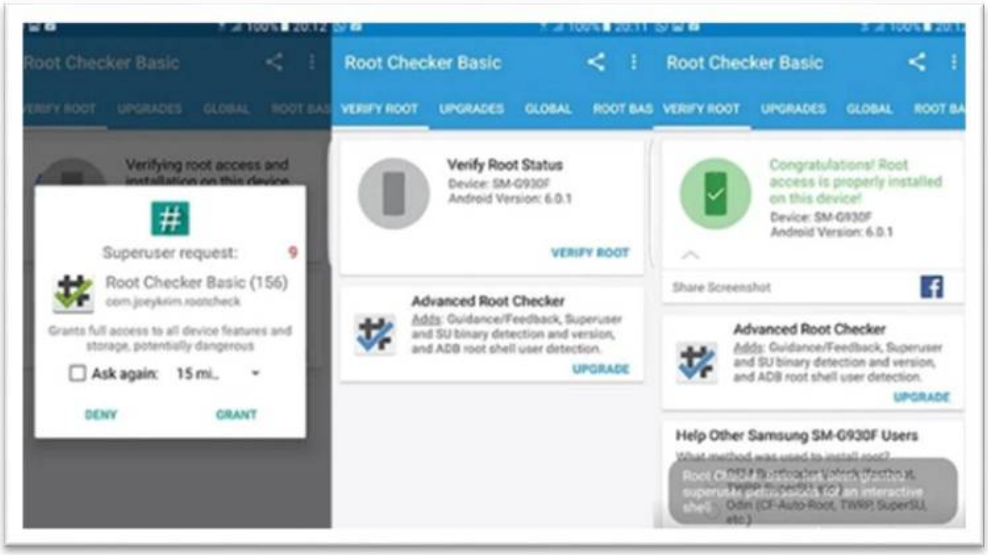
En esta etapa se procede a extraer los datos del dispositivo mediante algunas herramientas, para lo cual se debe seguir el siguiente procedimiento:

1. Verificar si el dispositivo tiene acceso root, lo que significa tener privilegios de administrador, si fuera el caso de que no, se recurre a utilizar herramientas de rootear. Para verificar que el dispositivo tenga dicho acceso, se puede instalar una aplicación llamada Root Checker, como se muestra en la Figura 4 donde aparece una ventana

flotante de la aplicación. De no ser así, no habrá permisos de acceso como administrador, es recomendable tener el acceso root ya que permite acceder a todo el almacenamiento del sistema, si no es posible obtener dichos privilegios también se puede obtener los datos del dispositivo para investigación, mediante la utilización de otra herramienta que posteriormente se presenta.

Figura 4

Verificación del móvil si dispone de acceso administrador



Nota. Fuente: Elaboración propia

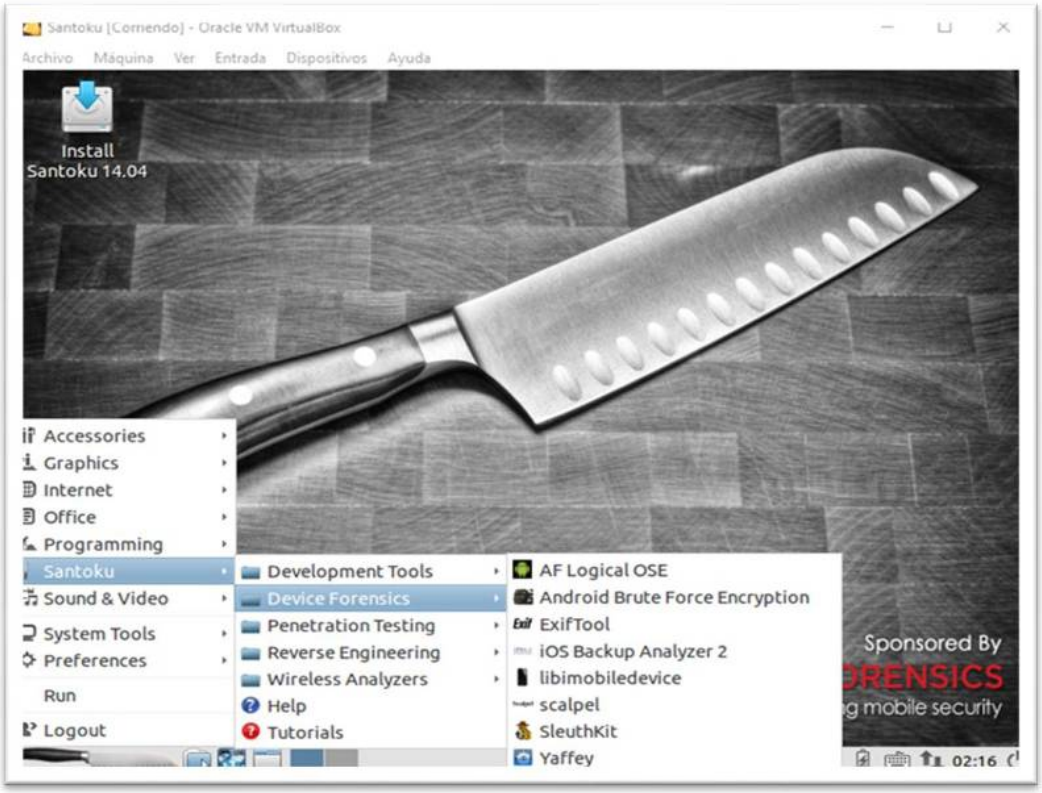
Si el dispositivo no se encuentra con acceso root, en este caso habrá que guiarse de la página web de Dr.fone, donde se puede encontrar la guía de cómo proceder a obtener acceso root al dispositivo en el siguiente enlace: https://n9.cl/fix42

Hay que tener en cuenta que el proceso de obtener privilegios de administrador en algunos dispositivos tiene riesgo ya que a partir de sistemas operativos con versión de Android 8 posterior tienen la seguridad de cifrar el dispositivo, lo cual al momento de rootear puede borrar los datos de dicho dispositivo, si fuera el caso ir al ítem 10.

2. Para dispositivos con acceso root se procede a usar la herramienta adb del sistema operativo *Santoku*, dicho sistema es una distribución de Linux el cual se lo puede cargar en modo Live sin necesidad de instalarlo o a su vez en una máquina virtual, como se puede observar en la Figura 5, este sistema contiene herramientas esenciales para el proceso. Se puede descargar en el siguiente enlace: https://n9.cl/l5a9r

Figura 5

Sistema Operativo Santoku montado en máquina virtual



Nota. Fuente: Elaboración propia

3. Se debe entrar en el dispositivo en modo Avión, también contar con privilegios *root* y estar activado la depuración USB, para activar dicha opción se puede regir en el siguiente enlace: https://n9.cl/noeb8.
4. Las herramientas que se dan a conocer permiten acceder a la información del dispositivo, con la finalidad de crear una imagen forense de los datos de usuario.
5. En este punto se procede a conectar del dispositivo a la computadora para escribir los comandos necesarios para generar la imagen de los datos del dispositivo móvil.
6. Se procede abrir una ventana de terminal y se escribe el comando adb devices, en donde mostrará en la pantalla del dispositivo un mensaje el cual se debe permitir la conexión con el equipo, luego en el terminal muestra el dispositivo conectado.
7. Se debe escribir el comando adb shell, para que se muestre el contenido del dispositivo como se muestra en la Figura 6.
8. Una vez que se muestra el contenido se procede a escribir el comando adb backup -f respaldo.ab -all con este comando se logra respaldar la información del dispositivo para posteriormente ser analizada.

