UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

ABRIL 2024 – AGOSTO 2024

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERA EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS DE HERRAMIENTAS FORENSES APLICADO A DISPOSITIVOS ANDROID

ESTUDIANTE:

ANGELI TAMARA GARCES MUÑOZ

TUTOR:

EC. GERSON LEDESMA ÁLVAREZ

AÑO 2024

CONTENIDO

RESUMEN

Este estudio examina la eficacia de las herramientas forenses utilizadas en dispositivos Android, centrándose en Andriller y AFLogical OSE. Los objetivos incluyen una revisión de la literatura sobre ciencia forense digital y sus aplicaciones en Android, identificando herramientas forenses clave y evaluando su efectividad en la recuperación de evidencia digital. Se abarcan temas como la ciencia forense digital, etapas y objetivos de la ciencia forense, evidencia digital, cibercrimen, Android y su funcionamiento, análisis forense en dispositivos móviles. Se revisaron herramientas como Andriller, AFLogical OSE, Cellebrite UFED, FTK Imager y Magnet AXIOM, pero las pruebas reales se centraron principalmente en Andriller y AFLogical OSE. Los resultados muestran que ambas herramientas son efectivas para recopilar y analizar datos de dispositivos Android, aunque tienen limitaciones según el tipo de datos y el estado del dispositivo. Andriller se destaca en la extracción de datos de aplicaciones específicas, mientras que AFLogical OSE muestra un rendimiento excelente en la recopilación de registros y comunicaciones del sistema. Este estudio concluyó que el uso combinado de varias herramientas forenses puede mejorar la precisión y cobertura de la recopilación de evidencia digital. Además, enfatiza la importancia de actualizar constantemente las herramientas y técnicas forenses para adaptarse a los avances tecnológicos y las nuevas amenazas. Estos hallazgos brindan orientación práctica para los investigadores forenses sobre la selección y el uso de herramientas forenses en dispositivos Android.

Palabras claves: Análisis forense digital, herramientas forenses, Android, Andriller, AFLogical OSE.

ABSTRACT

This study examines the effectiveness of forensic tools used on Android devices, focusing on Andriller and AFLogical OSE. The objectives include a literature review of digital forensics and its applications on Android, identifying key forensic tools and evaluating their effectiveness in recovering digital evidence. Topics covered include digital forensics, stages and objectives of forensics, digital evidence, cybercrime, Android and how it works, forensic analysis on mobile devices. Tools such as Andriller, AFLogical OSE, Cellebrite UFED, FTK Imager and Magnet AXIOM were reviewed, but the actual testing focused mainly on Andriller and AFLogical OSE. The results show that both tools are effective in collecting and analyzing data from Android devices, although they have limitations depending on data type and device state. Andriller excels at extracting data from specific applications, while AFLogical OSE shows excellent performance in collecting logs and system communications. This study concluded that the combined use of various forensic tools can improve the accuracy and coverage of digital evidence collection. It also emphasizes the importance of constantly updating forensic tools and techniques to adapt to technological advances and new threats. These findings provide practical guidance for forensic investigators on the selection and use of forensic tools on Android devices.

Keywords: Digital forensics, forensic tools, Android, Andriller, AFLogical OSE.

PLANTEAMIENTO DEL PROBLEMA

Hoy en día, las personas alrededor del mundo, realizan sus actividades rutinarias por medio del internet y con ayuda de dispositivos electrónicos. La tecnología y el internet han facilitado las actividades humanas, ha ilimitado el poder de la comunicación, pero al mismo tiempo han generado una brecha para los delitos informáticos o actos que están en contra de la ley. Cuando un dispositivo móvil se ve involucrado en un delito o incidente, debe examinarse teniendo en cuenta que este contiene datos personales y corporativos, pudiendo incluso proyectar las costumbres o hábitos de una persona, resultando así información altamente sensible para tomar en una investigación.

Actualmente, a través de diversas etapas e innumerables versiones, Android se ha vuelto el sistema operativo (SO) más utilizado en el mercado para dispositivos móviles como smartphone y tablets, es utilizado por muchas marcas y sus mejoras han alcanzado un alto nivel de calidad. El interés que generó se ha copiado a otro tipo de dispositivos y también ha entrado en el mercado de los portátiles. La mayoría de estos dispositivos tienen las siguientes características: Enviar mensajes de texto (SMS), mensajes multimedia (MMS), mensajería instantánea (IM), correo electrónico en cuentas comerciales y personales, acceso web, gestión de información personal, cámara Fotografía avanzada, conexión a la nube con determinadas apps, geolocalizador, videoconferencias, esto significa más poder para capturar, mantener, acceder y modificar la información.

La ciencia forense digital es una disciplina importante en el mundo actual, en la búsqueda de la verdad, no sólo juega un papel en las investigaciones de delitos cibernéticos, sino que también sirve como aliado proporcionando informes periciales sobre sujetos sospechosos de delitos físicos. Los dispositivos digitales son omnipresentes y su uso en actividades de investigación es

importante. Ya sea que el dispositivo pertenezca al sospechoso o a la víctima, el gran volumen de datos contenidos en estos sistemas puede ser suficiente para que los analistas formulen un caso. Por lo tanto, no siempre es una tarea fácil recuperar datos de forma segura, eficiente y legal. Los investigadores dependen cada vez más de nuevas herramientas forenses digitales para ayudarles.

Los desafíos que plantea la realización de análisis forense en los dispositivos Android son numerosos y pueden abordarse tanto a nivel hardware como software. La variedad de modelos y versiones son sólo algunas de las dificultades, los sistemas de archivos, los tipos de procesadores, las actualizaciones de software y cuál es el estado real del propio dispositivo, el uso de tecnologías tanto las regulaciones como el cifrado contribuyen a la complejidad de la extracción de datos y estatutos de privacidad, por ello surge la interrogante de si las herramientas forenses actuales son lo suficientemente eficaces para enfrentar los desafíos del análisis forense en dispositivos Android.

Un experto forense juega un papel importante en este proceso, ya que es fundamental para abordar estos desafíos, debe comprender las mejores prácticas y procedimientos (técnicos y legales) para la extracción. El desarrollo de métodos de extracción y herramientas de análisis técnico especializados en usuarios de dispositivos móviles puede mejorar la capacidad de recuperar evidencia, cumplir con las leyes, regulaciones y respetar la privacidad del usuario. Con la creciente evolución del sistema operativo Android y la variedad de versiones que posee, en este caso de estudio se realiza un análisis de las herramientas forenses aplicadas a los dispositivos móviles con las versiones recientes de sistema operativo Android, con el fin de identificar sus funcionalidades, limitaciones y efectividad en la investigación forense.

JUSTIFICACIÓN

En la actualidad, el análisis de herramientas forenses de dispositivos Android es muy significativo, debido al elevado uso de los dispositivos también aumentó la incidencia de delitos cibernéticos y otras acciones ilegales. Aplicar el análisis forense en los dispositivos Android concede a los profesionales forenses identificar, preservar, analizar y presentar de forma correcta la evidencia digital, la cual juega un papel de vital importancia para resolver casos delictivos y proteger la integridad de los datos (personales y laborales).

El estudio de las herramientas de análisis forense, es pertinente debido a la variedad y dificultad de las técnicas y herramientas que se utilizan en las investigaciones forenses. Los dispositivos móviles en especial, son utilizados en diferentes escenarios como redes sociales, negocios, banca y educación, debido a su popularidad se han vuelto atractivos para los ciberdelincuentes, cuando se trata de un proceso penal, con las herramientas adecuadas pueden identificar y recolectar pruebas para una investigación judicial de los autores de un delito.

Este análisis beneficia a los profesionales de la ciberseguridad que requieren conocer herramientas y tecnología de software gratuito, que permitan evaluar de forma adecuada este tipo de dispositivos móviles, ofreciendo un análisis a profundidad, ayudando a los usuarios a recuperar información eliminada por error o también ayudando a identificar algún hecho delictivo. El desarrollo de este estudio es factible porque existen muchos recursos académicos y herramientas tecnológicas proyectados a Android, el trabajo está enfocado en conocer el tema del análisis forense y las herramientas forenses disponibles a dispositivos Android, con el propósito de identificar sus capacidades y limitaciones, para aumentar la eficacia del análisis forense en dispositivos Android.

OBJETIVOS

Objetivo general

Analizar las herramientas forenses aplicadas a dispositivos Android y su efectividad en la recolección y análisis de datos.

Objetivos específicos

- Realizar el levantamiento de información sobre el análisis forense digital y su aplicación en dispositivos Android, mediante una revisión bibliográfica.
- Identificar las principales herramientas forenses aplicadas a dispositivos Android, por medio de una revisión de casos de estudios.
- Evaluar la eficacia de las herramientas forenses aplicadas a dispositivos Android, en la recuperación de evidencia digital, a través de la observación y análisis de las capacidades de las herramientas.

