UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TITULO DEL TRABAJO DE TITULACIÓN

COMPUTACIÓN FORENSE APLICADA EN DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID

AUTOR

Alejandro Alejandro Erick Jesús

PROYECTO DE UNIDAD DE INTEGRACIÓN CURRICULAR

Previo a la obtención del grado académico en
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

ING. OROZCO IGUASNIA JAIME BENJAMÍN

La Libertad, Ecuador

Año 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
JOSE MIGUEL SANCHEZ AQUINO

Ing. José Sánchez Aquino. Mgtr.
DIRECTOR DE LA CARRERA

Ing. Jaime Orozco Iguasnia. Mgtr.
TUTOR

Firmado electrónicamente por:
CARLOS ANDRES CASTILLO YAGUAL

Ing. Carlos Castillo Yagual. Mgtr.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
MARJORIE ALEXANDRA CORONEL SUAREZ

Ing. Marjorie Coronel Suárez. Mgtr.
DOCENTE GUÍA UIC

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACION

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por ALEJANDRO ALEJANDRO ERICK JESÚS, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 08 días del mes de diciembre del año 2023

TUTOR

Ing. Orozco Iguasnia Jaime. Mgtr.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Alejandro Alejandro Erick Jesús**

DECLARO QUE:

El trabajo de Titulación, "computación forense aplicada a dispositivos móviles con sistema operativo Android "previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 08 días del mes de diciembre del año 2023

EL AUTOR

Erick Alejandro

Erick Jesús Alejandro Alejandro

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **"Computación Forense aplicada a dispositivos móviles con sistema operativo Android"** presentado por el estudiante, **ALEJANDRO ALEJANDRO ERICK JESÚS** fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 5%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

TUTOR

Ing. Orozco Iguasnia Jaime. Mgtr.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Alejandro Alejandro Erick Jesús** autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de presente trabajo de titulación con fines de difusión pública, además apruebo la reproducción de este trabajo de titulación dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 08 días del mes de diciembre del año 2023

EL AUTOR

Erick Alejandro

Erick Jesús Alejandro Alejandro

AGRADECIMIENTO

Agradezco principalmente a Dios, por acompañarme durante todo este camino, por brindarme fuerza y sabiduría durante los momentos más difíciles de la carrea y ayudarme cumplir un objetivo muy importante en mi vida.

A mi familia, que es uno de los pilares más fundamentales por el cual lucho día tras día, a mi madre: Sharon Nancy Alejandro Alejandro, quien desde pequeño fue todo para mí, siempre estuvo apoyándome, enseñándome valores, inculcándome principios y virtudes, a mi abuelita Nancy María Alejandro Villao, quien me apoyo durante todos mis estudios y siempre quiso que fuera todo un profesional

A la Universidad Estatal Península de Santa, junto con la enseñanza de mis docentes por generar conocimientos indispensables para mi futuro y la oportunidad de formarme como profesional

A mi docente tutor, Ing. Jaime Orozco, quien ha dispuesto de su tiempo, paciencia y conocimiento ayudándome en el desarrollo de este proyecto

Erick Jesus Alejandro Alejandro

DEDICATORIA

A Dios que me dio la vida, salud, fuerza, entendimento, dedicación, sabiduría y las ganas de luchas día tras día para conseguir un buen futuro

A mi Madre, Sharon Nancy Alejandro Alejandro, por todo el amor y cariño que me brindo toda la vida, por todas las retadas que me daba, por cada uno de los consejos que me brindo y por estar conmigo en los buenos y malos momentos sin importar nada.

A mi Abuela, Nancy María Alejandro Villao, quien me apoyo económicamente durante todos mis estudios, estuvo conmigo en los momentos más difíciles dándome aliento para poder seguir, a mi Abuelo, Kleber Heraldo Alejandro Owen, quien en vida junto a mi madre me inculco los valores y que siempre estaba para mí, tuvo la paciencia de enseñarme mucho sobre la vida y que donde sea que este espero que se encuentre orgulloso de mi, todo lo que soy es gracias a él.

A mis amigos que siempre estuvieron conmigo durante todos los semestres, juntos pasamos buenos y malos ratos.

Erick Jesús Alejandro Alejandro

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

El uso de los dispositivos móviles ha ido incrementando con el paso de los años, así como las incidencias informáticas en los mismos, ya que, si un teléfono termina en las manos de ciberdelincuentes, podrían robar la identidad del propietario del dispositivo, comprar cosas con su dinero, piratear cuentas de email o redes sociales y extorsionar a la persona. Por tal motivo, se propone implementar un laboratorio de computación forense mediante el uso de máquinas virtuales y herramientas Open Source**,** con el fin de analizar evidencias digitales en dispositivos móviles. Se utilizó la metodología de investigación de tipo exploratoria, indagando trabajos similares y diagnóstica recabando datos a través de técnicas. Como conclusión, El diseño de pruebas experimentales a través de la descripción de casos de estudio, brindó la emulación de incidentes de seguridad informática en los dispositivos móviles, evaluando la resiliencia del sistema y capacidad de respuesta ante diversas situaciones.

Palabras claves: Dispositivo móvil, investigación forense, ciber amenaza.

ABSTRACT

The use of mobile devices has been increasing over the years, as have computer incidents on them, since, if a phone ends up in the hands of cybercriminals, they could steal the identity of the owner of the device, buy things with their money, hack email or social media accounts and extort money from the person. For this reason, it is proposed to implement a forensic computer laboratory through the use of virtual machines and Open-Source tools, in order to analyze digital evidence on mobile devices. The exploratory research methodology was used, investigating similar and diagnostic works by collecting data through techniques. In conclusion, the design of experimental tests through the description of case studies provided the emulation of computer security incidents on mobile devices, evaluating the resilience of the system and its ability to respond to various situations.

Keywords: Mobile device, forensic investigation, cyber threat.

INTRODUCCIÓN

La creciente adopción de los dispositivos móviles con sistema operativo Android, ha traído consigo un significativo aumento en la complejidad y relevancia de computación forense aplicada a dichos entornos. En la era actual digital, donde los dispositivos móviles son capaces de almacenar una gran cantidad de datos personales y profesionales, surge la necesidad de comprender y abordar desafíos específicos de investigación forense en los dispositivos Android. Los problemas que más destacan en cuanto a la seguridad son los riesgos de aplicaciones maliciosas, conteniendo malwares que comprometen la seguridad y roban información personal; así mismo, existen vulnerabilidades en el sistema operativo que pueden ser aprovechadas por ciberdelincuentes para realizar ataques; además de gestión de actualizaciones inconsistentes entre los fabricantes y proveedores de servicios.

Por esta razón, se propone implementar un laboratorio de computación forense mediante el uso de máquinas virtuales y herramientas Open Source**,** con el fin de analizar evidencias digitales en dispositivos móviles y determinar el nivel de exposición de ciber amenazas de los usuarios respecto al uso de los dispositivos móviles Android, mediante la aplicación de una encuesta.

Además, se realiza un levantamiento de información de dispositivos móviles con sistema operativo Android, identificando detalles técnicos del sistema y sus funcionalidades, se diseñan pruebas experimentales mediante la descripción de casos de estudio, que permitan emular incidentes de seguridad informática en dispositivos móviles, además de proponer medidas de seguridad basadas en normas internacionales ISO y NIST para mitigar las ciber amenazas identificadas, a fin de mejorar la seguridad de los dispositivos móviles.

Se recolectó información adecuada para la investigación acerca de análisis forense en dispositivos móviles para la extracción de datos mediante herramientas de entorno libre y métodos de análisis forenses, empleando la metodología de tipo exploratoria. De la misma forma, se aplicó la metodología de tipo diagnóstica, en la cual se pudo determinar un análisis físico del dispositivo móvil, para tomar en cuenta si se debe utilizar herramientas que ayuden con este tipo de defectos y así extraer de manera adecuada la información que se requiere.

La presente investigación, está estructurada de la siguiente manera:

El capítulo I, contempla los antecedentes, descripción del proyecto, objetivos de la investigación, justificación, alcance y metodología.

El capítulo II de la propuesta, abarca el marco contextual, marco conceptual, marco teórico y requerimientos.

El capítulo III contiene el diseño técnico, desarrollo y pruebas.

Finalmente, en el capítulo IV se muestran los resultados de la investigación, de la ficha de observación realizada, los estándares para gestionar la seguridad de Android y las buenas prácticas para el uso de dispositivos móviles.

CAPITULO 1. FUNDAMENTACION

1.1. Antecedentes

El uso de dispositivos móviles se ha ido extendiendo con el paso de los años, tanto así que en la actualidad hay más de seis mil millones de usuarios con teléfonos celulares en todo el mundo [1]. Este aumento de usuarios trae consigo amenazas hacia este tipo de dispositivos, las cuales son; los ataques de vulnerabilidad al hardware, integridad, disponibilidad, autenticación, autorización y amenazas de número de teléfono [1].

Anteriormente, las incidencias informáticas solo ocurrían en computadoras o servidores, sin embargo, actualmente los dispositivos móviles se han vuelto indispensables para la comunicación y el manejo de información de los usuarios [2]. Si un teléfono termina en las manos de ciberdelincuentes, podrían robar la identidad del propietario del dispositivo, comprar cosas con su dinero, piratear cuentas de email o redes sociales y extorsionar a la persona [2].

Muchas veces, los dueños de los dispositivos instalan aplicaciones de páginas no oficiales o piratas, incentivando a las personas mal intencionadas a rootear el teléfono y que accedan sin autorización a la información del celular [3]. Además, cuando un dispositivo móvil se ve involucrado en un incidente informático, se debe tener en cuenta que se encuentra a la mano información sensible o personal, como contraseñas, números de tarjetas de crédito, dirección domiciliaria, datos del usuario, lugar donde trabaja, etc; teniendo como consecuencia la contaminación de la evidencia digital, es decir, pérdida de la integridad de la información y modificaciones en la misma [3].

En la entrevista realizada al propietario del dispositivo móvil (Ver Anexo 1), se pudo determinar qué, las aplicaciones qué más utiliza son las redes sociales, mensajes, cámara, llamadas, galería, gestor de archivos y lector de documentos. En cuanto a la seguridad, manifiesta que no posee antivirus en el dispositivo y solo emplea métodos de bloqueo en el teléfono, como patrón, huella dactilar o clave, así mismo, utiliza el móvil de forma personal y para cuestiones laborales. Además, el celular no se encuentra en modo Root, solo tiene activada la opción de desarrollador; Como medio de almacenamiento, posee una tarjeta microSD de 64 GB, finalmente indica que ha tenido dos formateos y una restauración de fábrica.

Para conocer las aplicaciones y uso que dan los usuarios a los dispositivos móviles, se realizó una encuesta (Ver Anexo 2) a los estudiantes de la carrera de Tecnologías de la información de la facultad de sistemas y telecomunicaciones, desde el 5to al 8vo semestre durante el ciclo académico 2023-1 y 2023-2; se trabajó con una muestra de la población 79 estudiantes. la misma que se obtuvo mediante cálculos estadísticos.

Durante el proceso de adquisición del dispositivo móvil que fue analizado (**Ver Anexo 3**), se determinó que, el celular se encontraba en perfecto estado físico, sin embargo, para respaldar la información fue necesario realizar una copia exacta de la unidad de almacenamiento del dispositivo móvil.

Para la orientación acerca del trabajo, se realizó una investigación acerca del tema de tesis en la Universidad Tecnológica del Perú, ejecutada por el estudiante Bruno Dudu Ramos Anampa, el cual efectuó un trabajo de titulación denominado "Implementación de un Software Forense para el Análisis de Evidencia Digital en Dispositivos Móviles", obteniendo como resultado un análisis de evidencia digital para poder identificar la mejora mediante indicadores de tiempos de creación de la imagen forense, aplicando técnicas de recolección de datos, en donde los puntos fuertes fueron los indicadores que indicaron la vulnerabilidad en los dispositivos móviles Android, concluyendo con un aumento del 70% en relación con la activación del programa [2].

De la misma manera, a nivel nacional en la Pontifica Universidad Católica del Ecuador con sede en Ambato, el ingeniero Klever Washington Beltrán Tapia, realizó su sustentación de Magíster en Ciberseguridad con el tema "Modelo para análisis forense en dispositivos móviles con sistema operativo Android", teniendo como finalidad diseñar un modelo de análisis forense en dispositivos móviles que mantienen un sistema operativo Android, aplicando una metodología de trabajo de investigación bibliográfica usando modelos y normas nacionales e internacionales asegurando el motivo de investigación, identificar evidencia, adquirir datos, analizar datos y finalizando con la presentación de un informe, concediendo una guía para asegurar la escena, identificar evidencia, adquirir datos y analizarlos [4].

A nivel provincial, en la Universidad Estatal Península de Santa Elena se realizó un trabajo de tesis titulado "Diseño de una Guía Metodológica para el Análisis Forense Digital tomando como base Equipos con el Sistema Operativo Windows 8.1" por el

estudiante Freddy José Mirabá Quimí, con el objetivo de diseñar una guía metodológica para el análisis forense digital orientada a un sistema operativo muy utilizado, en el cual, se empleó software de código abierto, mostrando el proceso de una copia de seguridad de un disco duro para posteriormente sacar un análisis y extrayendo evidencia digital; finalizando su proyecto con una guía orientada a personas con conocimientos básicos de informática forense y documentación, manteniendo un ejemplo de informe pericial, el cual incluirá información, datos de recolección en base a los datos de estudio, mostrando los diferentes tipos de evidencias que se obtuvieron con el uso del programa [5].

Después de revisar los trabajos investigados para este estudio, se pudo determinar que el análisis forense hacia el dispositivo móvil Samsung Galaxy A03s, permitirá fomentando un avance para personas interesadas en el uso de herramientas precisas en determinados dispositivos. Por esta razón, el presente trabajo propone implementar un estudio a un sistema operativo para un dispositivo móvil dando como resultado una documentación del uso de herramientas que faciliten el análisis de estos, verificando los datos que se pueden extraer.

1.2. Descripción de proyecto

El presente proyecto se centra en el análisis forense de dispositivos móviles con Sistemas Operativos Android. Para realizar la investigación forense se aplica la metodología DoJ 1 desarrollada por El Departamento de Justicia de los Estados Unidos de América (DoJ EEUU), y definida como Electronic Crime Scene Investigation: A Guide for First Responders (Investigación en la Escena Del Crimen Electrónico).

Además, se plantea un marco teórico detallando conceptos de computación forense, evidencia digital, cadena de custodia, y técnicas de hacking avanzada, descritos en la norma ISO 27037:2012 para computación forense y en la guía de investigación DoJ 1. También, se implementa un laboratorio forense utilizando máquinas virtuales con sistemas operativos Caine, Santoku, Helix, Kali, IOS y Android. Se diseñan y emulan incidentes de seguridad informática en ambientes controlados de dispositivos móviles; para lo cual, se analizan 3 casos de estudio para la plataforma Android. Las técnicas de computación forense que se utilizan son: data carving, análisis de metadatos, trazabilidad de rutas, autenticidad e integridad de un fichero, y estegoanálisis. Los resultados serán

presentados mediante un informe técnico de los incidentes de seguridad analizados. Por último, se propone un conjunto de buenas prácticas y recomendaciones basadas en normas internacionales como ISO y NIST, con el fin de minimizar la exposición de ciber amenazas en las plataformas móviles.

Se emplea la metodología de la computación forense, la cual se divide en las siguientes fases:

Fase de identificación y preparación

Esta etapa se conforma de la asignación del caso, identificación de roles y funciones, reconocimiento de los involucrados e identificación de los dispositivos electrónicos incautados.

Además, se lleva a cabo una indagación visual con el objetivo de conocer la situación actual de los dispositivos móviles, determinando si se encuentran funcionando correctamente, logrando la posibilidad de acceder a la base de datos de las diferentes aplicaciones con información relevante.

Fase de adquisición y preservación

Se centra en la obtención de copias de información relevante, evitando la modificación de cualquier dato y garantizando que toda la información recopilada no sea transformada ni se destruya.

Con la finalidad de obtener datos relevantes del dispositivo mediante herramientas de distribución libre, adecuadas para Android, permitiendo la ejecución y proporcionando un análisis de datos de forma forense.

También, se administra un enlace entre el dispositivo móvil con sistema Android y el sistema computacional, sin antes, habilitar la depuración por USB del dispositivo en modo desarrollador.

Fase de análisis

Una vez obtenida la información, se utilizarán herramientas especializadas de computación forense, con el fin de buscar evidencia digital y posteriormente, analizarla. En esta fase se identificará la información adecuada para este estudio, el cual, se analiza empleando diversas herramientas, divididas por sistema operativo móvil, las cuales

estarán asistidas en un entorno investigativo por computadora y se detallan a continuación:

- ✓ AFLogical OSE
- ✓ Open Source Android Forensics
- ✓ LIME
- ✓ TestM
- ✓ Exiftool
- ✓ Meterpreter

Fase de presentación

En la etapa final, se documentan todas las acciones realizadas, para posteriormente, entregar un informe ejecutivo, mostrando los datos más importantes de manera resumida, siendo certero, claro y conciso.

Este proyecto contribuye a la línea de investigación de Tecnología y Sistemas de la Información (TSI), sub línea Inteligencia Computacional.

1.3. Objetivos del proyecto

1.3.1. Objetivo general

- Implementar un laboratorio de computación forense mediante el uso de máquinas virtuales y herramientas Open Source**,** con el fin de analizar evidencias digitales en dispositivos móviles.

1.3.2. Objetivos específicos

- Realizar un levantamiento de información de dispositivos móviles con sistema operativo Android, que permita identificar los detalles técnicos del sistema y sus funcionalidades.
- Evaluar el nivel de conocimiento de los usuarios respecto al uso y gestión de la ciber seguridad en los dispositivos móviles como herramienta tecnológica, mediante la aplicación de una encuesta.
- Diseñar pruebas experimentales mediante la descripción de casos de estudio, que permitan emular incidentes de seguridad informática en dispositivos móviles.

- Elaborar un informe detallado de las vulnerabilidades encontradas en los dispositivos móviles durante la investigación forense.
- Proponer medidas de seguridad basadas en normas internacionales ISO y NIST para mitigar las ciber amenazas identificadas, a fin de mejorar la seguridad de los dispositivos móviles.

1.4. Justificación del proyecto

En los últimos tiempos, el celular se ha transformado en una herramienta indispensable para la vida diaria, rompiendo la barrera de solo manejar llamadas y mensajes, ofreciendo un sin número de utilidades que facilitan las actividades diarias de cualquier persona y evolucionan con el pasar del tiempo; entre las características que poseen estos dispositivos, está la transmisión de video, cámara fotográfica, GPS, conexión de Wi-Fi y capacidad de guardar grandes cantidades de información en almacenamiento externo e interno, además que cuentan con una variedad extensa de aplicaciones [6].

La auditoría en dispositivos móviles ha avanzado en varios procesos, utilizando técnicas para la revisión e indagación de datos que referentemente se encuentran bloqueados, encriptados, ocultos y en mucha ocasiones borrados; Comúnmente, estos procesos se utilizan en áreas de criminalísticas para contrarrestar delitos financieros, fraudes, corrupción y lavados de activos, utilizando metodologías preventivas para ofertar evaluaciones como también auditorias detectivas, especificando ocurrencias de fraude y utilizando análisis técnicos e investigaciones de fondo [7].

Las tecnologías inalámbricas móviles se han hecho tan indispensables en la humanidad, que su utilización se ha requerido para varios y amplios ámbitos laborales, policiales y sobre todo, en el área criminal, siendo para las autoridades, una pieza clave para indagar sobre delitos que se han generado, por tal motivo estos equipos contienen información que ayudan a resolver crímenes y que a su vez la seguridad que ellos imponen a sus celulares es más fuerte de romper para acceder a sus datos, por ello en la actualidad los despachos de informática forense son esenciales para realizar estos trabajos.

Fomentando el conocimiento en el área forense para la auditoria de dispositivos móviles, se realizará un ejercicio práctico evaluando un smartphone con sistema operativo Android, el cual tiene características adecuadas para poder armar un laboratorio forense

con herramientas informáticas a nivel de software, permitiendo la extracción de datos, manipulación y desbloqueo de este tipo de celulares, teniendo como base un dispositivo Samsung A21 con sistema operativo Android 10 y Procesador Octa Core 1.8 GHz.

Este proyecto culminará con el uso de herramientas y tecnologías Open Source, que permitan realizar una adecuada auditoría en este tipo de dispositivos móviles o en teléfonos con características similares que brinden esta clase de análisis a profundidad, ayudando a los usuarios a recuperar información que por error se haya eliminado y a su vez, proporcionar una referencia a personas interesadas en el entorno de auditoría de dispositivos móviles siendo un complemento para sus estudios de datos de encriptación y recolección de información, tomando decisiones que se podrían llevar a cabo, en caso de que el dispositivo no cumpla con los requerimientos físicos para la extracción.

Concluyendo que, este trabajo se alinea al plan de oportunidades, tomando como objetivos los siguientes puntos [8]:

Objetivo del eje social:

Objetivo 7. Potenciar las capacidades de la ciudadanía y promover una educación innovadora, inclusiva y de calidad en todos niveles.

Según las políticas:

7.2 Promover la modernización y eficiencia del modelo educativo por medio de la innovación y el uso de herramientas tecnológicas.

7.4 Fortalecer el sistema de educación superior bajo los principios de libertad, autonomía responsable, igualdad de oportunidades, calidad y pertinencia; promoviendo la investigación de alto impacto.

1.5. Alcance del proyecto

Teniendo en cuenta la problemática planteada que se presenta en los laboratorios forenses acerca de la extracción de datos a los dispositivos móviles, se realizará un análisis forense a un smartphone Samsung Galaxy A03s, con sistema operativo Android 12 con versión One UI Core, el cual se utilizará para ejecutar las pruebas adecuadas con diversas técnicas y herramientas, mediante un laboratorio forense ambientado a software para la recuperación de datos.

Para gestionar diversos aspectos de auditoría a un dispositivo móvil, se debe tener en cuenta todo lo relacionado con el celular, ya sea que el propietario es una persona ordinaria, en el cual se podrán adquirir muchos más datos, a diferencia de un individuo con antecedentes delictivos. Para esto se aplicó una metodología investigativa, utilizando para ello una entrevista al dueño del dispositivo y una encuesta a múltiples estudiantes de la universidad, con el fin de conocer las aplicaciones más utilizadas, así mismo, se realizó un método de observación para determinar el estado físico del móvil.

Como parte de este estudio, es esencial saber el estado del dispositivo y sus características para así establecer todo lo necesario para la auditoría, definiendo que se debe analizar el estado del celular, y determinando que el equipo aún se encuentra en perfecto estado. Por otro lado, para comprobar la funcionalidad se ejecutará una prueba que medirá el rendimiento.

La fase de identificación y preparación se conforma de la asignación del caso, identificación de roles y funciones, reconocimiento de los involucrados e identificación de los dispositivos, llevando a cabo una indagación visual con el objetivo de conocer la situación actual de los dispositivos móviles.

La fase de adquisición y preservación **s**e centra en la obtención de respaldo de la información requerida, con la finalidad de adquirir datos relevantes del dispositivo mediante herramientas de distribución libre, evitando la modificación de información.

En la fase de análisis, se utilizarán herramientas especializadas de computación forense, con el fin de buscar evidencia digital y posteriormente, se identificará la información adecuada para este estudio, el cual, se analiza empleando herramientas computacionales tales como:

- AFLogical OSE.
- Exiftool
- Meterpreter

En la fase de presentación, se documentan todas las pruebas que se realizaron en el laboratorio forense, para luego, redactar un informe descriptivo de los datos, mostrando los puntos más importantes de manera resumida, siendo certero, claro y conciso.

1.6. Metodología del proyecto

1.6.1. Metodología de investigación

Se recolectó información adecuada para la investigación acerca de análisis forense en dispositivos móviles para la extracción de datos mediante herramientas de entorno libre y métodos de análisis forenses, empleando la metodología de tipo exploratoria [9]; por medio de los trabajos semejantes, se encamina el desarrollo de este trabajo de titulación.

Entre las referencias bibliográficas encontradas, está la investigación que se realizó a nivel mundial en la Universidad Tecnológica del Perú, titulada "Implementación de un Software Forense para el Análisis de Evidencia Digital en Dispositivos Móviles", dando como resultado un análisis de evidencias digitales mediante creación de imágenesforenses [2]. Así mismo, a nivel nacional en la Pontifica Universidad Católica del Ecuadoren la ciudad de Ambato se presentó un tema de tesis denominado "Modelo para análisis forense en dispositivos móviles con sistema operativo Android", el cual diseñó un modelo de análisis forense, evidenciando, adquiriendo, analizando datos y procedimientos logarítmicos [4], finalmente, a nivel provincial, en la Universidad Estatal Península de Santa Elena, se realizó el trabajo titulado "Diseño de una Guía Metodológica para el Análisis Forense Digital tomando como base Equipos con el Sistema Operativo Windows 8.1", basándose en el análisis forense a un sistema operativo que en su tiempo era muy usado por la comunidad, obteniendo herramientas especializadas para la extracción de la información [5].

Además, se aplicó la metodología de tipo diagnóstica, en la cual se pudo determinar un análisis físico del dispositivo móvil, para tomar en cuenta si se debe utilizar herramientas que ayuden con este tipo de defectos y así extraer de manera adecuada la información que se requiere [10].

1.6.2. Beneficiarios del proyecto

Los beneficiarios del presente proyecto son las personas auditoras, que requieren del conocimiento de herramientas y tecnologías de software libre, que permitan realizar una auditoría adecuada en este tipo de dispositivos móviles, brindando un análisis a profundidad, ayudando a los usuarios a recuperar información que por error se elimina.

1.6.3. Variables

Después de recolectar toda la información de los métodos ya descritos, se llega a la conclusión que, es de utilidad realizar un ensayo conformando un laboratorio forense con las herramientas de uso libre para extraer los datos mediante un análisis en el dispositivo móvil adquirido para este fin y tener como indicador la extracción de la mayor cantidad de archivos en el equipo durante el ejercicio.

1.6.4. Análisis de recolección de datos

- **Técnica:** Encuesta y entrevista.
- **Instrumentos:** En el presente proyecto se elabora un cuestionario de preguntas dirigidas a los estudiantes de la carrera de Tecnologías de la Información, Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, para conocer el nivel de conocimiento de los usuarios respecto al uso y gestión de la ciber seguridad en los dispositivos móviles como herramienta tecnológica; el cual será enviado a través de un enlace a Google Form, para que respondan de forma virtual.

Para comprender acerca de los problemas que se pueden suscitar durante este trabajo de computación forense, se procedió a recolectar información adecuada acerca de las características del dispositivo, aplicaciones usadas y estado físico del mismo, mediante diversas técnicas de recolección de datos, reuniendo información relevante del smartphone; empleando una entrevista al dueño del dispositivo móvil (Ver Anexo 1), se conocieron los aspectos integrales del equipo al que se le realizará la auditoría, como tiempo de uso, defectos, reparaciones y formateos.

Por otro lado, se recolectará información mediante una encuesta a los estudiantes de la Universidad Estatal Península de Santa Elena (Ver Anexo 2), en el área de Tecnologías de la Información, con el fin de conocer la utilidad de los dispositivos móviles como tiempo de uso diario, aplicaciones empleadas y métodos de seguridad que tienen en sus celulares, con el fin de determinar que app es la más utilizada y así poder empezar la auditoría.

Población: 300 **(**N)

$$n = \frac{N.\ Z_2\ c.\ p.}{(N-1).\ e^2 + Z^2\ c.\ p.\ q}$$

En este trabajo se consideró una muestra, debido al tamaño de la población ya que el número total de estudiantes de la carrera de tecnologías de la información desde 2do semestre hasta 8vo semestre es 300. La muestra se calcula con la fórmula de distribución normal, en la cual N significa el número de población; p, siendo la probabilidad de éxito; e es el error de estimación; Z siendo el nivel de confianza y n es el valor de muestra que va a ser calculado.

Se tienen en cuenta los siguientes valores:

N = 300 (Población)

P = 0.5 (Probabilidad de éxito)

E = 0.07 (Error de estimación)

Z = 1.44 (85% de confianza según la tabla de la distribución normal)

$$n = \frac{(Z^2 \text{ x } p\ (1 - p)) / e^2}{1 + ((Z^2 \text{ x } p(1-p))\ e^2 N)}$$

$$n = 79$$

Finalmente, se realizó un método de observación al equipo móvil (Ver Anexo 3), para poder determinar el estado físico en que se encuentra y así diagnosticar herramientas útiles, hallando lo siguiente:

- Dispositivo móvil de marca Samsung Galaxy A03s, a primera vista se ve en perfecto estado.
- Dispositivo móvil posee dos seguridades, una por huella dactilar en la pantalla Oled y otra por clave de patrón.
- Estado de depuración y modo desarrollador se encuentran en modo inactivo.
- Memoria de almacenamiento del dispositivo móvil unificada, para realizar almacenamiento virtual como si fuera uno.
- Puerto de datos del dispositivo móvil en perfecto estado, de categoría tipo C con depuración de almacenamiento USB 3.0.

Después de recolectar toda la información de los métodos ya descritos, se llega a la conclusión que, es de utilidad realizar un ensayo conformando un laboratorio forense con

las herramientas de uso libre para extraer los datos mediante una auditoría en el dispositivo móvil adquirido para este fin y tener como indicador la extracción de la mayor cantidad de archivos en el equipo durante el ejercicio.

1.7. Metodología de desarrollo

Para cumplir con el objetivo previsto en una computación forense para extracción de datos en dispositivos móviles, se requiere el uso de una metodología adecuada, en la cual se podrá extraer el mayor beneficio para el trabajo que se ejecutará, siendo la DIGITAL FORENSIC METHODOLOGY acorde para empezar y adaptándola al entorno en que se orienta el estudio, dividiéndose en 4 fases esenciales [11]:

Recolección: Se encargará de identificar el incidente por medio de la recolección de los datos adquiridos.

Inspección: En donde se determinarán las herramientas que se usarán para extraer los datos, como también la preservación y custodia de estos.

Análisis: En esta parte, se toma en cuenta el entorno en que se va a trabajar, en las cuales se deberá determinar reconstrucción de incidente, identificación de archivos y la evaluación del impacto.

Reportes: La respectiva documentación de todo el proceso desarrollado y resultados finales de la computación forense.

Figura 1: Metodología de desarrollo del proyecto

CAPITULO 2. MARCO REFERENCIAL

2.1. Marco Contextual

2.1.1. Institución

La Universidad Estatal Península de Santa Elena (UPSE), está localizada en el cantón La Libertad, en la Provincia de Santa Elena, República del Ecuador; siendo el primer centro de enseñanza autónomo que cuenta con la mayor población de estudiantes en la zona [12]. En la actualidad, se encuentra acreditada dentro del Sistema de Educación Superior, ubicada en categoría C, de acuerdo con la evaluación realizada por el Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior (CEAACES) [12].

Misión

Formar profesionales que aportan al desarrollo sostenible, contribuyendo a la solución de los problemas de la comunidad y promoviendo la cultura.

Visión

Ser reconocida por su calidad académica, impacto de sus investigaciones y el aporte al desarrollo de la sociedad.

Fines

Son fines de la institución:

- Producir propuestas y planteamientos para buscar solución de los problemas del país.
- Propiciar el diálogo entre culturas nacionales y a su vez, involucrar la cultura universal.
- Propiciar la difusión y fortalecimiento de sus valores en la sociedad del Ecuador.
- Propiciar la formación profesional, científica y técnica de sus estudiantes, docentes e investigadores, contribuyendo al logro de una sociedad más equitativa, justa y solidaria, en colaboración con los organismos del Estado y sociedad.
- Los demás establecidos en el artículo 8 de la LOES.

2.1.2. Aplicación de análisis forense en dispositivos móviles

Los avances en la tecnología inalámbrica y los dispositivos móviles han cambiado drásticamente nuestras vidas, haciendo que el número de usuarios de teléfonos inteligentes este aumentando diariamente y la mayoría de ellos dependen de estos equipos para fines comerciales y de comunicación; Si bien los teléfonos inteligentes se utilizan en aspectos positivos de nuestras vidas, los delincuentes también los utilizan como herramienta para sus delitos, por lo tanto, la posible información almacenada en los teléfonos inteligentes puede utilizarse como prueba digital para las investigaciones, sin embargo, los investigadores pueden enfrentar problemas para obtener información y datos importantes en los teléfonos inteligentes [13].

Los teléfonos móviles son sistemas dinámicos que presentan muchos desafíos para los examinadores a la hora de adquirir y analizar pruebas digitales, aunque, el rápido aumento en la cantidad de tipos de teléfonos celulares de diferentes compañías dificulta el desarrollo de un proceso o herramienta único para probar todo tipo de dispositivos. Los teléfonos móviles continúan evolucionando a medida que avanza la tecnología existente y se introducen nuevas tecnologías, además, cada teléfono móvil está diseñado con varios sistemas operativos integrados, por lo tanto, obtener y analizar estos dispositivos requiere conocimientos y habilidades especiales de los expertos forenses [13].

A lo largo de los años, la conducta delictiva ha evolucionado, como resultado de la actividad física y la participación de víctimas y delincuentes, pero desde la globalización de las nuevas tecnologías digitales han surgido nuevos y diferentes tipos de delitos. No existe consenso sobre tales conductas ilegales ni en el ámbito jurídico ni en el criminológico. Este tipo de conducta es conocida con diversos nombres como “crimen informático”, “crímenes cibernéticos”, “cibercrimen”, etc., que indican la falta de definiciones específicas [14].

La ciencia forense de dispositivos móviles es una rama de la ciencia forense digital que implica la recuperación y el examen de evidencia digital de dispositivos en un entorno forense. El proceso de extracción verifica sus datos móviles, datos SIM, memoria del dispositivo y tarjeta SD (si está conectada), etc. Utilizando herramientas forenses como MOBILedit, Cellibrite PREMIUM, Elcomsoft Forensic Toolkit y Tsurugi Linux para recuperar datos del dispositivo y examinarlos [14].

2.2. Marco Teórico

2.2.1. La importancia del análisis forense digital en la era tecnológica

El análisis forense digital se conoce comúnmente como computación forense, empleando técnicas científicas dentro del campo informático, con el fin de conservar, recopilar y analizar datos; identificando, documentando e interpretando información que pueda ayudar en las investigaciones judiciales y legales; las técnicas más utilizadas en la ciencia forense digital incorporan la reconstrucción de dispositivos informáticos; recuperación de información y autenticación de la información que se extrajo; los especialistas en dicho campo tienen una experiencia amplia en tecnología e informática, necesaria para la resolución de casos como descifrado, piratería informática y recuperación de datos [15].

El análisis forense informático no se centra en frustrar ataques cibernético o delitos, en cambio, se preocupa por la investigación y descubrimiento de datos importantes que sirven como evidencia en investigación legal; las medidas preventivas son la competencia de seguridad informática; la informática forense posee una variedad amplia de aplicaciones, especialmente en el campo del crimen digital, esta disciplina contribuye a identificar pistas en casos de delitos cibernéticos, seguimiento de delincuentes a través de correos electrónicos o chats, detección de robos de información y la recuperación de datos eliminados intencionalmente o disponibles en equipos dañados o perdidos [16].

En los últimos años, se produjo un exponencial aumento en el acceso y utilización de medios digitales, lo cual resultó en un incremento significativo en actividades ilegales como piratería y fraude; es por esto, que el campo de la informática forense desarrolla una herramienta importante para detectar las formas de operación e identificación de los responsables de dichos delitos mediante la extracción y evaluación de la información digital hallada en la auditoría [16].

Desde su origen hasta la actualidad, el campo de la investigación y análisis forense, ha permitido identificar nuevas maneras delictivas, como el espionaje, fraude y pornografía infantil; además, sirve como soporte para otras áreas de derecho, en especial lo relacionado con la extracción de datos claves; la informática forense ha evolucionado notablemente a lo que avanza la tecnología; actualmente, esta disciplina se enfoca en el análisis y recuperación de información almacenada en dispositivos [17].