Figura 6

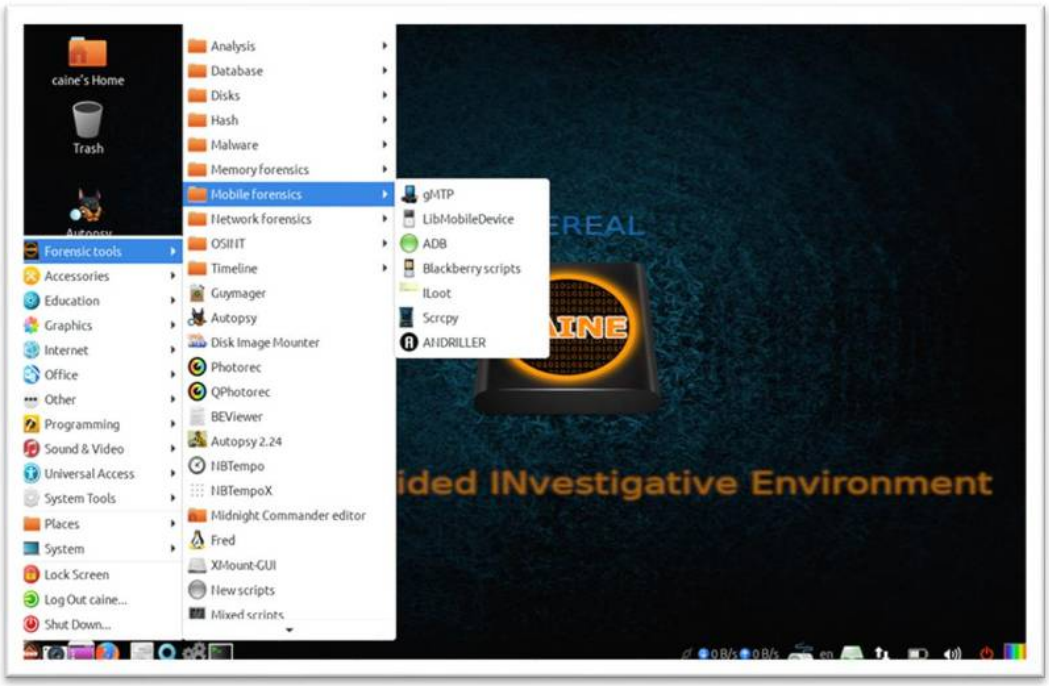
Datos obtenidos con adb shell en sistema operativo Santoku

Nota. Fuente: Elaboración propia

9. Inmediatamente el proceso comienza con la creación de la imagen creada de los archivos del usuario, estos datos obtenidos serán analizados posteriormente.
10. En el caso de que no se logró obtener privilegios de administrador del dispositivo se procede a utilizar otro método que es el caso de utilizar otra distribución de Linux conocida como CAINE, la cual se puede montar en un ambiente virtual como se muestra en los pasos anteriores.
11. En dispositivos sin acceso root se usa la herramienta Andriller del sistema operativo *CAINE*, dicho sistema es una distribución de Linux el cual se lo puede cargar en modo Live sin necesidad de instalarlo o a su vez en una máquina virtual; contiene herramientas esenciales para el proceso, este sistema operativo se muestra en la Figura 7. Puede descargarse en el siguiente enlace: https://n9.cl/sdsy3

Figura 7

Sistema Operativo CAINE montado en máquina virtual

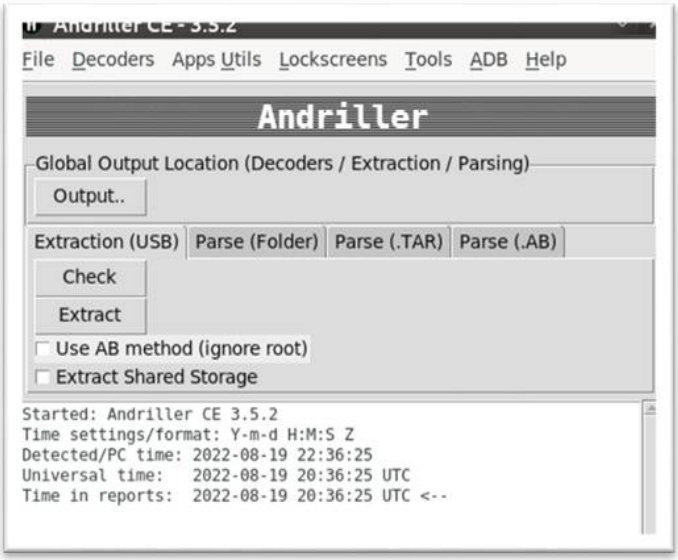


Nota. Fuente: Elaboración propia

12. Para utilizar la herramienta del sistema operativo CAINE hay que activar la depuración USB, para hacerlo se puede regir en el siguiente enlace: https://n9.cl/noeb8.
13. Abrir la herramienta ANDRILLER la cual permite conectar el dispositivo a la computadora para la extracción de los datos que son sujetos a posterior análisis, su interface se muestra en la Figura 8.

Figura 8

Pantalla principal de la aplicación Andriller



Nota. Fuente: Elaboración propia

14. Seleccionar el directorio en donde se guardará la extracción de datos en el icono Output. De igual manera en la pestaña de Parse(Folder) seleccionar el mismo directorio que selecciono en la carpeta anterior.
15. Colocar el dispositivo en modo Avión y luego conectar, seguidamente dar click en el botón Check, para que en la pantalla del dispositivo se muestre un mensaje en el que se debe permitir la conexión con el equipo, al ejecutar estas indicaciones aparecerá en la aplicación que el dispositivo está conectado.
16. Luego de haber conectado el dispositivo seleccionar las opciones de: Use AB method (ignore root) y la opción Extract Shared Storage, una vez seleccionado estas opciones está listo el dispositivo para la extracción de datos, finalmente dar click en el botón Extract, con lo cual se empieza a extraer la información, el tiempo del proceso es variable de acuerdo a la capacidad de almacenamiento del dispositivo.
17. Cuando finalice el proceso de extracción de la información se muestra una ventana en el navegador de internet con el resumen del proceso de extracción de datos.