LÍNEAS DE INVESTIGACIÓN

"Sistemas de información y comunicación, emprendimiento e innovación". Este caso de estudio sobre el análisis de herramientas forenses aplicado a dispositivos Android, está relacionada a la "Sistemas de información y comunicación, emprendimiento e innovación", ya que el estudio implica la investigación de herramientas tecnológicas de la investigación forense en dispositivos Android, a través del uso de las herramientas los investigadores pueden extraer y analizar los datos que son fundamentales para encontrar evidencia de delitos, recuperar datos perdidos, y garantizar la seguridad de los sistemas de información (SI). La ciencia forense de los dispositivos impulsa el emprendimiento y la innovación en el área de la seguridad mediante el desarrollo de nuevas herramientas y técnicas para el análisis forense en los dispositivos Android.

La sublínea de investigación "Redes y tecnologías de software y hardware", se relaciona con el estudio, porque el utilizar las herramientas de análisis forense implica usar técnicas específicas para buscar y recopilar las evidencias físicas y lógicas de dispositivos conectados a internet o redes inalámbricas. El crecimiento de Android, requiere que los investigadores no solo se mantengan al día con los avances en redes, sino también con el avance de software y hardware para realizar búsquedas efectivas.

El "análisis de herramientas forenses aplicado a dispositivos Android" está relacionado con la línea y la sublínea de investigación, porque ambas fomentan el desarrollo de nuevas herramientas forenses más efectivas, lo que aumenta la precisión eficiencia de estos análisis, se espera que los investigadores forenses tomen decisiones más informadas sobre qué herramienta se ajusta mejor a sus necesidades individuales, en función de sus pros y sus contras, gracias al análisis de las de las herramientas forenses.

ARTICULACIÓN DEL TEMA

El estudio "Análisis de herramientas forenses aplicadas a dispositivos Android" está relacionado con el proyecto de prácticas preprofesionales centrado en la aplicación de la tecnología y la comunicación en los sectores público y privado bajo la supervisión docente. Hoy en día los dispositivos móviles Android, son una parte integral de la vida cotidiana y se usan para todo, desde la comunicación personal hasta la gestión empresarial, es ahí donde surge la importancia de analizar estos dispositivos para garantizar la seguridad de la información y hacer frente a los incidentes informáticos en el sector público y privado.

Como sabemos en la actualidad los sectores públicos y privados enfrentan constantes desafíos de seguridad, los dispositivos móviles están involucrados en todas las actividades del día a día de las personas, a pesar de ser una fuente valiosa de información, también, pueden ser usados para cometer delitos, como espionaje industrial (obtener información de empresas sin permiso), difundir desinformación (Propagar información que es falsa o engañosa). El análisis de herramientas forenses aplicados a dispositivos Android, proporciona herramientas que pueden ser usadas para investigar esos incidentes de seguridad, ayudando a mantener integra la evidencia digital y garantizando la justicia.

Los avances en la tecnología móvil Android han impulsado el desarrollo de herramientas forenses para dispositivos Android, los investigadores pueden utilizar estas herramientas en una variedad de situaciones, como auditorías internas e investigaciones penales, y les permiten coordinar análisis y colaborar, para influir en la toma de decisiones en los sectores público y privado, los resultados deben comunicarse de manera concisa y clara.

MARCO CONCEPTUAL

Análisis forense digital

La informática forense, también conocida como análisis o ciencia forense digital, es una rama de la ingeniería informática que incluye un conjunto de técnicas y procesos que se centran en la identificación, almacenamiento, análisis y presentación de datos digitales que pueden utilizarse como prueba o evidencia. en un procedimiento legal. Estos datos no están fácilmente disponibles, por lo que los analistas tienen que profundizar más para conseguirlos, ya que no se pueden localizar a simple vista, si no que estos requieren de diferentes métodos o técnicas para su extracción.

La ciencia forense de sistemas se puede definir como un conjunto de métodos y procedimientos destinados a recuperar datos originados en un sistema operativo de un dispositivo, cuidarlos de posibles modificaciones y examinarlos para su futura presentación como evidencia (Melián Angel, 2023).

Este tema es muy importante en la investigación de delitos informáticos, porque este tipo de delitos se llevan a cabo utilizando equipos informáticos como computadoras, teléfonos móviles o medios digitales. Estos dispositivos pueden pertenecer a la fuente de delito como también a las víctimas. Su objetivo principal es recoger los datos sin que cambie su estado y luego verificar los datos recopilados. Este proceso es muy importante debido a que casi toda la información se genera y almacena en medios digitales.

La evidencia puede provenir de muchas fuentes diferentes; En este caso nos centraremos en el sistema operativo Android y examinaremos el sistema de archivos para recopilar la mayor cantidad de información posible. Se puede decir que además de la recuperación de la información

del sistema, también se realizaron trabajos de descubrimiento porque como un usuario normal del sistema no sólo tenemos acceso a información que se puede recuperar a simple vista, sino que también podemos detectar información que ha sido borrada, ocultada o alterada intencionadamente. Esto puede ser resultado de un error humano o de un error en propio archivo, pero no se puede descartar que estos incidentes se hayan producido con la intención delictiva de ocultar pruebas.

Objetivos del análisis forense digital

La informática forense es adecuada para situaciones en las que se producen brechas de seguridad (incidentes de seguridad que afectan a datos personales), sus principales objetivos son los siguientes (Ochoa Pérez, 2023):

Ayudar en la recuperación, análisis y almacenamiento de datos informáticos y relacionados para ayudar a las agencias de investigación a utilizarlos como prueba en los tribunales, ayudar a especular sobre el motivo del delito y la identidad del principal sospechoso, otro objetivo es desarrollar procesos en escenas de delitos sospechosos para garantizar que no se filtre la evidencia digital obtenida, la recopilación y copia de seguridad de datos, registros o archivos eliminados y particiones borradas de medios electrónicos para evidencias y verificaciones. Ayudar a identificar rápidamente pruebas y evaluar el impacto potencial del abuso en las víctimas, preparar un informe de informática forense que proporcione una descripción general completa del proceso de investigación, además de mantener la evidencia en la cadena de custodia, preservando así la evidencia digital del teléfono durante la investigación.

Principios de la ciencia forense digital

Existen algunos principios generales que se aplican a cualquier proceso de informática forense, según Chimbo (2022):

Actuar metódicamente, en este principio el investigador es su propio guardián durante todo el proceso, por lo que se documentará detalladamente cada paso dado, herramientas utilizadas y resultados obtenidos, este proceso es fundamental para garantizar la calidad y confiabilidad de los resultados. Evitar la contaminación, es otro principio en el que se trata de tomar todas las precauciones necesarias para evitar a toda costa la manipulación inadecuada de la evidencia analítica para evitar interpretaciones o análisis erróneos.

El principio de la cadena de custodia explica los procedimientos de recogida, transporte, almacenamiento y examen de las pruebas en el lugar del delito. Para garantizar la integridad y el rigor de la investigación y asegurarse de que las pruebas recogidas sean confiables y válidas, es esencial seguir este procedimiento, respetando los derechos de todas las partes implicadas, lo que puede lograrse sin sesgos ni prejuicios (Marchal González, 2019).

Fases del análisis forense digital

El análisis forense digital consta de 5 fases, a partir del criterio de Alemán (2024):

1. **Identificación**

Durante esta fase, se pueden identificar fuentes de evidencia, que pueden estar ubicadas en dispositivos digitales como discos duros, computadoras portátiles, teléfonos móviles y servidores, así como también en dispositivos de transmisión como enrutadores (Routers) y conmutadores

(Switches). Los límites de esta etapa están determinados por la naturaleza del incidente que se investiga.

2. Adquisición de pruebas

En esta fase, una vez identificadas las fuentes de pruebas o evidencias, el siguiente paso es adquirir las pruebas digitales, este proceso es crítico requiere la experiencia y el cumplimiento de pautas específicas para garantizar la integridad de las pruebas. Es sumamente importante tener en cuenta la naturaleza volátil de las evidencias digitales, por lo que deben seguirse protocolos estrictos para su recogida y manipulación. El uso de las herramientas forenses puede facilitar el proceso de adquisición, aunque no garantiza que se evite la contaminación o la pérdida de las pruebas o evidencias.

3. Preservación

Esta etapa requiere que se mantenga la integridad de las pruebas recogidas a lo largo del tiempo mediante copias forenses granulares o completas. Se utilizan algoritmos de verificación, como el hashing, para crear una cadena de longitud fija que actúa como referencia comparativa entre el original y las pruebas recogidas, garantizando su invariabilidad, se ponen en marcha protocolos de cadena de custodia para proteger las pruebas durante los análisis posteriores.