2.2.2. Informática forense en teléfonos celulares

Desde hace muchos años, se ha presenciado un crecimiento exponencial importante en el uso de dispositivos móviles en la vida cotidiana; El Instituto de Seguridad Informática expone cada año el reporte acerca de la situación actual de la seguridad y crímenes informáticos, ofreciendo datos estadísticos que se basan en la experiencia de muchas organizaciones en Estados Unidos; el reporte presenta los incidentes de seguridad más frecuentes en el país, pero los que no se detectan por expertos en seguridad de las diferentes compañías [18].

De acuerdo con las estadísticas, en el sector de los dispositivos móviles, para el año 2015, el número de teléfonos celulares en el mundo era 2168422600; mientras que, en el año 2018 ya habían 4.4 billones de teléfonos nuevos, con una estimación de 1000 nuevos clientes por cada minuto; en cuanto a la proporción del mercado entre las distintas marcas de dispositivos móviles y las mayores organizaciones de esta área tecnológica; en la masificación de las comunicaciones móviles, hay un crecimiento de las plagas informáticas concentradas en dispositivos celulares [19].

Un teléfono ya no es más que un dispositivo móvil, todos estos dispositivos son considerados como estaciones de trabajo empresariales móviles; siendo elementos que se encuentran en cualquier lugar, como restaurantes, aeropuertos, centros comerciales, entre otros lugares; cada vez más individuos los utilizan, entre ellos, empresarios que gracias a estos aparatos, se mantienen informados y en contacto con su negocio; A pesar de que los dispositivos son teléfonos celulares, en el fondo son ordenadores móviles, que contienen datos corporativos sensibles que pueden almacenarse fácilmente en un bolsillo [19].

La comunicación de los dispositivos móviles es inalámbrica, planteando una gran interrogante en cuanto a la seguridad de los datos; para entender estos inconvenientes y amenazas a los cuales están expuestos los celulares, es sumamente necesario comprender de manera general, las funcionalidades y características de los mismos [20].

La mayoría de las personas, actualmente poseen un dispositivo móvil; no obstante, múltiples virus han aparecido para infectar los teléfonos, convirtiéndose en el objetivo favorito por los ciberdelincuentes, debido a las vulnerabilidades y a la escasa protección con que cuentan; sin embargo, se exponen a fallas de seguridad como ataques directos, códigos maliciosos, ataques de autenticación e incidentes de instalaciones físicas [20].

2.2.3. Prueba de concepto para extracción de información con herramientas de análisis forense en dispositivos Android

En la actualidad, se videncia que la mayoría de los delitos informáticos, se realizaron desde dispositivos móviles, esto debido a la gran cantidad de individuos que cuentan con equipos móviles desde el cual acceden a sus redes sociales, incluso para realizar diversas transacciones en línea; es por esto que se hacen pruebas de concepto para la extracción de información en dispositivos móviles con sistema operativo Android a través de herramientas de análisis forense; sin embargo, son pocas las herramientas de software libre para utilizar al realizar casos forenses con relación a equipos móviles [21].

La evolución de dispositivos móviles ha ido en incremento notable, pasando de ser simples celulares a ser ordenadores de mano; motivo por el cual, las actividades diarias de las personas como revisar redes sociales, correos electrónicos, buscar sitios de interés o hacer transacciones online se realizan mediante dispositivos móviles; siendo estos en su gran mayoría, de sistema operativo Android, debido que es la plataforma más popular entre las personas, entre ellos, los ciberdelincuentes, el principal blanco entre todas las plataformas móviles [22].

El uso de dispositivos móviles ha crecido notablemente a razón de sus servicios, estando conectado desde cualquier lugar y en cualquier momento del día; trayendo grandes beneficios para los usuarios, pero también llamando la atención de los cibercriminales que ven un gran mercado, para su explotación en aumento, obteniendo provecho para sus intereses económicos o personales mediante los diversos delitos informáticos; es por esto que, los dispositivos móviles se encuentran expuestos a un sinnúmero de peligros, al igual que los equipos conectados a la red [22].

Los peligros a los que se exponen los usuarios son los mismos para distintos equipos informáticos, como spam, malware, robo o extravío físico del celular; es por esto que crecen los ataques, peligros e intrusiones informáticas, siendo necesaria la implementación de políticas que apoyen en la mitigación de los ataques, la sensibilización de las personas y en caso de ocurrencia de intrusiones, se establecen acciones relevantes en la investigación para poder esclarecer los mismos, así es como ingresa el concepto de informática forense, adquiriendo, preservando, obteniendo y presentando datos [23].

2.3. Marco Conceptual

2.3.1. Computación forense

La informática forense, también conocida como computación forense, computo forense, análisis forense digital o análisis forense informático, es la disciplina encargada de recopilar, preservar y analizar pruebas cuando falla la seguridad de los sistemas informáticos, las redes, los dispositivos móviles, el correo electrónico y los discos duros. y otros elementos informáticos [24].

La disciplina combina los elementos legales y de ciencia de datos del análisis de datos y se considera una rama de la seguridad cibernética junto con el hacking ético. La evidencia descubierta ayuda a los expertos en seguridad informática a determinar el origen de los ataques cibernéticos y puede usarse como prueba en casos judiciales [24].

2.3.2. Seguridad móvil

La seguridad móvil se refiere a las políticas, la infraestructura y el software utilizados para proteger cualquier dispositivo móvil que los usuarios lleven consigo, incluidos teléfonos inteligentes, tabletas y computadoras portátiles. La seguridad de los dispositivos móviles incluye la protección de datos en dispositivos locales, puntos finales conectados a dispositivos y dispositivos de red. Mientras los usuarios sigan favoreciendo estos dispositivos frente a los ordenadores de sobremesa, seguirán siendo un objetivo principal para los piratas informáticos [25].

2.3.3. Amenazas a la seguridad móvil

Si bien es fundamental crear e implementar políticas de seguridad en toda la empresa, las políticas por sí solas no son suficientes para combatir la escala y la diversidad de las amenazas móviles actuales. En 2019, Verizon realizó un estudio en asociación con empresas líderes en seguridad móvil, incluidas IBM, Lookout y Wandera, en el que encuestó a 670 profesionales de la seguridad. Las investigaciones muestran que un tercio de los encuestados informaron de un incidente relacionado con un dispositivo móvil. El 47% dijo que las reparaciones eran "difíciles y costosas" y el 64% dijo que experimentaron tiempo de inactividad. Las empresas que utilizan políticas de seguridad también enfrentan mayores riesgos al permitir que dispositivos potencialmente vulnerables accedan a servidores y bases de datos corporativos confidenciales,

exponiéndolos a ataques. Los ciberdelincuentes y estafadores pueden aprovechar estas vulnerabilidades para dañar a usuarios y organizaciones. Buscan secretos comerciales, conocimiento interno y acceso no autorizado a redes seguras para encontrar cualquier cosa que pueda resultar rentable [26].

2.3.4. Phishing

Se puede decir que un ataque de phishing a teléfonos móviles es una trampa en la que caemos y exponemos nuestros datos. Por ejemplo, hacer clic en un enlace te lleva a una página fraudulenta que pretende ser oficial. Cuando ingresamos una contraseña, normalmente no iniciamos sesión en la plataforma, sino que enviamos esta información directamente al hacker [26].

A menudo, los ciberdelincuentes utilizan algunas tácticas para engañarnos. Por ejemplo, díganos que hay un problema con su cuenta y que necesitamos ingresar cierta información para confirmar que todo está bien, etc. Suelen actuar con rapidez, por lo que la víctima tiene poco tiempo para pensar antes de aceptar finalmente [26].

2.3.5. Malware y Ransomware

El ransomware móvil es un tipo de código malicioso que bloquea el dispositivo y, en muchos casos, cifra los archivos del dispositivo, los atacantes exigen que las víctimas paguen para recuperar sus dispositivos y archivos. Hemos analizado algunos de estos ransomware de Android en los últimos años, como el ransomware detrás de una aplicación falsa de rastreo de contactos de COVID-19 dirigida a usuarios canadienses, o una campaña que utilizó sus propias listas de contactos para difundir ransomware. Le envió a la víctima un mensaje de texto con un enlace malicioso [27].

2.3.6. Criptojacking

El criptojacking es una variante de malware que actualmente es una de las tendencias más peligrosas por su conexión con las criptomonedas. La "minería" de monedas digitales se refiere a la asignación de potencia de procesamiento desde dispositivos como computadoras o teléfonos inteligentes para realizar cálculos que verifiquen las transacciones de criptomonedas. A cambio, los piratas informáticos reciben una compensación financiera de estas monedas virtuales, que luego pueden cambiar por dólares estadounidenses o euros y otras monedas. Debido a las elevadas ganancias

obtenidas con los criptoactivos, los piratas informáticos están promoviendo el desarrollo de malware criptográfico, los llamados cryptohacks [28].

2.4. Marco Legal

En este trabajo se analizan los siguientes artículos, en los cuales se podría incurrir una investigación forense en el dispositivo móvil, debido a que, ese dispositivo tecnológico puede ser usado para transmitir información que pudiera comprometer la integridad física y/o psicológica de un usuario.

A continuación, se describen la siguiente tipificación de delitos:

2.4.1. Código Orgánico Integral Penal, COIP

El COIP fue publicado en el Registro Oficial Suplemento N° 180, el 10 de febrero del año 2014, surgiendo de una necesidad por unificar en un solo escrito, la legislación existente del carácter punitivo, cuya mayor exigencia es reflejada en la seguridad jurídica; declarando los siguientes artículos [29].

Art. 103.- Pornografía con utilización de niñas, niños o adolescentes.

Art. 173.- Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos.

Art. 178.- Violación a la intimidad.

Art. 179.- Revelación de secretos.

Art. 186.- Estafa.

Art. 190.- Apropiación fraudulenta por medios electrónicos.

Art. 229.- Revelación ilegal de información de base de datos.

Art. 230.- Intercepción ilegal de datos.

Art. 231.- Transferencia electrónica de activo patrimonial.

Art. 232.- Ataque a la integridad de sistemas informáticos.

Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

2.4.2. Ley Orgánica de Protección de Datos Personales

Con la Ley de Protección de Datos Personales, se busca cuidar la integridad de las personas titulares de datos, para que puedan decidir a quién entregar la información personal, ya que, confían en los proveedores de los servicios digitales; A continuación, se detallan los artículos conformes al tema [30]:

Art. 5.- Integrantes del sistema de protección de datos personales.

Art. 8.- Consentimiento.

Art. 25.- Categorías especiales de datos personales.

Art. 36.- Excepciones de consentimiento para la transferencia o comunicación de datos personales.

Art. 37.- Seguridad de datos personales.

Art. 40.- Análisis de riesgos, amenazas y vulnerabilidades.

Art. 41.- Determinación de medidas de seguridad aplicables.

Art. 65.- Medidas correctivas.

Art. 70.- Infracciones graves del encargado de protección de datos.

Art. 75.- Autoridad de protección de datos personales.

Art. 76.- Funciones, atribuciones y facultades.

CAPITULO 3. PROPUESTA

El presente capítulo describe el análisis de evidencias digitales en los dispositivos móviles y sus resultados, mediante el desarrollo de cada una de las fases detalladas en el apartado de la metodología.

3.1 Análisis de requerimientos

3.1.1 Requerimientos funcionales

Código	Especificación de requerimientos

RQ01	Ejecutar una recolección de información, mediante una encuesta a los estudiantes, entrevista al propietario del teléfono celular y un método de observación a las características del dispositivo móvil.
RQ02	Determinar los resultados de la encuesta realizadas aplicando la escala de Likert, a su vez, utilizando gráficos estadísticos en el desglose de las preguntas.
RQ03	Adquirir los permisos adecuados del propietario del dispositivo móvil para realizar el respectivo análisis mediante computación forense.
RQ04	Identificar el grado de conocimiento que posee el propietario, con respecto a las seguridades que manejan los dispositivos móviles.
RQ05	Analizar el estado físico en que se encuentra el dispositivo para determinar el tipo de análisis que se manejará hacia el móvil.
RQ06	Aplicar el modo depuración del dispositivo móvil, activando la opción de desarrollador para poder rootearlo.
RQ07	Emplear la metodología que se determinó para el uso de computación forense en dispositivo móviles, propuesta en el proyecto.
RQ08	Seleccionar las técnicas adecuadas, programas y sistemas operativos especializados de computación forense, para aplicarlas en el dispositivo móvil.
RQ09	Aplicar los programas, mediante técnicas computacionales por comandos, utilizando APK y SO en Linux y Windows.
RQ10	Almacenar en un dispositivo, la evidencia recolectada en cada una de las técnicas empleadas en el móvil.
RQ11	Crear un informe de los ataques generados para constatar de qué manera se obtuvo la información, abarcando un análisis completo de los mismos.

RQ12	Elaborar una guía de buenas prácticas sobre el uso seguro de dispositivos móviles, a las personas que participaron en este estudio.
RQ13	Instalar diversas versiones de Linux, especializadas en análisis forense en una máquina virtual, para poder ejecutar la fase de ataques.
RQ14	Ejecutar las pruebas estratégicas de la versión establecida del dispositivo móvil, para realizar un ataque exitoso.
RQ15	Crear los ataques en base a estudios referenciados sobre computación forense en dispositivos Android, para obtener buenos resultados.

Tabla 1: Requerimientos

3.1.2 Requerimientos no funcionales

3.2 Diseño técnico

El presente capítulo describe el análisis de la integridad en dispositivos móviles con sistema Android, y sus respectivos resultados mediante determinados análisis en un laboratorio forense prefabricado y que mediante el desarrollo de cada una de las fases que se han detallado en el apartado de la metodología.

3.2.1 Componentes de la propuesta

El análisis forense al dispositivo móvil que se tiene como evidencia, se hará mediante un equipo de cómputo con características que no permitan ejecutar varios sistemas virtualizados para el montaje de este laboratorio:

Laboratorio Forense Hardware	
Equipo	**Características**
Laptop o pc de escritorio	• **Disco duro:** 1 Tera o más. • **Ram:** 16 gigas en adelante. • **Procesador:** Intel Core I5 o superior. • **SO:** Windows 10

Laboratorio Forense Software		
Virtualización	Oracle VM VirtualBox	Anexo 5
Ataque 1	Santoku	Anexo 6
Ataque 2	ExifTool	Anexo 7
Ataque 3	Kali Linux	Anexo 8

Tabla 2: Laboratorio forense hardware

3.2.2 Arquitectura del sistema Android

Para tener en claro una visión sobre la extracción de datos en Sistemas Operativo Android, se debe tener en cuenta como prioridad, la estructura donde se va a trabajar [3].

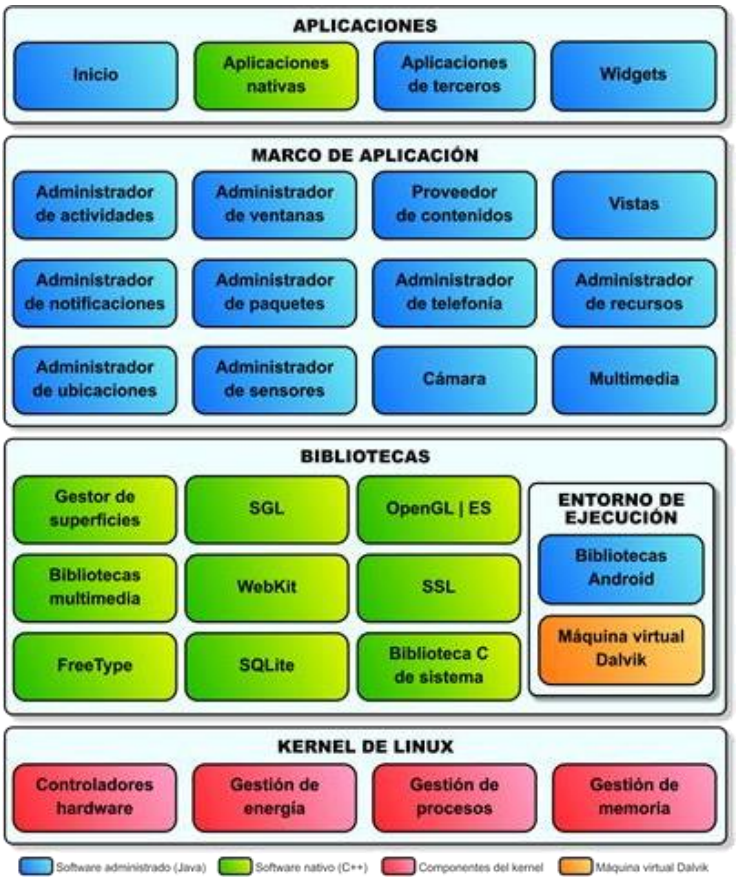


Figura 2. Arquitectura del sistema operativo Android

Entre los métodos más complejos de una extracción de datos en un dispositivo Android, está delimitar en que parte de la raíz o partición se debe de tomar en cuenta, ya sea de la memoria interna como externa:

ALMACENAMIENTO	
Interno	**Externo**
/boot /system /recovery /data /cache /misc	/sdcard /sd-ext

Tabla 3: Almacenamiento

3.3 Desarrollo & Pruebas

3.3.1 Implementación laboratorios virtuales

Para los diferentes escenarios se requiere de diversos programas y Sistemas Operativos para la ejecución de los ataques correspondientes en cada caso de estudio de los cuales se analizaron varias aplicaciones (**Anexo 4**) y tomando en cuenta las siguientes:

Laboratorio Forense Software		
Virtualización	Oracle VM VirtualBox	**Anexo 5**
Ataque 1	Santoku	**Anexo 6**
Ataque 2	ExifTool	**Anexo 7**
Ataque 3	Kali Linux	**Anexo 8**

Tabla 4: Laboratorio forense software

3.3.2 Escenarios de pruebas

3.3.2.1. Recolección

Testeo de funcionalidad del teléfono

Para saber en qué estado se encuentra el equipo en cuanto a la funcionalidad, tanto en audio, video o conectividad; se propone utilizar la app móvil TestM que permita acceder a las diversas funciones del equipo y proporcionar un veredicto de su estado [2].

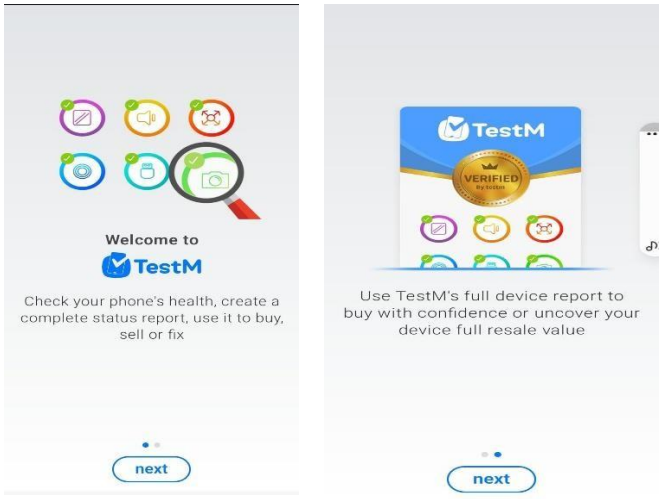


Figura 3. Testeo de funcionalidad del dispositivo móvil

Entre las opciones que se pueden ejecutar, se encuentran las siguientes:

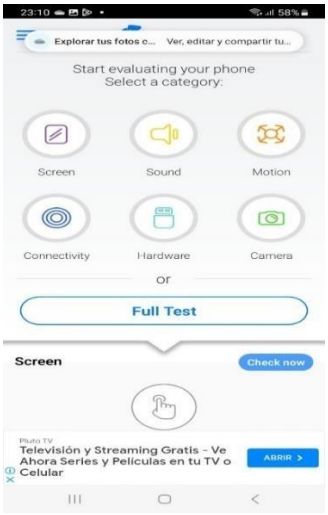


Figura 4. Opciones de testeo

Nivel de calidad del dispositivo móvil

Para medir la escala de la característica del equipo a atacar, se le asignará un valor en una escala del 1 al 10 según los resultados obtenidos en el testeo del apk TestM (**ver Anexo 10**) para medir la funcionalidad del dispositivo.

CARACTERISTICAS	CALIDAD (1-10)
Bluetooth	8/10
Acelerómetro	7/10
Botones	10/10
Cámara trasera	10/10
Micrófono	10/10
GPS	9/10
Cámara frontal	10/10
Salida de audio	10/10
Wifi	8/10
Táctil	8/10
Sensores	9.5/10

Tabla 5: Características y calidad

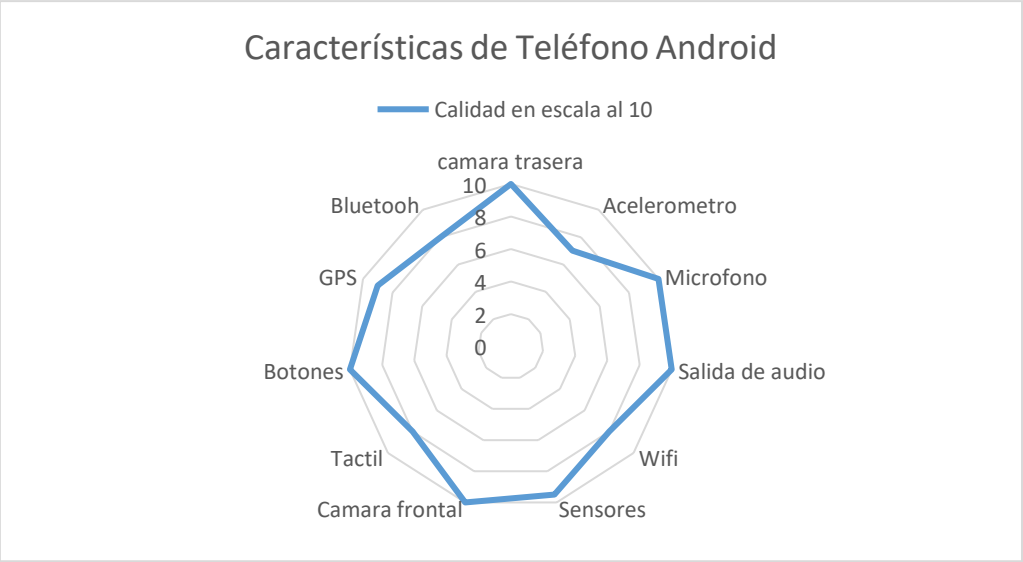


Figura 5: Características de teléfono Android

3.3.2.2. Inspección

Custodia y evidencias del dispositivo

Para ejecutar este estudio se necesitará del dispositivo físico, el cual será la evidencia del mismo y su entorno. Esta verificación se mostrará en la documentación con imágenes digitales del dispositivo Android (**ver Anexo 9**).

Figura 6. Dispositivo móvil

El equipo presentaba falta de actualización del sistema operativo, pero por la memoria no podía proceder, así que, se debió borra información para poderlo actualizar.

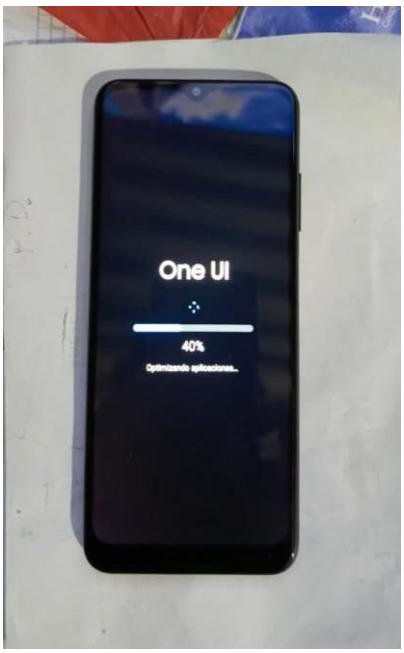


Figura 7. Actualización del dispositivo móvil

Se determinó que, su encendido es correcto y se procederá a evidenciar las características del celular.

Figura 8. Encendido del dispositivo móvil

Al arrancar, se presentó la información del teléfono para ver en qué se va a trabajar.

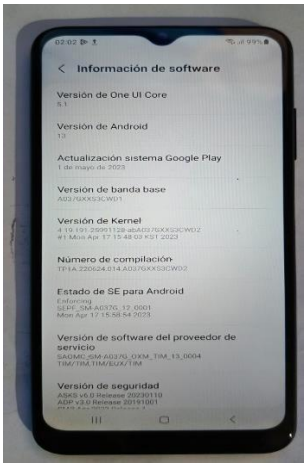


Figura 9. Características del dispositivo móvil

Las características del dispositivo se encontrarán en los anexos del documento (Ver Anexo 2) para poder evidenciar los demás hallazgos.

3.3.2.3. Análisis

Evaluación Ataque 1 (AFlogical OSE)

Para la práctica de este ataque se necesitará la implementación del sistema operativo Santoku, los cuales brindan una herramienta adecuada para la realización de la extracción de información en modo Forense de esta simulación (ver Anexo 11), creando una APK que se instalara en el dispositivo móvil conectado y nos brindara información interna del dispositivo desde contactos, mensaje, llamadas y log.

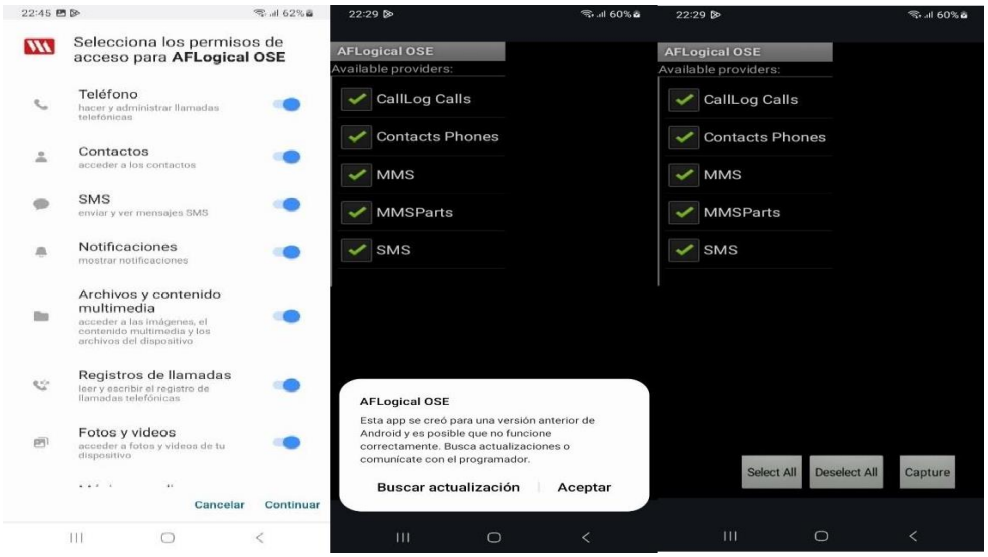


Figura 10. Conexión con Santoku

Como se observa en la imagen de arriba se instala el apk creado por el sistema santoku denominado AFlogical OSE permitiendo arrancar desde el sistema operativo este aplicativo y extraer la información que se desea del dispositivo móvil.

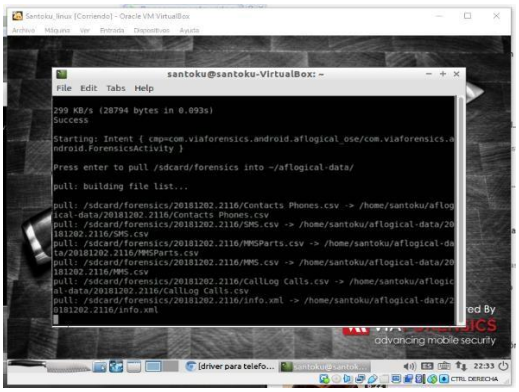


Figura 11. Extracción que realiza Santoku

Una vez realizado todo este proceso los archivos que se generaron se preservaran en una carpeta del sistema para su determinado análisis.

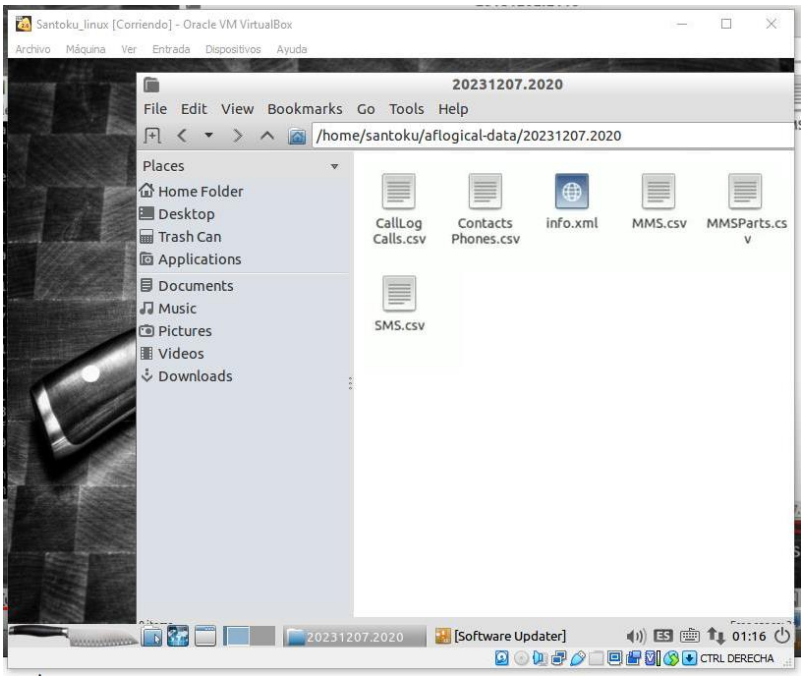


Figura 12. Hallazgos

Evaluación Ataque 2 (Exiftool)

Entre la información que se puede obtener habitualmente de los dispositivos Android en la actualidad, están las imágenes, documentos y otros datos (ver Anexo 12). Esto es denominado como información relevante, pero al ser copiados directamente desde el dispositivo, no se puede contemplar un nivel avanzado de datos internos que ocultan dichos archivos, mismos que se denominan metadatos.

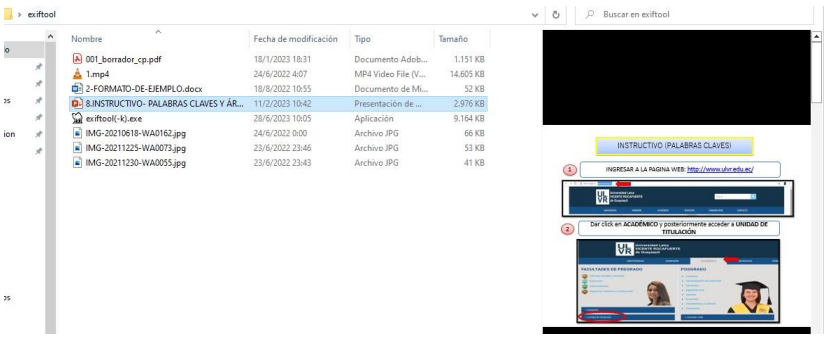


Figura 13. Creación de carpeta

Cuando se obtienen los dataos a analizar y el programa mediante CMD se hará arrancar los metadatos de los archivos para poder encontrar información que a simple vista no se aprecian en las propiedades del archivo a analizar.

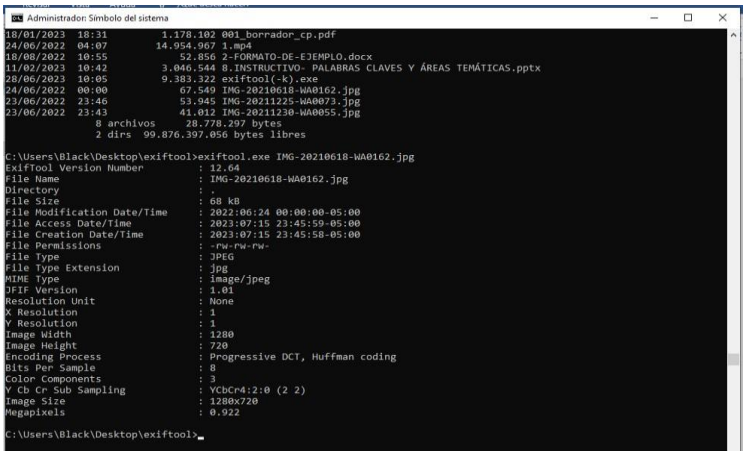


Figura 14. Arranque de exiftool

Evaluación Ataque 3 (Meterpreter)

Meterpreter es una carga útil que permite la realización de tareas de forma remota en una computadora, siendo un software que se ejecuta a un nivel de máquina muy bajo, por lo que es difícil de detectar; Con la carga útil de Meterpreter, es posible conectarse a la cámara web y al teclado de la computadora infectada y tomar capturas de pantalla (ver Anexo 13). Sin embargo, es importante recordar que el software no funciona igual en todos los sistemas operativos, ya que, la versión más completa de este programa es para Windows [9].

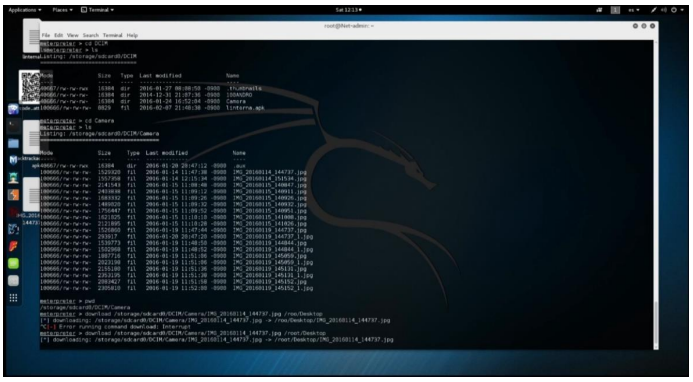


Figura 15: Evaluación de ataque 3

Extracción de datos en WhatsApp con Meterpreter

Una vez ejecutado el Meterpreter, se podrá acceder al equipo y las raíces para interpretar carpetas ocultas, de tal manera que, con este método pasa los permisos para poder ver esta misma información.

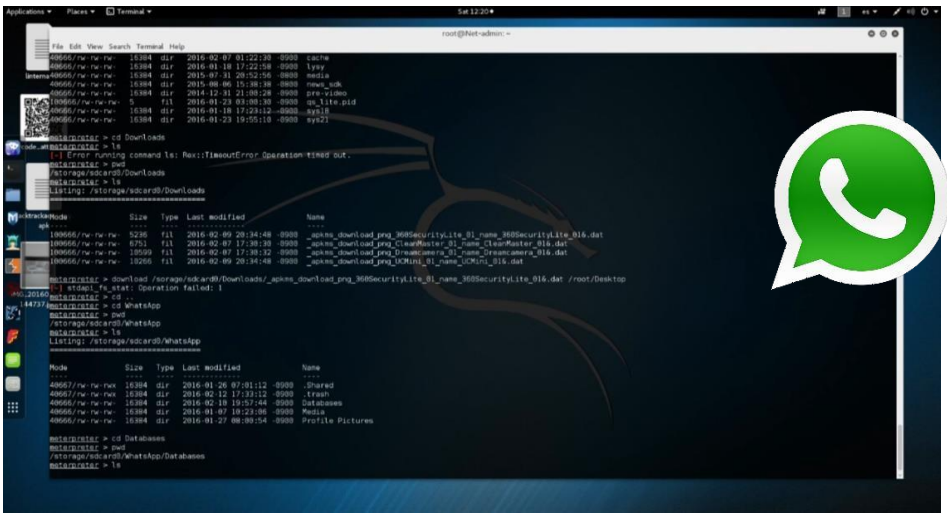


Figura 16: Extracción de datos

Extracción de datos en Dropbox con Meterpreter

Para ver la carpeta que se aloja en el Dropbox, se ingresa a la parte denominada com.dropbox.android para extraer la información, estas acciones dan como resultado tres archivos asset_cache, cache y files.