18. Con el proceso de extracción de los datos por cualquiera de los medios que anteriormente se menciona se procede a realizar una clave de algoritmo mediante la herramienta HashCalc con la que se identifica que la información extraída no se ha sometido a modificaciones, garantizando la autenticidad en futuras extracciones para investigación.
19. Dentro de la aplicación, se genera los hashes (md5, sha1, sha256) o algún otro tipo de algoritmo matemático, que permite validar la obtención de los datos de una imagen generada durante los procesos de investigación. Para lo cual se utiliza la herramienta de HashCalc que se puede descargar desde el enlace: https://n9.cl/0ch0z
20. Una vez que se obtiene la imagen del dispositivo se sube al aplicativo HashCalc como se muestra en la Figura 9 para obtener un identificador de hash el cual si a un futuro se hace alguna modificación del sistema se podrá identificar mediante la comparación con otra imagen del dispositivo que se carga nuevamente al programa y se generara otro hash que al momento de confrontar el algoritmo debe ser el mismo no debería cambiar, si aconteciera quiere decir que el dispositivo o la imagen del dispositivo que se obtuvo se modificó.

Figura 9

Generar un hash de la imagen obtenida del dispositivo

Nota. Fuente: Elaboración propia

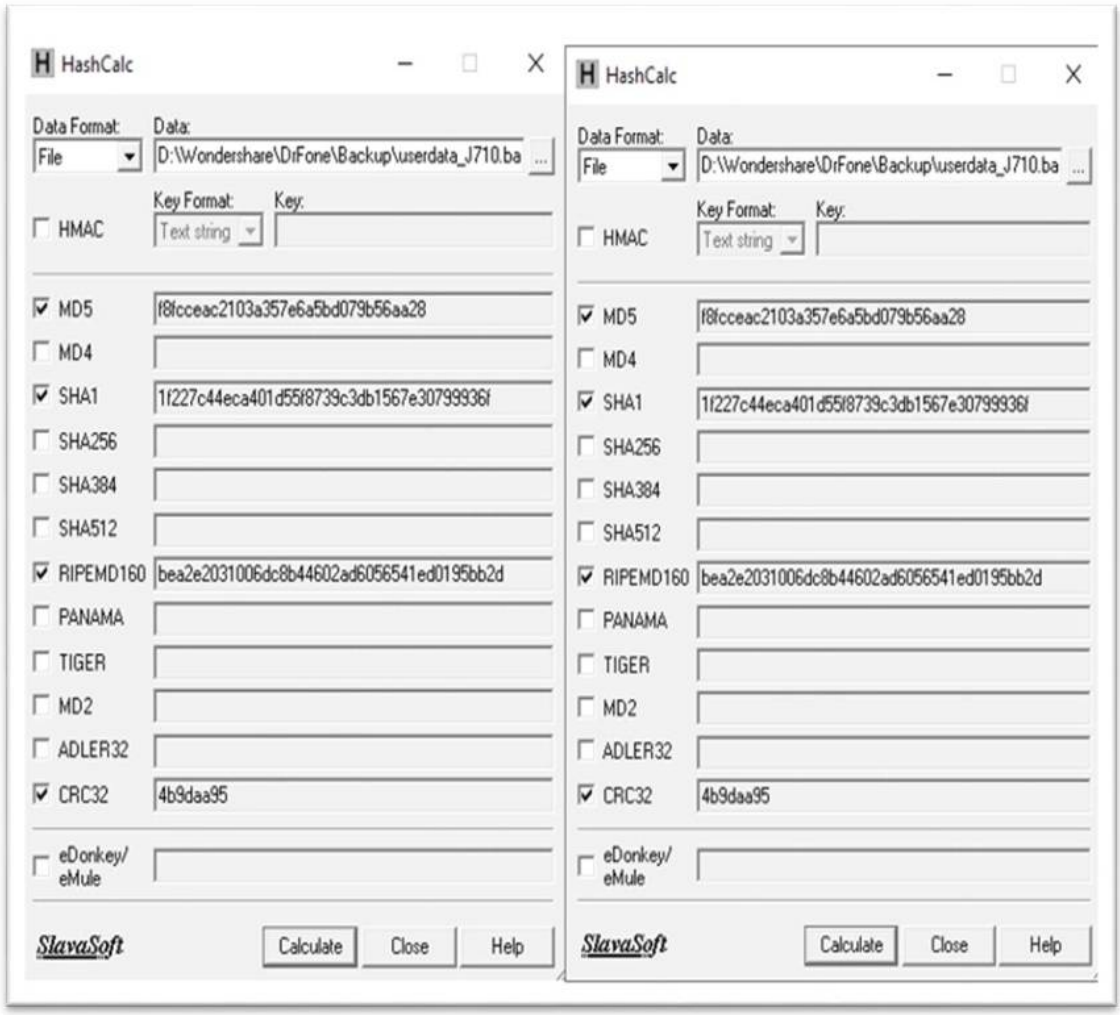
Etapa de análisis

Una vez que se ha comprobado el hash con el algoritmo matemático se procede a cargar los datos obtenidos en la herramienta de análisis Autopsy. Se puede utilizar en el sistema operativo CAINE ya que se encuentra precargado o a su vez se obtiene en Windows, para obtener la herramienta se puede dirigir al siguiente enlace: https://n9.cl/nmhg9f

Luego de comparar los hashes constatando que la imagen no ha sido alterada, como se muestra en la Figura 10 se procede a cargar los datos obtenidos y se configura los módulos a ejecutarse en el proceso de análisis con el programa Autopsy.