4. Análisis

En esta fase, las pruebas o evidencias recopiladas se procesan utilizando herramientas forenses, se indexa su contenido y, en caso necesario, se aplican filtros y técnicas de descifrado para extraer datos relevantes para la investigación. Se establecen cronogramas para analizar los eventos de manera organizada.

5. Informe

En esta etapa se registran los resultados del análisis de evidencia. La estructura del informe puede cambiar dependiendo del contexto legal y corporativo. Por ejemplo, en Panamá, el informe pericial computarizado debe seguir la estructura de causas penales establecida en el artículo 411 del código procesal penal del país.

El análisis forense digital es una disciplina que permite investigar y recolectar evidencias con el fin de descubrir delitos cibernéticos, las 5 fases del análisis forense digital son muy importantes a la hora de realizar un análisis forense a cualquier dispositivo tecnológico que contenga datos digitales o estén relacionados con una situación legal, la correcta utilización de estas fases permite conocer la causa principal del incidente, así como también permite garantizar la integridad y validez de la evidencia.

Evidencia digital

La evidencia digital es una agrupación de datos en forma digital (código binario), como registro de contenido discos duros, metadatos, tarjetas o unidades USB, conexiones de tráfico de red, que los tribunales pueden utilizar para establecer hechos. En otras palabras, la evidencia digital es el término utilizado para describir la información que se ha registrado en componentes informáticos. La evidencia digital suele estar escondida, parecen huellas dactilares o ADN dejado en la escena de un crimen. Puede modificarse, dañarse o destruirse fácilmente de forma remota. La información es altamente sensible al paso del tiempo (Martín, 2021).

Delitos cibernéticos

Según Carboné (2021), el delito cibernético es cualquier acto ilegal cometido en un entorno digital, espacio digital o en línea. La democratización de las nuevas tecnologías, especialmente

Internet, y el creciente número de usuarios han creado nuevos tipos de actividad ilícita por parte de los ciberdelincuentes, protegidos por el anonimato que proporciona Internet. Los tipos de delitos informáticos más comunes son:

Tabla 1

Delitos Informáticos.

Tipo de Delito Informático	Descripción
Acceso e Interceptación Ilícita	Revelación o filtración no autorizada de información confidencial, así como el acceso ilegal a sistemas informáticos.
Interrupciones de Datos y Sistemas	Daño intencional a sistemas informáticos mediante la alteración, eliminación o corrupción de datos.
Falsificación Informática	Creación de datos falsos con la intención de que sean utilizados como si fueran auténticos.
Fraude Informático	Uso ilícito de sistemas informáticos para obtener beneficios económicos de manera fraudulenta.
Delitos Sexuales	Actos de naturaleza sexual llevados a cabo a través de medios digitales, como la pornografía infantil o el acoso sexual en línea.
Violación del Honor	Delitos contra la reputación de una persona, como la calumnia e insultó, a través de medios digitales.
Amenazas y Coacciones	Uso de amenazas o violencia para coaccionar a otros, a menudo con motivaciones raciales o religiosas.

El delito informático o ciberdelito es una actividad ilegal, que viola los derechos de propiedad intelectual privada de las sociedades, organizaciones y países enteros. Con la creciente digitalización de todos los ámbitos de la sociedad, los delitos informáticos han crecido

exponencialmente en el sentido de que estos delitos se cometen no sólo mientras se navega por internet sino también mediante cualquier tipo de dispositivo o plataforma digital, cualquier persona, comunidad, gobierno, institución u organización puede convertirse en víctima de actividades delictivas.

Android

Android, el sistema operativo móvil más común, fue creado por Google en los Estados Unidos, su objetivo principal es simplificar y facilitar el uso del sistema, que se basa en Linux (sistema operativo). Android es una plataforma móvil gratuita, versátil, de código abierto y muy segura que se desarrolló exclusivamente para dispositivos móviles, como tablets y smartphone. Desde su publicación, el sistema ciertamente ha llamado la atención para desarrolladores, por lo que tiene una versión Java llamada Dalvik que facilita la construcción de aplicaciones de una manera simple y eficiente.

Android tiene muchas funciones y aplicaciones (apps) integradas entre ellas están el asistente de voz de Google, el servicio de mensajería Google News, almacenamiento en la nube Google drive. También, tiene varias aplicaciones que son muy necesarias para los usuarios como son Google Maps, YouTube, Gmail y Google Fotos. También cuenta con una tienda de aplicaciones llamada Play Store, donde el usuario puede descargar y comprar aplicaciones de terceros. Por otro lado, el SO Android es altamente personalizable, permite a los usuarios cambiar la funcionalidad y apariencia del dispositivo por medio de la instalación de temas y personalización de apps (Campos Gavilanes, 2023).

Funcionamiento de Android

Android trabaja con un sistema de software multicapa. La capa superior es la interfaz de usuario, donde el usuario interactúa con el dispositivo, la plataforma de aplicaciones, que incluye aplicaciones de terceros y nativas, es la siguiente etapa, el núcleo del sistema operativo es la capa más baja, que maneja recursos como la memoria, el procesador, la batería y otros.

Android para tener trabajando cada aplicación (app) en su propio entorno usa un sistema de aislamiento de aplicaciones con el fin de proteger la privacidad y la seguridad del usuario, También cuenta con un sistema de autorización que permite a los usuarios controlar el acceso de las aplicaciones a sus datos y a las funciones del dispositivo, este sistema operativo móvil es muy flexible y personalizable que tiene múltiples funciones y herramientas integradas centradas en la privacidad y la seguridad del usuario (Cruz, 2023)**.**

Aplicación del análisis forense de dispositivos móviles

El continuo desarrollo de la tecnología de red inalámbrica y los teléfonos móviles han cambiado en gran manera nuestras vidas, lo que ha generado un aumento en la cantidad de usuarios de teléfonos inteligentes, y la mayoría de estos dispositivos se utilizan para los negocios y las comunicaciones, aunque los teléfonos inteligentes desempeñan un papel vital en la vida diaria, los delincuentes también lo utilizan como medio para cometer delitos. Por lo tanto, cualquier información almacenada en los teléfonos inteligentes puede utilizarse como prueba digital en una investigación.

Los dispositivos móviles son sistemas dinámicos que presentan muchos desafíos a los investigadores en la adquisición y análisis de la evidencia digital, debido a que cada vez existen más tipos de teléfonos móviles, se dificulta el desarrollo de un único proceso o herramienta para

probar todo tipo de dispositivo. Los teléfonos móviles continúan evolucionando dado que avanzan las tecnologías actuales y se incluyen nuevas tecnologías. Por otro lado, cada teléfono móvil lleva integrados diferentes sistemas operativos. Por lo tanto, requiere conocimientos y habilidades especiales por parte de los expertos forenses (Alejandro Alejandro, 2024).

Análisis forense en dispositivos móviles Android

Android es el sistema más utilizado en dispositivos móviles. Las entidades desarrolladoras de sistemas operativos lanzan constantemente actualizaciones para corregir las vulnerabilidades existentes. A medida que el internet ha dado paso a las conexiones de redes globales entre dispositivos móviles, la seguridad se ha convertido en una preocupación para los desarrolladores, cada día surgen millones de ataques cibernéticos a las empresas privadas y usuarios comunes de esta forma las investigaciones forenses se están convirtiendo en una parte esencial para resolver estos delitos (Beltran Tapia, 2021).

Métodos de recuperación de datos.

El análisis forense actualmente tiene un lugar muy importante en los casos judiciales porque forma parte de las pruebas que se necesitan para resolver un caso, los datos o evidencia de los dispositivos móviles se extraen y analizan utilizando diferentes métodos y procedimientos, entre los que se incluyen los siguientes métodos más comunes;

- **Extracción física:** Se trata de hacer un duplicado bit a bit de la memoria del dispositivo, esta incluye los datos almacenados y el sistema operativo, y se puede lograr mediante la clonación del dispositivo con herramientas especializadas o mediante la extracción del chip.

- **Extracción lógica:** para extraer los datos del sistema operativo y las aplicaciones se utiliza la memoria física del dispositivo, las herramientas de software extraen los datos a nivel de archivo cuando se conectan al dispositivo a través de interfaces como USB o Wi-Fi.

- **Adquisición del sistema de archivos:** le permite recuperar los archivos visibles por medio del sistema de archivos, sin incluir archivos eliminados o borrados ni particiones ocultas. dependiendo del tipo de estudio se puede utilizar este método, que es menos complejo que la extracción física. Para ello se utiliza el mecanismo integrado en el sistema operativo para realizar copias de archivos, Android Device Bridge (ADB) para Android. De esta manera se puede obtener parte de la información que ha sido eliminada debido al uso de algunos sistemas operativos (como Android e iOS), usan una infraestructura que guarda la mayor parte de información mediante una base de datos SQlite (Ortiz de la cruz, 2023).