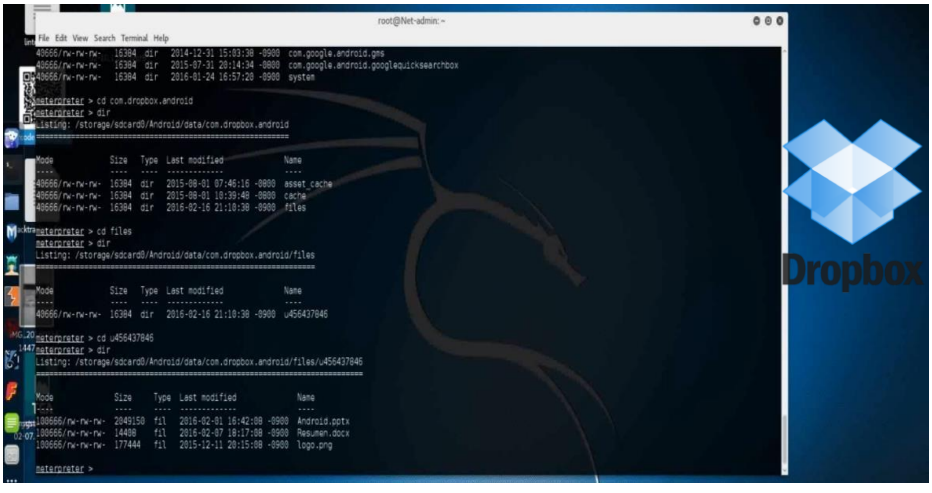


Figura 17: Dropbox

3.3.2.4. Reportes

El desarrollo de los siguientes apartados se documenta según el (**ver Anexo 14**). Formato de informe para los análisis, pero al ser un tema de investigación, los datos generales se adaptan para la capacitación y se omiten detalles para mantener la integridad de la información.

Estas revisiones tienen su propia estructura, como se muestra arriba, y deben realizarse de la misma manera en cada caso para mantener el paradigma interpretativo correcto, estos informes incluirán todo el proceso, software forense y técnicas utilizadas, desde la recogida de pruebas hasta su recuperación y análisis, válidas para los juicios de que se trate.

CAPITULO 4. RESULTADOS

4.1. Resultados de la entrevista dirigida al propietario del dispositivo móvil

Objetivo: Verificar el estado que presenta el dispositivo móvil y los datos requeridos por el dueño para el análisis forense.

1. **¿Cuál era el uso que le daba al dispositivo móvil?**

El dispositivo móvil lo uso con fines personales, sin embargo, también lo uso para cuestiones laborales, almacenando información del trabajo.

2. **¿Cuáles eran los fallos que presentaba el celular cuando lo utilizaba?**

Tenían problemas de memoria, es decir, ya no le cabe mucha información; así mismo, muchas veces se tornaba lento y me generaba problemas. Yo creo que estaba infectado por un virus o algo similar, debido a que, ni las redes sociales me abrían.

3. **¿Se le extravió información en el tiempo de uso del dispositivo? ¿Qué tipo de información?**

Si, muchas veces de la nada se me perdía información del trabajo y de la universidad, siendo un dolor de cabeza para mí, ya que, tenía que volver a pedir esos datos.

4. **Entre las aplicaciones que el celular tenía, ¿Cuáles eran las que más utilizaba durante el día?**

Las aplicaciones que más utilizaba durante el día son: redes sociales, mensajes, cámara, llamadas, galería, gestor de archivos y lector de documentos.

5. **¿Contaba con alguna aplicación para la seguridad de su dispositivo móvil?**

Tengo un antivirus en el celular y solo bloqueo el celular con patrón y huella dactilar.

6. **¿Cuál de las aplicaciones que tenía en el celular, presentaba publicidad sin previo permiso? ¿Por qué?**

Más que nada, el antivirus y ciertos juegos que tenía; a fin de cuentas, terminé desinstalando todo eso.

7. **¿El equipo tenía alguna falla física que impedía su buen funcionamiento? ¿Cuáles?**

   Sí, se me había caído un par de veces, la mica estaba rota y ciertas partes del táctil fallaban.

8. **En la actualidad. ¿En qué utiliza el dispositivo móvil? ¿Por qué lo cambió?**

Lo cambié por otro smartphone porque necesitaba mayor capacidad para guardar archivos e instalar más aplicaciones que requería.

4.2. Resultados de la encuesta dirigida a los estudiantes de la carrera de Tecnologías de la información

Objetivo: Analizar el uso del dispositivo móvil y sus diferentes aplicaciones.

1. **¿Qué aplicaciones utiliza habitualmente?**

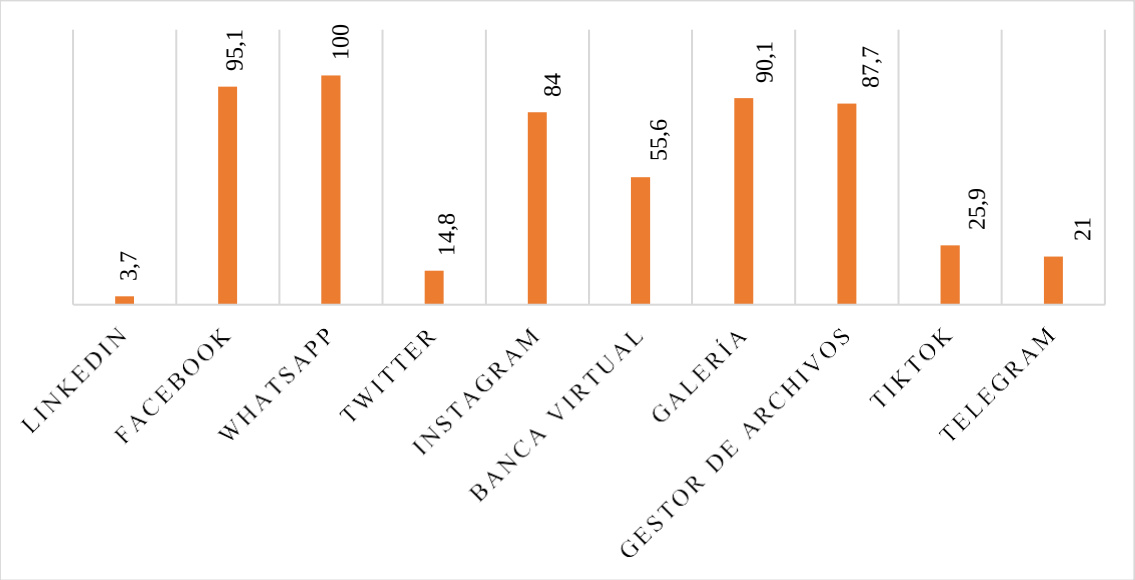


Figura 18. Aplicaciones utilizadas

En la primera pregunta de la encuesta se pudo determinar que, el 3.7% utiliza LinkedIn, el 95.1% Facebook, el 100% WhatsApp, el 14.8% Twitter, el 84% Instagram, el 55.6% banca virtual, el 90.1% galería, el 87.7% gestor de archivos, el 25.9% Tiktok y el 21% telegram.

2. ¿Qué tiempo utiliza su celular durante el día?

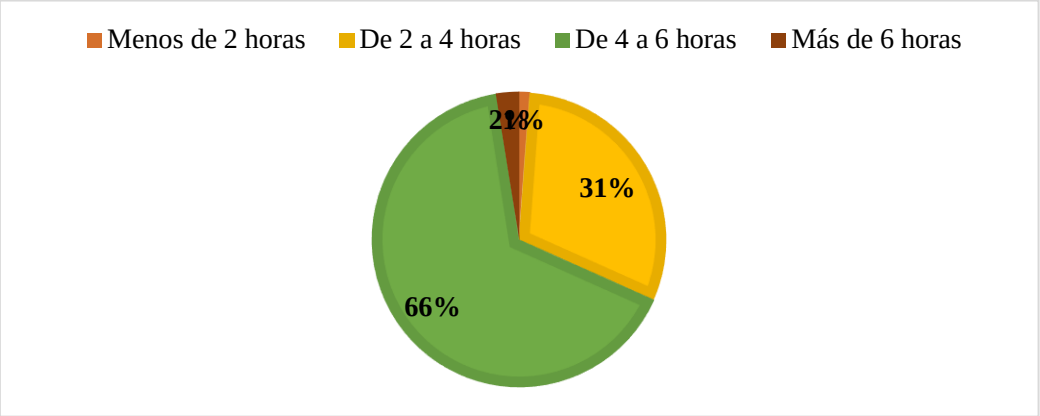


Figura 19. Tiempo de uso del celular

En la segunda pregunta de la encuesta se pudo determinar que, el 66% utiliza su celular de 4 a 6 horas durante el día, mientras que, el 31% lo usa de 2 a 4 horas, el 2% lo emplea más de 6 horas y el 1% lo utiliza menos de 2 horas diariamente.

3. **¿Ha presentado pérdida de información en alguna de las aplicaciones qué utiliza?**

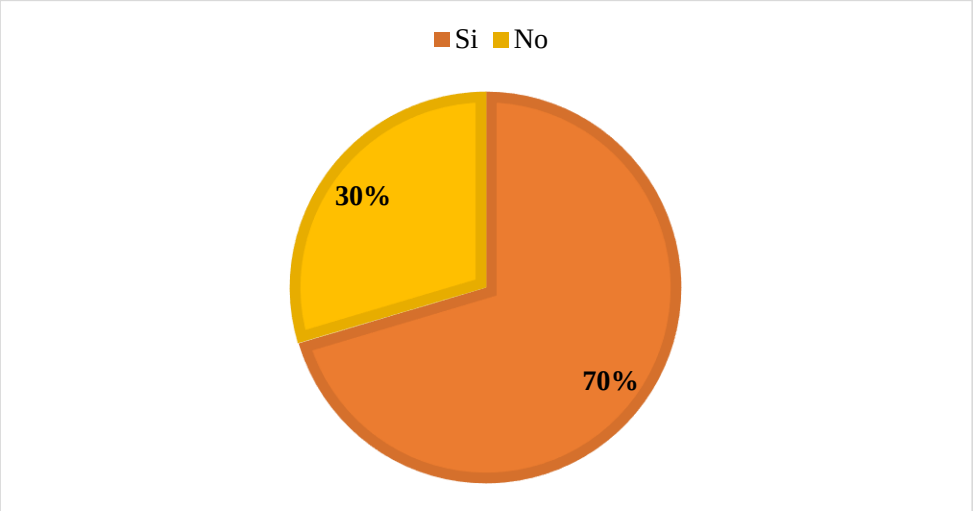


Figura 20. Pérdida de información en aplicaciones

En la tercera pregunta de la encuesta se pudo determinar que, el 70% si ha presentado pérdida de información en alguna de las aplicaciones que utiliza, mientras que, el 30% no.

4. ¿Posee seguridad de bloqueo en el dispositivo? Seleccione cual utiliza

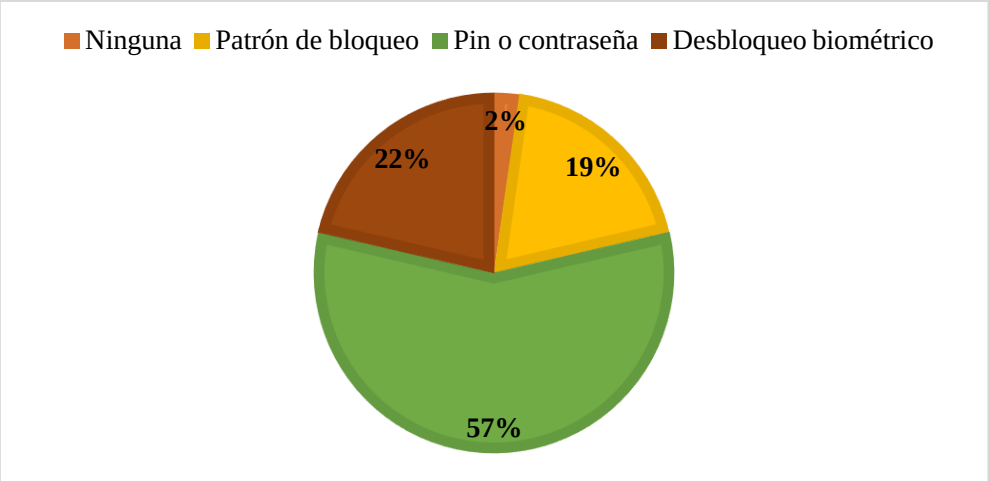


Figura 21. Seguridad de bloqueo

En la cuarta pregunta de la encuesta se pudo determinar que, el 57% posee como seguridad de bloqueo en el dispositivo el pin o contraseña, mientras que, el 22% tiene desbloqueo biométrico, el 19% posee patrón de bloqueo y el 2% no tiene ninguna seguridad en el dispositivo.

5. En la actualidad, ¿Qué uso le da a su dispositivo móvil?

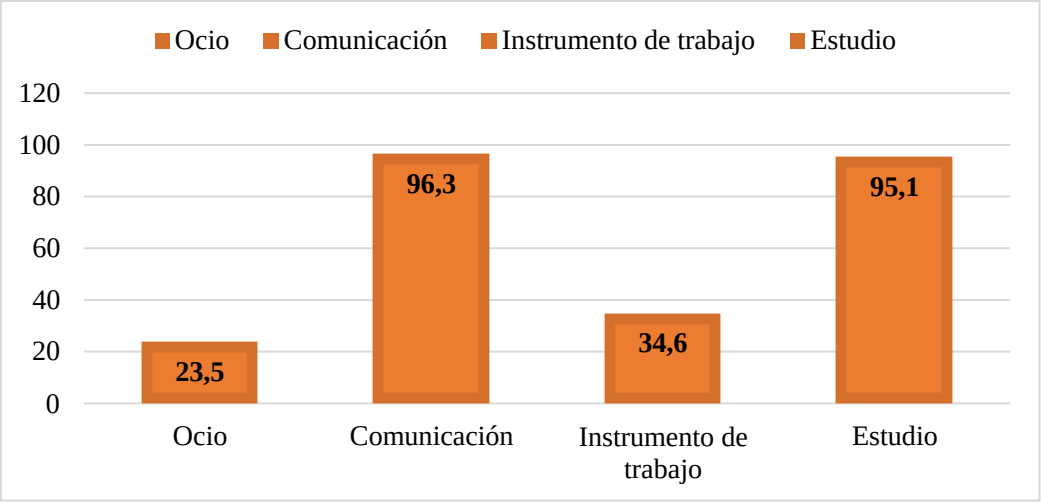


Figura 22. Uso del dispositivo móvil

En la quinta pregunta de la encuesta se pudo determinar que, el 23.5% utiliza su dispositivo móvil para ocio, mientras que, el 96.3% para comunicarse, el 34.6% como instrumento de trabajo y el 95.1% lo usa para estudio.

6. ¿En qué momento lo usa mayor tiempo?

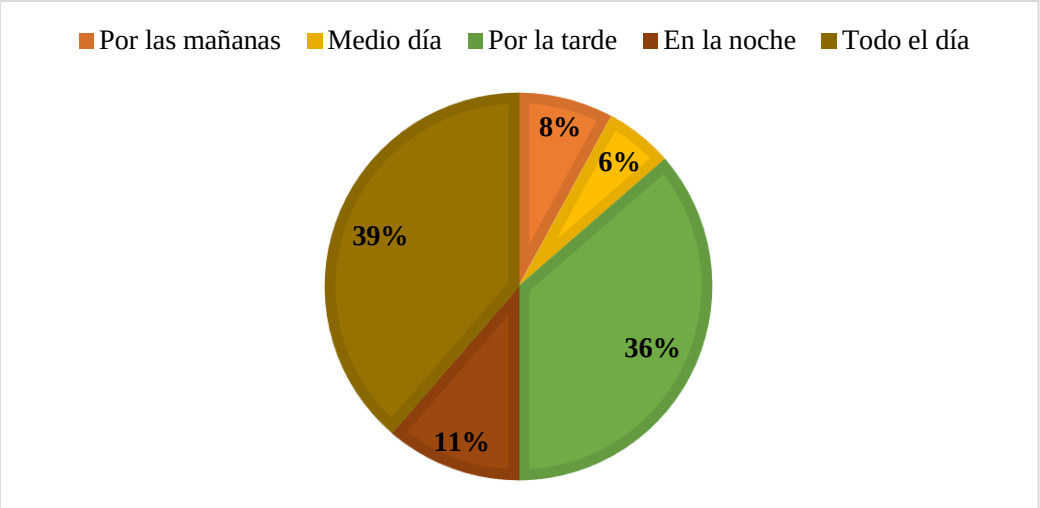


Figura 23. Mayor tiempo de uso

En la sexta pregunta de la encuesta se pudo determinar que, el 39% usa el dispositivo móvil todo el día, mientras que, el 36% lo utiliza mayor tiempo por la tarde, el 11% lo emplea más en la noche, el 8% por las mañanas y el 6% al medio día.

7. ¿Qué tan seguro cree que es utilizar aplicaciones en el teléfono móvil?

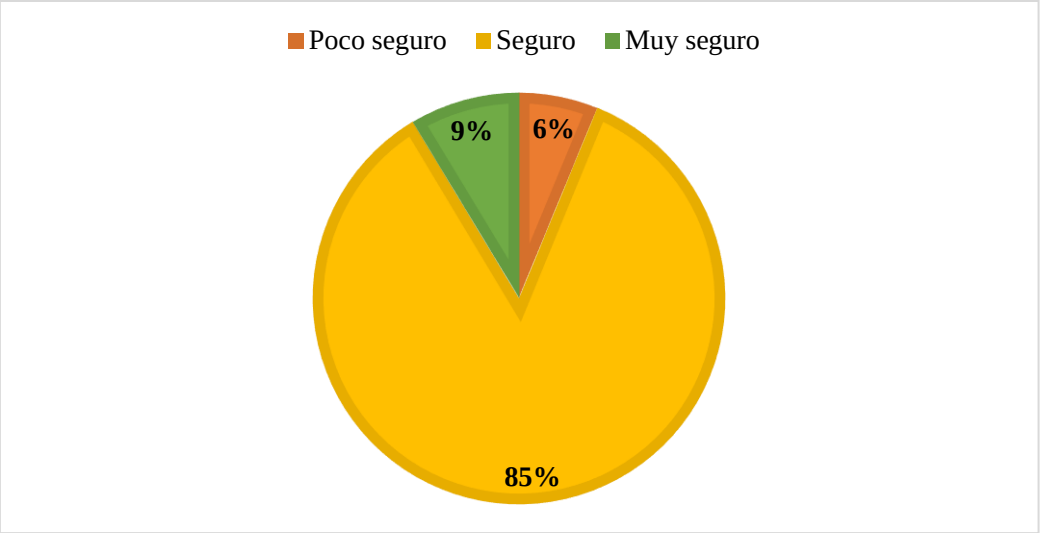


Figura 24. Seguridad en aplicaciones móviles

En la séptima pregunta de la encuesta se pudo determinar que, el 85% manifiesta que es seguro utilizar aplicaciones en el teléfono móvil, mientras que, el 9% opina que es muy seguro y el 6% dice que es poco seguro.

8. **Aproximadamente, ¿Cuántas veces ha tenido que reparar su dispositivo móvil?**

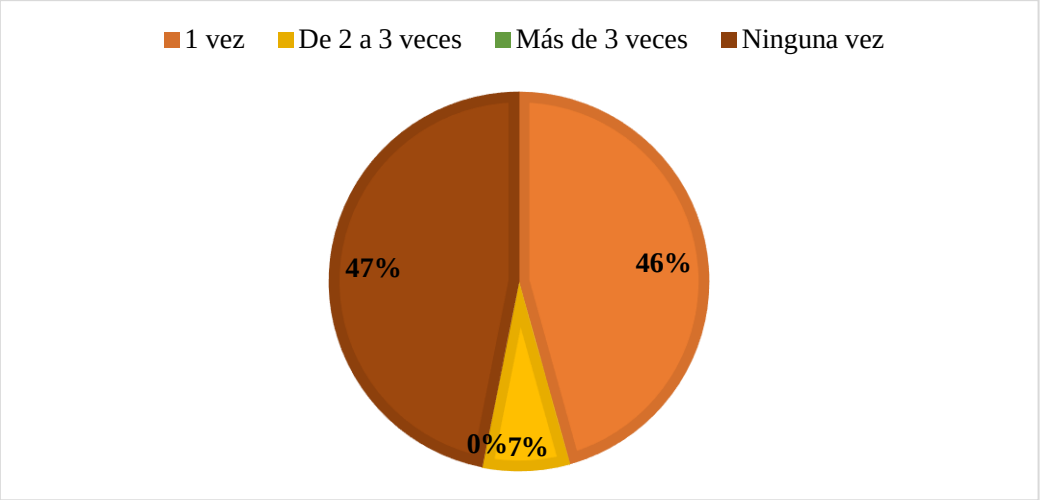


Figura 25. Reparaciones en el dispositivo móvil

En la octava pregunta de la encuesta se pudo determinar que, el 47% no ha tenido que reparar su dispositivo móvil, mientras que, el 46% lo ha hecho una vez y el 7% de 2 a 3 veces.

4.3. Resultados de la ficha de observación realizada al dispositivo móvil en cuestión

Objetivo: Determinar el estado físico y las características del dispositivo.

- Dispositivo móvil de marca Samsung Galaxy A03s, a primera vista se ve en perfecto estado.

- Dispositivo móvil posee dos seguridades, una por huella dactilar en la pantalla Oled y otra por clave de patrón.

- Estado de depuración y modo desarrollador se encuentran en modo inactivo.

- Memoria de almacenamiento del dispositivo móvil unificada, para realizar almacenamiento virtual como si fuera uno.

- Puerto de datos del dispositivo móvil en perfecto estado, de categoría tipo C con depuración de almacenamiento USB 3.0.

4.3.1. Ficha técnica del dispositivo móvil

Figura 26: Dispositivo móvil

A continuación, se presentan las características del dispositivo móvil Samsung Galaxy A03s, utilizado en este proyecto [1].

Pantalla	LCD 6,3" HD+

Dimensiones y peso	164,2 x 75,9 x 9,1 mm 196 g.
Procesador	Ocho núcleos a 2,3 GHz y 1,8 GHz
RAM	3 / 4 GB
Almacenamiento	32 / 64 GB
Cámara Frontal	5 MP f/2.2
Cámara Trasera	13 MP f/2.2 2 MP f/2.4 2 MP f/2.4
Batería	5.000 mAh
Sistema Operativo	Android One UI
Conectividad	LTE Wi-Fi b/g/n Bluetooth 5.0 USB-C Minijack
Otros	Lector de huellas en un lateral

Tabla 6. Ficha técnica del dispositivo móvil

4.4. Estándares para gestionar la seguridad de Android

Los objetivos de control y controles que se describen a continuación se consideran comparables porque su aplicabilidad no es específica de conceptos empresariales u organizacionales y son comparables a la luz de los objetivos y controles de gestión

descritos por cada objetivo y control. En consecuencia, la seguridad de los teléfonos inteligentes se probará en la siguiente fase del proyecto.

Protección para códigos maliciosos en dispositivos móviles (Numeral 10.4 en la norma ISO

17799)

Objetivo: Proteger la integridad del software y la información. Se deben tomar precauciones para prevenir y detectar la entrada de códigos maliciosos y códigos móviles no autorizados.

Control de códigos maliciosos

Controles: Deben existir controles de detección, prevención y recuperación para prevenir códigos maliciosos, así como procedimientos adecuados de notificación al usuario.

Respaldar o realizar Back-up (Numeral 10.5 en la norma ISO 17799)

Objetivo: Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información. Se deben establecer procedimientos de rutina para implementar la estrategia de respaldo acordada y la estrategia de recuperación oportuna.
Copia de seguridad de la información.

Control: La información y el software deben respaldarse y probarse periódicamente de acuerdo con una estrategia de respaldo acordada.

Gestión de medios (Numeral 10.7 en la norma ISO 17799)

Objetivo: Evitar la divulgación no-autorizada, modificación, eliminación o destrucción de activos; y la interrupción de las actividades comerciales.

Procedimientos para el manejo de información.

Control: Se debieran establecer los procedimientos para el manejo y almacenaje de información para proteger esta información de una divulgación no- autorizada o mal uso**.**

Compromisos de los usuarios (Numeral 11.3 en la norma ISO 17799)

Objetivo: Evitar que usuarios no autorizados accedan, sustraigan o comprometan la información y los servicios de procesamiento de la información.

Los usuarios deben comprender su responsabilidad de mantener controles de acceso efectivos, particularmente con respecto al uso de claves y la seguridad del equipo del usuario.

Uso de controles de seguridad

Control: Los usuarios deben seguir buenas prácticas de seguridad en la elección y uso de claves.

Controles Criptográficos (Numeral 12.3 en la norma ISO 17799)

Finalidad: Proteger la confidencialidad, autenticidad o integridad de la información mediante cifrado.

Se debe desarrollar una política con respecto al uso de controles de contraseñas y se debe establecer una gestión de claves para respaldar el uso de métodos criptográficos.

Política de uso de controles de cifrado

Controles: Se deben desarrollar e implementar políticas que utilicen controles de cifrado para proteger la información.

4.5. Buenas prácticas para el uso de teléfonos Android

A continuación, se detallan los pasos que puede seguir para mejorar la seguridad de cada uno de los sistemas operativos móviles más comunes.

Bloqueo de contraseñas

La mayoría de los dispositivos tienen medidas de bloqueo cuando entran en modo de suspensión. Este recurso garantiza que sólo el personal autorizado que conozca la contraseña pueda acceder al terminal. Si pierde o roba, la única forma de usar el dispositivo es la restauración del valor de fábrica para que se pierdan todos los datos de configuración y almacenamiento.

Existen varios métodos para limitar el uso de equipos. Varían según el fabricante. Los más utilizados son un código PIN de 4 dígitos, una contraseña alfanumérica o un patrón

de desbloqueo. También es importante configurar el terminal para que hiberne y bloquee la pantalla automáticamente tras un determinado periodo de inactividad. Si no se utiliza esta medida, la tecnología de bloqueo perderá prácticamente toda su eficacia.

Cifrado de memoria

Esta práctica suele complementar el método anterior, esto incluye cifrar la memoria de almacenamiento para que los datos no se puedan copiar ni extraer sin conocer la contraseña de desbloqueo. Dependiendo del modelo, se pueden cifrar tanto la memoria interna como la externa (como una tarjeta de memoria flash). Después del cifrado, solo se puede acceder a los datos almacenados cuando el dispositivo está desbloqueado usando la contraseña de bloqueo de pantalla.

Sin conocer la clave, es difícil recuperar información, incluso con técnicas forenses de extracción y replicación de datos, siendo el único método, posible es utilizar técnicas de fuerza bruta, que implican probar automáticamente todas las combinaciones de contraseñas posibles hasta encontrar una que permita el acceso.

Por lo tanto, para que este ataque sea imposible, es importante utilizar una contraseña compleja que sea una combinación de letras y números, letras mayúsculas y caracteres especiales.

Borrado vía remota

Al hacer esto, puede borrar de forma remota los datos de su dispositivo y restaurarlos a su configuración original de fábrica. Suponiendo que la información almacenada sea sensible, es importante tener este recurso a mano en caso de pérdida o robo del dispositivo. Esta función depende del tipo de dispositivo, fabricante u operador y puede generar un cargo.

CONCLUSIONES

- Se realizó un levantamiento de información de los dispositivos móviles con sistema operativo Android, identificando de forma precisa los detalles técnicos del sistema con sus funcionalidades, comprendiendo la arquitectura y comportamiento del sistema operativo, siendo esencial para las fases aplicadas en la investigación forense.

- Se llevó a cabo una evaluación del nivel de conocimiento que poseen los usuarios con respecto al uso y gestión de la ciber seguridad en los dispositivos móviles, recabando información sobre la preparación de los encuestados con relación a las amenazas cibernéticas existentes.

- El diseño de pruebas experimentales a través de la descripción de casos de estudio brindó la emulación de incidentes de seguridad informática en los dispositivos móviles, evaluando la resiliencia del sistema y su capacidad de respuesta ante diversas situaciones.

- Se elaboró un informe detallado de las vulnerabilidades encontradas durante la investigación forense en los dispositivos móviles, ofreciendo una visión completa de los riesgos y debilidades, proporcionando una base sólida para tomar decisiones informadas, asegurando un enfoque proactivo en seguridad.

- Se proponen medidas de seguridad basadas en las normas internacionales ISO y NIST, para mitigar las ciber amenazas identificadas, con recomendaciones que fortalezcan la postura de la seguridad, en conjunto con la implementación de medidas correctivas y preventivas.

RECOMENDACIONES

- Se deben utilizar los métodos de recolección de información adecuados, asegurando una recopilación detallada del sistema operativo Android, para mantenerse al tanto de las nuevas versiones y actualizaciones.

- Es recomendable diseñar encuestas claras, abordando aspectos clave sobre la ciberseguridad en los dispositivos móviles, incorporando preguntas acerca de la privacidad, almacenamiento de información, entre otros.

- Se recomienda desarrollar más casos de estudio que reflejen diferentes escenarios actuales y realistas de amenazas cibernéticas en los dispositivos móviles Android, permitiendo la evaluación del sistema frente a diversas vulnerabilidades.

- Es importante presentar de manera jerárquica las vulnerabilidades en el informe forense, destacando las que poseen mayor riesgo y brindando información detallada sobre cómo pueden ser evadidas.

- Es recomendable tomar en consideración las medidas de seguridad basadas en las normas internacionales ISO y NIST, adaptándolas a la realidad requerida en los entornos Android.

REFERENCIAS

[1] M. García García, «Análisis de riesgos, de vulnerabilidades y auditorías de dispositivos,» Barcelona, 2020.

[2] B. D. Ramos Anampa, «Implementación de un Software Forense para el Análisis de la Evidencia Digital en Dispositivos Móviles,» Universidad Tecnológica del Perú, Lima, 2019.

[3] Comisión Federal de Comercio, «Cómo proteger su teléfono de los piratas informáticos,» 2023. [En línea]. Available: https://consumidor.ftc.gov/articulos/como-proteger-su-telefono-de-los-piratas-informaticos. [Último acceso: 07 06 2023].

[4] K. W. Beltrán Tapia, «MODELO PARA ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID,» UPSE, Santa Elena, 2021.

[5] F. J. Mirabá Quimí, «Diseño de una Guía Metodológica para el Análisis Forense Digital tomando como base Equipos con el Sistema Operativo Windows 8.1,» UPSE, Santa Elena, 2021.

[6] E. Nuñez Soto, «Investigación forense de dispositivos móviles: metodologías y herramientas,» red seguridad, 21 10 2020. [En línea]. Available: https://www.redseguridad.com/especialidades-tic/activos-de-informacion/investigacion-forense-de-dispositivos-moviles-metodologias-y-herramientas_20201021.html. [Último acceso: 18 06 2023].

[7] User_tematico, «La auditoría forense: prevención y evidencia de los delitos financieros,» Pais dominicano tematico, 06 01 2020. [En línea]. Available: https://paisdominicanotematico.com/2020/01/06/la-auditoria-forense-prevencion-y-evidencia-de-los-delitos-financieros/. [Último acceso: 18 06 2023].

[8] Ecuador, «Plan de Creación de Oportunidades 2021-2025,» 2021. [En línea]. Available: https://www.planificacion.gob.ec/wp-content/uploads/2021/09/Plan-de-Creacio%CC%81n-de-Oportunidades-2021-2025-Aprobado.pdf.

[9] Z. G. M. Coronel Orlando, «Tipos de investigacion,» Jóse María Córdova, Bogota, 2020.

[10] O. Zafra Galvis, «Tipos de investigacion,» Revista Científica General José María, Colombia, 2020.

[11] I. V. Medellino, «Análisis Forense de Dispositivos Móviles Android,» STIT, Caracas, 2018.

[12] Universidad Estatal Península de Santa Elena, «Reseña histórica de la creación de la universidad,» 2023. [En línea]. Available: https://www.upse.edu.ec/index.php?option=com_content&view=article&id=10&Itemid=166.

[13] ciberseguridad, «ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES,» 2023. [En línea]. Available: https://ciberseguridad.com/servicios/analisis-forense/dispositivos-moviles/.

[14] r. Serrano, «Analisis forense en dispositivos moviles,» 2022. [En línea]. Available: https://www.ucapem.com/.

[15] A. Muñoz Bermudez, «La importancia del análisis forense digital en la era tecnológica,» 2022. [En línea]. Available: https://www.pwc.com/co/es/pwc-insights/importancia-analisis-forense.html#:~:text=En%20resumen%2C%20la%20inform%C3%A1tica%20forense,en%20procesos%20legales%20y%20judiciales..

[16] M. López Delgado, «Análisis forense digital,» 2021.

[17] Masters Mag, «Análisis forense digital ¿Cómo se realiza? Técnicas, pasos y mejores prácticas,» 01 06 2023. [En línea]. Available: https://www.itmastersmag.com/noticias-analisis/como-se-realiza-un-analisis-forense-digital-tecnicas-pasos-y-mejores-practicas/.

[18] J. Cano, *Revista Ciencia Unemi*, vol. 1, nº 1, p. 7, 2019.

[19] Ondata, «Equipos de análisis informático forense para teléfonos móviles,» 2022. [En línea]. Available: https://www.ondata.es/recuperar/analisis-forense-moviles.htm.

[20] Universidad Veracruzana, «¿CÓMO EXTRAER DATOS FORENSES DEL DISPOSITIVO MÓVIL DE ANDROID?,» 2023. [En línea]. Available: https://www.uv.mx/infosegura/general/noti_forense/.

[21] D. R. Chimbo Fernández, «Prueba de concepto para extraer información con herramientas de análisis forense open source en dispositivos Android,» Ambato, 2022.

[22] F. González, «Análisis forense de dispositivos Android,» 24 04 2023. [En línea]. Available: https://keepcoding.io/blog/analisis-forense-de-dispositivos-android/.

[23] K. W. Beltrán Tapia, «Modelo para análisis forense en dispositivos móviles con sistema operativo Android,» Ambato, 2021.

[24] K. Ortega, «¿Qué es la informática forense?,» 07 09 2022. [En línea]. Available: https://worldcampus.saintleo.edu/noticias/que-es-la-informatica-forense-analisis-forense-informatico.

[25] proofpoint, «¿Qué es la seguridad móvil?,» 2023. [En línea]. Available: https://www.proofpoint.com/es/threat-reference/mobile-security.

[26] IBM, «¿Qué es la seguridad móvil?,» 2023. [En línea]. Available: https://www.ibm.com/mx-es/topics/mobile-security.

[27] L. Stefanko, «Los 3 tipos de malware más peligrosos para Android,» 09 05 2022. [En línea]. Available: https://www.welivesecurity.com/la-es/2022/05/09/tipos-malware-mas-peligrosos-android/.

[28] D. Jerez, «Cryptojacking: ¿Cómo saber si están USANDO mi teléfono celular para MINAR criptomonedas?,» 06 05 2022. [En línea]. Available: https://www.heraldobinario.com.mx/criptomonedas/2022/5/6/cryptojacking-como-saber-si-estan-usando-mi-telefono-celular-para-minar-criptomonedas-25524.html.

[29] República del Ecuador, «Código Orgánico Integral Penal, COIP,» Quito, 2021.

[30] Presidencia de la República del Ecuador, «Ley Orgánica de Protección de Datos Personales,» Quito, 2021.

[31] Santoku, «Cómo: Usar AFLogical OSE para el análisis forense lógico de un dispositivo Android,» 2023. [En línea]. Available: https://santoku-linux.com/howto/howto-use-aflogical-ose-logical-forensics-android/.

[32] Quora, «What are open source tools for Android mobile forensics?,» 2022. [En línea]. Available: https://www.quora.com/What-are-open-source-tools-for-Android-mobile-forensics.

[33] F. Ávila, «LIME,» 2019. [En línea]. Available: http://www.disoftin.com/2019/07/lime-linux-memory-extractor.html.