Figura 10

Generar un hash de la imagen obtenida del dispositivo



Nota. Fuente: Elaboración propia

Figura 11

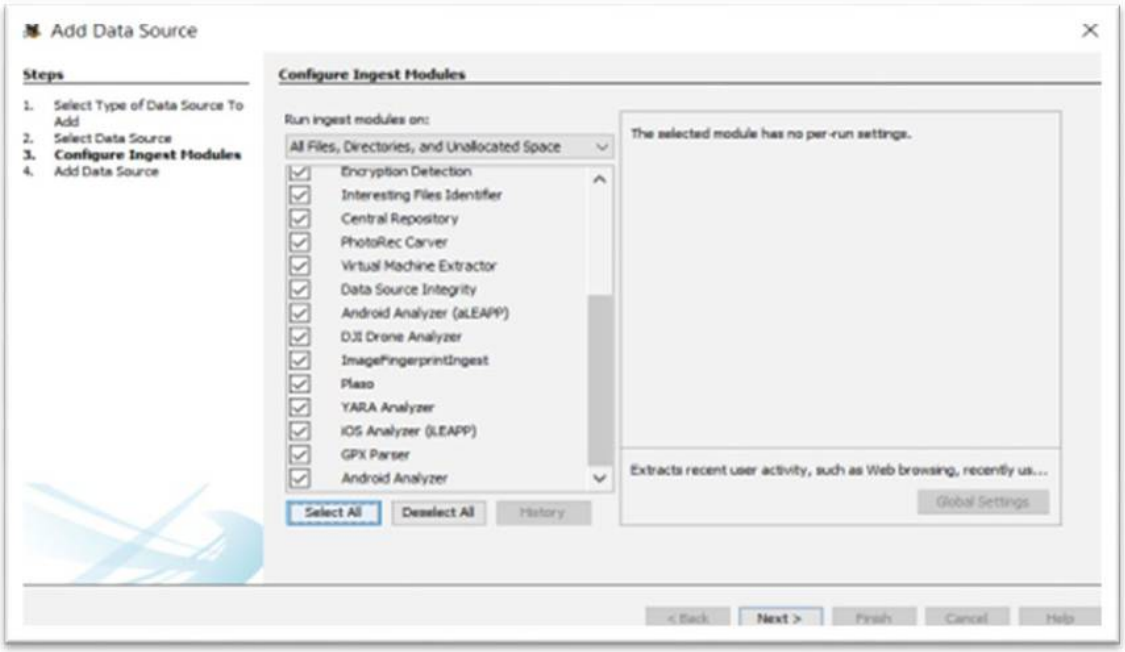
Interface inicial de herramienta de análisis Autopsy

Nota. Fuente: Elaboración propia

En este punto se inicia con el análisis de los datos cargados a través de los módulos que tiene Autopsy, en donde se crea un nuevo caso y se llena los datos correspondientes a identificar en el caso de investigación culminado el proceso se muestra los datos del análisis encontrando como se muestra en la Figura 12 los archivos que pueden ser considerados probatoria para el caso de delito, como registros de llamada, mensajes, archivos borrados y otros datos comprometedores para registrar en el informe como evidencias en el caso de estudio.

Figura 12

Backup del dispositivo cargada para análisis en Autopsy

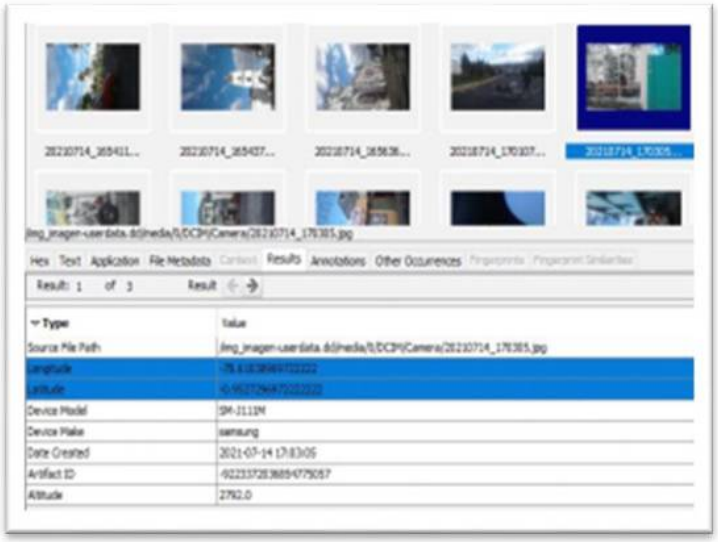


Nota. Fuente: Elaboración propia

Después de seleccionar los módulos de análisis, se comienza a revisar los datos encontrados en este caso siendo una simulación, se encuentra imágenes captadas con el dispositivo incautado.

Figura 13

Hallazgos del dispositivo que se encontraron como evidencia



Nota. Fuente: Elaboración propia

Etapa de reporte

En esta etapa se procede a elaborar el respectivo informe con los hallazgos encontrados en donde se registra las fotografías tomadas del dispositivo recibido, la información del dispositivo, los datos encontrados o evidencia para que posteriormente se remita dicho informe a la autoridad correspondiente.

Elaboración y presentación de informe pericial

Luego del análisis de los datos y obtención de la información que puede ser evidencia se procede a elaborar el informe pericial de referencia al formato que se puede observar en el Anexo 2, del Consejo Nacional de la Judicatura de acuerdo al Reglamento del Sistema Pericial Integral de Función Judicial, establecido en los artículos 19 y 20 de los peritos, en donde se debe registrar el proceso de investigación.

d. Técnicas

Mediante la aplicación de la metodología y la utilización de herramientas de análisis forense en dispositivos móviles con sistema Android permite obtener datos relevantes que pueden ser utilizados como evidencia en el caso de un delito que se encarga de hacer peritaje las autoridades correspondientes para aclarecer los actos de delito cometido. Con la propuesta se puede canalizar técnicas para obtener información en dispositivos de casos de investigación y esta técnica al ser aplicable en dispositivos móviles con sistema Android, permite realizar una investigación forense sobre el mismo.

1.3. Validación de la propuesta

Según (Palacios, 2022), dice que el método Delphi es un proceso de consentimiento que requiere la participación de un grupo de personas que conocen de una temática los cuales evalúan un proyecto de forma anónima sin interacción entre ellos. Para la valoración del proyecto se recurre a utilizar el método Delphi para posteriormente aplicar una serie de preguntas en base a una encuesta utilizando la herramienta de la web QuestionPro para el diseño y obtención de resultados.

Situación

Evaluar el uso de aplicación de una metodología forense para dispositivos con Sistema Operativo Android, en base a un modelo previamente enviado a los profesionales que se seleccionó como se muestra en la Tabla 9.

Tabla 9

Participantes para la evaluación de la propuesta

Participante	Rama del profesional	Conocimiento
Barahona Gustavo	Informática	Sistemas Informáticos Hardware y Software Dispositivos celulares y computadoras
Castillo Carlos	Informática	Sistemas Informáticos Hardware y Software Dispositivos celulares y computadoras
Escobar Fernanda	Electrónica	Electrónica Dispositivos celulares
Haro Carlos	Telecomunicaciones	Telecomunicaciones Hardware dispositivos celulares
Sánchez Omar	Electrónica	Electrónica y Telecomunicaciones Dispositivos celulares

Nota. Fuente: Elaboración propia

Preguntas para evaluación

Se diseña una encuesta, ver Anexo 1, con preguntas para validar la propuesta, a continuación, se describen las preguntas planteadas.

1.- ¿Seleccione la rama profesional a la que pertenece?

2.- ¿La metodología puede usarse con previos conocimientos?

3.- ¿Logró descargar las herramientas desde los links que se encuentran en la metodología?

4.- ¿Al aplicar la metodología pudo obtener información sobre el dispositivo que uso?

5.- ¿En qué fase de la metodología tuvo dificultad?

6.- ¿Recomendaría a otras personas la metodología opuesta?

Resultados

En los resultados de la encuesta aplicada se procede al análisis y tabulación de los mismos los cuales se presentan a continuación.

Pregunta número 1 de la validación de la propuesta que se muestra en la Tabla 10.