Herramientas utilizadas en informática forense.

Para determinar el estado del sistema después de una violación de seguridad, es decir Después de que se intenta o comete un ciberdelito, la informática forense emplea las herramientas necesarias (en función de lo que se investiga) para buscar y analizar pruebas para identificar un mecanismo o tecnología de sistema de acceso inapropiado (Murudumbay Huerta, 2022).

Herramientas forenses Aplicadas a dispositivos Android

FTK Imager

Es una herramienta gratuita, para obtener imágenes y vista previa de datos utilizados para adquirir datos (evidencia) de manera forense, por medio de la creación de copias de datos sin cambiar la evidencia original. FTK Imager le permite crear imágenes digitales forenses desde una memoria USB u otro dispositivo electrónico. Se recomienda utilizar un bloqueador de escritura cuando se ejecute esta acción, esto garantiza que el sistema operativo (SO) no cambie la unidad fuente original cuando está conectada a la computadora.

FTK Imager crea una copia bit a bit de la evidencia original. Esta actividad tiene el fin de prevenir la manipulación accidental o intencional de las pruebas originales. La imagen digital forense es idéntica a la original, en toda su estructura, esto le permite proteger la fuente original en un lugar seguro, mientras se utilizan copias o duplicados de las imágenes para la respectiva investigación. (Suárez Bohórquez, 2020).

Ventajas y desventajas de FTK Imager

Una de las ventajas es que permite exportar archivos y carpetas a partir de imágenes creadas. Además, AccessData cuenta con una solución completa de análisis forense llamada Forensic Toolkit (FTK), para poder crear un tándem completo y consistente al que tendría que adaptar alguna aplicación preferente si así lo requiere (Muñiz Da Costa, 2021). Las principales desventajas de FTK Imager son que no admite funciones de secuencia de comandos, no tiene capacidades multitarea, no tiene una vista de línea de tiempo (Montesinos Abad, 2022).

AFLogical OSE

Según Aji et al. (2020), es una herramienta forense de código abierto diseñada para ser utilizada fácilmente por personas que no pertenecen a las fuerzas del orden, es decir no se necesita experiencia. La función de AFLogical OSE es recopilar o extraer información de un teléfono inteligente con sistema operativo Android, como Contactos telefónicos, Registros de llamadas, Mensajes (SMS), Mensajes multimedia (MMS) y partes de MMS. AFLogical OSE tiene dos modelos disponibles: como aplicación Android y como parte del sistema operativo Santoku Linux en forma de máquina virtual.

Con AFLogical OSE pueden recogerse diversos tipos de datos de mensajería, llamadas e información de los contactos. Además, al ser de código abierto, puede adaptarse para satisfacer necesidades propias. Sin embargo, su uso presenta algunos inconvenientes, ya que no es posible recuperar cierta información de dispositivos no rooteados, lo que limita su alcance en algunos estudios. Gracias a estas características, AFLogical OSE es una potente herramienta que debe trabajar en conjunto con otras utilidades especializadas.

Andriller

Según Nieto (2020), es un software que contiene varias herramientas forenses para dispositivos móviles, que permite hacer adquisiciones forenses sin cambiar los datos desde dispositivos Android. Su utilidad radica en su facilidad de uso, y sobre todo porque muchas veces es requerida para peritaje informático de WhatsApp. Las funcionalidades que ofrece incluyen: descifrar patrones de pantalla de bloqueo, PIN o contraseña, Decodificador de datos de aplicaciones de bases de datos personalizadas que permiten el descifrado de las comunicaciones.

También, puede obtener informes en formatos HTML y Excel de la extracción ejecutada. Las características principales de Andriller son:

Permite la recuperación y el análisis automático de datos, incluso sin necesidad de rootear el dispositivo, al poder trabajar con copias de seguridad, permite la recuperación de datos utilizando privilegios de root, permite seleccionar decodificadores individuales para Android y Apple de la base de datos, Permite descifrar la base de datos de WhatsApp, permite descifrar patrones, PIN y contraseñas, así como también permite extraer archivos de respaldo del sistema Android.

Su interfaz fácil de usar es una ventaja de Andriller; también permite a los usuarios realizar extracciones sin conocimientos profundos de informática forense; incluye funcionalidad para descifrar contraseñas y bases de datos cifradas; y permite la extracción de una variedad de tipos de datos, como registros de llamadas, SMS, contactos y otros. Aunque es una herramienta común, la cantidad de documentación y soporte técnico puede ser limitada; además, carece de ciertas características y funcionalidades especiales.

Cellebrite UFED

Esta herramienta es una solución completa para el análisis forense de teléfonos móviles, práctica y adaptable para la investigación, Cellebrite UFED funciona diferentes dispositivos (iOS, BlackBerry y Android). Su principal ventaja es que permite la extracción física, lógica y a nivel se sistemas de archivos incluidos teléfonos, tablets y otros dispositivos, además tiene la capacidad de recuperar datos borrados como mensajes, fotos y registros de llamadas. La principal desventaja es que el precio de adquisición puede ser muy elevado (Palacios Carvajal, 2020).

Magnet AXIOM

Magnet AXIOM Software de análisis para teléfonos celulares, dispositivos de cómputo y datos en la nube, permite extraer información de contactos, mensajes de texto, registros de llamadas, multimedia, audio, redes sociales, video e imágenes. La principal ventaja de Magnet AXIOM es que la herramienta es multiplataforma, puede extraer y analizar datos de una amplia variedad de dispositivos, también ofrece capacidades de análisis profundas y detalladas, por otro lado, su principal desventaja es el alto costo que posee (Gutiérrez Salvador, 2022).

MARCO METODOLÓGICO

En el presente estudio se empleó el método bibliográfico y exploratorio, ya que para el desarrollo se consultaron distintas fuentes de información existentes, entre las cuales están tesis, libros, sitios web, revistas, artículos. Esta metodología tiene como propósito principal recolectar la información de documentos escritos por otros autores, los cuales tengan investigaciones similares o que estén relacionados al tema a tratar en este estudio, se utilizaron bases de datos especializadas como Google académico. El método exploratorio se utiliza para explorar las herramientas de análisis forense en dispositivos móviles Android, siendo estas, Andriller y AFLogical OSE.

Se aplicó el enfoque cualitativo, por la necesidad de explorar y comprender las experiencias, perspectivas y conocimientos de profesionales relacionados a los temas de ciberseguridad y auditoría. Este enfoque resulta útil para comprender las dificultades del uso práctico de las herramientas Andriller y AFLogical OSE, así como también para identificar desafíos y mejores prácticas para la recopilación de evidencia digital en dispositivos Android.

Para recopilar información, se utilizó una guía de entrevistas como herramienta principal para obtener información general detallada de personas con conocimiento en seguridad cibernética y temas relacionados, sobre el uso y la efectividad de las herramientas Andriller y AFLogical OSE. La guía de entrevista asegura que los aspectos importantes se abordan de manera sistemática y comparable, haciendo posible un análisis en profundidad de las experiencias y percepciones de los profesionales. Este enfoque cualitativo resulta fundamental en la comprensión de los problemas y retos específicos que trae la recolección de evidencia digital en los dispositivos Android.

RESULTADOS

A través de la revisión exhaustiva de la literatura, se logró identificar aspectos clave del análisis forense digital aplicado a dispositivos Android, además, por medio de la revisión de casos de estudio y documentación técnica se identificaron las principales herramientas forenses gratuitas utilizadas en la investigación de dispositivos Android, como son Magnet AXIOM, AFLogical OSE, Andriller, FTK Imager y Cellebrite UFED. Se prestó especial atención a la funcionalidad, y características técnicas, así como su eficiencia y efectividad en la recolección de datos.

Tabla 2

Herramientas de análisis forense para dispositivos Android.

Herramienta	Sistema Operativo	Precio	Capacidad de adquisición	Facilidad de uso	Tipo de Análisis	Compatibilidad con Android
Magnet AXIOM	Windows	Comercial	Alta	Media-Alta	Análisis forense detallado, recuperación de datos.	Alta
AFLogical OSE	Linux, Windows, macOS	Gratuito	Media	Alta	Análisis de sistemas de archivos, recuperación de datos	Alta
Andriller	Linux Windows	Gratuito	Media	Alta	Especializado en dispositivos Android	Completa
FTK Imager	Windows, macOS, Linux	Gratuito	Alta	Media-Alta	Adquisición de imágenes forenses	Alta
Cellebrite UFED	Windows	Comercial	Baja	Media-Alta	Recuperación de datos, desencriptación.	Alta

Fuente: *Elaboración propia*

Por medio de los resultados de la tabla se decidió utilizar Andriller y AFLogical OSE para realizar una evaluación, la elección está basada en sus funcionalidades específicas para el análisis forense en dispositivos Android, su facilidad de uso y el hecho de que son herramientas gratuitas y de código abierto. La evaluación se realiza con el fin de analizar sus funcionalidades, y brindar información que aporte a mejorar la elección de la herramienta en los procesos de análisis forense.