ANEXOS

Anexo 1. Entrevista dirigida al propietario del dispositivo móvil

<table>
<tr><td colspan="3"> 
Universidad Estatal Península de Santa Elena
Facultad de Sistemas y Telecomunicaciones
Carrera de Tecnologías de la Información</td></tr>
<tr><td colspan="3">Entrevista dirigida al propietario del dispositivo móvil</td></tr>
<tr><td colspan="3">Objetivos: Verificar el estado que presenta el dispositivo móvil y los datos requeridos por el dueño para el análisis forense.</td></tr>
<tr><td>1.</td><td colspan="2">¿Cuál era el uso que le daba al dispositivo móvil?</td></tr>
<tr><td>2.</td><td colspan="2">¿Cuáles eran los fallos que presentaba el celular cuando lo utilizaba?</td></tr>
<tr><td>3.</td><td colspan="2">¿Se le extravió información en el tiempo de uso del dispositivo? ¿Qué tipo de información?</td></tr>
<tr><td>4.</td><td colspan="2">Entre las aplicaciones que el celular tenía, ¿Cuáles eran las que más utilizaba durante el día?</td></tr>
<tr><td>5.</td><td colspan="2">¿Contaba con alguna aplicación para la seguridad de su dispositivo móvil?</td></tr>
<tr><td>6.</td><td colspan="2">¿Cuál de las aplicaciones que tenía en el celular, presentaba publicidad sin previo permiso? ¿Por qué?</td></tr>
<tr><td>7.</td><td colspan="2">¿El equipo tenía alguna falla física que impedía su buen funcionamiento? ¿Cuáles?</td></tr>
<tr><td>8.</td><td colspan="2">En la actualidad. ¿En qué utiliza el dispositivo móvil? ¿Por qué lo cambió?</td></tr>
<tr><td colspan="2">Resumen:</td><td>A través de esta información, se registrarán los problemas que posee el dispositivo móvil.</td></tr>
<tr><td colspan="2">Responsable:</td><td>Alejandro Alejandro Erick Jesús.</td></tr>
</table>

Anexo 2. Encuesta dirigida la comunidad universitaria de la carrera de Tecnología de la información.

Universidad Estatal Península de Santa Elena **Facultad de Sistemas y Telecomunicaciones** **Carrera de Tecnología de la Información.**	
Encuesta dirigida a los estudiantes de la carrera de Tecnologia de la información.	
Objetivos: Analizar El uso del dispositivo móvil y sus diferentes aplicaciones.	
1.	**¿Qué aplicaciones utiliza habitualmente?** **Linkedin__ Facebook__WhatsApp___Twitter___Instagram___** **Banca virtual__Galería____Gestor de archivos___** **Otros (Especifique cual) _____**
2.	**¿Qué tiempo usa su celular durante el día?** **Menos de 2 horas_ De 2 a 4 horas____ De 4 a 6 horas____** **Más de 6 horas__**
3.	**¿Ha presentado pérdida de información en alguna de las aplicaciones qué utiliza?** **Si___ No___**
4.	**¿Posee seguridad de bloqueo en el dispositivo? Seleccione cual** **Ninguna___ Patrón de bloqueo___ Pin o contraseña__** **Desbloqueo biométrico (huella dactilar, rostro, etc) ___**
5.	**En la actualidad, ¿Que uso le da a su dispositivo móvil?** **Ocio__ Comunicación__Instrumento de trabajo____Estudio__**

6.	**¿En qué momento lo usa la mayor parte del tiempo?** **Por las mañanas__Medio día_____Por la tarde___En la noche___** **Todo el día__**
7.	**¿Qué tan seguro cree que es utilizar aplicaciones en el teléfono móvil??** **Poco seguro____ Seguro_____ Muy Seguro_____**
8.	**¿Aproximadamente cuánto veces ha tenido que reparar su dispositivo móvil?** **1 vez___De 2 a veces____Mas de 3 veces ___**

Resumen:	Analizar El uso del dispositivo móvil y sus diferentes aplicaciones en el ares de Tecnologías de la Información.
Responsable:	Alejandro Alejandro Erick Jesús.

Anexo 3. Observación realizada en el dispositivo móvil en cuestión

<table>
<tr><th colspan="2">Registro descriptivo de la información</th></tr>
<tr><td colspan="2">Fecha: 10 de mayo del 2023
Lugar: Santa Elena</td></tr>
<tr><td colspan="2"># Personas: 1
Proceso: Estado físico del dispositivo
Duración: 2 horas</td></tr>
<tr><th colspan="2">Hechos observados</th></tr>
<tr><td colspan="2">• Dispositivo móvil de marca Samsung Galaxy A03s, a primera vista se ve en perfecto estado.
• Dispositivo móvil posee dos seguridades, una por huella dactilar en la pantalla Oled y otra por clave de patrón.
• Estado de depuración y modo desarrollador se encuentran en modo inactivo.
• Memoria de almacenamiento del dispositivo móvil unificada, para realizar almacenamiento virtual como si fuera uno.
• Puerto de datos del dispositivo móvil en perfecto estado, de categoría tipo C con depuración de almacenamiento USB 3.0.</td></tr>
<tr><td>Resumen:</td><td>Se determinaron las características del dispositivo y las opciones previas del mismo.</td></tr>
<tr><td>Responsable:</td><td>Alejandro Alejandro Erick Jesús.</td></tr>
</table>

Anexo 4. Software para el análisis forense a Android

CELLEBRITE PHYSICAL ANALYZER

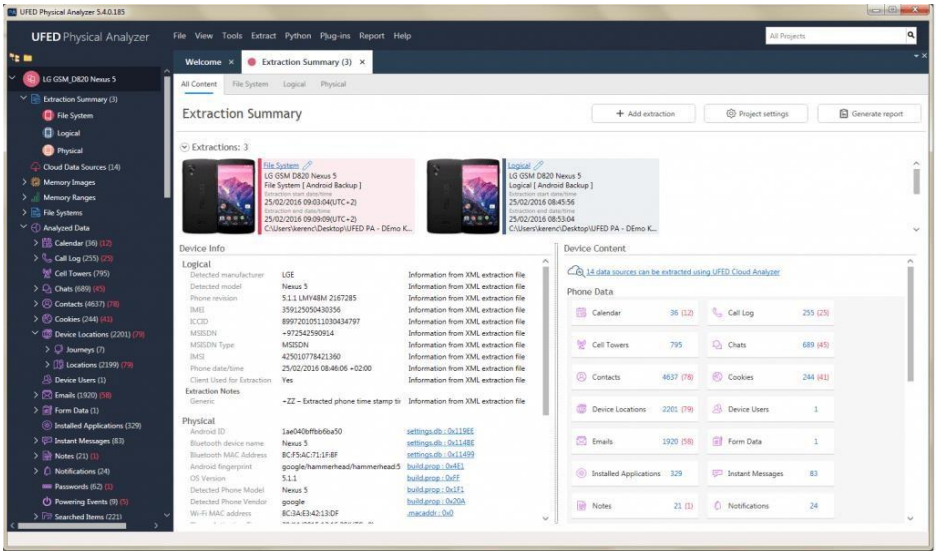


Figura 27. Cellebrite Physical Analyzer

Muchos organismos encargados de hacer cumplir la ley, utilizan esta herramienta para detectar la vigilancia móvil de cualquier teléfono inteligente; siendo capaz de verificar diferentes tipos de teléfonos, lo cual permite profundizar en teléfonos encriptados y no encriptados [10].

UFED 4PC

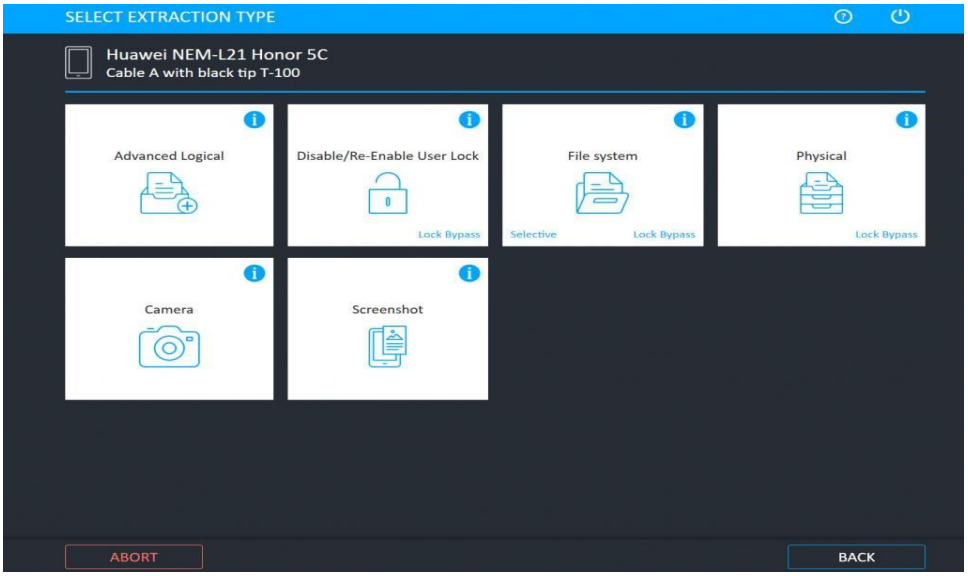


Figura 28. UFED 4PC

Los organismos encargados de hacer cumplir la ley también utilizan dispositivos universales de extracción forense (UFED) para piratear celulares, siendo una solución basada en software para PC o portátiles existentes [11].

DB BROWSER FOR SQLITE

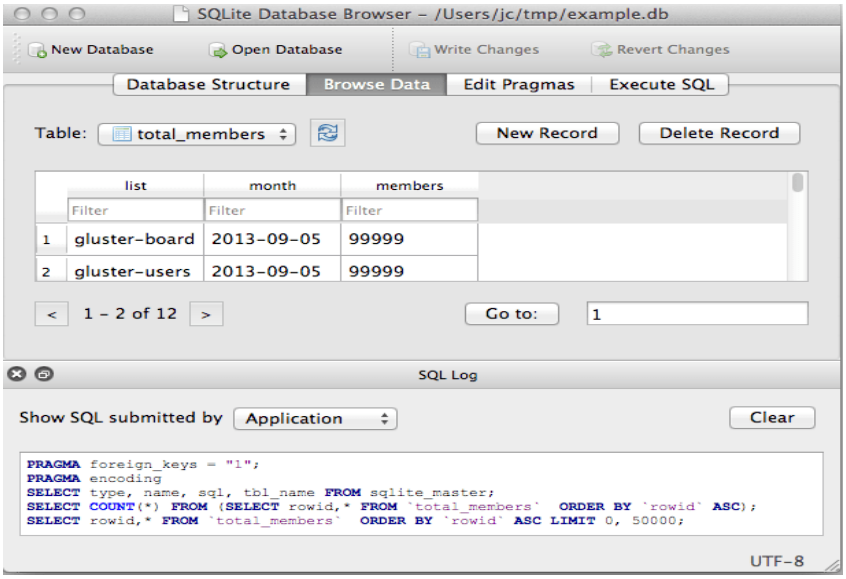


Figura 29. DB Browser for SQLITE

SQLite es un software de código abierto para el almacenamiento y recuperación de datos en aplicaciones móviles. Esta es una base de datos ligera para todas las aplicaciones móviles; permitiendo la recuperación de datos relacionados con varias aplicaciones [12].

OXYGEN FORENSICS DETECTIVE

Figura 30. Oxygen Forensics Detective

Es una herramienta forense todo en uno para extraer, descifrar y analizar datos de muchos dispositivos diferentes, como IoT, teléfonos móviles, drones, tarjetas multimedia, etc [13].

MAGNET AXIOM

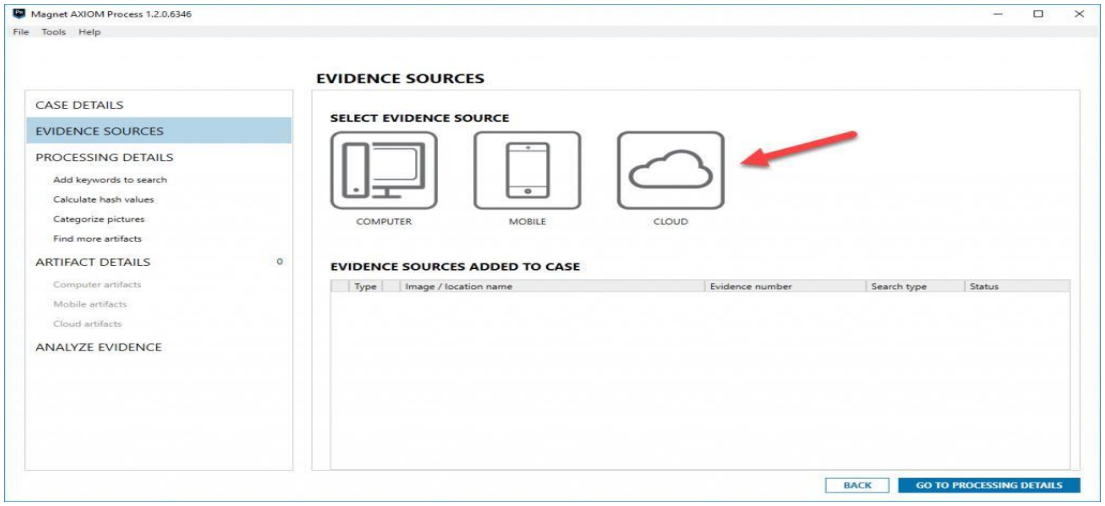


Figura 31. Magnet Axiom

Esta es una herramienta utilizada por investigadores forenses para indagar sobre malware, ransomware, phishing, casos de APT y más; Múltiples empresas emplean Magnet Axiom para adquirir y analizar pruebas de forma remota, mediante una plataforma en la nube para el análisis forense a través de software personalizado [14].

ANDRILLER

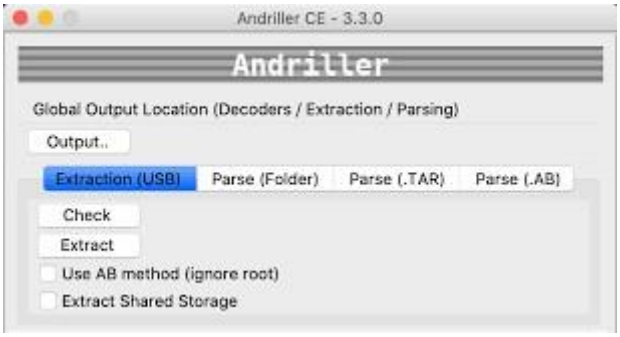


Figura 32. Andriller

Este es un paquete de software que contiene una colección de herramientas para la investigación de teléfonos inteligentes. Sus características son las siguientes [15]:

- Crack para pantalla rota
- Código PIN o contraseña
- Un decodificador personalizado para datos de aplicaciones de Android
- Extractor y decodificador

La herramienta genera informes en formatos HTML y Excel.

FRHED

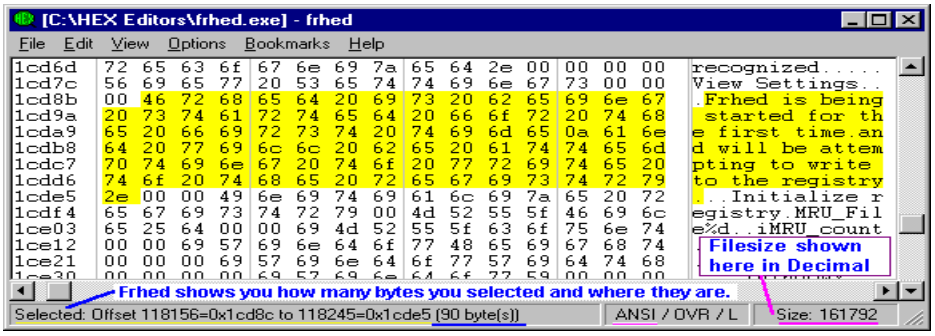


Figura 33. Fhred

Es un editor hexadecimal gratuito para leer archivos binarios; sus características son las siguientes [16]:

- Puede cargar archivos parcialmente
- Exportar el volcado hexadecimal a un archivo o portapapeles
- Los volcados se pueden buscar por texto y valores binarios
- Se puede utilizar para comparar archivos

JADX

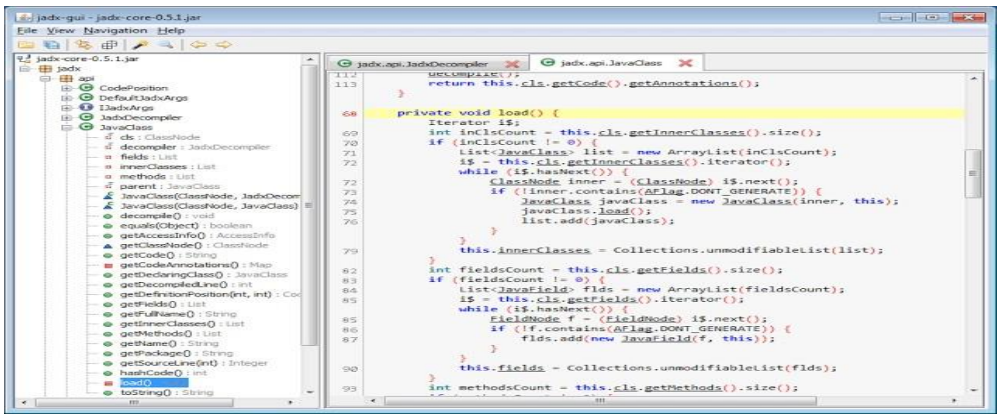


Figura 34. JADX

JADX es una herramienta de línea de comandos con una interfaz gráfica de usuario que se puede utilizar para generar código fuente de Java a partir de archivos APK y Android Dex [17].

ELECTRONIC EVIDENCE EXAMINER (E3)

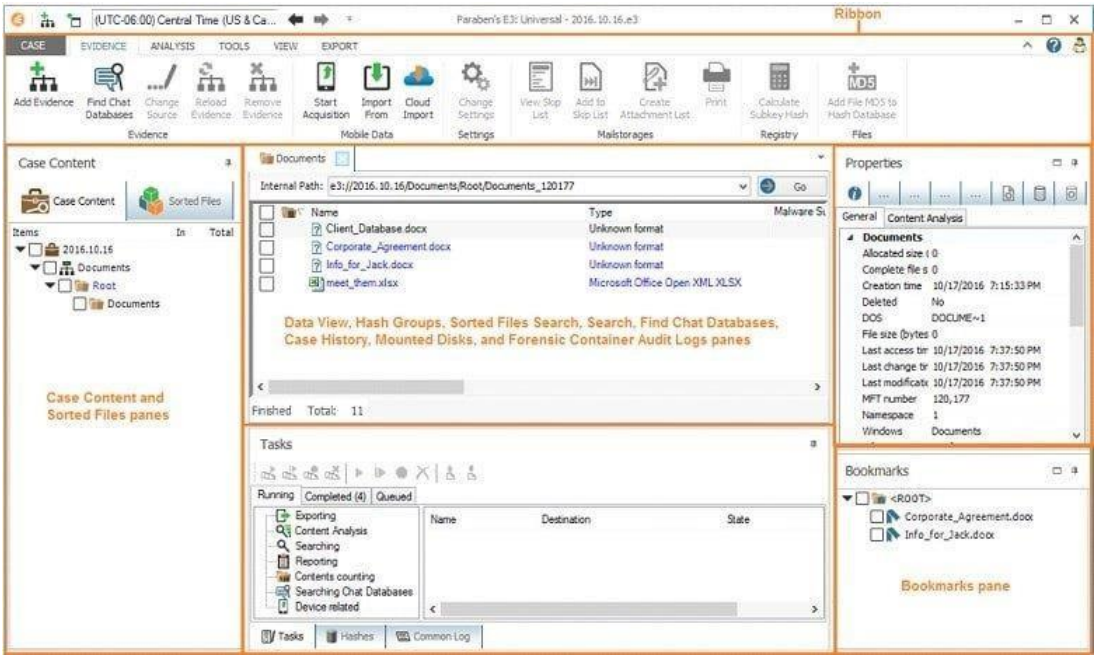


Figura 35. Electronic Evidence Examiner

Todo en una herramienta forense digital para análisis forense de medios digitales; sus características incluyen [18]:

Investigación informática

- Análisis forense de teléfonos inteligentes
- Análisis forense en la nube
- encuesta por correo electrónico
- Artefactos de Windows
- Reporte de revisión

Anexo 5. Instalación de Virtual Box

Lo primero que debes hacer es descargar e instalar VirtualBox. Para hacer esto, visite VirtualBox.org y haga clic en el botón Descargar en la pantalla de inicio, que lo llevará a la página donde encontrará el paquete que desea descargar.

Figura 36: Descargar virtual box

Una vez que llegue a la página de descarga, encontrará muchas cosas, como archivos binarios para usuarios avanzados. Para descargar simplemente el instalador, haga clic en el nombre del sistema operativo que muestra los paquetes de la plataforma, es decir, los paquetes del instalador. Por defecto, el contenido correspondiente a la última versión siempre aparecerá en la parte superior.

Figura 37: Página de descarga

Una vez que haya descargado el instalador, ejecútelo para acceder al proceso de instalación de VirtualBox. Es un proceso muy sencillo y puedes dejar todo como está, pero también puedes elegir dónde descargar o crear accesos directos.

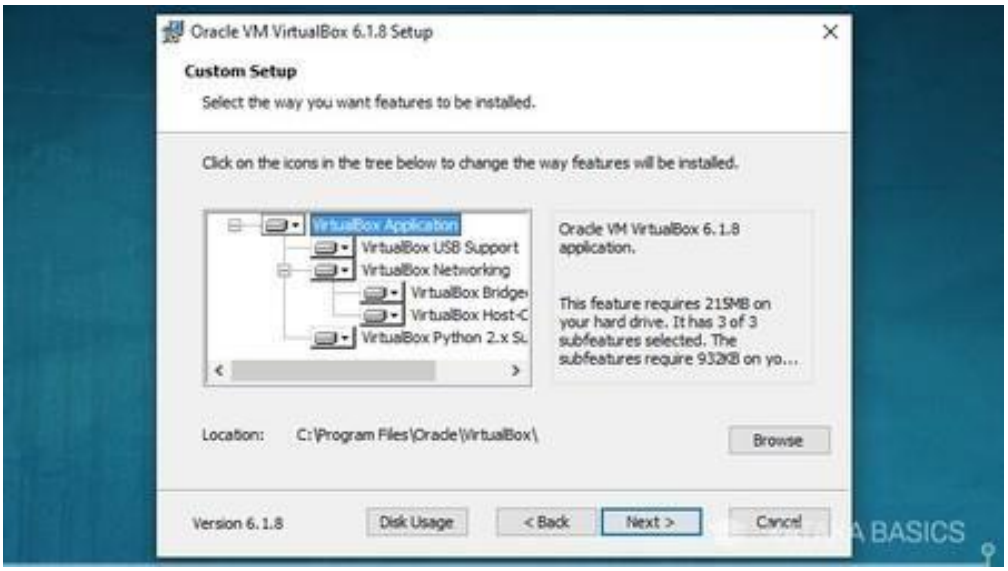


Figura 38: Instalación de virtual box

Anexo 6. Instalación de Santoku

Para la práctica se necesitará la implementación de sistemas operativos, los cuales brindan herramientas adecuadas para la realización de la extracción de información en modo Forense de esta simulación, teniendo la aplicación de una máquina virtual (Virtual box) especializada en crear escritorios basados en ambientes computacionales Window, Linux y solaris.

Figura 39. Virtual Box

Como primera instancia se crea el apartado del sistema; en el botón añadir se desplegará un cuadro de diálogo que pedirá el nombre y el tipo de sistema operativo que se va a utilizar. En este caso, será un sistema operativo basado en Unix que es la distribución de Linux.

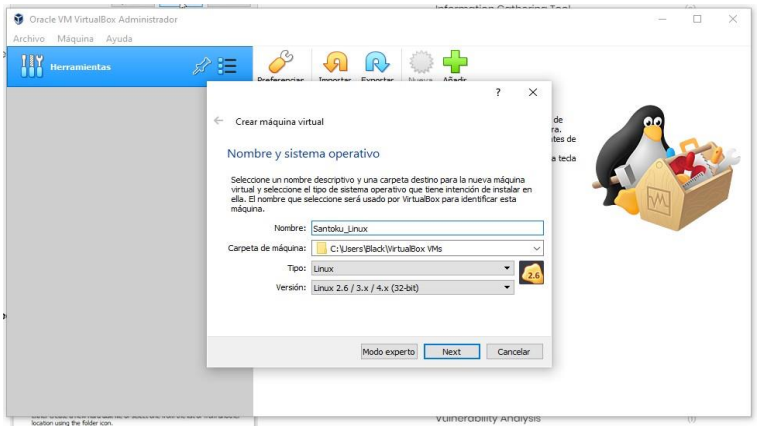


Figura 40. Apartado del sistema

Luego de hacer el llenado correspondiente al sistema operativo, se comienzan a desplegar opciones que simularán ser un equipo computacional físico en un entorno virtualizado, las cuales se describirán a continuación:

Cantidad de memoria RAM

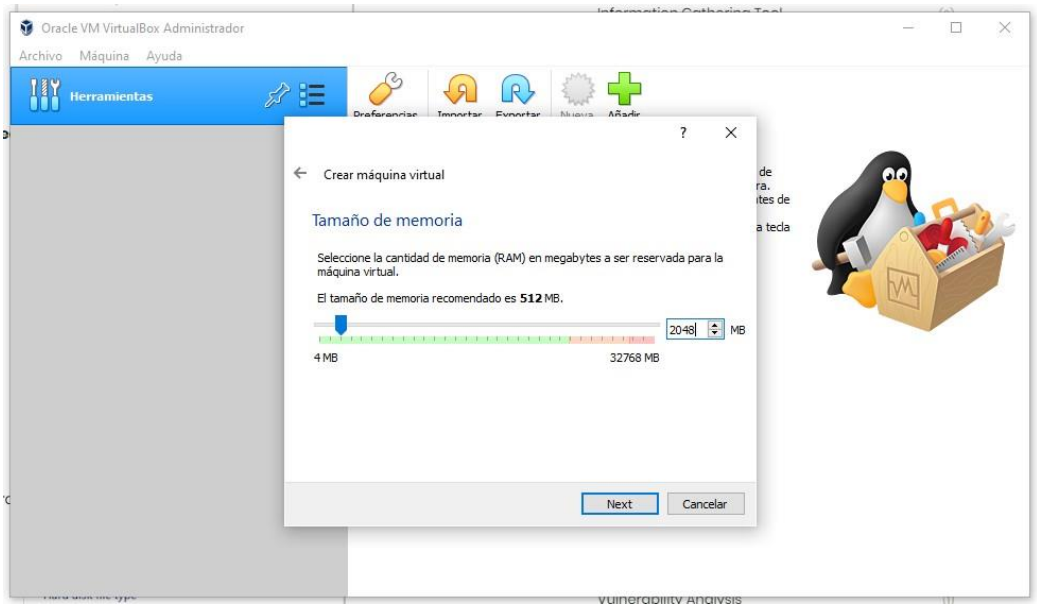


Figura 41. Cantidad de memoria RAM

Modo y capacidad de disco duro

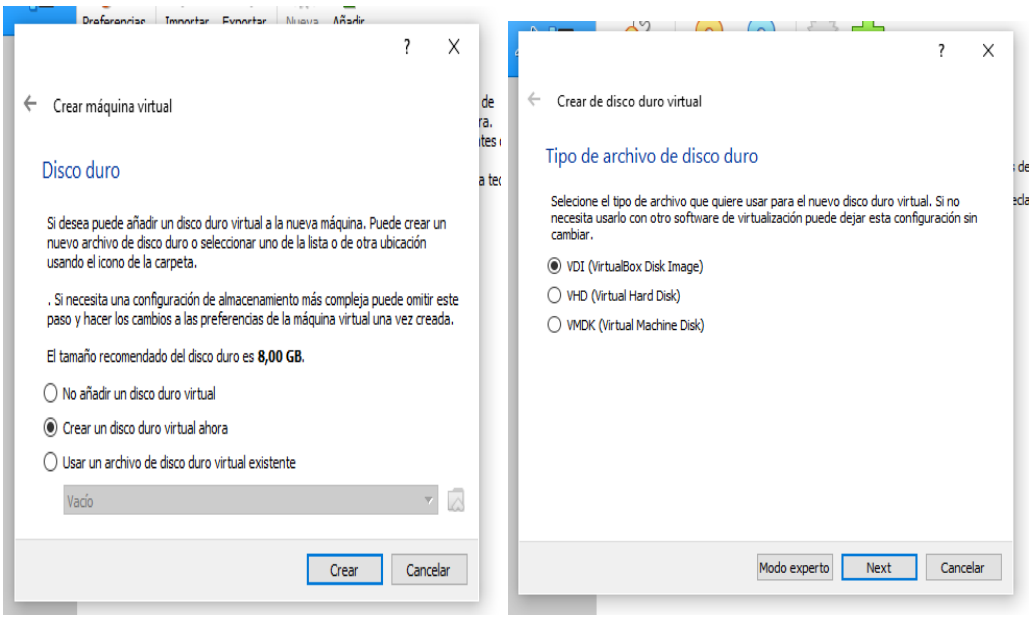


Figura 42. Modo y capacidad del disco duro

Es importante saber que si se crea un disco en modo Reservado automáticamente el tamaño del disco duro se tomará gradualmente según lo requiera el virtualizado hasta llegar al tope fijado, dejando que el computador base tenga uso del mismo, caso contrario, si no lo llega a utilizar, en Tamaño fijo contendrá todo sin permitir su uso por terceros.

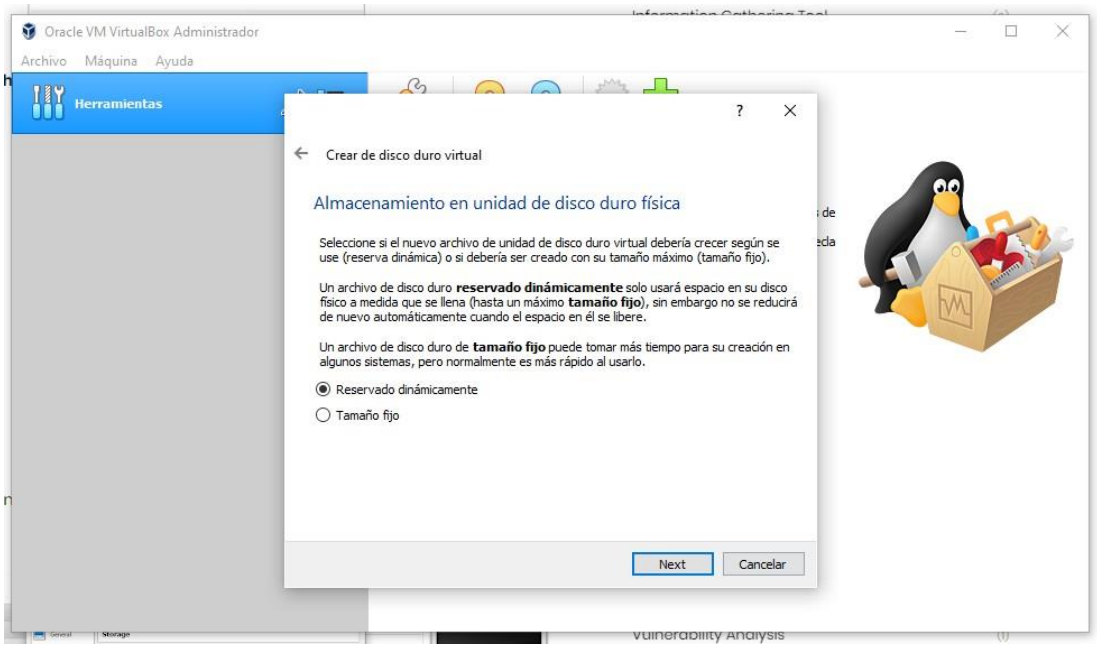


Figura 43. Crear disco duro virtual

Se selecciona la capacidad del disco duro que se brindará para este sistema operativo, fijándolo en 40 Gb.

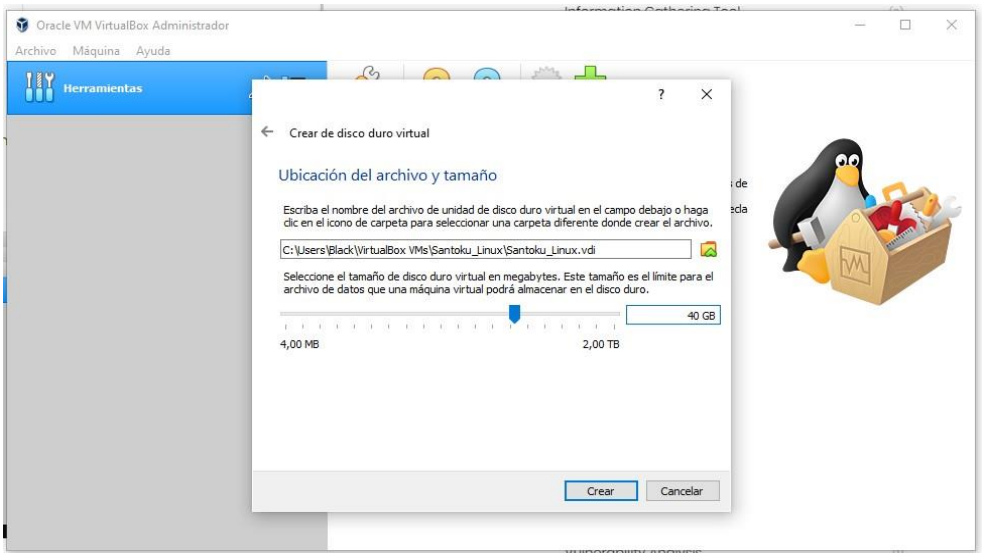


Figura 44. Capacidad del disco duro

Generados todos los pasos anteriores, ya se observará que en la pantalla principal existe un reservado para el sistema operativo, en este caso Santoku.

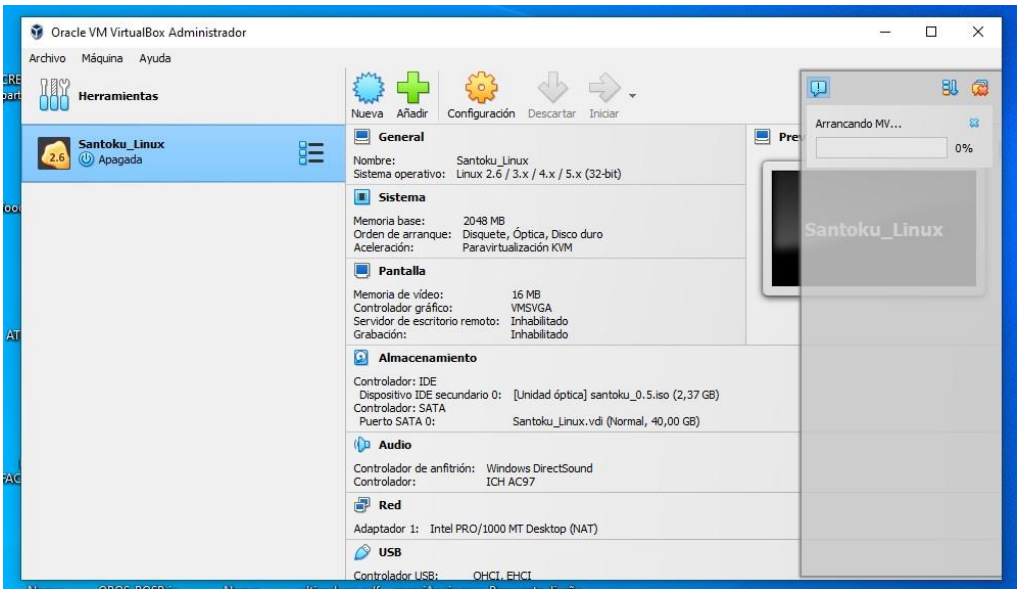


Figura 45. Reservado para el sistema operativo

Terminado este proceso, se comenzará la instalación del sistema operativo en este espacio virtual creado, tomando en cuenta que la computadora entre las opciones de la BIOS, debe mantener las virtualizaciones en modo enabled. Una vez arrancando el sistema pidela localización de la ISO que se utilizará.