Tabla 10

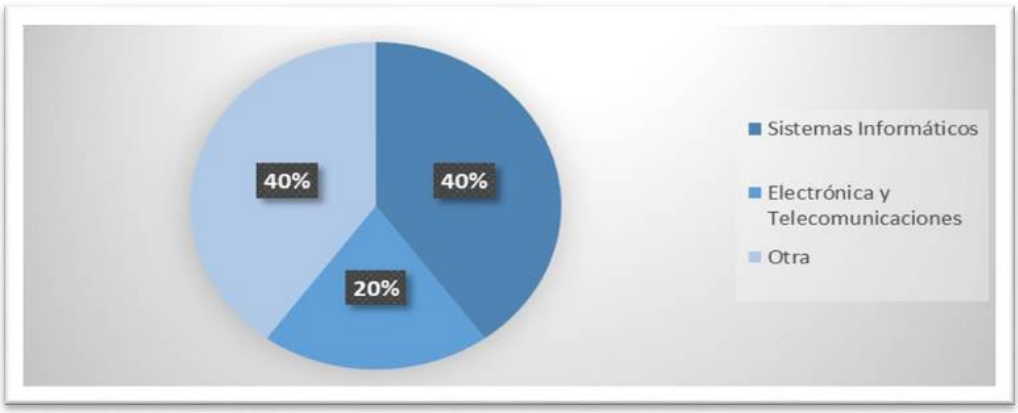
Encuesta pregunta 1

1.- ¿Seleccione la rama profesional a la que pertenece?	
Sistemas Informáticos	40%
Electrónica y Telecomunicaciones	20%
Otra	40%
Total	**100%**

Nota. Fuente: Elaboración propia

Figura 14

Encuesta pregunta 1



Nota. Fuente: Elaboración propia

En el resultado de la pregunta 1 se puede observar que el 40% de los encuestados es de la rama de Informática, así como también el otro 40% es de la rama de Electrónica y Telecomunicaciones, a diferencia que solo el 20% es de otra rama.

Pregunta número 2 de la validación de la propuesta que se muestra en la Tabla 11.

Tabla 11

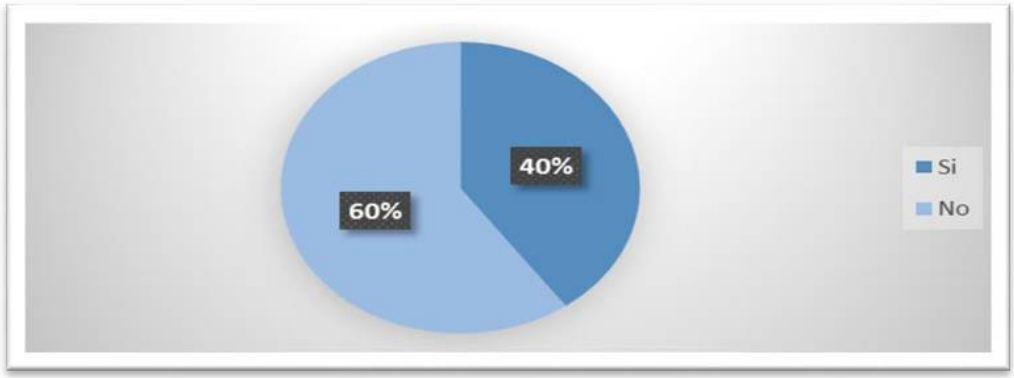
Encuesta pregunta 2

2.-¿La metodología puede usarse con previos conocimientos?		
Si	2	40%
No	3	60%
Total	**5**	**100%**

Nota. Fuente: Elaboración propia

Figura 15

Encuesta pregunta 2



Nota. Fuente: Elaboración propia

En el resultado de la pregunta 2 se puede observar que el 60% de los encuestados dice que no hace falta conocimientos previos a diferencia del 40% que opina que si se necesitaría conocimientos previos.

Pregunta número 3 de la validación de la propuesta que se muestra en la Tabla 12.

Tabla 12

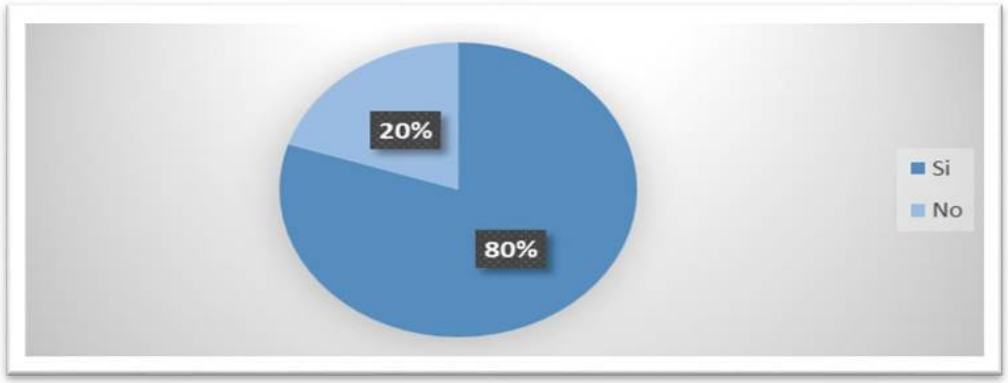
Encuesta pregunta 3

3.- ¿Logró descargar las herramientas desde los links que se encuentran en la metodología?		
Si	4	80%
No	1	20%
Total	**5**	**100%**

Nota. Fuente: Elaboración propia

Figura 16

Encuesta pregunta 3



Nota. Fuente: Elaboración propia

En el resultado de la pregunta 3 se puede observar que el 80% de los encuestados dice que logró descargar los recursos desde los links, del 20% que no lo pudo hacerlo.

Pregunta número 4 de la validación de la propuesta que se muestra en la Tabla 13.

Tabla 13

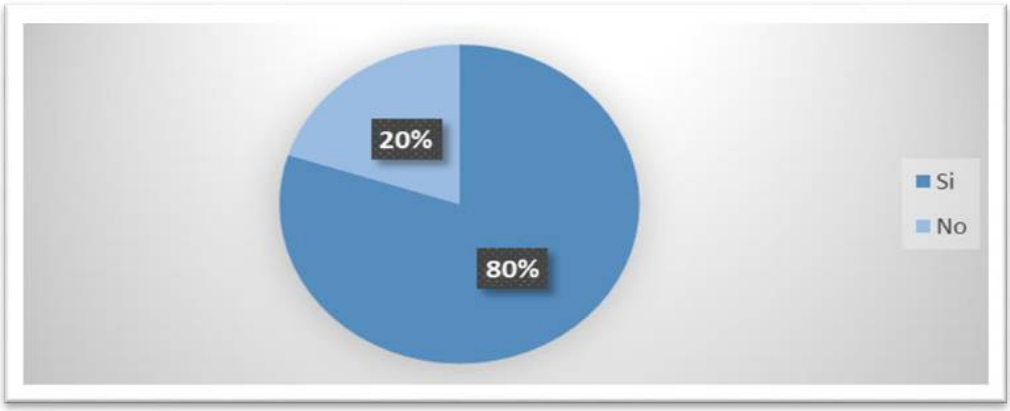
Encuesta pregunta 4

4.- ¿Al aplicar la metodología pudo obtener información sobre el dispositivo que uso?		
Si	4	80%
No	1	20%
Total	**5**	**100%**

Nota. Fuente: Elaboración propia

Figura 17

Encuesta pregunta 4



Nota. Fuente: Elaboración propia

En el resultado de la pregunta 4 se puede observar que el 80% de los encuestados dice que obtuvo datos del dispositivo, mientras que el 20% que no obtuvo la información.