A continuación, se muestran los resultados obtenidos de la práctica de recolección de datos forense en dispositivos Android con las herramientas forenses Andriller y AFLogical OSE se instalaron y configuraron siguiendo los pasos respectivos, incluyendo las capturas de pantalla que ilustran la información obtenida del dispositivo móvil Android con el uso de las herramientas. Para llevar a cabo la práctica se utilizaron dos dispositivos con diferente versión de Android (Android 10 – 11).

Herramienta Andriller

Ilustración 1

Carpeta de archivos extraídos del teléfono móvil Android con Andriller.

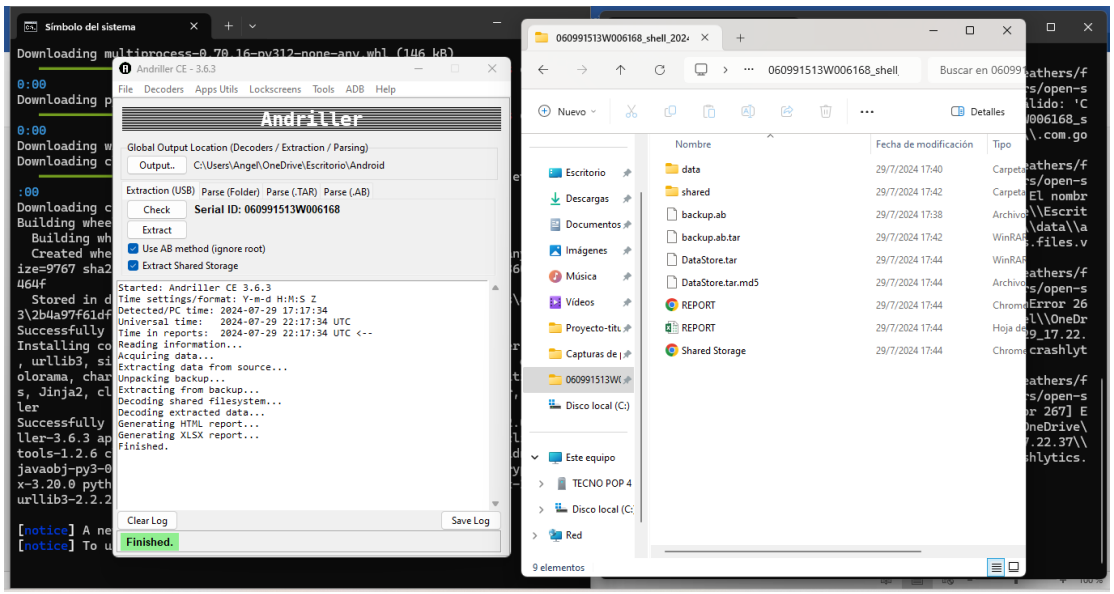


Ilustración 2

Reporte del teléfono Android.

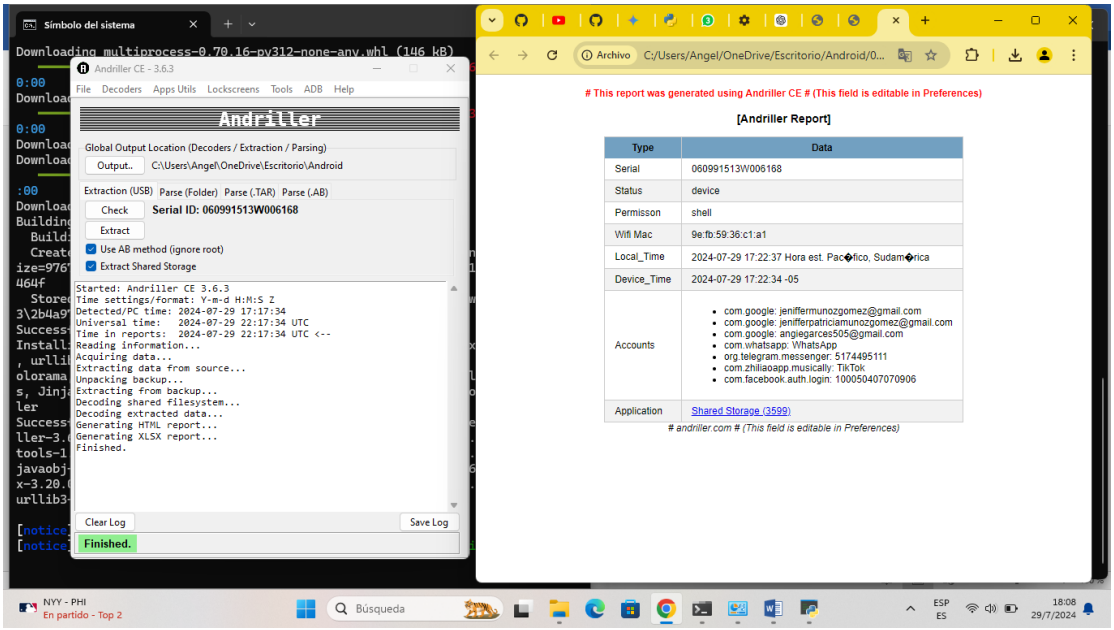
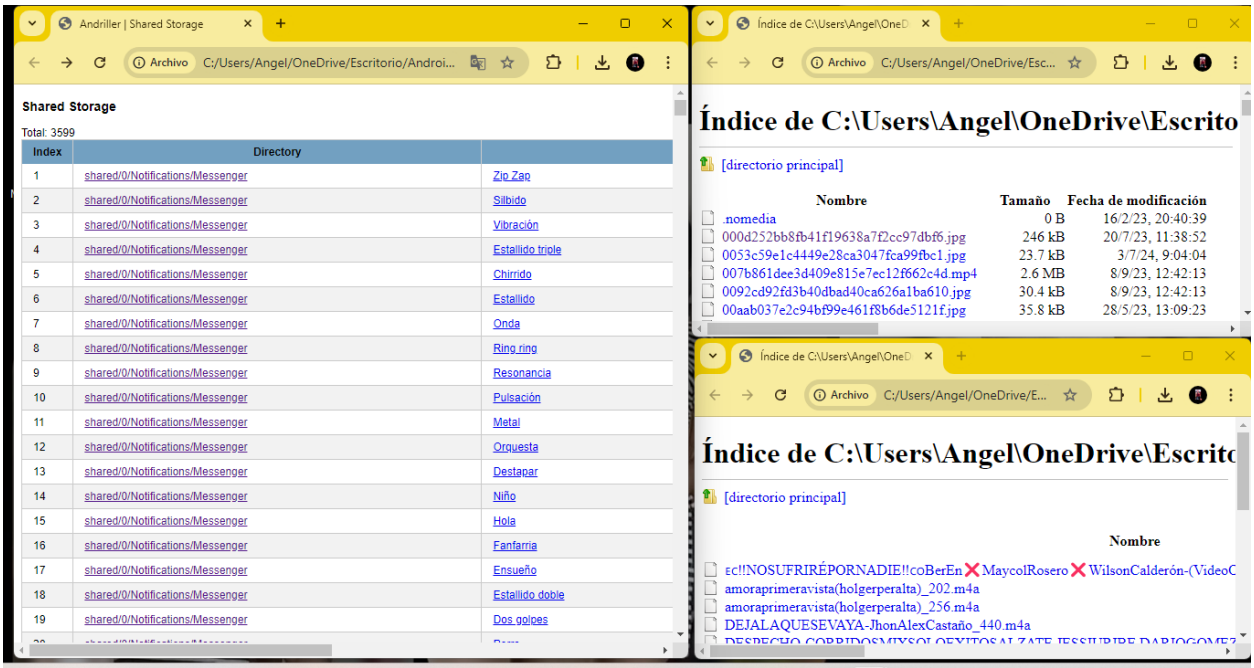


Ilustración 3

Información obtenida del dispositivo Android.



Herramienta AFLogical OSE

Ilustración 4

Archivos extraídos del dispositivo móvil Android con AFLogical OSE.