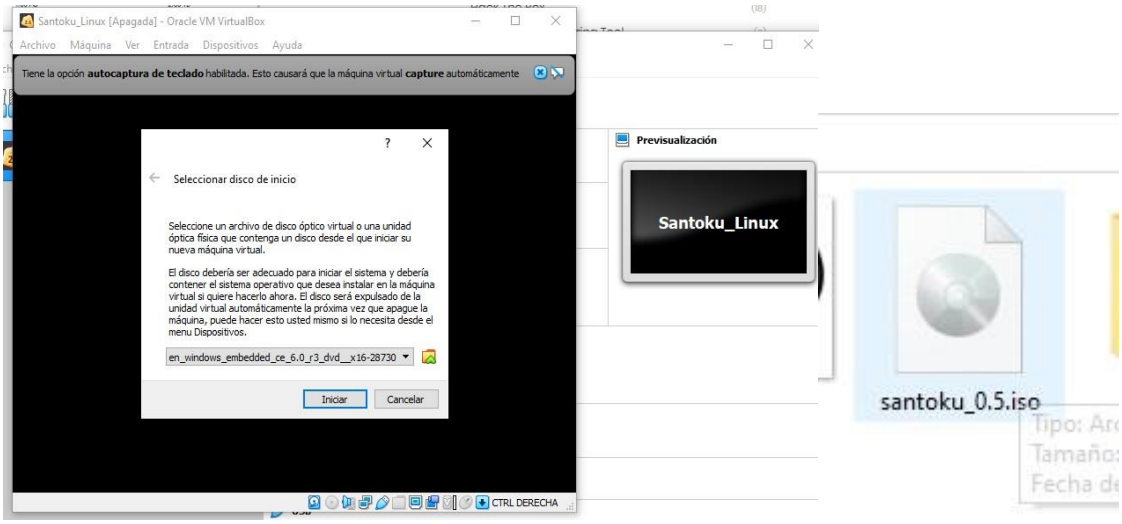


Figura 46. Instalación del sistema operativo

Comenzará el proceso de instalación en donde dará la opción de poderlo arrancar en dos modos:

- **Live:** Que abre el sistema operativo en modo demostrativo, pero con las herramientas de forma muy limitada de uso.
- **Installer:** Que instala todas las herramientas y complementos para su utilización completa.

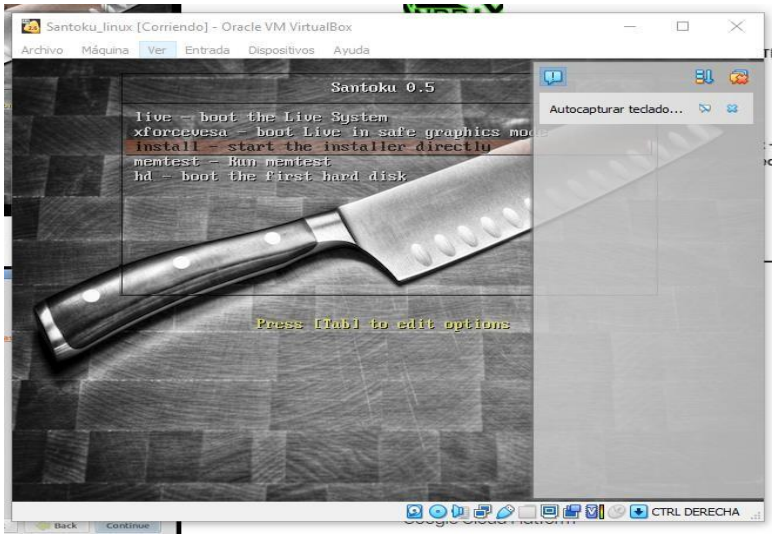


Figura 47. Arranque del sistema

Se procederá a hacer la instalación del sistema operativo; las opciones al ser intuitivas, hacen que la instalación resulte sumamente fácil.

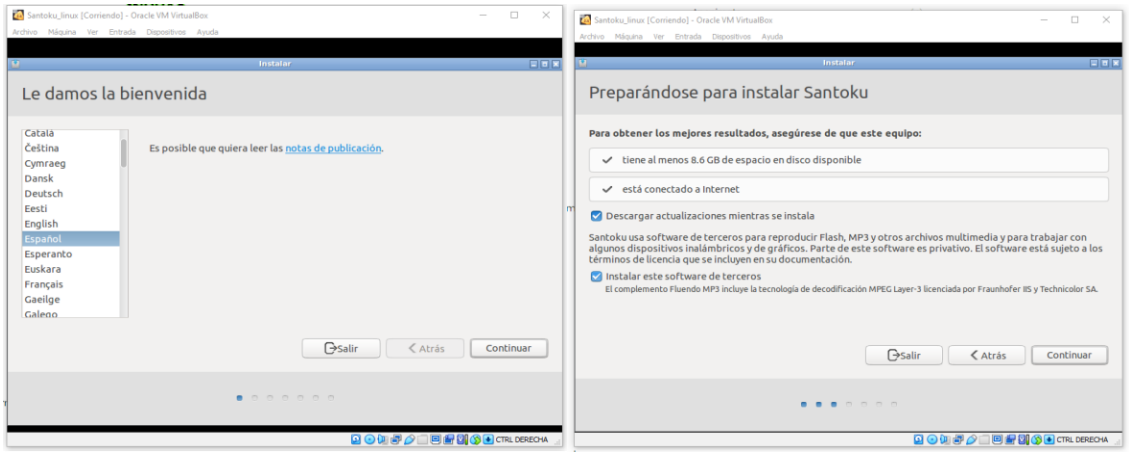


Figura 48. Inicio para instalar Santoku

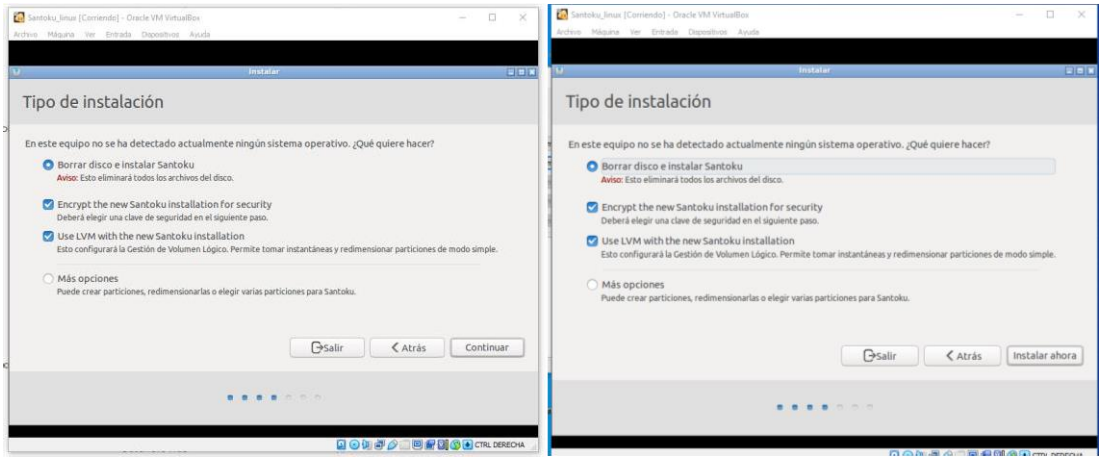


Figura 49. Tipo de instalación

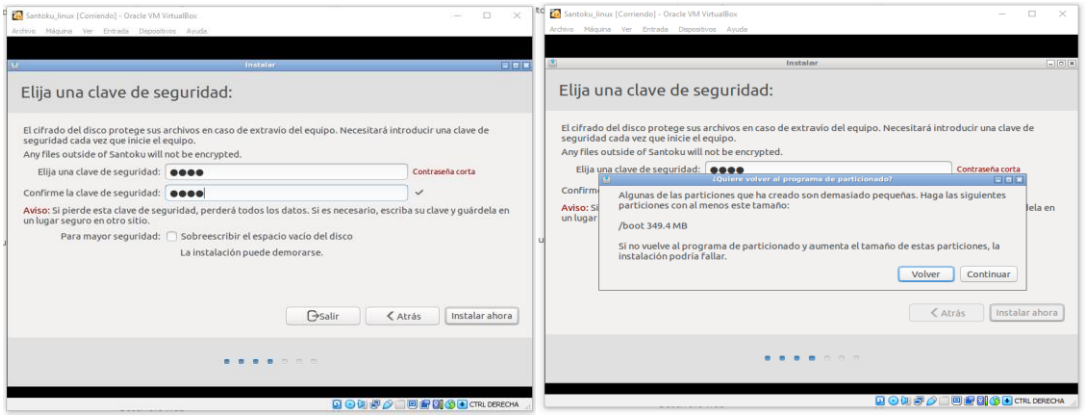


Figura 50. Clave de seguridad

En el apartado de la región, mantener la opción Guayaquil, aunque si aparece la opción de Santa Elena se crea un volcado de sistema y la instalación termina fallando.

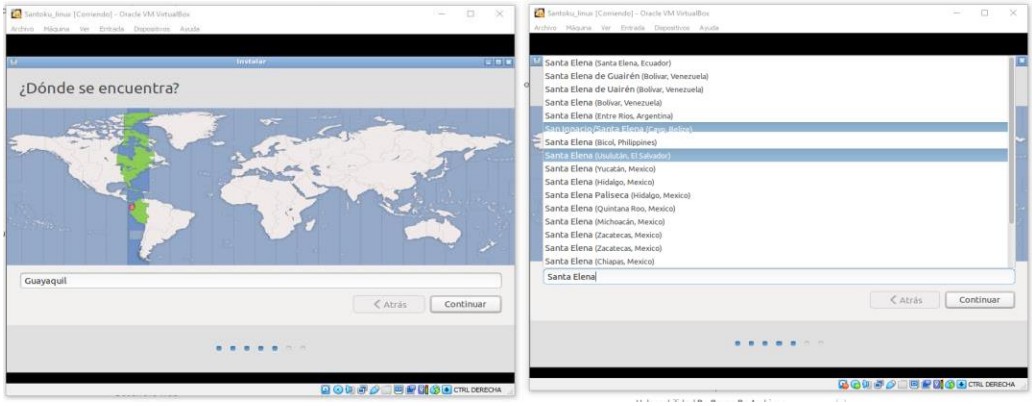


Figura 51. Región

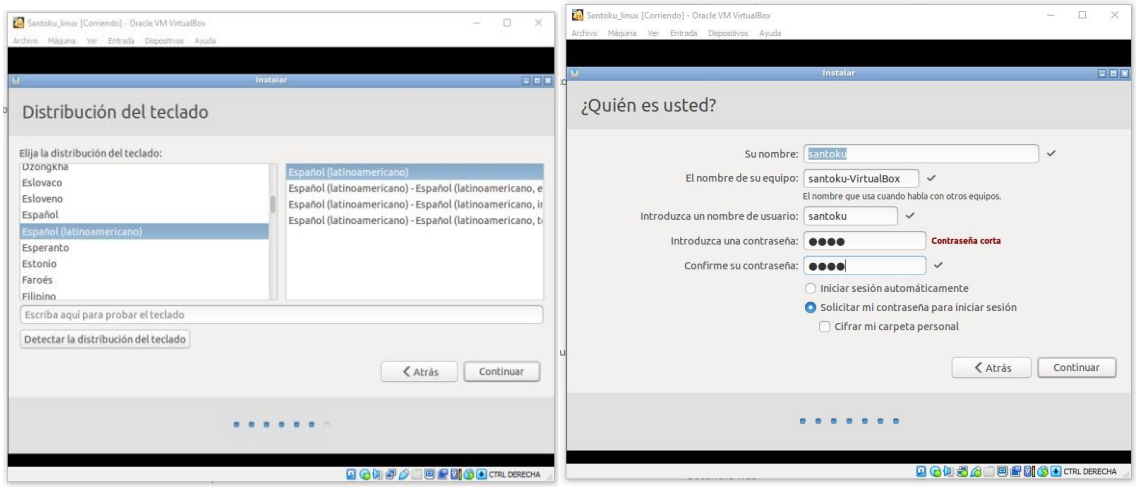


Figura 52. Distribución de teclado

Una vez terminados los pasos como se acaba de mostrar, se reinicia el sistema para arrancar de manera satisfactoria el S.O.

Figura 53. Reinicio del sistema

Una vez arrancando el sistema, se percata que el mismo, no aceptaba el dispositivo móvil y se procedió a permitir accesos a la máquina virtual sobre USB.

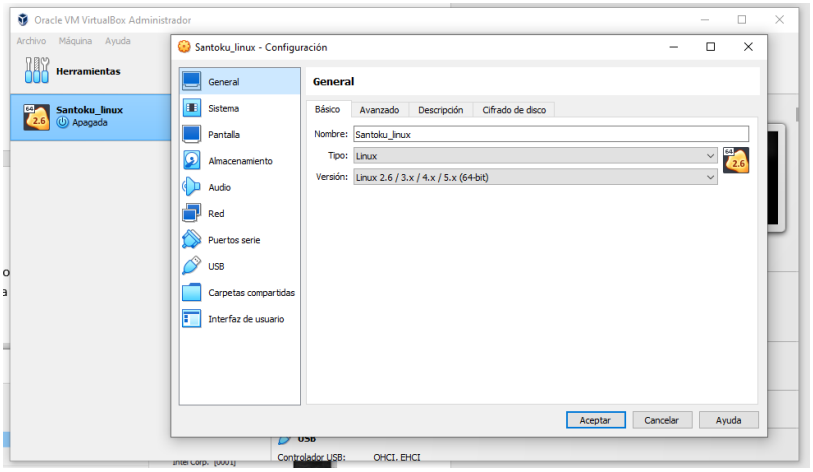


Figura 54. Acceso a la máquina virtual

Y de esta manera, reconocerá el dispositivo.

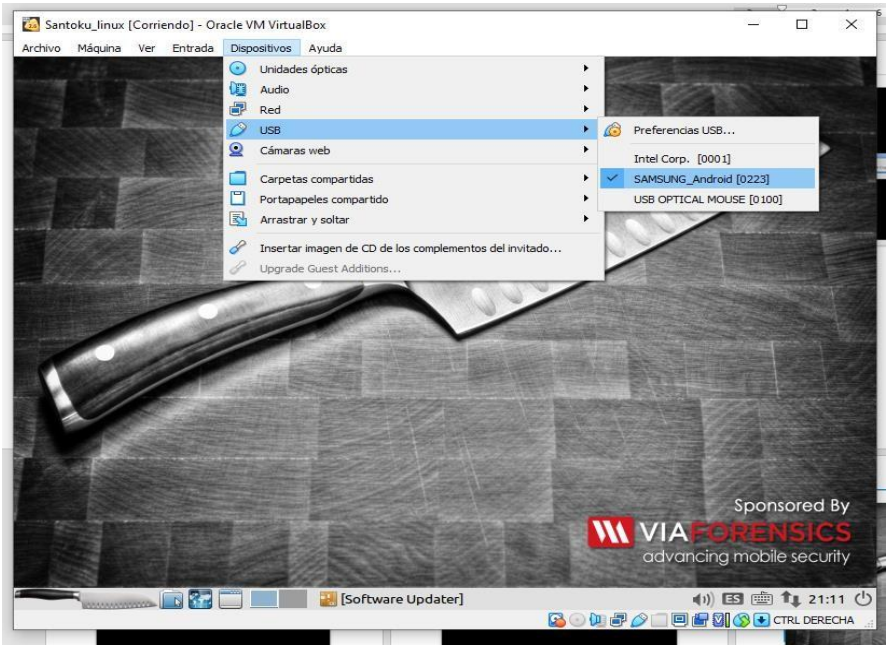


Figura 55. Reconocimiento del dispositivo

Anexo 7. Instalación de Exiftool

Entre la información que se puede obtener habitualmente de los dispositivos Android en la actualidad, están las imágenes, documentos y otros datos. Esto, es denominado como información relevante, pero al ser copiados directamente desde el dispositivo, no se puede contemplar un nivel avanzado de datos internos que ocultan dichos archivos, mismos que se denominan metadatos.

PASOS PARA EXTRAER INFORMACIÓN EN METADATOS

Este programa puede ser utilizado tanto para Windows como Linux; Para su instalación se necesita el CMD de Windows y en caso de Linux, se usa el terminal mediante una instalación previa en el navegador.

Figura 56. Búsqueda de la herramienta ExifTool

Al comenzar a revisar la página, se aprecia toda la información necesaria que contiene esta herramienta, se descarga la misma y se procede a la instalación siendo un archivo arrancable.

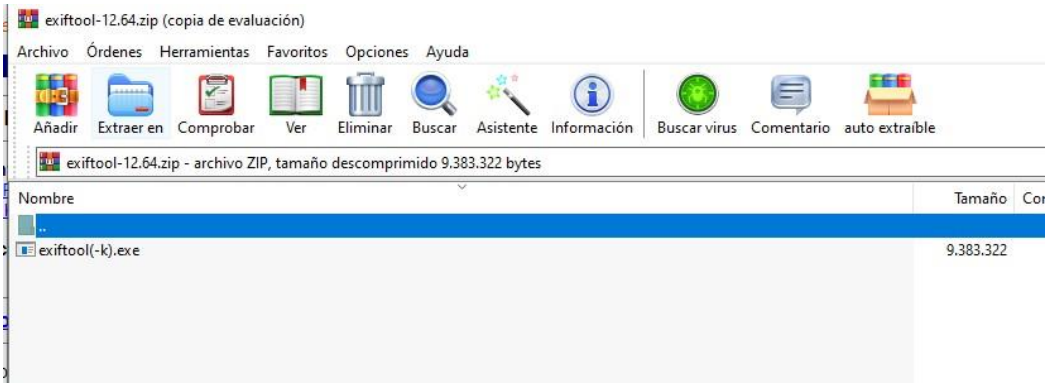


Figura 57. Información necesaria de la herramienta

A continuación, se detallan las características que posee la herramienta Exiftool [19]:

- Potente, rápido, flexible y personalizable
- Admite una gran cantidad de formatos de archivos diferentes
- Lee EXIF, GPS, IPTC, XMP, JFIF, MakerNotes, GeoTIFF, perfil ICC, Photoshop IRB, FlashPix, AFCP, ID3, Lyrics3, etc... Escribe EXIF, GPS, IPTC, XMP, JFIF, MakerNotes, GeoTIFF, perfiles ICC, Photoshop IRB, AFCP, etc.
- Leer y escribir la mayoría de las notas del fabricante sobre la cantidad de cámaras de código
- Determinación del tiempo de lectura meta -data -data (por ejemplo, GPS -monitoring) Mov/MP4/M2TS/AVI
- Muchas configuraciones de formato de salida (incluida la fórmula, HTML, XML y JSON)
- Salida multilingüe (CS, CS, IN, IN, En-CA, En-GB FI, FR, IT, sí, CO nl, PL, RU, SK, SV, TR, TR, TR, TR, TR, ZH-CN o zh -tw)
- Imagen de geoetiquet de archivo de monitoreo GPS (¡corrección de deriva en cualquier momento!)
- Generar registros de monitoreo a partir de imágenes geográficas
- Cambie el valor de fecha/hora para corregir la marca de tiempo de imagen
- Cambiar el nombre del archivo y organizarlos en la biblioteca (fecha u otra metainformación)
- Eliminar imágenes en miniatura, vistas previas y grandes imágenes JPEG
- Copia metainformación entre archivos (o incluso archivos en diferentes formatos)
- Lectura/escritura Información de XMP estructurada
- Formación individual, agrupación o metain
- Fecha de determinación de fecha (y fecha de la creación Mac y Windows)
- Información XMP, PNG, ID3, Fuente, QuickTime, ICC, MIE y MXF Archivos de configuración
- Trate todo el árbol del catálogo
- Cree un archivo de salida de texto para cada archivo de imagen
- Crear archivos para copias de metadatos -seguridad en solo dos formatos de producción (MIE, EXV)

- Copia automática de la imagen original al momento de escribir
- Grupo de exportación organizacional
- Archivo de procesamiento de acuerdo con el valor de la metainformación
- Agregue la opción de agregar marca personalizada de marca personalizada
- Compatible con MWG (grupo de trabajo de metadatos)
- Puede leer etiquetas a la vez en múltiples archivos que le permiten comparar metadatos entre archivos combinados
- MD5/SHA256/SHA512 (para datos de imagen de comparación y verificación) Solo los datos de los datos generan para muchos archivos generados
- Identificar decenas de miles de etiquetas diferentes
- Consulte con miles de modelos de cámara diferentes
- Salida detallada de desechos hexadecimales de alto nivel y enchufe basado en HTML

TIPOS DE ARCHIVOS QUE UTILIZA

Tipo de archivo	Apoyo	Descripción	EXIF	IPTC	XMP	CPI 1	Otro
360	L/E	Vídeo GoPro 360 (basado en QuickTime)	L/E 3	L/E 3	L/E/C	-	R/W/C QuickTime , R GoPro
3FR	R	Hasselblad RAW (basado en TIFF)	R	R	R	R	-
3G2, 3GP2	L/E	Proyecto de asociación de tercera generación 2 a/v (basado en QuickTime)	L/E 3	L/E 3	L/E/C	-	L/E/C QuickTime
3GP, 3GPP	L/E	Proyecto de asociación de tercera generación a/v (basadoen QuickTime)	L/E 3	L/E 3	L/E/C	-	L/E/C QuickTime
7z	R	Archivo 7z	-	-	-	-	C.P.R. _
A	R	Archivo de código de biblioteca estática de Unix	-	-	-	-	R EXE

Automóvil club británico	R	Audiolibro audible	-	-	-	-	R Audible
AAE	R	Información de edición de Apple (basada en XML PLIST)	-	-	-	-	R PLISTA
AAX	L/E	Audiolibro Audible mejorado (basado en QuickTime)	L/E 3	L/E 3	L/E/C	-	L/E/C QuickTime
ACR	R	Colegio Americano de Radiología ACR-NEMA (similar a DICOM)	-	-	-	-	R DICOM
AFM, ACFM, AMFM	R	Métricas de fuentes de Adobe [compuestas/múltiples maestras]	-	-	-	-	Fuente R
IA, IA	L/E	Adobe Illustrator [Plantilla] (PS o PDF)	L/E/C 4	L/E/C 4	L/E/C 5	L/E/C 4	R/W/C PDF PostScript , R Photoshop
AIFF, AIF, AIFC	R	Formato de archivo de intercambio de audio [comprimido]	-	-	-	-	R AIFF ID3 Letras3
MONO	R	audio de mono	-	-	-	-	R APE ID3 Letras3

ARQ	L/E	Sony Alpha Pixel-Shift RAW (basado en TIFF)	L/E/C	L/E/C	L/E/C	L/E/C	R/W Sony SonyIDC
ARW	L/E	Sony Alpha RAW (basado en TIFF)	L/E/C	L/E/C	L/E/C	L/E/C	R/W Sony SonyIDC
PPA	R	Formato de sistemas avanzados de Microsoft	-	-	R	-	PPA R
AVI	R	Audio Video intercalado (basado en RIFF)	R 3	-	R	-	R RIFF
AVIF	L/E	Formato de archivo de imagen AV1 (basado en QuickTime)	L/E/C	-	L/E/C	L/E	L/E QuickTime
BMP, DIB	R	Mapa de bits de Windows/mapa de bits independiente del dispositivo	-	-	-	-	R BMP
GBP	R	Mejores gráficos portátiles	R	-	R	R	R BPG
BTF	R	BigTIFF (formato de archivo de imagen etiquetada de 64 bits)	R	R	R	R	-

CHM	R	Formato HTML compilado de Microsoft	-	-	-	-	R EXE
porque	R	Configuración de Capture One (basada en XML)	-	-	-	-	R XML
CR2	L/E	Canon RAW 2 (basado en TIFF) (especificación CR2)	L/E/C	L/E/C	L/E/C	L/E/C	R/W Canon , R/W/C CanonVRD 2
CR3	L/E	Canon RAW 3 (basado en QuickTime) (especificación CR3)	L/E/C	-	L/E/C	-	R/W Canon QuickTime , R/W/C CanonVRD 2
CRM	L/E	Vídeo RAW de Canon (basado en QuickTime)	L/E/C	-	L/E/C	-	R/W Canon QuickTime
CRW, CIFF	L/E	Formato de archivo de imagen de cámara RAW de Canon(especificación CRW)	-	-	L/E/C	-	R/W CanonRaw , R/W/C CanonVRD 2
CS1	L/E	Sinar CaptureShop RAW de 1 disparo (basado en PSD)	L/E/C	L/E/C	L/E/C	L/E/C	Photoshop _

CSV	R	Valores Separados por Comas	-	-	-	-	R Texto
CZI	R	Software integrado Zeiss RAW (ZISRAW)	-	-	-	-	R ZISRAW , R XML
DCM, DC3, DIC, DICM	R	DICOM - Imagen Digital y Comunicaciones en Medicina	-	-	-	-	R DICOM
DCP	L/E	Perfil de cámara DNG (tipo DNG)	L/E/C	L/E/C	L/E/C	L/E/C	-
RDC	R	Cámara digital Kodak RAW (basado en TIFF)	R	R	R	R	-
DFONT	R	Fuente de bifurcación de datos de Macintosh	-	-	-	-	Fuente R
DIVX	R	Formato multimedia DivX (basado en ASF)	-	-	R	-	PPA R
DJVU, DJV	R	Imagen DjVu (similar a AIFF)	-	-	R	-	R DJVU
DNG	L/E	Negativo digital (basado en TIFF)	L/E/C	L/E/C	L/E/C	L/E/C	-

DOC, PUNTO	R	Documento/plantilla de Microsoft Word (similar a FPX)	-	-	R	R	R FlashPix
DOCX, DOCM	R	Documento XML abierto de Office [habilitado para macros]	-	-	-	-	R XML ZIP
DOTX, DOTM	R	Plantilla de documento XML abierto de Office [habilitada para macros]	-	-	-	-	R XML ZIP
DPX	R	Intercambio de imágenes digitales	-	-	-	-	R DPX
DR4	L/E/C 2	Receta de la versión 4 de Canon DPP	-	-	-	-	R/W/C CanonVRD 2
DSS, DS2	R	Estándar de voz digital [2]	-	-	-	-	R Olimpo
DYLIB	R	Archivos ejecutables y de biblioteca de MacOS Mach-O	-	-	-	-	R EXE
VD	R	Video digital	-	-	-	-	R VD
TDT	L/E	Difusión de video digital (basado en QuickTime)	L/E 3	L/E 3	L/E/C	-	L/E/C QuickTime

DVR-MS	R	Grabación de video digital de Microsoft (basada en ASF)	-	-	R	-	PPA R
EIP	R	Paquete de imágenes mejoradas Capture One (basado en ZIP)	R	-	-	-	R XML ZIP
EPS, EPSF, PS	L/E	[Encapsulado] Formato PostScript	L/E/C	L/E/C	L/E/C	L/E/C	R/W/C PostScript , R Photoshop
EPUB	R	Publicación electrónica (basada en ZIP/XML)	-	-	-	-	R XML ZIP
ERF	L/E	Formato Epson RAW (basado en TIFF)	L/E/C	L/E/C	L/E/C	L/E/C	R/W Olimpo
EXE, DLL	R	Archivos ejecutables y de biblioteca de DOS/Windows	-	-	-	-	R EXE
EXIF	L/E/C	Metadatos de formato de archivo de imagen intercambiable (basado en TIFF)	L/E/C	-	-	-	-
EXR	R	EXR abierto (rango extendido)	-	-	-	-	R AbrirEXR

EXV	L/E/C	Archivo de metadatos Exiv2 (basado en JPEG)	L/E/C	L/E/C	L/E/C	L/E/C	Metainformación JPEG admitida
F4A, F4B, F4P, F4V	L/E	Adobe Flash Player 9+ Audio/Video (basado en QuickTime)	L/E 3	L/E 3	L/E/C	-	L/E/C QuickTime
FFF	L/E 6	Formato de archivo flexible de Hasselblad (basado en TIFF)	L/E/C	L/E/C	L/E/C	L/E/C	-
FFF	R	Formato de archivo de imagen térmica de FLIR Systems	-	-	-	-	R FLIR
ENCAJA	R	Sistema de transporte de imágenes flexible	-	-	-	-	AJUSTES R
FLA	R	Proyecto Macromedia/Adobe Flash (similar a FPX)	-	-	R	R	R FlashPix
FLAC	R	Códec de audio sin pérdida gratuito	-	-	-	-	R FLAC ID3 Letras3
FLIF	L/E	Formato de imagen sin pérdida gratuito	L/E/C	-	L/E/C	L/E/C	R FLIF

FLV	R	Vídeo Flash	-	-	R	-	Destello R
FPF	R	FLIR Formato de imagen pública	-	-	-	-	R FLIR
FPX	R	Imagen FlashPix	-	-	R	R	R FlashPix
GIF	L/E	Formato de intercambio de gráficos Compuserve	-	-	L/E/C	L/E/C	R/W/C GIF
GLV	L/E	Vídeo de baja resolución de Garmin (basado en QuickTime)	L/E 3	L/E 3	L/E/C	-	L/E/C QuickTime
GPR	L/E	GoPro RAW (basado en DNG)	L/E/C	L/E/C	L/E/C	L/E/C	-
GZ, GZIP	R	Archivo comprimido GNU ZIP	-	-	-	-	C.P.R. _
HDP... WDP... JXR	L/E	Windows HD Photo/Media Photo/JPEG XR (basado en TIFF)	L/E/C	L/E/C	L/E/C	L/E/C	-
HDR	R	Radiance RGBE alto rango dinámico	-	-	-	-	Resplandor R

HEIC, HEIF, HIF	L/E	Formato de imagen de alta eficiencia (basado en QuickTime)	L/E/C	-	L/E/C	L/E	L/E QuickTime
HTML, HTM, XHTML	R	[Extensible] Lenguaje de marcado de hipertexto	-	-	-	-	R HTML
CPI, MCI	L/E/C 1	Perfil de color del Consorcio Internacional del Color	-	-	-	L/E/C	-
OIC, CUR	R	Icono de Windows / Cursor	-	-	-	-	RICO _
ICS, ICAL	R	Calendario iCalendar	-	-	-	-	R VCalendario
IDML	R	Lenguaje de marcado de Adobe InDesign (basado en ZIP/XML)	-	-	-	-	R XML ZIP
IIQ	L/E	Phase One Intelligent Image Quality RAW (basado en TIFF)	L/E/C	L/E/C	L/E/C	L/E/C	R/W PhaseOne
IND, INDD, INDT	L/E	Documento/plantilla de Adobe InDesign	-	-	L/E/C	-	-

EN SP	L/E	Imagen Insta360 (basada en JPEG)	L/E/C	L/E/C	L/E/C	L/E/C	Metainformación JPEG admitida
INV	R	Vídeo Insta360 (basado en QuickTime)	-	-	R	-	R QuickTime
INX	R	Intercambio de Adobe InDesign (basado en XML)	-	-	R	-	-
YO ASI	R	Imagen de disco ISO 9660	-	-	-	-	RISO _
TIC	R	Ilustraciones de iTunes Cover Flow	-	-	-	-	RTIC _
J2C, J2K, JPC	R	Flujo de código JPEG 2000	R 3	R 3	R	R	R JPEG2000 Photoshop 3
JP2, JPF, JPM, JPX	L/E	Imagen JPEG 2000 [Compuesto/Extendido]	L/E/C 3	L/E/C 3	L/E/C	R	R/W/C Jpeg2000 , R Photoshop 3
JPEG, JPG, JPE	L/E	Imagen del Grupo Conjunto de Expertos en Fotografía	L/E/C	L/E/C	L/E/C	L/E/C	Metainformación JPEG admitida
JSON	R	Notación de objetos de JavaScript	-	-	-	-	R JSON

JXL	L/E	JPEG XL (codestream e ISO BMFF) (basado en Jpeg200)	L/E/C	-	L/E/C	-	-
K25	R	Kodak DC25 RAW (basado en TIFF)	R	R	R	R	-
KDC	R	Cámara digital Kodak RAW (basado en TIFF)	R	R	R	R	R Kodak
CLAVE, KTH	R	Presentación/tema principal de Apple iWork '09	-	-	-	-	R XML ZIP
LA	R	Audio sin pérdidas (basado en RIFF)	R 3	-	R	-	R RIFF
LFP, LFR	R	Imagen del campo de luz Lytro	-	-	-	-	R Lytro
VIDA	R	Archivo de imagen Leica	-	-	-	-	R VIDA
LNK	R	Microsoft Shell Link (acceso directo de Windows)	-	-	-	-	R LNK
LRV	L/E	Video de baja resolución (basado en QuickTime)	L/E 3	L/E 3	L/E/C	-	L/E/C QuickTime

M2TS, MTS, M2T, TS	R	Flujo de transporte MPEG-2 (utilizado para video AVCHD)	-	-	-	-	R M2TS H264 MISB
M4A, M4B, M4P, M4V	L/E	MPEG-4 Audio/Video (basado en QuickTime)	L/E 3	L/E 3	L/E/C	-	L/E/C QuickTime
MAC OS	R	Archivo sidecar "._" de MacOS (puede tener cualquier extensión)	-	-	-	-	R XAttr RSRC
MÁX.	R	3D Studio MAX (similar a FPX)	-	-	R	R	R FlashPix
MEF	L/E	Formato electrónico Mamiya (RAW) (basado en TIFF)	L/E/C	L/E/C	L/E/C	L/E/C	-
MIE	L/E/C	Encapsulación de metainformación (especificación MIE)	L/E/C	L/E/C	L/E/C	L/E/C	L/E/C MIE
FOMIN, FOMIN	R	Formato de archivo de imagen mágica	R	R	R	R	R MIFF Photoshop
MKA, MKV, MKS	R	Matroska Audio/Video/Subtítulos	-	-	-	-	R Matroska

MOBI, AZW, AZW3	R	Libro electrónico Mobipocket (basado en Palm)	-	-	-	-	R Palma MOBI
MODD	R	Metadatos de Sony Picture Motion (basado en XML PLIST)	-	-	-	-	R PLISTA
MOI	R	Archivo de información MOD	-	-	-	-	R MOI
MOS	L/E	Creo Leaf Mosaic (basado en TIFF)	L/E/C	L/E/C	L/E/C	L/E/C	Hoja R
MOV, QT	L/E	Película QuickTime de Apple	L/E 3	L/E 3	L/E/C	-	L/E/C QuickTime
MP3	R	audio MPEG-1 capa 3	-	-	-	-	R MPEG ID3 Letras3 APE
MP4	L/E	Motion Picture Experts Group versión 4 (basado en QuickTime)	L/E 3	L/E 3	L/E/C	-	L/E/C QuickTime
MPC	R	audio musepack	-	-	-	-	R MPC ID3 Letras3 APE
MPEG, MPG, M2V	R	Motion Picture Experts Group versión 1 o 2	-	-	-	-	R MPEG ID3 Letras3

MPO	L/E	Formato de imagen múltiple extendido (JPEG con extensiones MPF)	L/E/C	L/E/C	L/E/C	L/E/C	Metainformación JPEG admitida
MQV	L/E	Vídeo QuickTime de Sony Mobile	L/E 3	L/E 3	L/E/C	-	L/E/C QuickTime
MRW	L/E	Minolta CRUDO	L/E/C	L/E/C	L/E/C	L/E/C	R/W MinoltaRaw Minolta
MRC	R	Consejo de Investigación Médica	-	-	-	-	R MRC
MXF	R	Formato de intercambio de materiales	-	-	-	-	R MXF
NEF	L/E	Formato electrónico Nikon (RAW) (basado en TIFF)	L/E/C	L/E/C	L/E/C	L/E/C	R/W Nikon Nikon Capture
NKSC	L/E	Nikon Sidecar (basado en XMP)	-	-	L/E/C	-	-
PLANTILLA NMB	R	Plantilla de números de Apple iWork '09	-	-	-	-	R XML ZIP
NRW	L/E	Nikon RAW (2) (basado en TIFF)	L/E/C	L/E/C	L/E/C	L/E/C	R/W Nikon Nikon Capture