Pregunta número 5 de la validación de la propuesta que se muestra en la Tabla 14.

Tabla 14

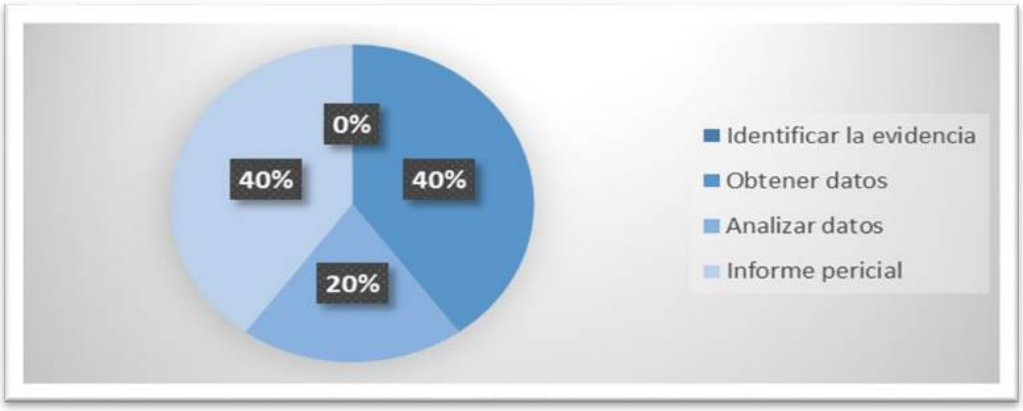
Encuesta pregunta 5

5.- ¿En qué fase de la metodología tuvo dificultad?	
Identificar la evidencia	0%
Obtener datos	40%
Analizar datos	20%
Informe pericial	40%
Total	**100%**

Nota. Fuente: Elaboración propia

Figura 18

Encuesta pregunta 5



Nota. Fuente: Elaboración propia

En el resultado de la pregunta 5 se puede observar que el 40% de los encuestados tuvo dificultad en obtener datos, al igual que el 40% que tuvo inconvenientes en el informe, a diferencia del 20% que se le dificulto en el análisis de los datos.

Pregunta número 6 de la validación de la propuesta que se muestra en la Tabla 15.

Tabla 15

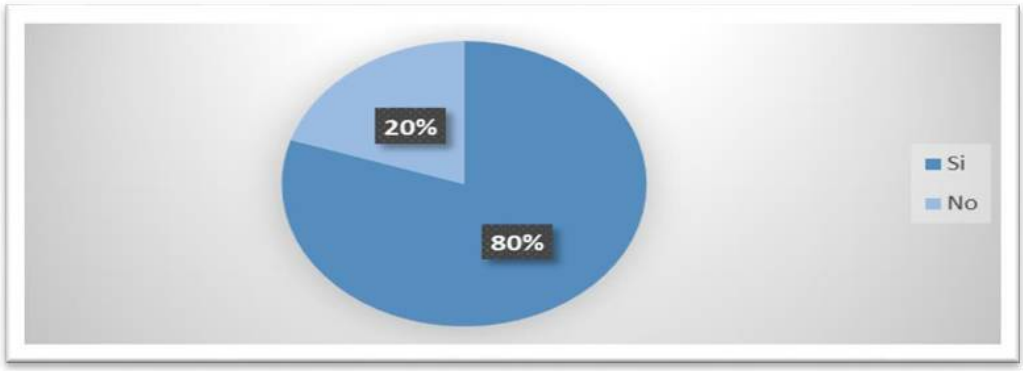
Encuesta pregunta 6

6.- ¿Recomendaría a otras personas la metodología propuesta?		
Si	4	80,00%
No	1	20,00%
Total	**5**	**100%**

Nota. Fuente: Elaboración propia

Figura 19

Encuesta pregunta 6



Nota. Fuente: Elaboración propia

En el resultado de la pregunta 6 se puede observar que el 80% de los encuestados dice que, si recomendaría la guía, a diferencia del 20% que opina que no la recomendaría.

Después de haber demostrado los resultados se llega a la conclusión que los participantes que evaluaron la metodología forense la mayor parte de los encuestados ejecuto satisfactoriamente el modelo propuesto como demuestra los resultados que antecede, evidenciando que al someter a prueba la guía se pudo obtener datos del dispositivo que investigaron.

1.4. Matriz de articulación de la propuesta

En la siguiente matriz se resume la propuesta del proyecto de investigación la cual se encuentra compuesta por; sustentos teóricos, metodológicos, técnicas e instrumentos utilizados en la elaboración del presente documento.

Tabla 16

Matriz de articulación

E. PRINCIPALES	S. TEÓRICO	S. METODOLÓGICO	TÉCNICAS	RESULTADOS	INSTRUMENTOS
Asegurar escena	Resguardar las posibles evidencias en este caso el dispositivo móvil en lugar seguro de trabajo.	Procedimiento de recibir y guardar el dispositivo móvil en el lugar de trabajo seguro.	Modelo Basado en Dispositivos Móviles Android (MBDA)	Se recibe el dispositivo y se procede a almacenarlo en un lugar seguro para ambiente de trabajo.	Dispositivo de captura de fotografías
Identificar la evidencia	Identificar el equipo móvil determinar características y acceso al dispositivo.	Se determina características del dispositivo en las propiedades del sistema operativo y se verifica si hay acceso como usuario Administrador.	Modelo Basado en Dispositivos Móviles Android (MBDA)	Para determinar las características del equipo se obtienen en la información del sistema operativo Android, con el uso de herramienta proporcionar privilegios de usuario administrador.	Módulo de información y etiquetas del dispositivo Android
Obtener datos	Utilización de herramientas para obtener datos del dispositivo investigado.	Obtener y recopilar datos del dispositivo, para posterior análisis en el modelo propuesto.	Modelo Basado en Dispositivos Móviles Android (MBDA)	Conectado el dispositivo al computador con el sistema operativo Linux para obtener una imagen del dispositivo para posterior análisis.	Adb para Android Sistema operativo Linux Santoku Linux CAINE