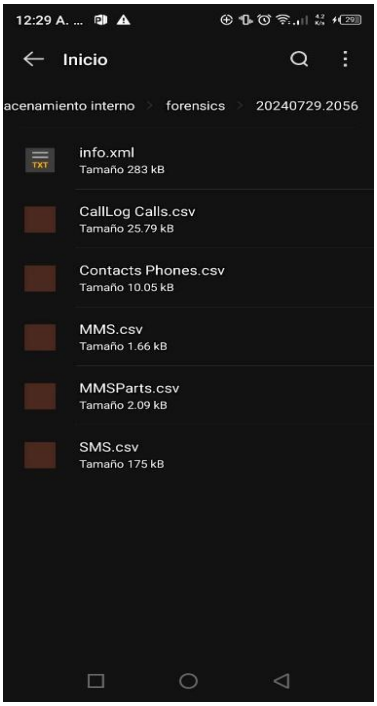


Ilustración 5

Datos obtenidos.

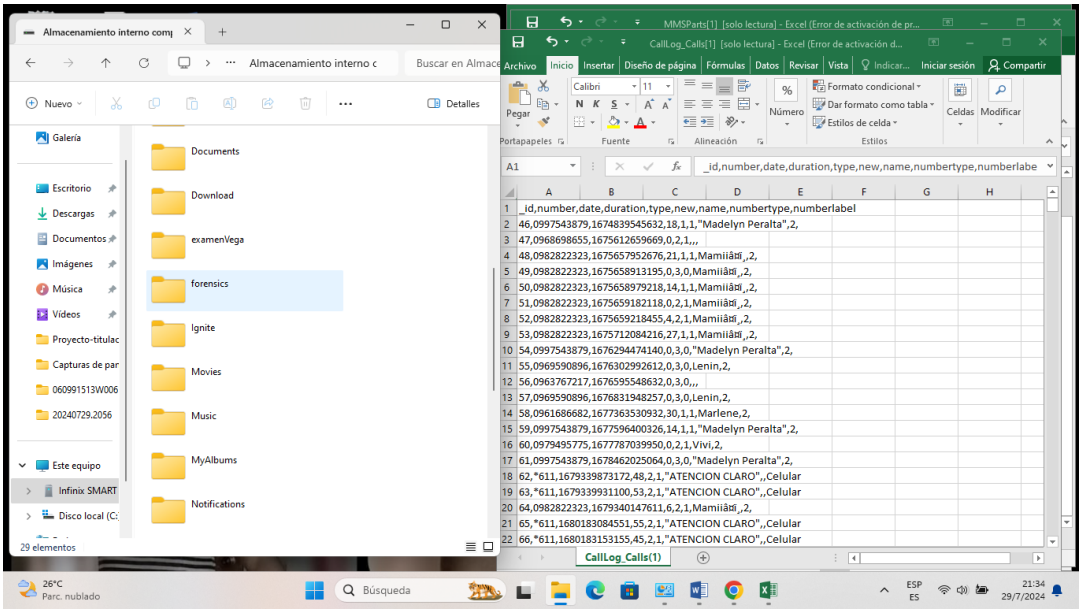


Ilustración 6

Datos obtenidos.

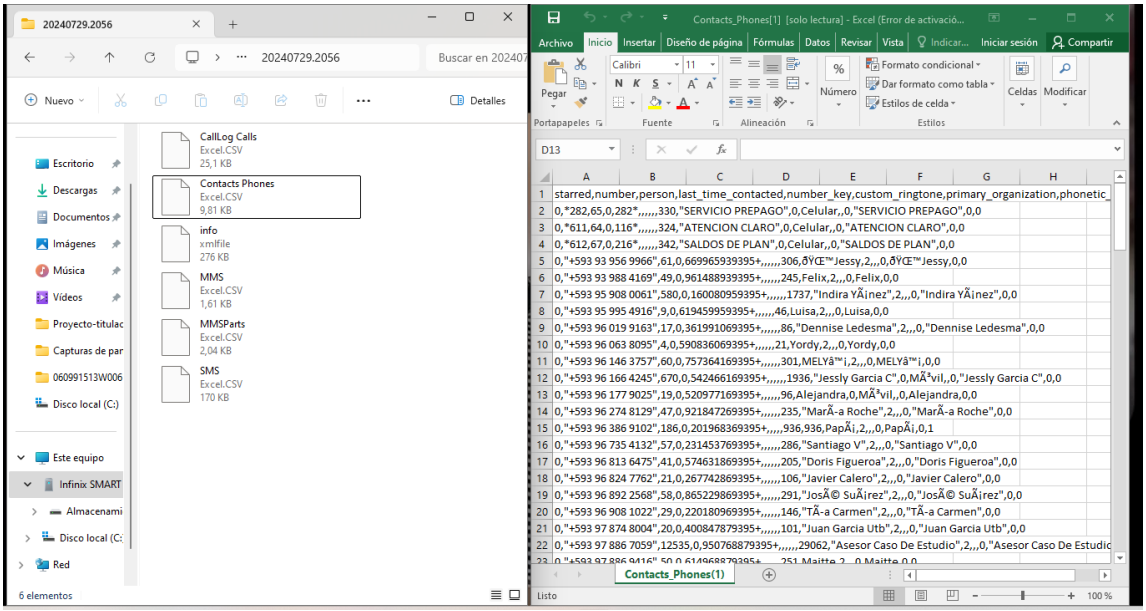
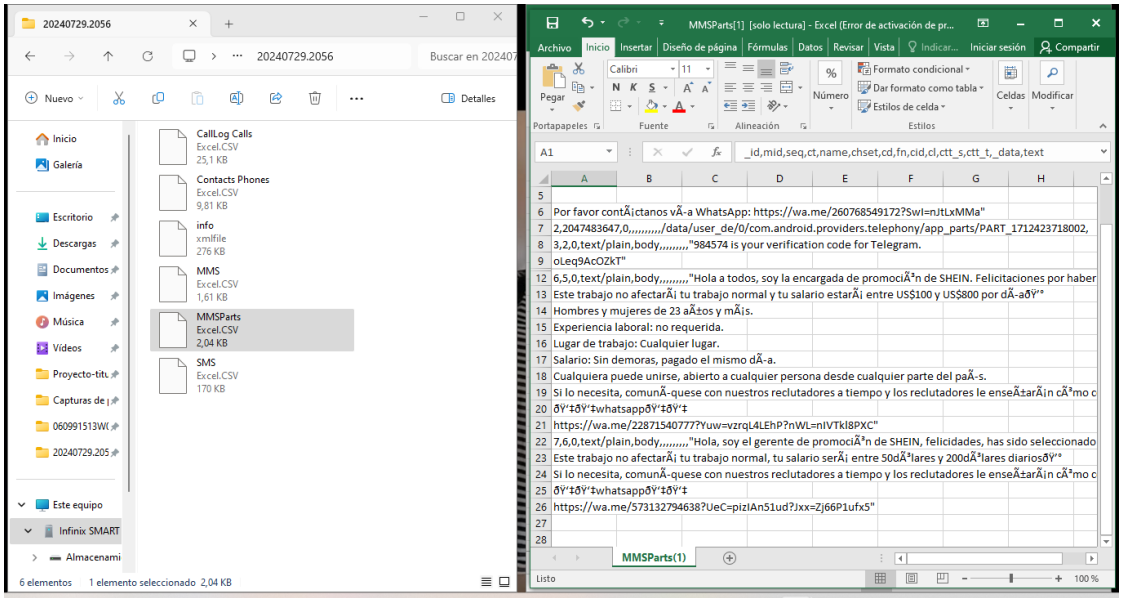


Ilustración 7

Datos obtenidos.



Como se puede observar en las ilustraciones, cada una de las herramientas usadas demostró su utilidad en el análisis forense de dispositivos Android, aunque cabe recalcar que cada una tiene sus ventajas y desventajas. Durante el uso de Andriller se pudo observar que logró extraer varios archivos, aunque no todos pudieron ser visualizados, esto debido a la necesidad de que el dispositivo este rooteado y también por las medidas de seguridad que posee Android, sin embargo, se recolectaron datos de contactos, archivos multimedia. En el caso de AFLogical OSE, si se pudo recolectar más información como contactos, registros de llamadas y mensajes. Por esto, se puede decir que en este estudio AFLogical OSE superó a Andriller en cuanto la cantidad de datos recolectados y la facilidad de uso.

Por medio de la entrevista realizada se descubrió que Andriller y AFLogical OSE son útiles para analizar los dispositivos Android, aunque también se mencionaron las limitaciones en comparación a herramientas más avanzadas. Las opiniones de los entrevistados aportan una guía útil para seleccionar herramientas, en el desarrollo de futuras investigaciones en este campo.

DISCUSIÓN DE RESULTADOS

En el estudio análisis de herramientas forenses aplicado a dispositivos Android, se lograron identificar los fundamentos teóricos del análisis forense y su creciente relevancia en el ámbito de la investigación digital. La proliferación de dispositivos móviles y la creciente dependencia de la información almacenada en ellos han convertido al análisis forense de dispositivos Android en una disciplina esencial para la resolución de casos legales, investigaciones internas y la protección de la seguridad informática.