NÚMEROS	R	Hoja de cálculo de números de Apple iWork '09	-	-	-	-	R XML ZIP
O	R	Código compilado de Unix Objeto	-	-	-	-	R EXE
ODB, ODC, ODF, ODG, ODI, ODP, SAO, ODT	R	Base de datos de documentos abiertos/Gráfico/Fórmula/Gráficos/ Imagen/Presentación/Hoja de cálculo/Texto (basado en ZIP/XML)	-	-	-	-	R XML ZIP
OFR	R	Audio OptimFROG (basado en RIFF)	R 3	-	R	-	R RIFF
OGG, OGV	R	Contenedor de flujo de bits Ogg	-	-	-	-	R FLAC ID3 Lyrics3 Theora Vorbis
EN P	R	Preajustes ON1	-	-	-	-	R JSON PLISTA
OPUS	R	Audio Ogg Opus	-	-	-	-	R FLAC ID3 Letras3 Opus Vorbis
ORF, ORI	L/E	Formato RAW de Olympus (basado en TIFF)	L/E/C	L/E/C	L/E/C	L/E/C	R/W Olimpo
OTF	R	Fuente de tipo abierto	-	-	-	-	Fuente R

PAC	R	Compresión de audio predictiva sin pérdidas (basada en RIFF)	R 3	-	R	-	R RIFF
PÁGINAS	R	Documento de páginas de Apple iWork '09	-	-	-	-	R XML ZIP
DCP	R	Kodak Photo CD Imagen Pac	-	-	-	-	CD de fotos R
PCX	R	Pincel para PC	-	-	-	-	RPCX _
AP, República Popular China	R	Base de datos de palma	-	-	-	-	palma de la mano
PDF	L/E 7	Formato de documento portátil de Adobe	R 3	R 3	L/E/C	R 3	R/W/C PDF , R Photoshop
FEM	L/E	Formato electrónico Pentax (RAW) (basado en TIFF)	L/E/C	L/E/C	L/E/C	L/E/C	R/W Pentax
PFA, PFB	R	Fuente PostScript ASCII/Binario	-	-	-	-	Fuente R
GFP	R	Métricas de fuente de impresora	-	-	-	-	Fuente R

GFP	R	Mapa flotante portátil	-	-	-	-	R PFM
PGF	R	Archivo de gráficos progresivos	-	-	-	-	R PGF PNG
PICT, PCT	R	Archivo de imagen de Apple	-	-	-	R	R PICT Photoshop
PLISTA	R	Lista de propiedades de Apple (formatos binario y XML)	-	-	-	-	R PLISTA
PMP	R	Imagen Cyber-Shot de la Sony DSC-F1	-	-	-	-	Sony _
PNG , JNG, MNG	L/E	Gráficos de red portátiles/JPEG/múltiples imágenes	L/E/C 3	L/E/C 3	L/E/C	L/E/C	L/E/C PNG
PPM, PBM, PGM	L/E	Mapa portátil de píxeles/bits/grises	-	-	-	-	R PPM, L/E/C Comentario
PPT, PPS, Olla	R	Presentación de PowerPoint/presentación de diapositivas/plantilla (similar a FPX)	-	-	R	R	R FlashPix

POTX, POTM	R	Plantilla de presentación de Office Open XML [habilitada para macros]	-	-	-	-	R XML ZIP
PPAX, PPAM	R	Complemento de presentación Open XML de Office [habilitado para macros]	-	-	-	-	R XML ZIP
PPSX, PPSM	R	Presentación de diapositivas de Office Open XML [habilitado para macros]	-	-	-	-	R XML ZIP
PPTX, PPTM	R	Presentación de Office Open XML [habilitado para macros]	-	-	-	-	R XML ZIP
PSD, PSB, PSDT	L/E	Documento de Photoshop / Documento grande / Plantilla	L/E/C	L/E/C	L/E/C	L/E/C	Photoshop _
PSP, PSP IMAGEN	R	Taller de pintura profesional	R	-	-	-	R PSP
QTIF, QTI, QIF	L/E	Archivo de imagen de QuickTime	L/E 3	L/E 3	L/E/C	-	L/E/C QuickTime
R3D	R	Vídeo RAW de código rojo	-	-	-	-	rojo _

REAL ACADEMIA DE BELLAS ARTES	R	Audio real	-	-	-	-	R Real ID3 Letras3
Royal Air Force	L/E	Formato FujiFilm RAW	L/E/C	L/E/C	L/E/C	L/E/C	R/W FujiFilm
RAM, RPM	R	Metarchivo de audio real/complemento	-	-	-	-	R reales
RAR	R	Archivo RAR	-	-	-	-	C.P.R. _
CRUDO	R	Kyocera Contax N Digital RAW	-	-	-	-	R KyoceraRaw
CRUDO	L/E	Panasonic RAW (basado en TIFF)	L/E/C	L/E/C	L/E/C	L/E/C	R/W PanasonicRaw Panasonic
RIF, RIF	R	Formato de archivo de intercambio de recursos	R 3	-	R	-	R RIFF
RM, RV, RMVB	R	Real Media/Video [tasa de bits variable]	-	-	-	-	R reales
RSRC	R	Recurso de Mac OS	-	-	-	-	Fuente R RSRC Photoshop PostScript

RTF	R	Formato de texto enriquecido	-	-	-	-	R RTF
RW2	L/E	Panasonic RAW 2 (basado en TIFF)	L/E/C	L/E/C	L/E/C	L/E/C	R/W PanasonicRaw Panasonic
RWL	L/E	Leica RAW (basado en TIFF)	L/E/C	L/E/C	L/E/C	L/E/C	R/W PanasonicRaw Panasonic
RWZ	R	Imagen comprimida Rawzor	R	R	R	R	R Rawzor
SEC	R	Secuencia de imágenes de FLIR Systems	-	-	-	-	R FLIR
BOSQUEJO	R	Archivo de diseño de croquis	-	-	-	-	R JSON C.P.
ENTONCES	R	Archivos de objetos compartidos y ejecutables ELF de Unix	-	-	-	-	R EXE
SR2	L/E	Sony RAW 2 (basado en TIFF)	L/E/C	L/E/C	L/E/C	L/E/C	L/E Sony
SRF	R	Formato Sony RAW (basado en TIFF)	R	R	R	R	Sony _

SRW	L/E	Formato Samsung RAW (basado en TIFF)	L/E/C	L/E/C	L/E/C	L/E/C	L/E Samsung
SVG	R	Gráficos vectoriales escalables (basados en XML)	-	-	-	-	R SVG
SWF	R	Shockwave Flash	-	-	R	-	Destello R
THM	L/E	Imagen en miniatura (JPEG)	L/E/C	L/E/C	L/E/C	L/E/C	Metainformación JPEG admitida
THMX	R	Tema XML abierto de Office	-	-	-	-	R XML ZIP
TIFF, TIFF	L/E	Formato de archivo de imagen etiquetado	L/E/C	L/E/C	L/E/C	L/E/C	R/W/C GeoTIFF 1 , R/W Remolques
TTF, TTC	R	Fuente/Colección True Type	-	-	-	-	Fuente R
TORRENTE	R	Archivo de descripción de BitTorrent	-	-	-	-	R Torrente
TXT	R	archivos de texto	-	-	-	-	R Texto
VCF, VCARD	R	Tarjeta virtual	-	-	-	-	R VCard

VNT	R	Viñeta de Scene7 (tipo FPX)	-	-	-	R	R FlashPix
VNT	R	Documento V-Note	-	-	-	-	R VNota
VOB	R	Objeto de video (basado en MPEG)	-	-	-	-	R MPEG
VRD	L/E/C 2	Datos de receta de Canon DPP	-	-	L/E/C	-	R/W/C CanonVRD 2
CIV	R	Dibujo de Microsoft Visio (similar a FPX)	-	-	R	R	R FlashPix
WAV	R	Forma de onda de audio digital de Windows (basada en RIFF)	R 3	-	R	-	R RIFF
WEBM	R	Película web de Google (basada en Matroska)	-	-	-	-	R Matroska
WEBP	L/E	Imagen web de Google (basada en RIFF)	L/E/C	-	L/E/C	L/E/C	R RIFF
WMA, WMV	R	Windows Media Audio/Video (basado en ASF)	-	-	R	-	PPA R

WPG	R	Gráficos de WordPerfect	-	-	-	-	R WPG
WTV	R	Programa de TV grabado de Windows	-	-	-	-	R WTV
VIRGINIA OCCIDENTAL	R	Audio sin pérdidas WavePack (basado en RIFF)	R 3	-	R	-	R RIFF
X3F	L/E	Sigma/Foveon CRUDO	L/E/C	L/E/C	L/E/C	L/E/C	R/W Sigma , R SigmaRaw
XCF	R	Formato de imagen nativo de GIMP	R	R	R	R	R GIMP
XLS, XLT	R	Hoja de cálculo/plantilla de Microsoft Excel (similar a FPX)	-	-	R	R	R FlashPix
XLSX, XLSM, XLSB	R	Hoja de cálculo de Office Open XML [habilitado para macros/binario]	-	-	-	-	R XML ZIP
XMP	L/E/C	Archivo sidecar de plataforma de metadatos extensible	-	-	L/E/C	-	-
CREMALLERA	R	archivo ZIP	-	-	-	-	C.P.R. _

Tabla 7. Tipos de archivos de ExifTool

METAINFORMACIÓN JPG ADMITIDA

Metainformación JPEG	Apoyo	Descripción
APP0- JFIF	L/E/C	Formato de intercambio de archivos JPEG
APP0 - JFXX	R	JFIF extendido
APP0 - CIFF	L/E	Formato de archivo de imagen de la cámara (utilizado por algunos modelos de Canon)
APP0 - AVI1	R	Información JPEG AVI
APP0 - OCAD	R	Photobucket Segmento Ocad
APP1- EXIF	L/E/C	Formato de archivo de imagen intercambiable (multisegmento)
APP1- XMP	L/E/C	Plataforma de metadatos extensible (multisegmento)
APP1- QVCI	R	Información de Casio QV-7000SX QVCI
APP1- FLIR	R	Datos de imágenes térmicas de FLIR (multisegmento)
APP1 - Imagen térmica sin procesar	R	Imagen térmica del dron Parrot Bebop-Pro Thermal
APP2 - CPI	L/E/C	Consorcio Internacional del Color (multisegmento)
APP2- FPXR	R	FlashPix Ready (multisegmento)
APP2 - MPF	R	Formato de múltiples imágenes
APP2 - Versión InfiRay	R	Encabezado de la versión InfiRay IJPEG

APP2 - Imagen de vista previa	R	Imagen de vista previa de Samsung/GE APP2 (multisegmento)
APP3 - Meta Kodak	L/E	Metainformación de Kodak (tipo EXIF)
APP3 - Estimulación	R	Formato de imagen fija estéreo
APP3- JPS	R	Imagen estéreo JPEG
APP3 - Datos Térmicos	R	Datos térmicos DJI RJPEG (multisegmento)
APP3 - Datos de imagen	R	InfiRay IJPEG IR+térmico+datos visibles (multisegmento)
APP3 - Imagen de vista previa	R	Imagen de vista previa de Samsung/HP (multisegmento)
APP4 - Escalado	R	(presumiblemente escrito por el software móvil Scaledo)
APP4 - Parámetros térmicos	R	Parámetros térmicos del archivo DJI RJPEG
APP4 - ThermalParams2	R	Parámetros térmicos DJI tipo 2
APP4 - ThermalParams3	R	Parámetros térmicos DJI tipo 3
APP4- FPXR	R	FlashPix Ready en una ubicación no estándar (multisegmento)
APP4 - Fábrica InfiRay	R	Temperatura de fábrica de InfiRay IJPEG
APP4 - Imagen de vista previa	R	(continuación de APP3)
APP5 - Ricoh RMETA	R	Campos personalizados de Ricoh

APP5 - Identificación única de Samsung	R	Identificación única de Samsung
APP5 - Calibración térmica	R	Datos de calibración térmica del archivo DJI RJPEG
APP5 - Imagen InfiRay	R	Temperatura de imagen InfiRay IJPEG
APP5 - Imagen de vista previa	R	(continuación de APP4)
APP6 - EPPIM	R	Toshiba PrintIM
APP6- NITF	R	Formato Nacional de Transmisión de Imágenes
APP6- HP TDHD	R	Hewlett-Packard Photosmart R837 TDHD información
APP6- GoPro	R	Información del formato de metadatos de GoPro (GPMF)
APP6-DJI DTAT	R	Registro de la herramienta de análisis térmico DJI (formato JSON)
APP6 - Modo mixto InfiRay	R	Modo de mezcla InfiRay IJPEG
APP7- Pentax	R	Notas del fabricante Pentax APP7
APP7- Qualcomm	R	Atributos de la cámara Qualcomm
APP7-Huawei	R	Notas del fabricante de Huawei APP7 (extracto con opción Desconocida)
APP7 - Modo operativo InfiRay	R	Modo de funcionamiento InfiRay IJPEG

APP6 - DJI Información	R	Información de depuración de DJI
APP8 - SPIFF	R	Formato de archivo de intercambio de imágenes fijas
APP8 - Isotérmica InfiRay	R	Isotérmico InfiRay IJPEG
APP9 - Tocadiscos multimedia	R	Información XML de Media Jukebox
APP9 - Sensor InfiRay	R	Información del sensor InfiRay IJPEG
APP10 – Comentar	R	Comentario de PhotoStudio Unicode
APP11 - JPEG-HDR	R	Imagen de relación comprimida JPEG-HDR
APP11 - JUMBF	R	Formato de cuadro de metadatos universal Jpeg (multisegmento)
APP12 - Información de la imagen	R	Información de imagen basada en ASCII
APP12 - Patito	L/E/C	Photoshop "Guardar para Web"
APP13 - IRB de Photoshop	L/E/C	Bloque de recursos de imagen (multisegmento, incluye IPTC)
APP13- Adobe CM	R	Administración de color de Adobe
APP14 - Adobe	L/E/C	Filtro DCT de Adobe
APP15 - Convertidor gráfico	R	Calidad del convertidor gráfico
COM	L/E/C	Comentario JPEG (multisegmento)

DQT	R	(utilizado para calcular el valor de la etiqueta Extra:JPEGDigest)
SOF	R	Inicio de cuadro JPEG
Tráiler JPEG 1	**Apoyo**	**Descripción**
Remolque AFCP	L/E	Protocolo de concatenación de archivos AXS (incluye IPTC)
Tráiler de CanonVRD	L/E/C	Datos de receta de Canon DPP (incluye DR4)
Tráiler de FotoStation	L/E	FotoWare FotoStation (incluye IPTC)
Tráiler fotomecánico	L/E	Mecánico de fotos de bits de câmara
Tráiler MIE	L/E	Encapsulación de metainformación
Tráiler de Samsung	R	Tráiler de Samsung Galaxy
Tráiler de Insta360	R	Tráiler de Insta360 encontrado en archivos INSP
Tráiler de la aplicación Nikon	R	Tráiler de Nikon añadido por NX Studio a archivos NEF/NRW
AvanceImagen de tráiler	L/E/C	(imagen de vista previa escrita después de JPEG EOI)
Tráiler de video integrado	R	(extraído solo con la opción ExtractEmbedded)

Tabla 8. Metainformación JPG admitida en ExifTool

Anexo 8. Instalación de Kali Linux

Descargue la imagen ISO del sitio web oficial:

Ya que iniciamos la imagen de VirtualBox, elegimos una instalación gráfica:

Figura 58: Descarga de la ISO

Esperamos un momento a que cargue, y luego seleccionamos el idioma de instalación:

Figura 59: Idioma de instalación

Elegimos un lugar:

Figura 60: Elección del lugar

Seleccionamos el idioma que tendrá el teclado:

Figura 61: Idioma

Mientras esperamos que se cargue la configuración, agregamos el nombre de host:

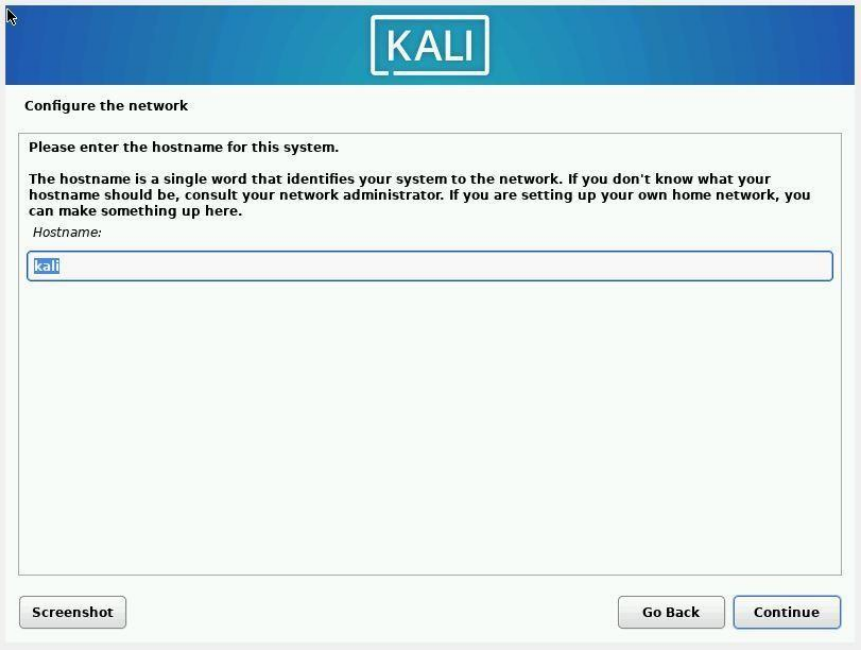


Figura 62: Cargar la configuración

Si tenemos un nombre de dominio, lo agregaremos aquí; de lo contrario, déjelo en blanco y haga clic en Continuar:

Figura 63: Nombre de dominio

El nombre del nuevo usuario que agregamos:

Figura 64: Nombre de usuario

Ahora que hemos añadido el usuario, podemos guardarlo sin problemas:

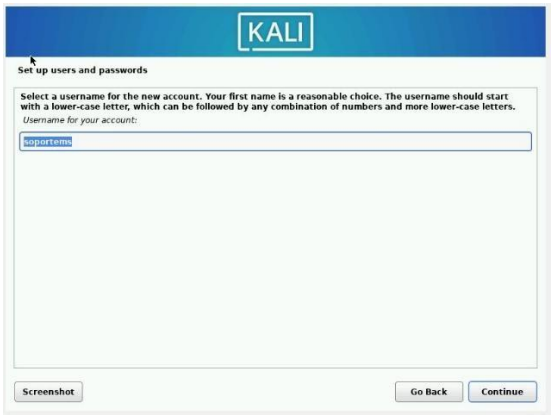


Figura 65: Guardar usuario

La contraseña que añadiremos al usuario tendrá:

Figura 66: Contraseña

Seleccionamos la zona horaria:

Figura 67: Zona horaria

Este paso lo usaremos para particiones de disco, lo dejamos automático:

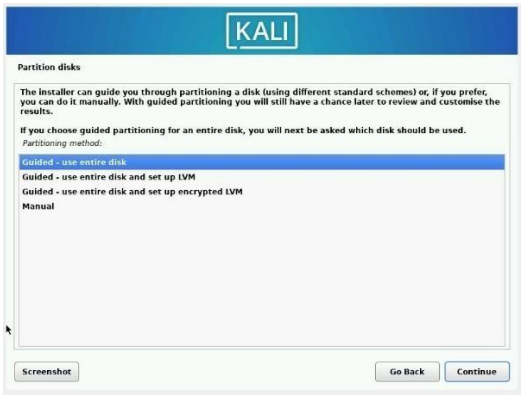


Figura 68: Particiones de disco

Seleccionamos un disco para particionar:

Figura 69: Seleccionar disco

Elegimos un esquema de partición predefinido:

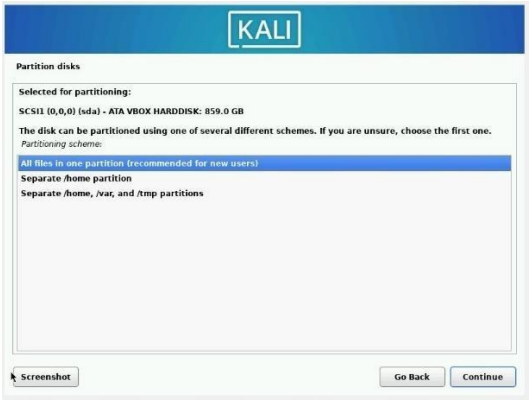


Figura 70: Esquema de partición

Confirmamos haciendo clic en "Continuar":

Figura 71: Confirmación

Elegimos "Sí" para indicar si queremos escribir los cambios en el disco:

Figura 72: Elegir si

Elegimos el software y el estándar es suficiente:

Figura 73: Elección del software

Instalamos el gestor de arranque GRUB:

Figura 74: Instalación del gestor de arranque

Seleccionamos la partición a instalar:

Figura 75: Selección de la partición

Cuando finalice la instalación damos clic en continuar y se reinicia el inicio de sesión:

Figura 76: Finalización de la instalación

Anexo 9. Características del dispositivo móvil empleado para la auditoria

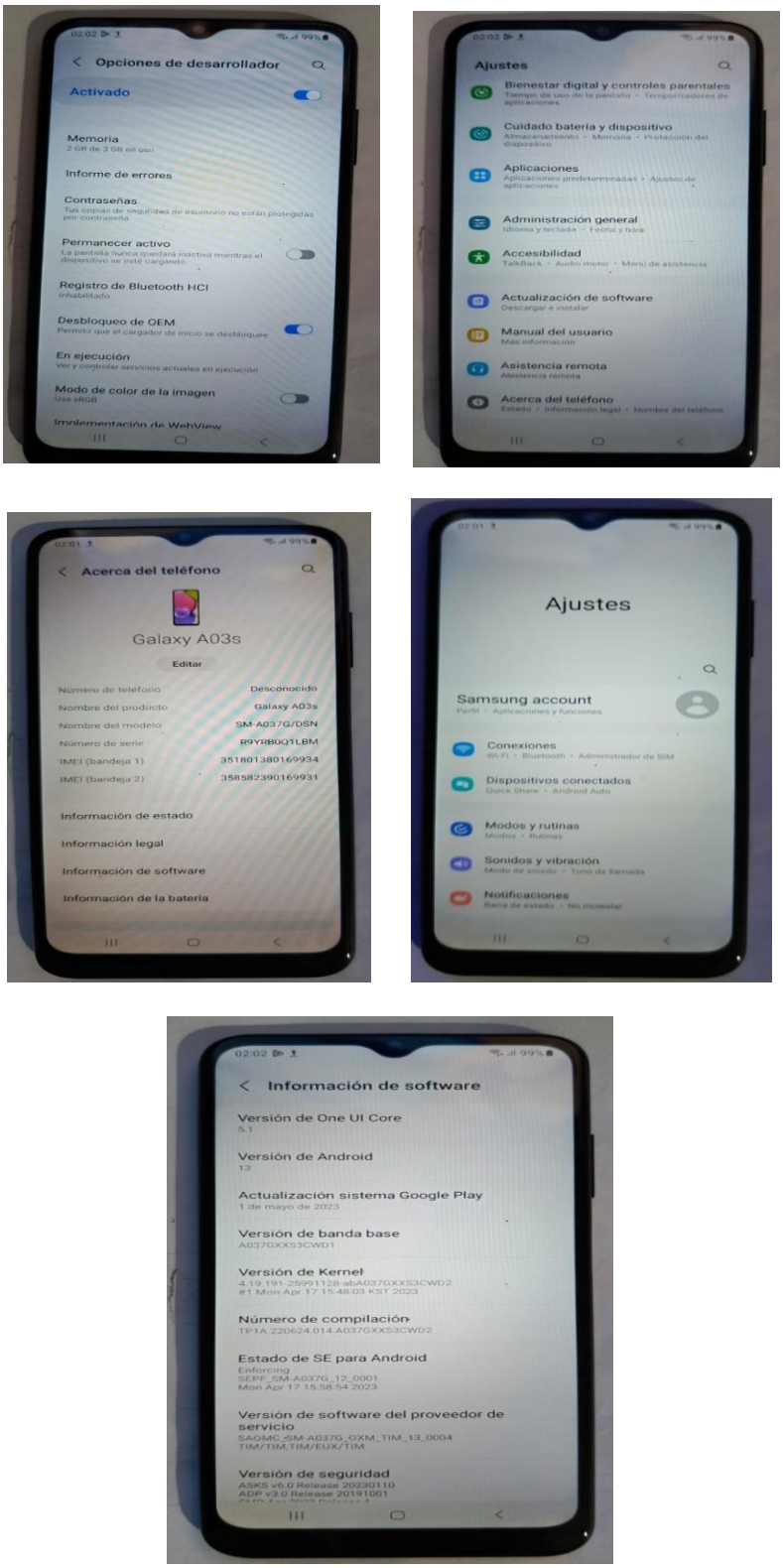


Figura 77. Características del dispositivo móvil

Anexo 10. Testeo del equipo

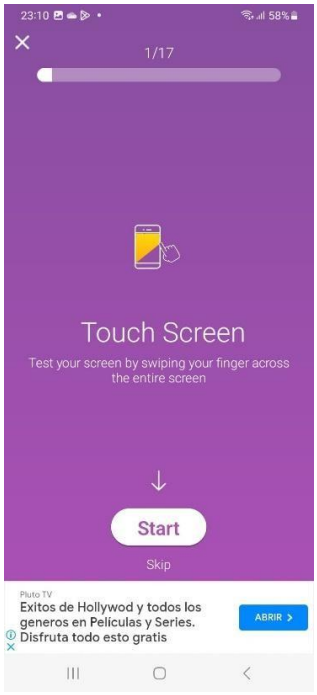
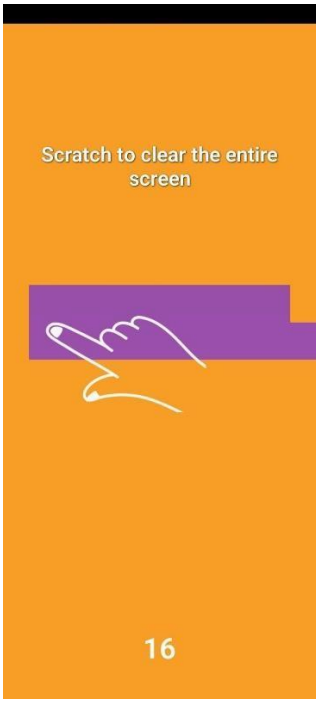
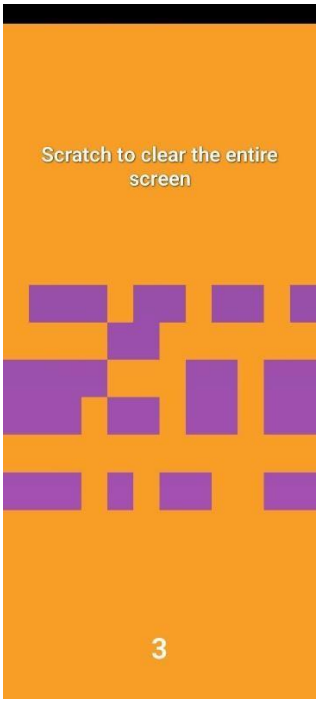
<table>
<tr><th colspan="3">TÁCTIL</th></tr>
<tr><th>Inicio</th><th>Proceso</th><th>Resultado</th></tr>
<tr>
<td> 
</td>
<td> 
</td>
<td> 
</td>
</tr>
<tr><th colspan="3">RESULTADOS</th></tr>
<tr><td colspan="3">Según lo mostrado en la pantalla, el dispositivo móvil presenta daños en el táctil, reflejando que ciertos sectores ya no detectan la pulsación.</td></tr>
</table>

Tabla 9. Testeo del táctil

PARLANTE		
Inicio	**Proceso**	**Resultado**

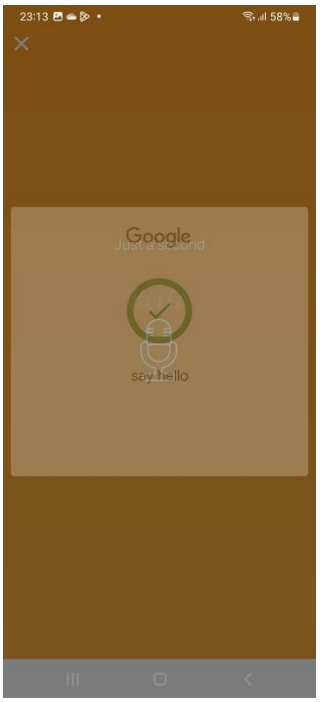
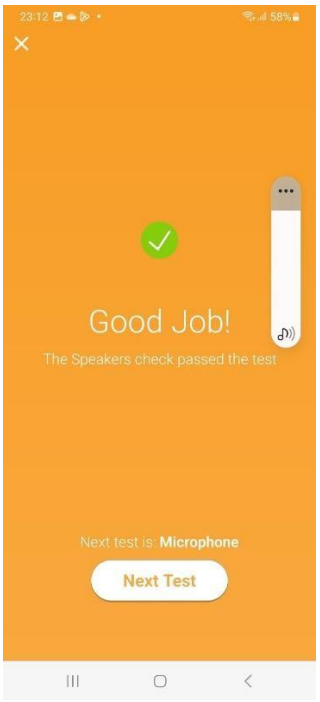
		
RESULTADOS		
Según lo que se muestra, el funcionamiento del parlante en el dispositivo móvil se encuentra en perfecto estado.		

Tabla 10. Testeo del parlante

MICRÓFONO		
Inicio	**Proceso**	**Resultado**

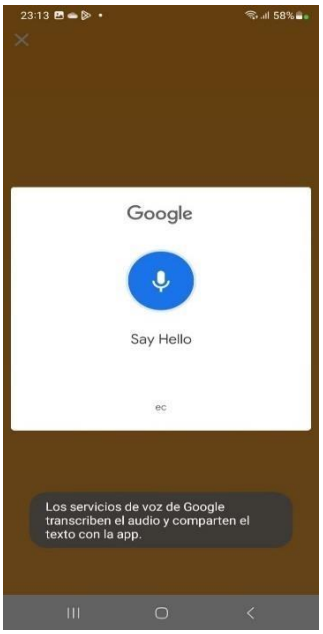
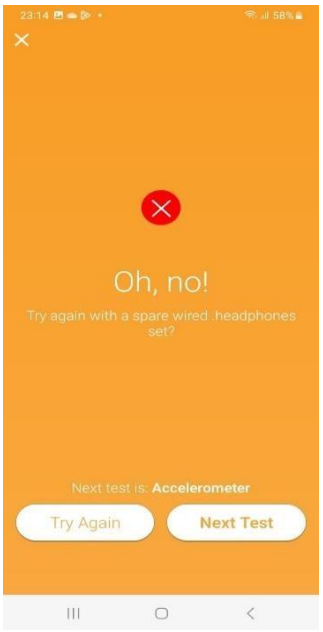
		
RESULTADOS		
Según lo que se muestra, el funcionamiento del micrófono en el dispositivo móvil está presentando fallas.		

Tabla 11. Testeo del micrófono

ACELERÓMETRO		
Inicio	**Proceso**	**Resultado**

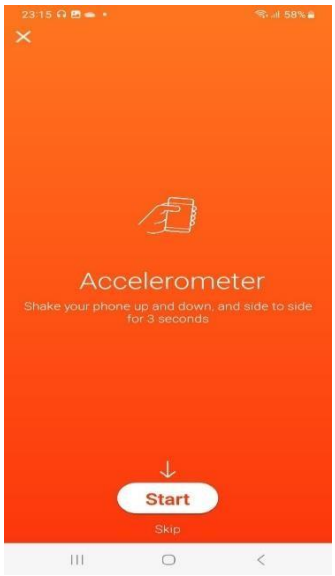
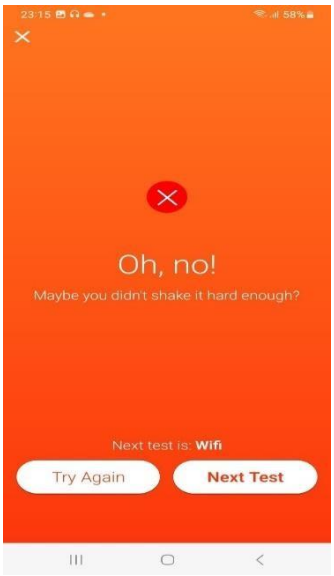
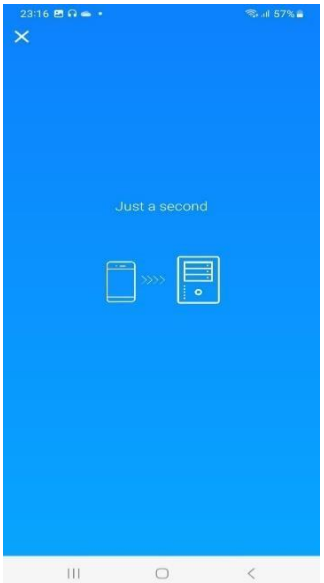
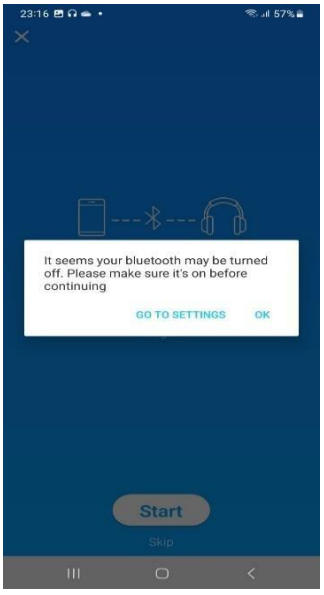
		
RESULTADOS		
Según lo que se muestra, el funcionamiento del acelerómetro en el dispositivo móvil está presentando fallas.		

Tabla 12. Testeo del acelerómetro

BLUETOOH		
Inicio	**Proceso**	**Resultado**
		

RESULTADOS
Según lo que se muestra, el funcionamiento del bluetooth en el dispositivo móvil se encuentra en perfecto estado.

Tabla 13. Testeo del bluetooth

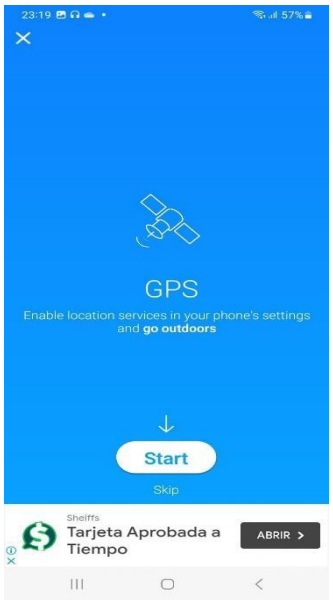
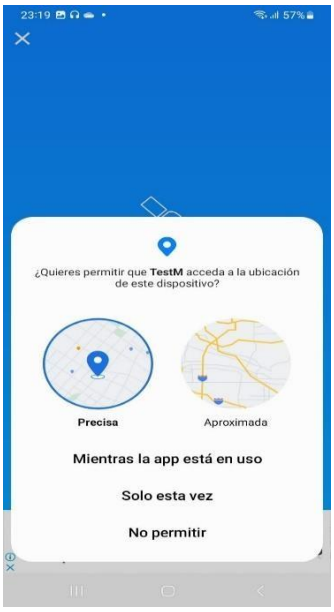
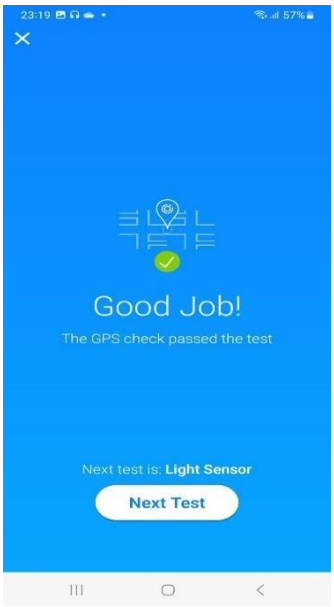
GPS		
Inicio	**Proceso**	**Resultado**
		
RESULTADOS		
Según lo que se muestra, el funcionamiento del GPS en el dispositivo móvil se encuentra en perfecto estado.		