Analizar datos	Analizar los datos obtenidos que permitan identificar evidencias.	Analizar los datos obtenidos sobre el modelo planteado que permitan determinar procesos legales.	Modelo Basado en Dispositivos Móviles Android (MBDA)	Con la imagen obtenida del dispositivo se obtiene una copia con una base de datos del dispositivo que se va analizar en la herramienta Autopsy.	Generación de algoritmo de autenticidad de datos obtenidos HashCalc Análisis de datos con Autopsy
Informe	Informe en donde se evidencia los datos obtenidos en la investigación forense.	Comparar los datos y resultados obtenidos de la implementación del modelo, para emitir el informe.	Modelo Basado en Dispositivos Móviles Android (MBDA)	Después de analizar y recopilar los datos con la anterior herramienta se emite el respectivo informe con evidencia encontrada.	Formato para informes adjunto en el Anexo 2

Nota. Fuente: Elaboración propia

CONCLUSIONES

Se investigó sobre términos de análisis forense, así como también las herramientas que se utilizan para esta metodología con el propósito de conocer aspectos relacionados con el análisis forense en dispositivos móviles con sistema operativo Android.

Se pudo indagar sobre herramientas para análisis forense, en donde se logró identificar que existen herramientas de uso libre y también de pago o comerciales las cuales permiten realizar investigación forense a dispositivos móviles Android, dichas herramientas permitieron obtener la información necesaria que después se sometió a análisis para identificar evidencias.

Para el diseño de la metodología de análisis forense en dispositivos Android se recurrió al uso del Modelo Basado en Dispositivos Móviles Android (MBDA) el cual sirvió para aplicar la metodología mediante un conjunto de etapas a seguir para ejecutar procedimientos de obtención de datos que pueden servir como evidencia en un caso de delito cometido con un dispositivo móvil con sistema Android.

En base a la metodología Delphi se pudo evaluar la propuesta de la metodología de análisis forense en dispositivos móviles con sistema operativo Android, la cual fue validada por un grupo de profesionales de las áreas de Informática y telecomunicaciones en base a la aplicación de la guía y conjuntamente con una encuesta aplicada a estos participantes, en donde durante su aplicación lograron obtener información del dispositivo que investigaron.

RECOMENDACIONES

Se recomienda profundizar en temas sobre otros dispositivos tecnológicos con los que se podría hacer una investigación forense para identificar delitos cometidos con estos dispositivos, ya que los usuarios disponen de otros tipos de dispositivos que utilizan.

Se recomienda el uso de herramientas comerciales puesto que estas ofrecen más utilidades y sus procesos para investigación forense son más rápidos, en el aspecto comercial estas herramientas permiten obtener datos del dispositivo cuando hay limitaciones en el que el dispositivo no se encuentra accesible.

Se recomienda tener precaución cuando se somete un dispositivo al proceso de tener acceso root o derechos de usuario administrador, hay que considerar que en algunos dispositivos viene cifrado el sistema como es el caso de versiones superiores a Android 8 en las que en el proceso de tener privilegios de administrador se puede perder la información del dispositivo ya que se formatea o se reinicia de fábrica.

Se recomienda que para la activación de servicios de modo depuración USB y para obtener acceso root, buscar información referente al modelo de dispositivo ya que su proceso es distinto por la variedad de marcas de celulares que existen en el mercado.

BIBLIOGRAFÍA

Arias M. (2016). PANORAMA GENERAL DE LA INFORMÁTICA FORENSE Y DE LOS DELITOS INFORMÁTICOS EN COSTA RICA. InterSedes: Revista de las Sedes Regionales, VII(12),141-154. ISSN: 2215-2458. Disponible en: https://www.redalyc.org/articulo.oa?id=66612867010.

Ascheri, M. E., Testa, O., Pizarro, R., Camiletti, P., & Diaz, L. (2017). Utilización de dispositivos móviles con sistema operativo Android para matemáticas.

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. (2016). Dispositivos móviles y apps: Características y uso actual en educación médica.

Carrera Calderón, F. A., & Aguilar Martínez, M. R. (2020). Guía integral de empleo de la informática forense en el proceso penal de Ecuador. Universidad Y Sociedad, 12(S(1), 182-190. Recuperado a partir de https://rus.ucf.edu.cu/index.php/rus/article/view/1773.

CIBERSEGURIDAD (2021, 2 marzo). Análisis forense en dispositivos móviles. Ciberseguridad. https://ciberseguridad.com/servicios/analisis-forense/dispositivos-moviles/.

Código Orgánico Integral Penal. (2018). COIP: Ministerio del Interior. https://n9.cl/xu3yj

Estrada, A. C. (2017). La informática forense y los delitos informáticos. Revista Pensamiento Americano, 4, 81-88.

Herrera, S. I., Figueroa, L. M., Ghunter, D., Lara, C., Viaña, G., Mendez, A., & Lesca, N. (2019). Métodos y herramientas para análisis forense en dispositivos móviles. In XXI Workshop de Investigadores en Ciencias de la Computación (WICC 2019, Universidad Nacional de San Juan)

INDICIOS. (2018, August 23). Historia de la Informática forense | Detectives Madrid. Detectives Madrid. https://detectives-madrid.es/historia-informatica-forense-aplicacion/

Lesca, N. B., Lara, C. C., Figueroa, L. M., & Viaña, G. (2017). Gestión de evidencia digital en dispositivos móviles. In Simposio Argentino de Informática y Derecho (SID)-JAIIO 46 (Córdoba, 2017).

Ley de Comercio Electrónico, Firmas y Mensajes de Datos. (2020). Prueba y Notificaciones Electrónicas. Quito: Ministerio del Interior. https://n9.cl/l1srj.

Lockheimer, H. (2019). Android es para todos. Android; Android. https://www.android.com/intl/es_es/everyone/

Monterrubio-Hernandez, E. (2019). Sistema Operativo. Con-Ciencia Serrana Boletín Científico de la Escuela Preparatoria Ixtlahuaco).

NTS Solutions. (2020, febrero 10). El uso de los dispositivos móviles. https://www.nts-solutions.com/blog/dispositivos-android.html

Palacios, D. (2022, March 23). Qué es el método Delphi, para qué sirve y ejemplos. Hubspot.es. https://blog.hubspot.es/sales/metodo-delphi

Polanco, K. M., & Taibo, J. L. B. (2017). "Android" el sistema operativo de Google para dispositivos móviles. Negotium: revista de ciencias gerenciales, 7(19), 79-96.)

Quispe, H. (2017). Metodología de Análisis Forense Digital para la Extracción de Datos Almacenados en Dispositivos Móviles Basados en Sistema Operativo Android. Umsa.bo. https://doi.org/http://repositorio.umsa.bo/xmlui/handle/123456789/7874.

Revista Ingenio. (2017, May 11). La informática forense en dispositivos Android. ResearchGate; Universidad Francisco de Paula Santander. https://www.researchgate.net/publication/316427536_La_informatica_forense_en_dispositivos_Android.