El estudio encontró algunas herramientas útiles para el análisis forense de dispositivos Android, como Magnet AXIOM, Cellebrite UFED, AFLogical OSE y Andriller. El análisis de archivos del sistema, la extracción de datos de aplicaciones populares como Telegram y WhatsApp, entre otras funciones, están disponibles por cada una de estas herramientas. Se determinó utilizar las herramientas Andriller y AFLogical OSE.

El estudio se centra en comparar y evaluar la eficacia de las herramientas AFLogical OSE y Andriller para llevar a cabo un análisis forense en dispositivos Android. Los resultados que se obtuvieron revelaron tanto las fortalezas como las limitaciones de estas herramientas en el contexto actual de la investigación digital.

En este estudio Andriller y AFLogical OSE se identificaron como herramientas importantes para el análisis forense de los dispositivos Android, por su facilidad de uso y debido a que son gratis. AFLogical OSE demostró ser efectiva para el análisis forense de dispositivos Android, permitiendo capturar datos como registro de llamadas, SMS, y archivos. Durante la práctica se recuperaron varios registros de llamadas y mensajes, aunque la herramienta demostró

ser precisa, se observó una ligera demora en el proceso de extracción de datos. La interfaz de AFLogical OSE es simple, lo que la hace fácil de usar.

Por otro lado, en la herramienta forense Andriller se encontraron algunos problemas que limitaron el proceso de recolección de datos, aunque es conocida por su capacidad para extraer datos de llamadas y mensajes, en esta práctica no se logró recolectar ese tipo de información, ya que la herramienta requiere que el dispositivo analizado este rooteado, sin embargo, se pudo observar información de archivos y carpetas del dispositivo, que contienen imágenes, un reporte del teléfono que brinda información de correo e información de aplicaciones como WhatsApp.

Las herramientas demostraron ser útiles para el análisis forense de dispositivos Android; sin embargo, tienen limitaciones para analizar aplicaciones cifradas y dispositivos con sistemas operativos extremadamente personalizados. Es necesario crear nuevas técnicas y herramientas para abordar estas limitaciones, ya que los investigadores forenses se enfrentan constantemente al reto de la fragmentación de Android. Este estudio se suma al conocimiento actual de la investigación forense de dispositivos móviles y puede servir de base para futuras investigaciones.

CONCLUSIONES

Con la investigación de la literatura y el análisis de estudios previos, fue posible recopilar y combinar información detallada sobre el análisis forense digital y su aplicación en dispositivos Android. Se identifican las etapas clave del análisis forense, incluida la recopilación de datos, el análisis y la interpretación de la evidencia digital, Se destaca su importancia en las investigaciones de ciberdelito y la recolección de evidencia digital en dispositivos móviles Android.

Se descubrió a través de la investigación que existen varias herramientas para el análisis forense de dispositivos Android, algunas gratuitas y otras de pago. En esta ocasión, se han elegido Andriller y AFLogical OSE, ya que tienen la capacidad de extraer datos de dispositivos Android y son muy conocidas en la comunidad forense. Aunque cada uno tiene sus propias limitaciones y ventajas, los expertos pueden elegir la que mejor se adapta a las necesidades particulares de su investigación.

La evaluación práctica de las herramientas mostró que existen diferencias significativas en la efectividad de cada herramienta para la recolección de evidencia digital en dispositivos móviles Android. Andriller resultó ser eficaz para la recopilación de archivos multimedia, pero tuvo limitaciones para extraer datos de llamadas y mensajes de texto, en cambio AFLogical OSE demostró ser más eficaz para recopilar contactos, datos de llamadas y mensajes. De forma general se puede decir que AFLogical OSE es más precisa y recomendable para realizar la extracción de datos.

RECOMENDACIONES

Continuar y mantener actualizados los conocimientos sobre las herramientas de análisis forense aplicado a dispositivos Android, así como también las técnicas de uso, es necesario que los profesionales estén informados sobre los avances recientes en el campo de la informática forense de los dispositivos Android, ya que estos poseen nuevas regulaciones de seguridad, también se debe considerar la creación de un repositorio donde se recopilen y compartan los conocimientos adquiridos en la investigación forense de Android.

Identificar y seleccionar herramientas adecuadas de acuerdo con las necesidades propias de cada investigación, se debe revisar constantemente las herramientas disponibles para mantenerse informado sobre si las herramientas siguen siendo útiles y efectivas con las versiones más recientes de Android, se debe evaluar las ventajas y desventajas de cada herramienta y ajustarlas a las necesidades específicas de cada investigación.

Usar las herramientas combinadas puede ayudar a recolectar más datos del teléfono Android, mediante la práctica realizada con las dos herramientas utilizadas en este estudio Andriller y AFLogical OSE, se pudo recolectar información distinta, esto quiere decir que si se usan las dos conjuntamente se realizara un análisis más profundo en el dispositivo. Hacer comparaciones entre herramientas también puede ayudar a encontrar mejoras potenciales y adecuar de una mejor manera las estrategias del análisis forense en los dispositivos Android.

REFERENCIAS

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

Alejandro Alejandro, E. J. (2024). *Computación forense aplicada en dispositivos móviles con sistema operativo Android.* La Libertad: Universidad Estatal Península de Santa Elena. 2024. Obtenido de https://repositorio.upse.edu.ec/handle/46000/10933

Alemán Ariza, A. (2024). Analisis forense digital en dispositivos móviles. *Revista Cathedra, 1*(21), 45-64. doi:https://doi.org/10.37594/cathedra.n21.1419

Beltran Tapia, K. W. (2021). *MODELO PARA ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES CON.* Obtenido de https://repositorio.puce.edu.ec/server/api/core/bitstreams/3d13dcdb-2f6e-4450-863a-5f350ac0ad2f/content

Campos Gavilanes, D. M. (2023). *Análisis comparativo entre sistemas operativos de dispositivos móviles ANDROID, IPHONE OS y MIUI.* Obtenido de http://dspace.utb.edu.ec/handle/49000/13969

Carboné Mejías, P. (2021). *Estudio comparativo de distribuciones linux para análisis forense.* Obtenido de https://oa.upm.es/70654/

Chimbo Fernández , D. R. (2022). *Prueba de concepto para extraer información con herramientas de análisis forense open-source en dispositivos Android.* Ambato. Obtenido de https://repositorio.puce.edu.ec/items/e8bdc277-efc4-480b-bc46-9936c5df8f10

Cruz, A. (31 de enero de 2023). *Android: El sistema operativo móvil de Google*. Obtenido de MundoPcComponentes: https://www.pccomponentes.com/sistema-operativo-android

Gutiérrez Salvador, W. R. (2022). *Extracción de información de teléfonos celulares y su relación con hechos delictivos en la oficina de peritajes del ministerio público - lima 2020.* Universidad Norbert Wiener. Obtenido de https://hdl.handle.net/20.500.13053/7661

Marchal González, A. N. (2019). *La cadena de custodia y su impacto en el proceso judicial.* Obtenido de https://dialnet.unirioja.es/descarga/articulo/9425258.pdf

Martín, F. (11 de Agosto de 2021). *Evidencias digitales: significado, objetivo y tratamiento*. Obtenido de lemontech Blog: https://blog.lemontech.com/evidencias-digitales/

Melián Angel, J. (2023). *Análisis forense de la huella digital de un usuario en sistemas informáticos.* Universitat Politecnica de Valencia. Obtenido de http://hdl.handle.net/10251/198592

Montesinos Abad, F. M. (2022). *Informática forense: Herramientas open source y análisis de datos para el Volcado de memoria "MEMDUMP" y su aplicabilidad en la investigación de delitos informáticos.* Obtenido de https://repositorio.uide.edu.ec/bitstream/37000/5248/1/T-UIDE-0255.pdf

Muñiz Da Costa, A. (2021). *Análisis forense de eventos en Infraestructuras críticas.* Universitat Politècnica de València. Obtenido de https://riunet.upv.es/handle/10251/173163

Murudumbay Huerta, M. J. (2022). *Marco de trabajo y herramientas para el análisis forense en la atención de los delitos informáticos de Cibergrooming bajo los dispositivos móviles Android.* Obtenido de https://journalprosciences.com/index.php/ps/article/download/545/591/1499

Nieto Guerrero, C. F. (2020). *Descripcion de la metodologia para el analisis forense realizado.* Universidad Distrital Francisco Jose de Caldas. Obtenido de

https://repository.udistrital.edu.co/bitstream/handle/11349/28146/NietoGuerreroCristhianFerney2020.pdf?sequence=1&isAllowed=y