Tabla 14. Testeo del GPS

CARGA – WIFI – SENSOR DE LUZ		
Proceso	**Proceso**	**Proceso**

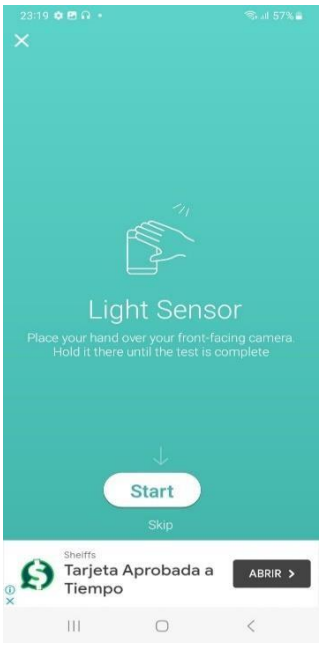
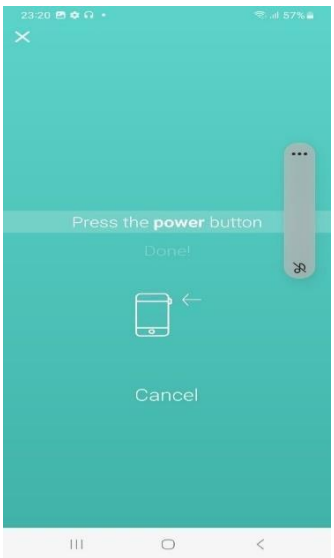
		
RESULTADOS		
Según lo que se muestra, el funcionamiento de los procesos en el dispositivo móvil se encuentra en buen estado.		

Tabla 15. Testeo de la carga, wifi y sensor de luz

BOTONES		
Inicio	**Proceso**	**Resultado**
		

RESULTADOS
Según lo que se muestra, el funcionamiento de los botones volumen + / - y power en el dispositivo móvil, se encuentran en buen estado.

Tabla 16. Testeo de los botones

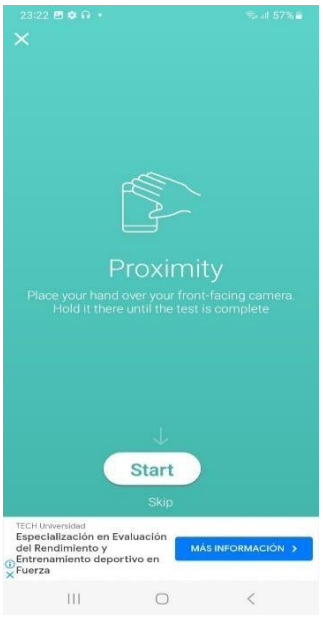
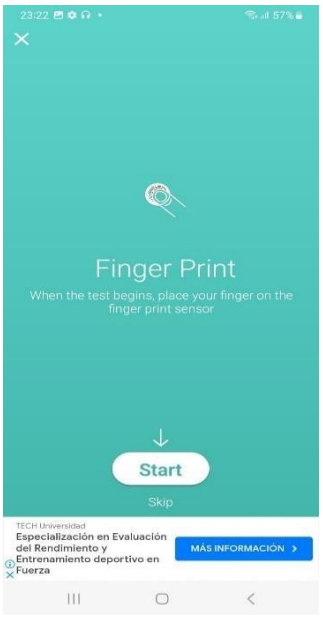
VIBRACIÓN – PROXIMIDAD – DACTILAR		
Inicio	**Proceso**	**Resultado**
		
RESULTADOS		
Según lo que se muestra, el funcionamiento del vibrador y la proximidad, están en perfecto estado, mientras que, el dactilar presenta fallas.		

Tabla 17. Testeo de la vibración, proximidad y dactilar

CÁMARA FRONTAL		
Inicio	**Proceso**	**Resultado**

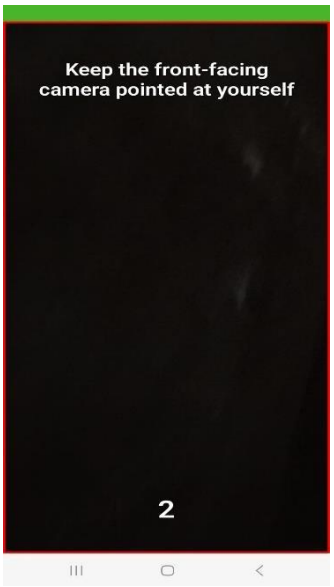
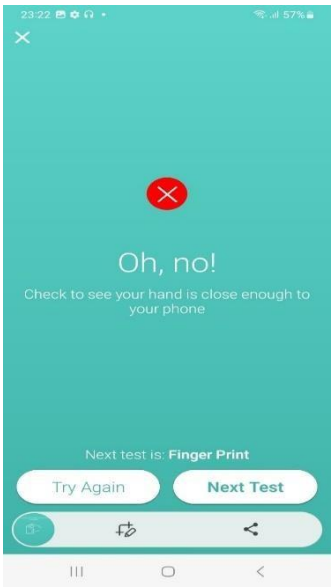
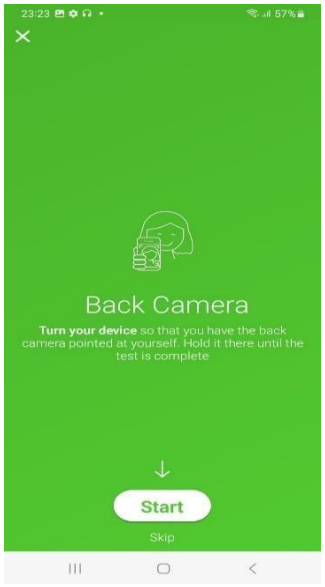
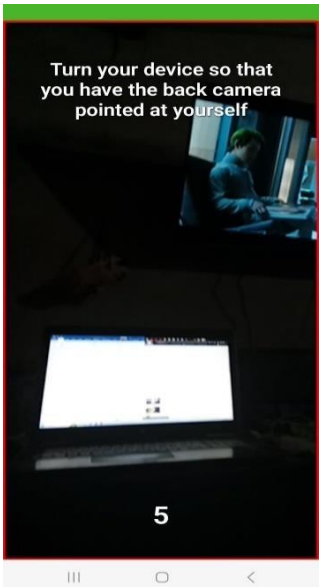
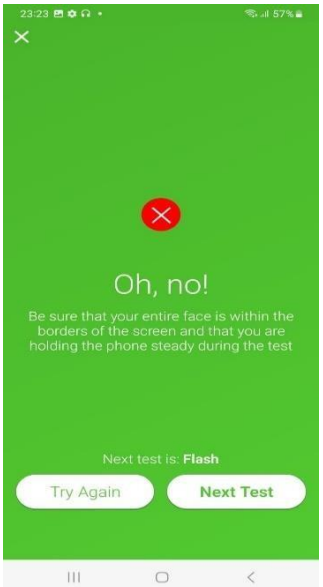
		
RESULTADOS		
Según lo que se muestra, el funcionamiento de la cámara frontal en el dispositivo móvil está presentando fallas.		

Tabla 18. Testeo de la cámara frontal

CÁMARA TRASERA		
Inicio	**Proceso**	**Resultado**
		

RESULTADOS
Según lo que se muestra, el funcionamiento de la cámara trasera en el dispositivo móvil está presentando fallas.

Tabla 19. Testeo de la cámara trasera

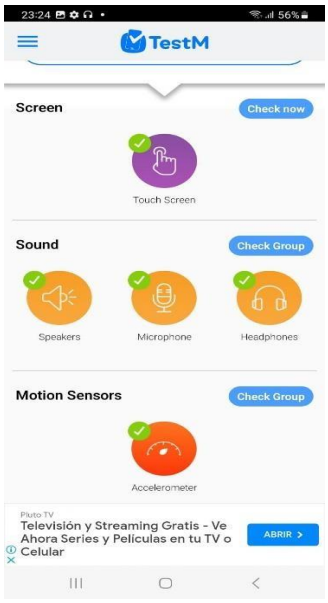
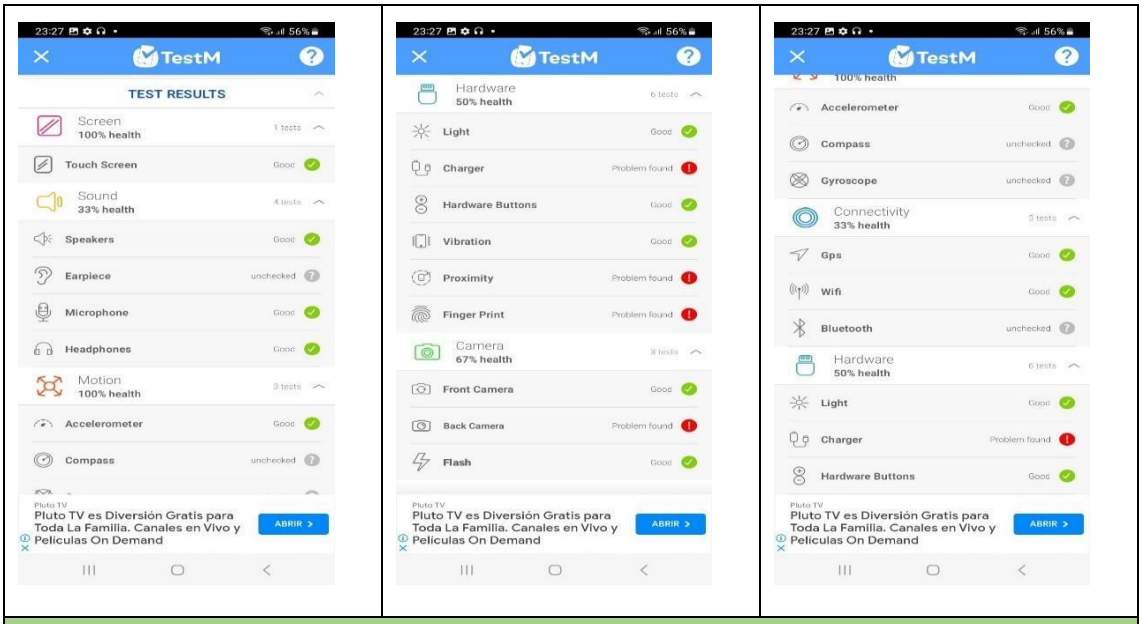
RESULTADOS FINALES		
Proceso	**Proceso**	**Proceso**
		
RESULTADOS		
Visualización de los resultados arrojados, de forma gráfica.		

Tabla 20. Resultados finales

REPORTES		
Proceso	**Proceso**	**Proceso**



RESULTADOS
Visualización de los resultados arrojados, de forma detallada.

Tabla 21. Reportes

CARACTERÍSTICAS ARROJADAS POR EL SISTEMA

En este apartado, la aplicación muestra todas las características del dispositivo móvil.

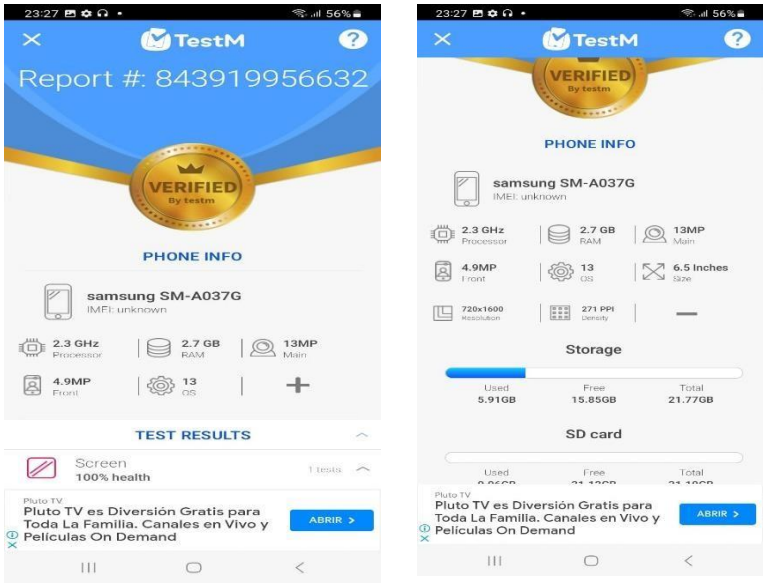


Figura 78. Características del dispositivo móvil

Anexo 11. Análisis Santoku

Dentro del sistema forense Santoku, por defecto se debe activar el Android SDK de reconocimiento del teléfono.

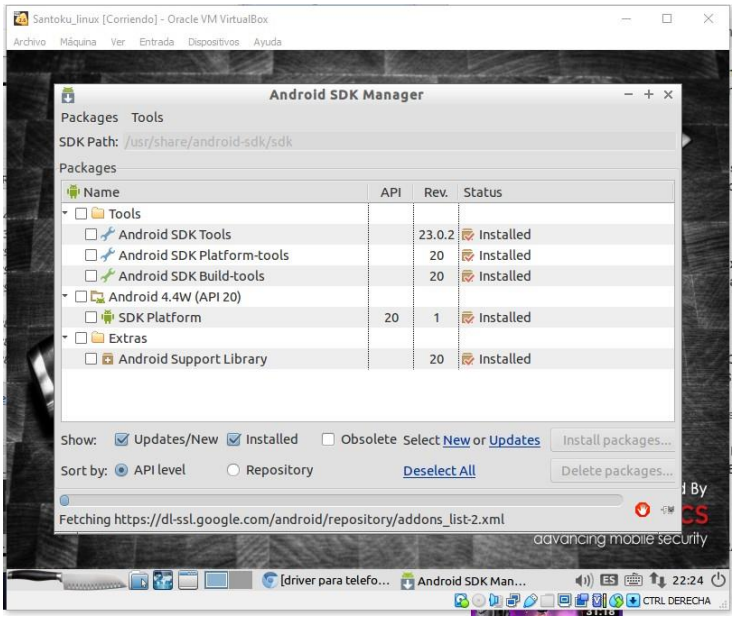


Figura 79. Activación de Android SDK

Antes de realizar los siguientes pasos, se debe de conceder servicios para que el celular permita acceso desde el sistema operativo y poder administrar. Para esto se debe activar el modo desarrollador.

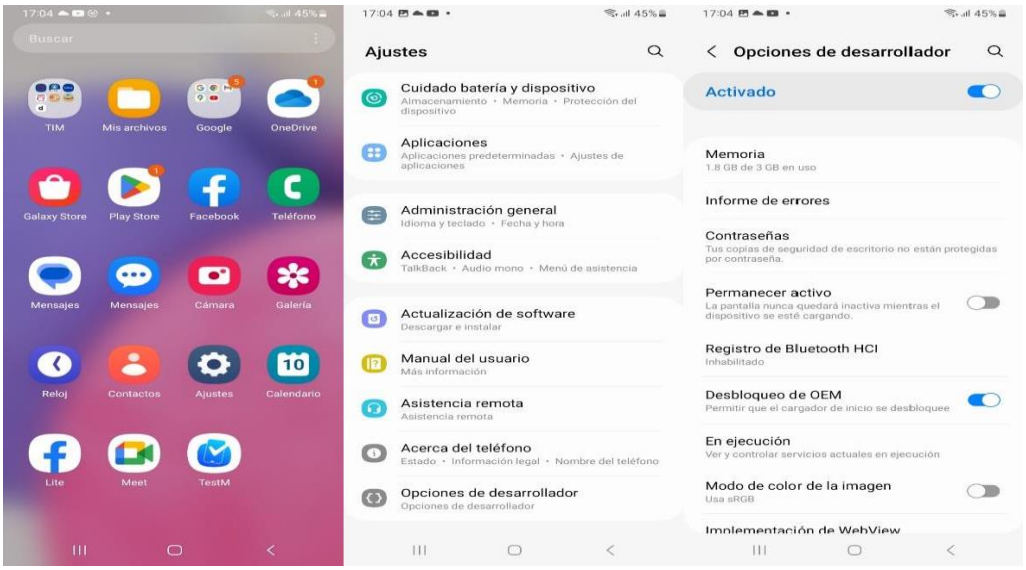


Figura 80. Conceder servicios

A continuación, también se debe proceder a dar acceso a los servicios de USB del dispositivo en el modo desarrollador

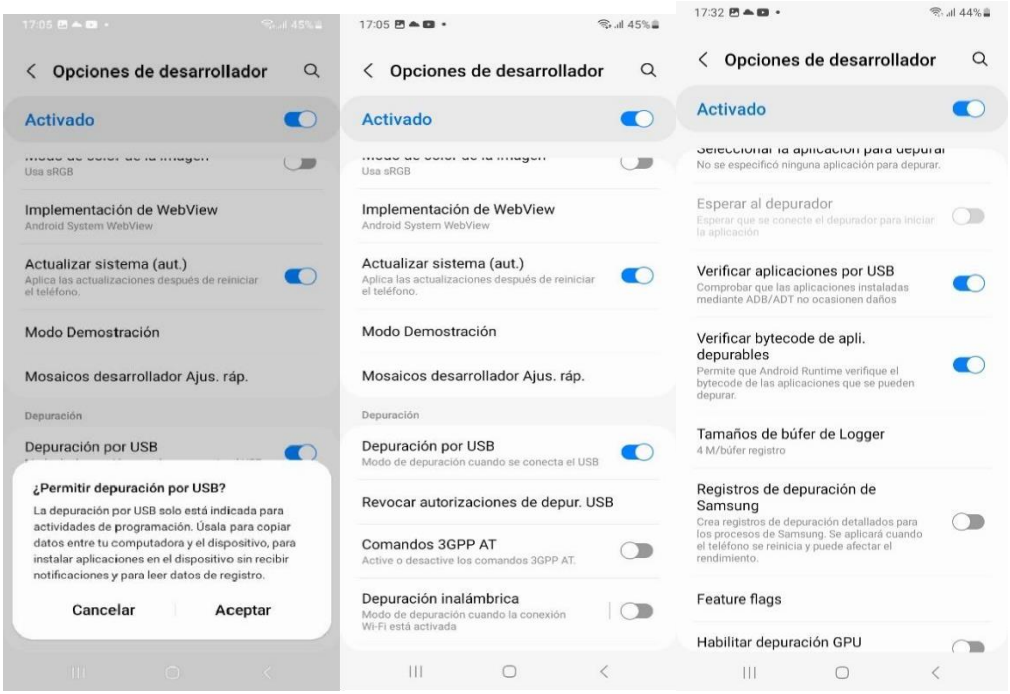


Figura 81. Acceso a servicios USB

Otras de las opciones que también se deben habilitar en el celular, es el uso de instalaciones apk por terceros para dar los permisos.

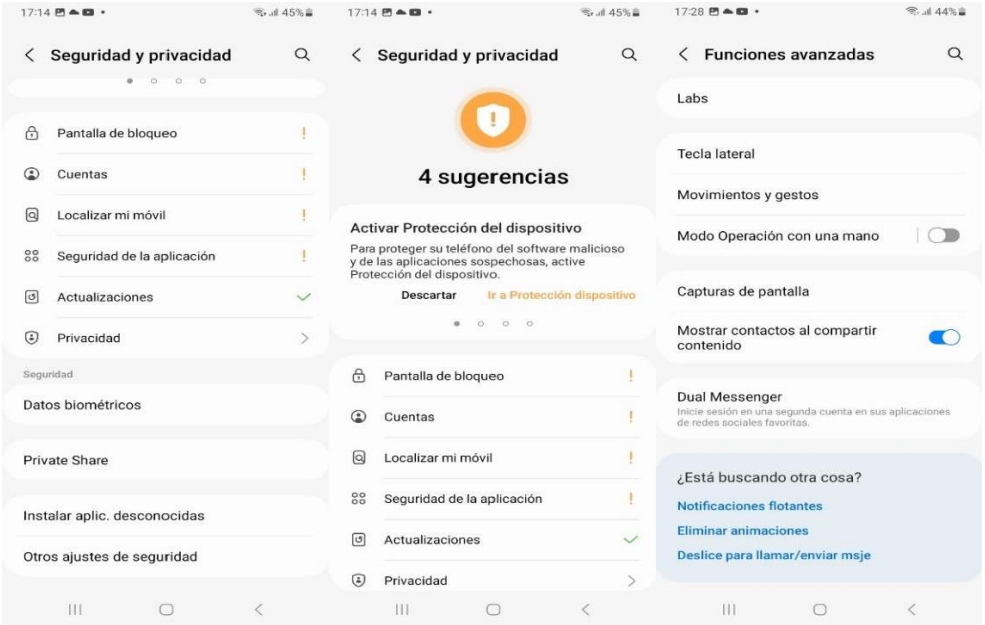


Figura 82. Uso de instalaciones APK

Una vez vinculado el dispositivo, se realiza el proceso para creación de la APK mediante el sistema operativo en el apartado santoku-> Devices Forensics-> AF Logical OSE.

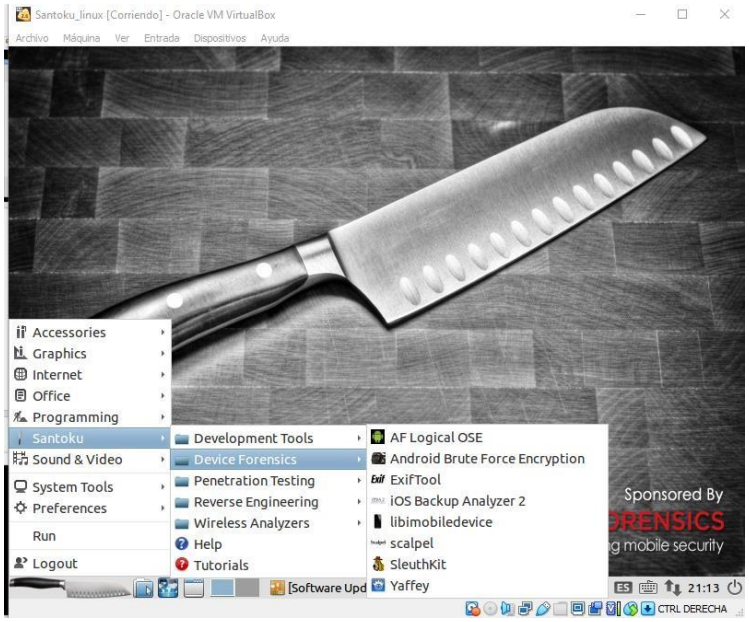


Figura 83. Creación de la APK

Se abrirá un terminal, en el cual se escribe **adb devices** para que muestre que existe el dispositivo y que se encuentra autorizado.

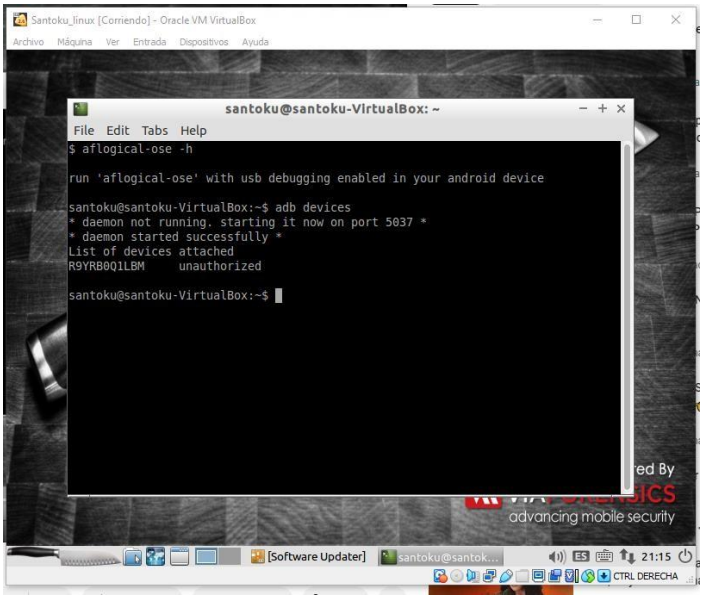


Figura 84. Comando adb devices

Realizada la autorización, se procede a escribir el comando **aflogical-ose**, el cual trata de realizar la conexión USB con el dispositivo para luego pedir la contraseña del Root.

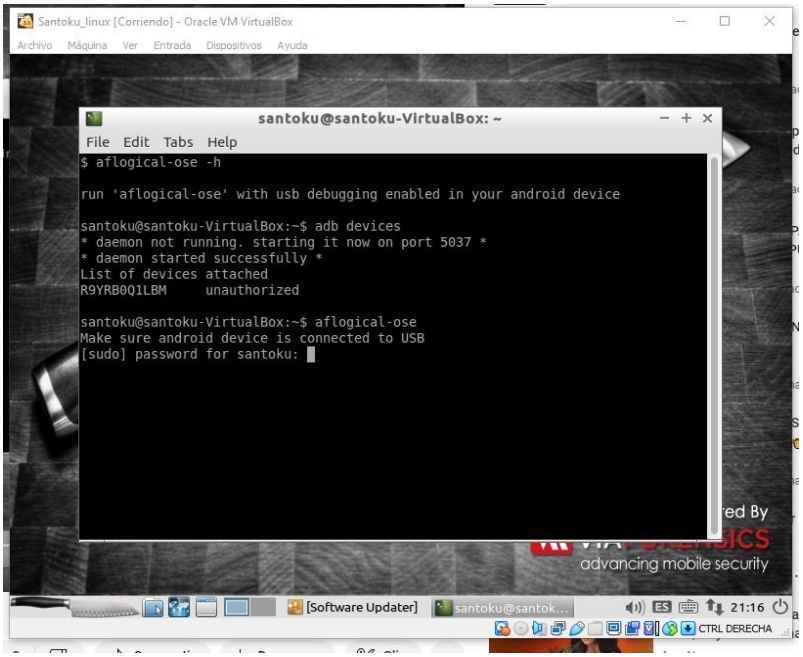


Figura 85. Comando aflogical - ose

Una vez puesta la contraseña se procede al envío de la apk hacia el dispositivo móvil para que se inserte el aplicativo.

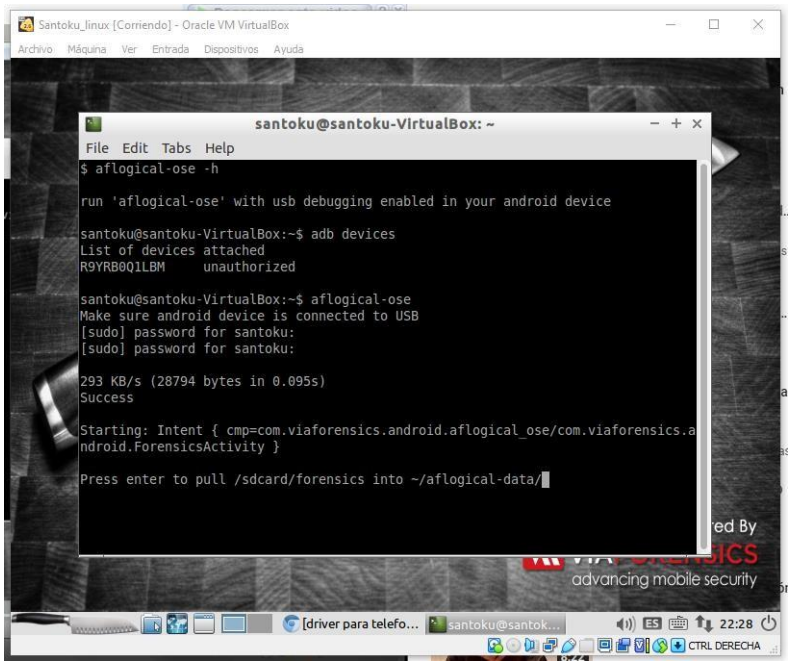


Figura 86. Envío de la APK al dispositivo móvil

El dispositivo se conectará con el Santoku y realizará el proceso enviado al celular.

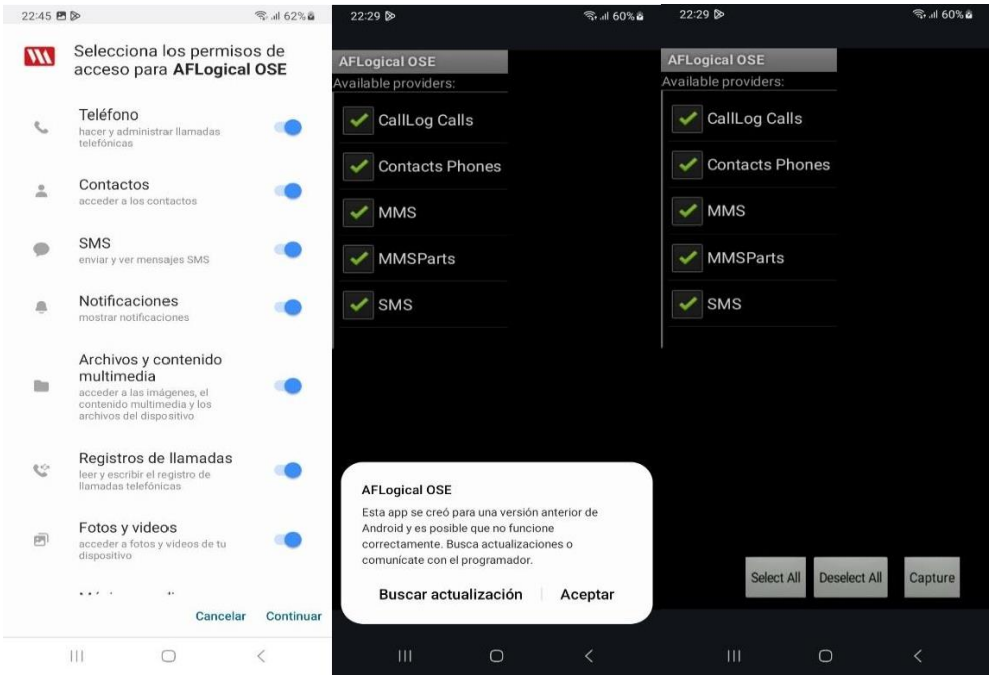


Figura 87. Conexión con Santoku

Después de realizar el proceso de actualización, se procederá a la extracción de los datos de llamadas, contactos, MMS, MMSParts y SMS.

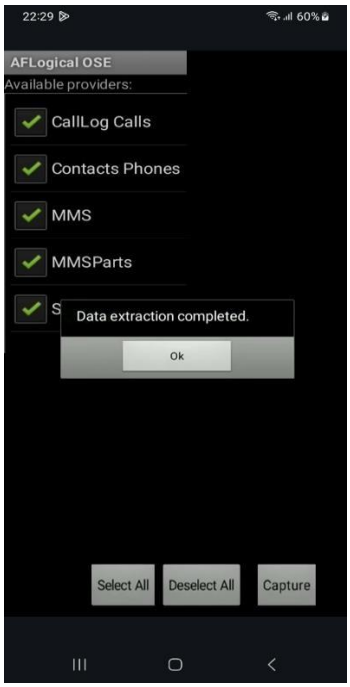


Figura 88. Extracción de información relevante

Internamente, el proceso de extracción que realiza el Santoku se ejecuta trayendo a la información.

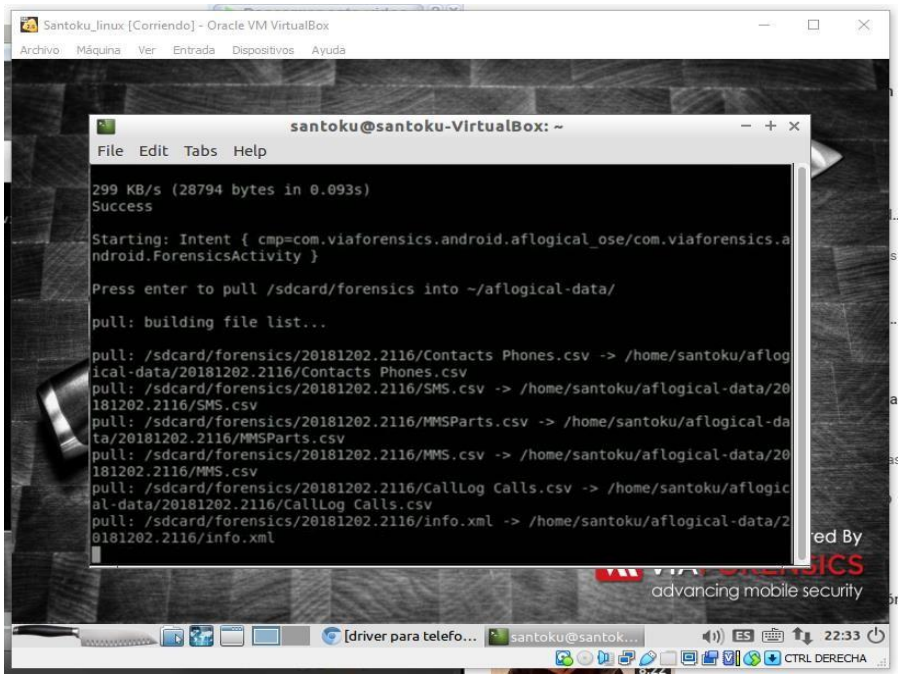


Figura 89. Extracción que realiza Santoku

Una vez concluido el proceso, se genera la información en una carpeta en la raíz lógica del aflogical-seo.

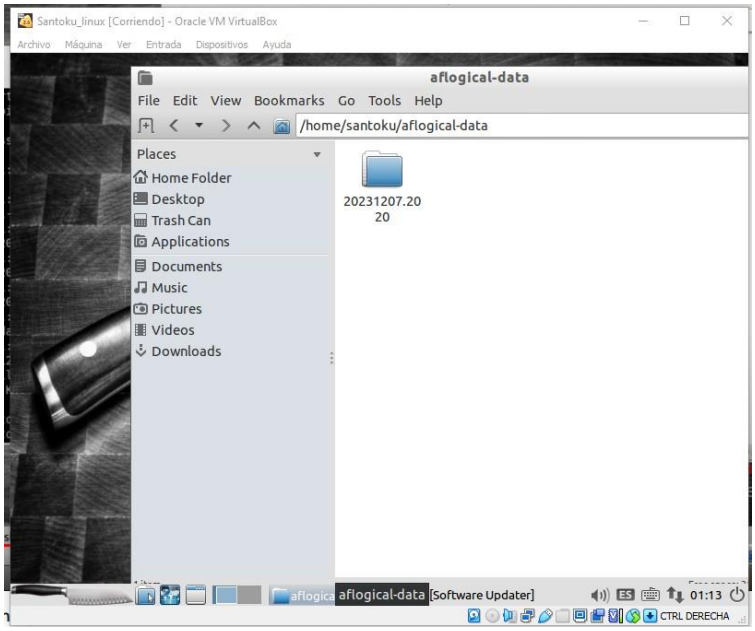


Figura 90. Generación de información

Sondeando el archivo para ver si se cumplió con los datos recabados, se halla lo siguiente.