Revista_Líderes_EC. (2018). Seguridad Informática Regional. Obtenido de https://flashstart.com/es/malware-en-dispositivos-moviles/

Reglamento del Sistema Pericial Integral de la Función Judicial. (2014). Obligación de Peritos. https://www.funcionjudicial.gob.ec/www/pdf/Reglamento%20del%20Sistema%20Pericial%20Integral%20de%20la%20Funcion%20Judicial2.PDF

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

Sistema Pericial Integral. (2014). Normativa: Vigente. https://www.funcionjudicial.gob.ec/www/pdf/Reglamento%20del%20Sistema%20Pericial%20Integral%20de%20la%20Funcion%20Judicial2.PDF

SlavaSoft Inc. (2022). HashCalc. Downloadastro.com. https://hashcalc.es.downloadastro.com/

Tapia, K. (2021). Proyecto de investigación: Modelo de análisis forense en dispositivos móviles con sistema Android. https://repositorio.pucesa.edu.ec/bitstream/123456789/3293/1/77448.pdf

Tapia, B., & Washington, K. (2021). Modelo para análisis forense en dispositivos móviles con sistema operativo Android. https://repositorio.pucesa.edu.ec/handle/123456789/3293.

Tusclases. (2022). Autopsy, una herramienta de análisis digital forense.Tusclases.com.ar. https://www.tusclases.com.ar/blog/autopsy-herramienta-analisis-digital-forense

Tiffany Estupiñan Londoño, K. M. (2019). Gestión De Evidencia Digital En Escenarios Convencionales e IoT.

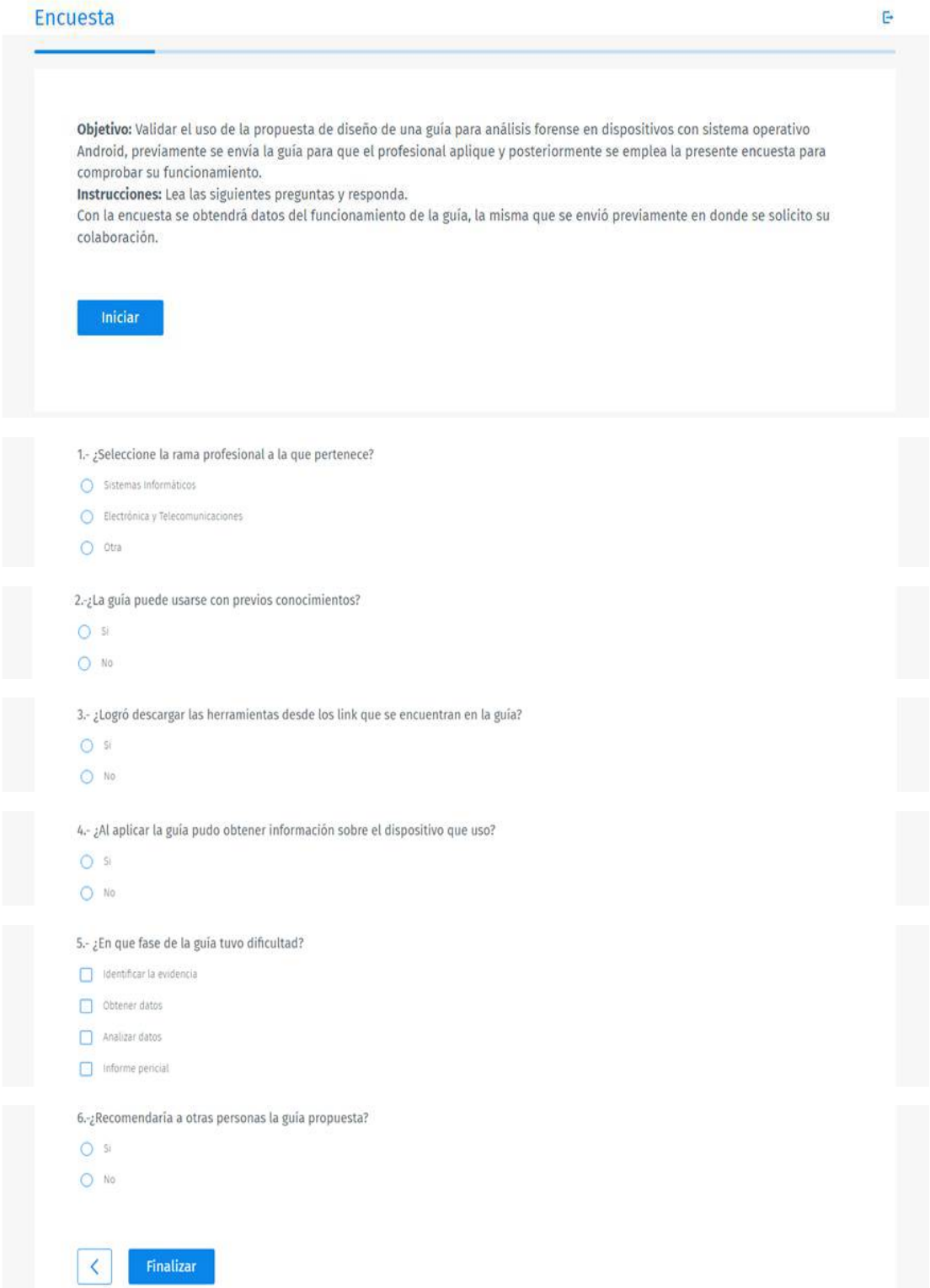
Velasco, R. (2018, March 14). Santoku Linux, un sistema operativo para auditar dispositivos móviles. RedesZone; RedesZone. https://www.redeszone.net/2015/03/14/santoku-linux-un-sistema-operativo-para-auditar-dispositivos-moviles/.

Villacreses Parrales, C. A., Chóez Calle, J. E., Figueroa Castillo, V. A., & Barreto Pin, J. X. (2021). ANÁLISIS DE DISPOSITIVOS TECNOLÓGICOS. Edu.ec. https://revistas.unesum.edu.ec/index.php/unesumciencias/article/view/390/355.

ANEXOS

ANEXO 1

FORMATO DE ENCUESTA



ANEXO 2

MODELO DE FORMATO DE INFORME PERICIAL

FORMATO DE INFORME PERICIAL

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

"INFORME PERICIAL

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

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

2. **PARTE DE ANTECEDENTES**, en donde se 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. El perito/a 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 del perito/a.

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 del perito/a 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. El perito/a 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 del perito.

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

7. **INFORMACIÓN ADICIONAL.** el perito o la perita 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; y, siempre y cuando esta información se encuentre dentro de los límites del objeto de la pericia.

8. **DECLARACIÓN JURAMENTADA,** el perito o la perita 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 del perito o perita, el número de su cédula de ciudadanía, y el número de su calificación y acreditación pericial."