Ochoa Pérez, A. E. (2023). *Metodología para la recoleccion de evidencias digitales en dispositivos moviles con sistema operativo Android aplicado a hechos delictivos en facebook.* Obtenido de http://repositorio.umsa.bo/xmlui/handle/123456789/34480

Ortiz de la cruz, M. K. (2023). *Técnicas de recuperación de datos en dispositivos móviles.* La Libertad: Universidad Estatal Península de Santa Elena, 2023. Obtenido de https://repositorio.upse.edu.ec/handle/46000/10410

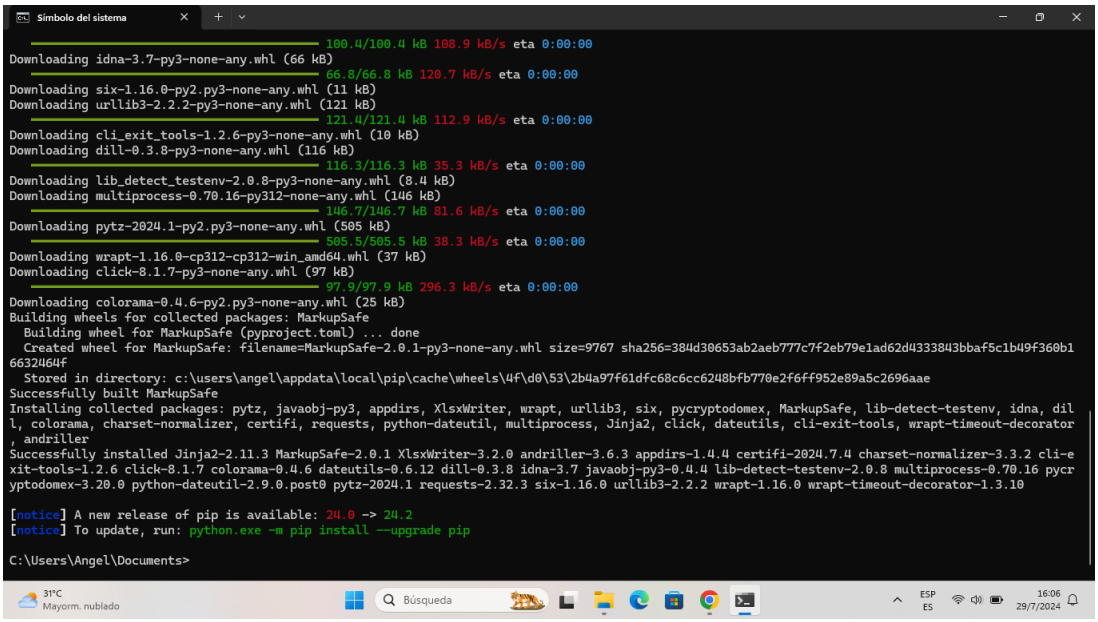
Palacios Carvajal, J. E. (2020). *Diseñar un Laboratorio de Ciencias Forenses Digitales en el Cuerpo Técnico de Investigación de la Fiscalía General de la Nación, Seccional Medellín.* Obtenido de http://hdl.handle.net/20.500.12622/4460

Suárez Bohórquez, W. J. (2020). *Utilización de herramientas informáticas FTK Imager y Autopsy para el análisis forense de evidencia digital a una memoria USB.* Obtenido de https://utb.alma.exlibrisgroup.com/view/delivery/57UTB_INST/1216606780005731

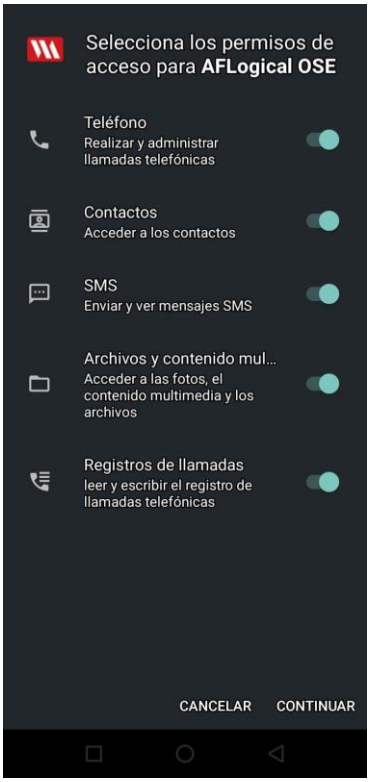
ANEXOS

Anexo Nº1

Instalación de Andriller.



Instalación de AFLogical OSE



Anexo Nº2

Entrevista Nº 1

Entrevistado: Ing. Raúl Ramos

¿Cuál es su conocimiento general sobre el análisis forense digital?

El análisis forense digital se utiliza en diversas situaciones, como investigaciones criminales, litigios civiles, investigaciones internas de empresas, y respuesta a incidentes de seguridad informática. Los profesionales en este campo deben tener conocimientos técnicos avanzados, estar familiarizados con las leyes y regulaciones relacionadas con la privacidad y la evidencia digital, y poseer habilidades de análisis crítico y atención al detalle.

¿Conoce usted las herramientas de análisis forense Andriller y AFLogical OSE?, ¿Que tan efectivas cree que son?

Andriller es bastante útil para recuperar datos de dispositivos Android, especialmente en lo que respecta a archivos de registros y bases de datos de aplicaciones. Sin embargo, puede tener limitaciones en términos de recuperación de datos eliminados en dispositivos más recientes. Por otro lado, AFLogical OSE es una herramienta gratuita y útil para análisis básicos, pero su efectividad puede ser limitada en comparación con herramientas comerciales más avanzadas

¿Ha oído hablar de otras herramientas de análisis forense aplicadas a dispositivos Android? Si es así, ¿cuáles?

Cellebrite UFED, XRY de MSAB, y Oxygen Forensic Detective son las más conocidas

En su opinión, ¿cuáles son las características más importantes que debería tener una herramienta forense para ser efectiva en la recolección de evidencia digital?

Compatibilidad amplia, extracción lógica y física, recuperación de datos eliminados, análisis avanzado, generación de informes, seguridad de la evidencia, facilidad de uso, soporte y actualizaciones, y automatización.

¿Qué aspectos considera usted más críticos al evaluar la eficacia de una herramienta forense?

La capacidad de extracción y recuperación de datos es fundamental para el éxito del análisis forense.

¿Qué desafíos específicos cree usted que presenta la recolección de evidencia digital en dispositivos Android en comparación con otros sistemas?

Fragmentación de Android, cifrado y seguridad, permisos y acceso root, variedad de aplicaciones de terceros, preservación de la integridad de la evidencia, constante actualización del ecosistema, y limitaciones técnicas de los dispositivos móviles.

Entrevista Nº2

Entrevistado: Ing. Jordy Ayala.

¿Cuál es su conocimiento general sobre el análisis forense digital?

Consiste en la recuperación y análisis de datos digitales para investigaciones legales.

¿Conoce usted las herramientas de análisis forense Andriller y AFLogical OSE?, ¿Que tan efectivas cree que son?

Sí, Andriller es buena para registros y mensajes; AFLogical OSE es útil para análisis básicos

¿Ha oído hablar de otras herramientas de análisis forense aplicadas a dispositivos Android? Si es así, ¿cuáles?

Sí, X1 Social Discovery y Oxygen Forensic Detective.

En su opinión, ¿cuáles son las características más importantes que debería tener una herramienta forense para ser efectiva en la recolección de evidencia digital?

Compatibilidad, recuperación de datos detallada, y facilidad de uso.

¿Qué aspectos considera usted más críticos al evaluar la eficacia de una herramienta forense?

Fiabilidad en la recolección de datos

¿Qué desafíos específicos cree usted que presenta la recolección de evidencia digital en dispositivos Android en comparación con otros sistemas?

Fragmentación del sistema operativo Android y la encriptación avanzada en dispositivos recientes.

Anexo Nº3

Informe anti plagio

INFORME DE ANÁLISIS
magister

ANGELI TAMARA GARCES MUÑOZ - SISTEMAS - 2024

4% Textos sospechosos

0% Similitudes
0% similitudes entre comillas
0% entre las fuentes mencionadas
2% Idiomas no reconocidos
2% Textos potencialmente generados por la IA

Nombre del documento: ANGELI TAMARA GARCES MUÑOZ - SISTEMAS - 2024.pdf
ID del documento: df649260fba341586b8e428d99de8f25a092176e
Tamaño del documento original: 317,87 kB

Depositante: LEDESMA ALVAREZ GERSON DAMACIO
Fecha de depósito: 8/8/2024
Tipo de carga: interface
fecha de fin de análisis: 8/8/2024

Número de palabras: 6427
Número de caracteres: 44.612

Ubicación de las similitudes en el documento:

Fuentes de similitudes