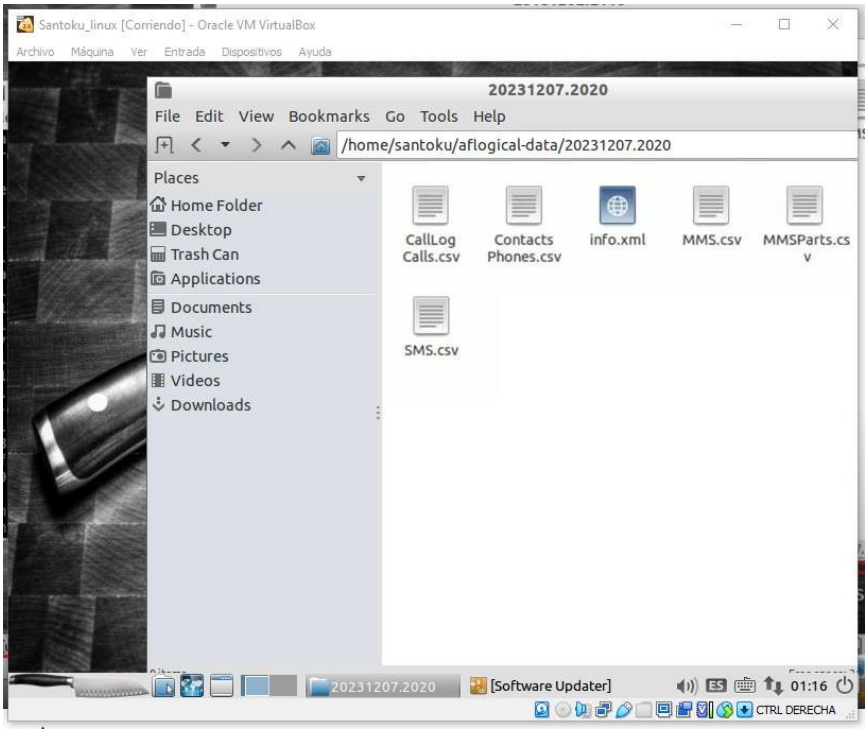


Figura 91. Hallazgos

REPORTES REFERENTES AL PRIMER ATAQUE DE EXTRACCIÓN DE INFORMACIÓN

UPSE	**Universidad Estatal Península de Santa Elena** **Facultad de Sistemas y Telecomunicaciones** **Carrera de Tecnologías de la Información**	
INFORME DE EXTRACCIÓN		
Dispositivo	Samsung Galaxy A03s	
Fecha	11/07/2023	
Responsable: ALEJANDRO ALEJANDRO ERICK JESÚS		

Medio	Linux Santoku -aflogical-seo
Tipo de extracción	Extracción de datos

Objetivos:

- Adquirir información del equipo CallLog Calls

Pruebas:

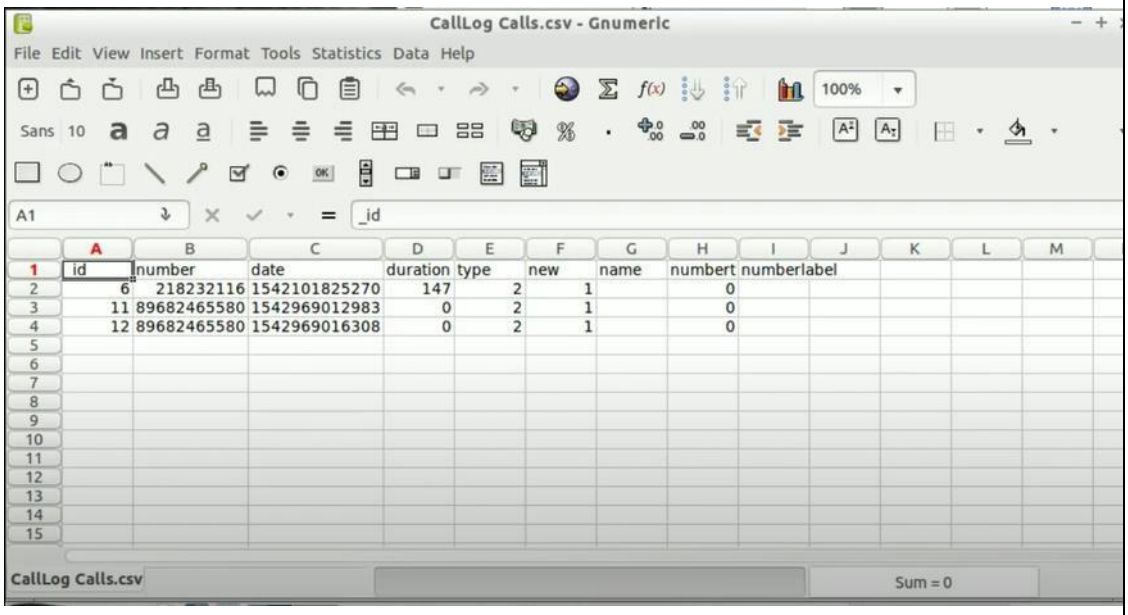


Tabla 22. Extracción de datos de CallLog Calls

	Universidad Estatal Península de Santa Elena **Facultad de Sistemas y Telecomunicaciones** **Carrera de Tecnologías de la Información**	

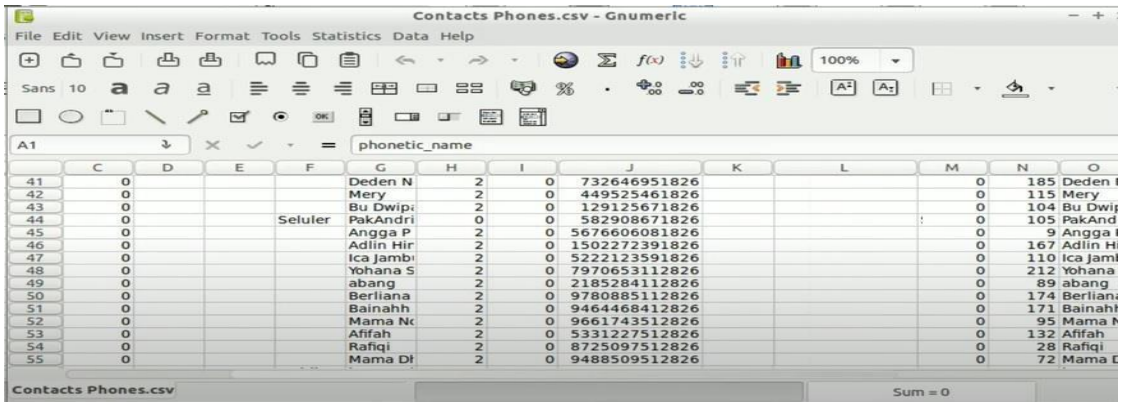
INFORME DE EXTRACCIÓN	
Dispositivo	Samsung Galaxy A03s
Fecha	11/07/2023
Responsable: ALEJANDRO ALEJANDRO ERICK JESÚS	
Medio	Linux Santoku -aflogical-seo
Tipo de extracción	Extracción de datos
Objetivos: • Adquirir información del equipo Contactos	
Pruebas: 	

Tabla 23. Extracción de datos de Contactos

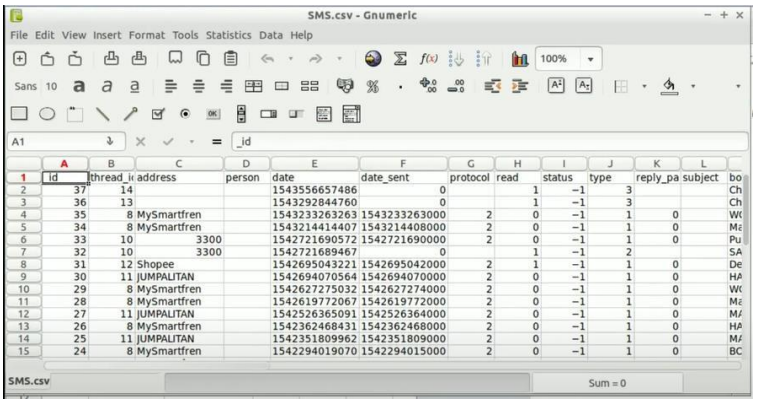
	Universidad Estatal Península de Santa Elena **Facultad de Sistemas y Telecomunicaciones** **Carrera de Tecnologías de la Información**	

INFORME DE EXTRACCIÓN	
Dispositivo	Samsung Galaxy A03s
Fecha	11/07/2023
Responsable: ALEJANDRO ALEJANDRO ERICK JESÚS	
Medio	Linux Santoku -aflogical-seo
Tipo de extracción	Extracción de datos

Objetivos:

- Adquirir información del equipo SMS

Pruebas:



	A	B	C	D	E	F	G	H	I	J	K	L	
1	_id	thread_id	address	person	date	date_sent	protocol	read	status	type	reply_pa	subject	bo
2	37	14			1543556657486	0		1	-1	3			Ch
3	36	13			1543292844760	0		1	-1	3			Ch
4	35	8	MySmartfren		1543233263263	1543233263000	2	0	-1	1	0		W(
5	34	8	MySmartfren		1543214414407	1543214408000	2	0	-1	1	0		Ma
6	33	10	3300		1542721690572	1542721690000	2	0	-1	1	0		Pu
7	32	10	3300		1542721689467	0		1	-1	2			SA
8	31	12	Shopee		1542695043221	1542695042000	2	1	-1	1	0		De
9	30	11	JUMPALITAN		1542694070564	1542694070000	2	0	-1	1	0		HA
10	29	8	MySmartfren		1542627275032	1542627274000	2	0	-1	1	0		W(
11	28	8	MySmartfren		1542619772067	1542619772000	2	0	-1	1	0		Ma
12	27	11	JUMPALITAN		1542526365091	1542526364000	2	0	-1	1	0		MA
13	26	8	MySmartfren		1542362468431	1542362468000	2	0	-1	1	0		HA
14	25	11	JUMPALITAN		1542351809962	1542351809000	2	0	-1	1	0		MA
15	24	8	MySmartfren		1542294019070	1542294015000	2	0	-1	1	0		BC

Tabla 24. Extracción de datos de SMS

Anexo 12. Análisis Exiftool

Se crea una carpeta en donde se contendrá este archivo exiftool y los demás que se les va a realizar la extracción de los meta datos, así mismo, se conectará el dispositivo y se copiarán los archivos.

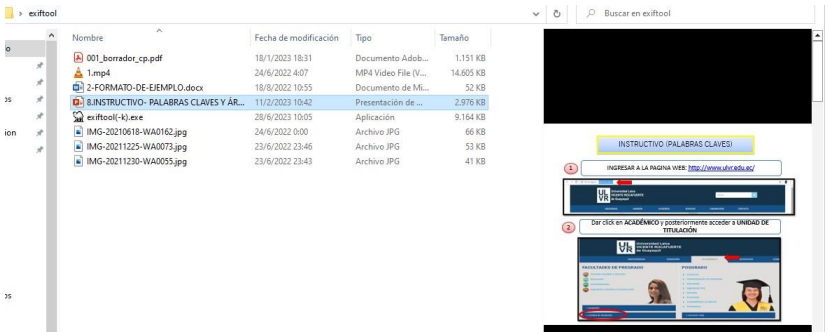


Figura 92. Creación de carpeta

Se usará el cmd para realizar las opciones adecuadas para este análisis de los datos extraídos (se debe ejecutar como administrador).

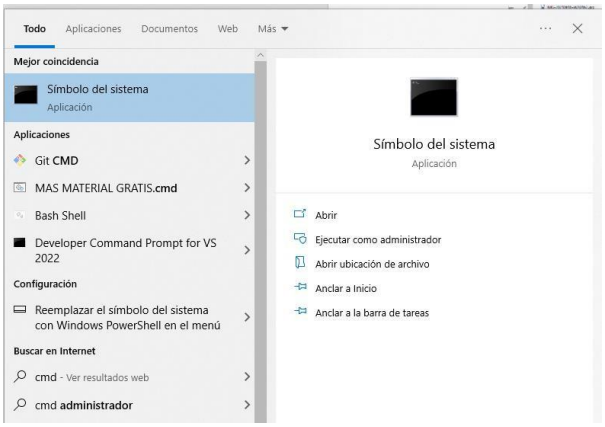


Figura 93. CMD

Se ingresará a la carpeta que se creó previamente, para poder interactuar.

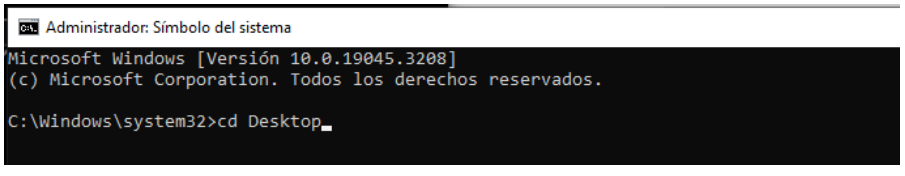


Figura 94. Ingreso a la carpeta

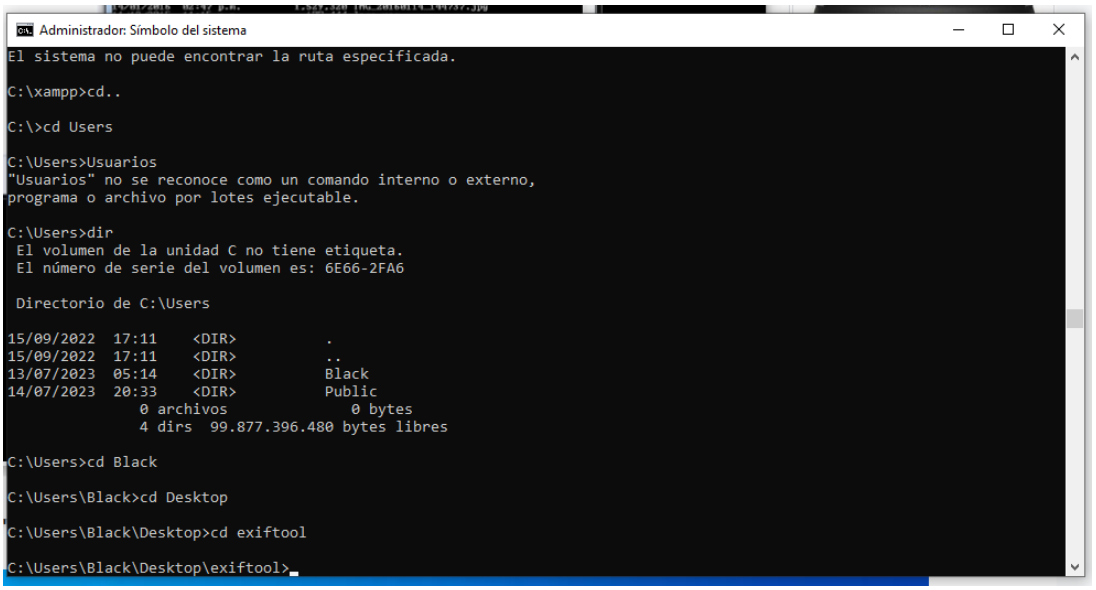


Figura 95. Comando para acceder a la carpeta

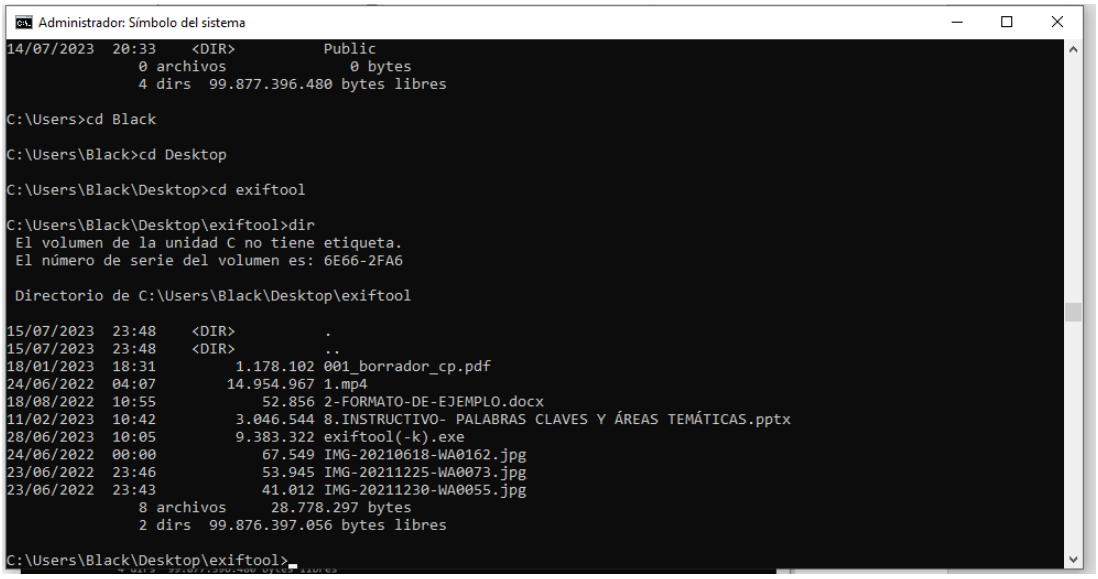


Figura 96. Acceso a la carpeta

Una vez en la carpeta donde se encuentran los archivos, se procede a arrancar el exiftool junto al nombre del documento que se le desea extraer la información de los metadatos con el comando **exiftool.exe IMG-20210618-WA0162.jpg.**

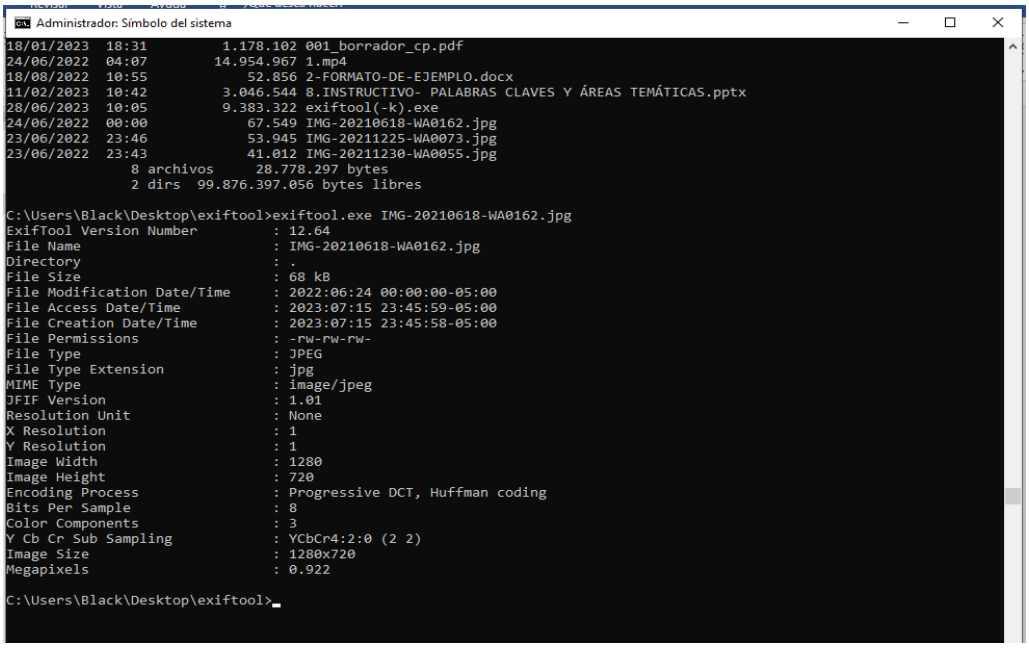


Figura 97. Arranque de exiftool

REPORTE REFERENTE AL SEGUNDO ATAQUE DE EXTRACCIÓN DE INFORMACIÓN

UPSE	**Universidad Estatal Península de Santa Elena** **Facultad de Sistemas y Telecomunicaciones** **Carrera de Tecnologías de la Información**	
INFORME DE EXTRACCION		
Dispositivo	Samsung Galaxy A03s	
Fecha	11/07/2023	
Responsable:	ALEJANDRO ALEJANDRO ERICK JESÚS	
Medio	CMD Windows 10 exiftool	
Tipo de extracción	Extracción de metadatos	

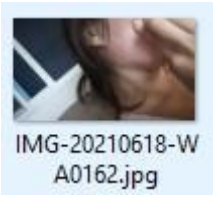
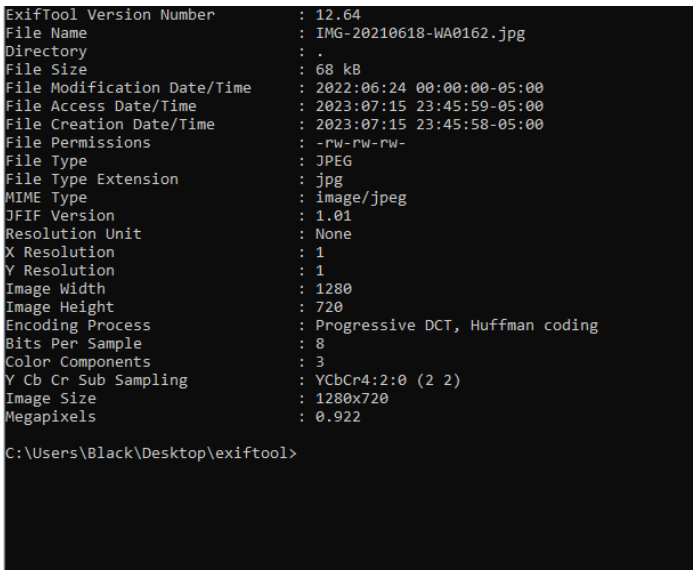
Objetivos:	Adquirir información de un archivo jpg
Archivo:  	
Pruebas: 	

Tabla 25. Adquisición de información de archivo jpg

	Universidad Estatal Península de Santa Elena **Facultad de Sistemas y Telecomunicaciones** **Carrera de Tecnologías de la Información**	

INFORME DE EXTRACCION	
Dispositivo	Samsung Galaxy A03s
Fecha	11/07/2023
Responsable:	ALEJANDRO ALEJANDRO ERICK JESÚS
Medio	CMD Windows 10 exiftool
Tipo de extracción	Extracción de metadatos
Objetivos:	Adquirir información de un archivo mp4
Archivo:	
Pruebas:	

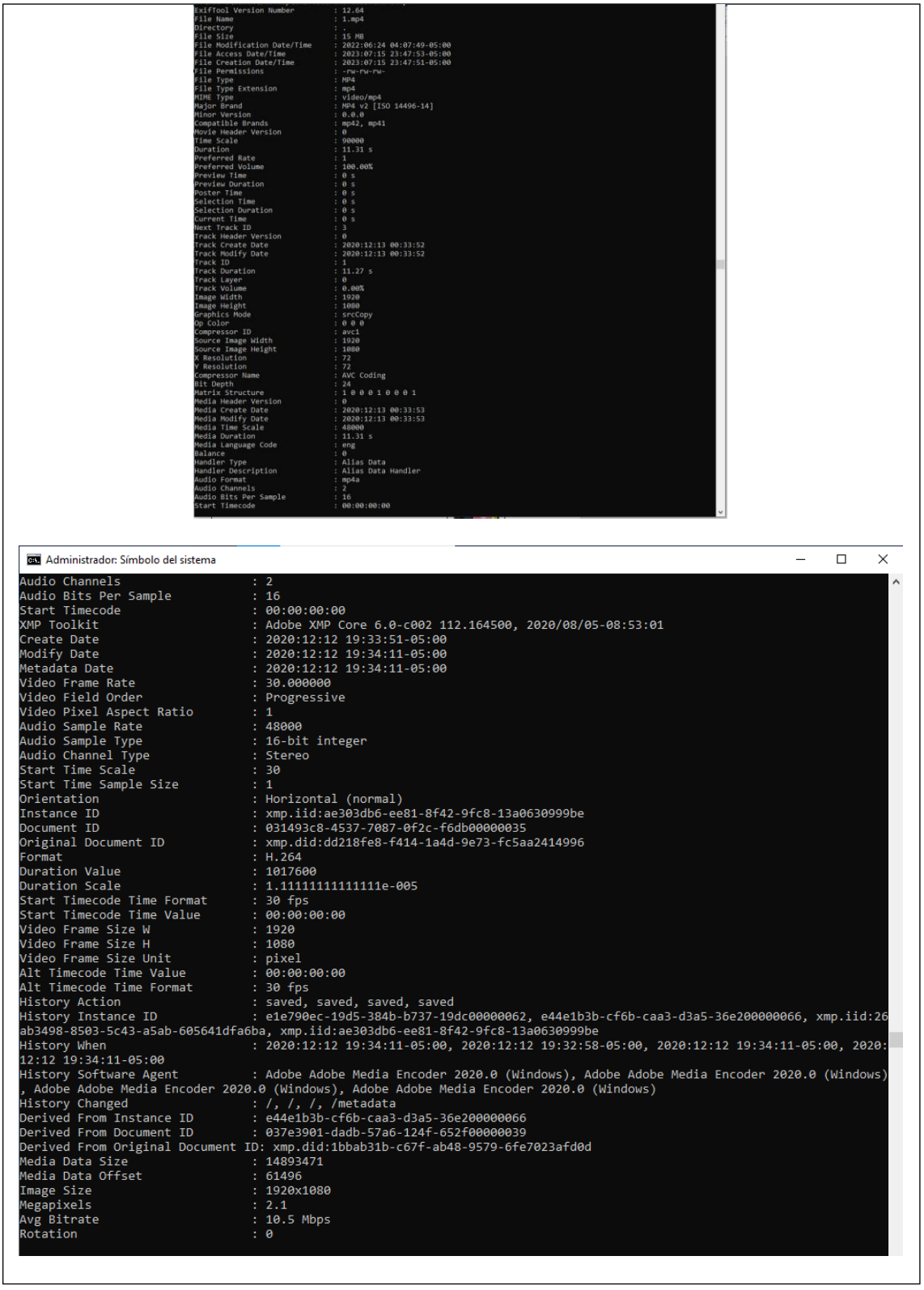
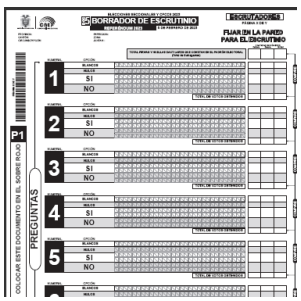
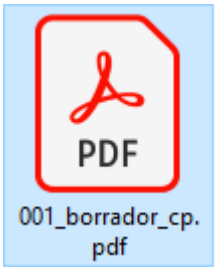


Tabla 26. Adquisición de información de archivo mp4

	Universidad Estatal Península de Santa Elena **Facultad de Sistemas y Telecomunicaciones** **Carrera de Tecnologías de la Información**	

INFORME DE EXTRACCION	
Dispositivo	Samsung Galaxy A03s
Fecha	11/07/2023
Responsable:	ALEJANDRO ALEJANDRO ERICK JESÚS
Medio	CMD Windows 10 exiftool
Tipo de extracción	Extracción de metadatos
Objetivos:	Adquirir información de un archivo PDF
Archivo:	 
Pruebas:	

Administrador: Símbolo del sistema

```
ExifTool Version Number         : 12.64
File Name                       : 001_borrador_cp.pdf
Directory                       : .
File Size                       : 1178 kB
File Modification Date/Time     : 2023:01:18 18:31:44-05:00
File Access Date/Time           : 2023:07:15 23:48:23-05:00
File Creation Date/Time         : 2023:07:15 23:47:33-05:00
File Permissions                : -rw-rw-rw-
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.6
Linearized                      : No
XMP Toolkit                     : Adobe XMP Core 6.0-c002 79.164460, 2020/05/12-16:04:17
Format                          : application/pdf
Title                           : 001_borrador_cp
Metadata Date                   : 2022:12:02 10:55:14-05:00
Modify Date                     : 2022:12:02 10:55:14-05:00
Create Date                     : 2022:12:02 10:55:14-05:00
Creator Tool                    : Adobe Illustrator 24.2 (Macintosh)
Thumbnail Width                 : 184
Thumbnail Height                : 256
Thumbnail Format                : JPEG
Thumbnail Image                 : (Binary data 19778 bytes, use -b option to extract)
Instance ID                     : uuid:38501177-7dd0-2942-9f57-4b6d1b8c8036
Document ID                     : xmp.did:9f6b2dba-2001-459f-86fa-782c4fac72f6
Original Document ID            : uuid:5D20892493BFDB11914A8590D31508C8
Rendition Class                 : proof:pdf
Derived From Instance ID        : uuid:361c26b0-7255-1d43-a886-38b695dc0ced
Derived From Document ID        : xmp.did:d722ee4f-9610-495a-aeea-4c5259c141e1
Derived From Original Document ID: uuid:5D20892493BFDB11914A8590D31508C8
Derived From Rendition Class    : proof:pdf
History Action                  : saved, saved
History Instance ID             : xmp.iid:0580117407206811822A922E281F5EF0, xmp.iid:9f6b2dba-2001-459f-86fa-782c4fac72f6
History When                    : 2016:03:17 09:57:15-05:00, 2022:12:02 10:55:10-05:00
History Software Agent          : Adobe Illustrator CS6 (Macintosh), Adobe Illustrator 24.2 (Macintosh)
History Changed                 : /, /
Manifest Link Form              : EmbedByReference, EmbedByReference
Manifest Reference File Path    : ECU MAGENTA.jpg, ECU CYAN.jpg
Ingredients File Path           : ECU MAGENTA.jpg, ECU CYAN.jpg
Startup Profile                 : Print
Creator Sub Tool                : Adobe Illustrator
Has Visible Overprint           : True
Has Visible Transparency        : False
N Pages                         : 1
Max Page Size W                 : 42.000000
Max Page Size H                 : 59.400000
Max Page Size Unit              : Centimeters
Font Name                       : Arial-BoldMT, ArialMT
Font Family                     : Arial, Arial
Font Face                       : Bold, Regular
Font Type                       : Open Type, Open Type
Font Version                    : Version 5.01.2x, Version 5.01.2x
Font Composite                  : False, False
Font File Name                  : Arial Bold.ttf, Arial.ttf
Plate Names                     : Cyan, Magenta, Yellow, Black
Swatch Group Name               : Grupo de muestras por defecto, Grises, Brillantes
Swatch Group Type               : 0, 1, 1
Swatch Colorant Swatch Name     : Blanco, Negro, Rojo CMYK, Amarillo CMYK, Verde CMYK, Cian CMYK, Azul CMYK, Magenta CMYK, C=15 M=100 Y=90 K=10, C=0 M=90
 Y=85 K=0, C=0 M=80 Y=95 K=0, C=0 M=50 Y=100 K=0, C=0 M=35 Y=85 K=0, C=5 M=0 Y=90 K=0, C=20 M=0 Y=100 K=0, C=50 M=0 Y=100 K=0, C=75 M=0 Y=100 K=0, C=85 M
```

Administrador: Símbolo del sistema

```
Font Name                       : Arial-BoldMT, ArialMT
Font Family                     : Arial, Arial
Font Face                       : Bold, Regular
Font Type                       : Open Type, Open Type
Font Version                    : Version 5.01.2x, Version 5.01.2x
Font Composite                  : False, False
Font File Name                  : Arial Bold.ttf, Arial.ttf
Plate Names                     : Cyan, Magenta, Yellow, Black
Swatch Group Name               : Grupo de muestras por defecto, Grises, Brillantes
Swatch Group Type               : 0, 1, 1
Swatch Colorant Swatch Name     : Blanco, Negro, Rojo CMYK, Amarillo CMYK, Verde CMYK, Cian CMYK, Azul CMYK, Magenta CMYK, C=15 M=100 Y=90 K=10, C=0 M=90
 Y=85 K=0, C=0 M=80 Y=95 K=0, C=0 M=50 Y=100 K=0, C=0 M=35 Y=85 K=0, C=5 M=0 Y=90 K=0, C=20 M=0 Y=100 K=0, C=50 M=0 Y=100 K=0, C=75 M=0 Y=100 K=0, C=85 M
=10 Y=100 K=10, C=90 M=30 Y=95 K=30, C=75 M=0 Y=75 K=0, C=80 M=10 Y=45 K=0, C=70 M=15 Y=0 K=0, C=85 M=50 Y=0 K=0, C=100 M=95 Y=5 K=0, C=100 M=100 Y=25 K=
25, C=75 M=100 Y=0 K=0, C=50 M=100 Y=0 K=0, C=35 M=100 Y=35 K=10, C=10 M=100 Y=50 K=0, C=0 M=95 Y=20 K=0, C=25 M=25 Y=40 K=0, C=40 M=45 Y=50 K=5, C=50 M=
50 Y=60 K=25, C=55 M=60 Y=65 K=40, C=25 M=40 Y=65 K=0, C=30 M=50 Y=75 K=10, C=35 M=60 Y=80 K=25, C=40 M=65 Y=90 K=35, C=40 M=70 Y=100 K=50, C=50 M=70 Y=8
0 K=70, PANTONE P 48-8 U, PANTONE P 109-8 U, PANTONE P 179-3 U, PANTONE P 179-2 U, C=0 M=0 Y=0 K=100, C=0 M=0 Y=0 K=90, C=0 M=0 Y=0 K=80, C=0 M=0 Y=0 K=7
0, C=0 M=0 Y=0 K=60, C=0 M=0 Y=0 K=50, C=0 M=0 Y=0 K=40, C=0 M=0 Y=0 K=30, C=0 M=0 Y=0 K=20, C=0 M=0 Y=0 K=10, C=0 M=0 Y=0 K=5, C=0 M=100 Y=100 K=0, C=0
M=75 Y=100 K=0, C=0 M=10 Y=95 K=0, C=85 M=10 Y=100 K=0, C=100 M=90 Y=0 K=0, C=60 M=90 Y=0 K=0
Swatch Colorant Mode            : CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK,
 CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CM
YK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK, CMYK
Swatch Colorant Type            : PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PR
OCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PR
OCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PR
OCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS, PROCESS
Swatch Colorant Cyan            : 0.000000, 0.000000, 0.000000, 0.000000, 100.000000, 100.000000, 100.000000, 0.000000, 15.000000, 0.000000, 0.000000, 0.
000000, 0.000000, 5.000000, 20.000000, 50.000000, 75.000000, 85.000000, 90.000000, 75.000000, 80.000000, 70.000000, 85.000000, 100.000000, 100.000000, 75
.000000, 50.000000, 35.000000, 10.000000, 0.000000, 25.000000, 40.000000, 50.000000, 55.000000, 25.000000, 30.000000, 35.000000, 40.000000, 40.000000, 50
.000000, 0.000000, 100.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.
000000, 0.000000, 0.000000, 0.000000, 85.000000, 100.000000, 60.000000
Swatch Colorant Magenta         : 0.000000, 0.000000, 100.000000, 0.000000, 0.000000, 0.000000, 100.000000, 100.000000, 100.000000, 90.000000, 80.000000,
 50.000000, 35.000000, 0.000000, 0.000000, 0.000000, 0.000000, 10.000000, 30.000000, 0.000000, 10.000000, 15.000000, 50.000000, 95.000000, 100.000000, 10
0.000000, 100.000000, 100.000000, 100.000000, 95.000000, 25.000000, 45.000000, 50.000000, 60.000000, 40.000000, 50.000000, 60.000000, 65.000000, 70.00000
0, 70.000000, 99.000001, 34.999999, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.00000
0, 0.000000, 100.000000, 75.000000, 10.000000, 10.000000, 90.000000, 90.000000
Swatch Colorant Yellow          : 0.000000, 0.000000, 100.000000, 100.000000, 100.000000, 0.000000, 0.000000, 0.000000, 90.000000, 85.000000, 95.000000,
100.000000, 85.000000, 90.000000, 100.000000, 100.000000, 100.000000, 100.000000, 95.000000, 75.000000, 45.000000, 0.000000, 0.000000, 5.000000, 25.00000
0, 0.000000, 0.000000, 35.000000, 50.000000, 20.000000, 40.000000, 50.000000, 60.000000, 65.000000, 65.000000, 75.000000, 80.000000, 90.000000, 100.00000
0, 80.000000, 91.000003, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000
, 0.000000, 100.000000, 100.000000, 95.000000, 100.000000, 0.000000, 0.003100
Swatch Colorant Black           : 0.000000, 100.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 10.000000, 0.000000, 0.000000, 0.0000
00, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 10.000000, 30.000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.000000, 25.000000, 0.000000, 0.0000
00, 10.000000, 0.000000, 0.000000, 0.000000, 5.000000, 25.000000, 40.000000, 0.000000, 10.000000, 25.000000, 35.000000, 50.000000, 70.000000, 0.000000, 0
.000000, 20.000000, 11.000000, 100.000000, 89.999400, 79.998800, 69.999700, 59.999100, 50.000000, 39.999400, 29.998800, 19.999700, 9.999100, 4.998800, 0.
000000, 0.000000, 0.000000, 0.000000, 0.000000, 0.003100
Swatch Colorant Tint            : 100.000000, 100.000000, 100.000000, 100.000000
Producer                        : Adobe PDF library 15.00
Page Count                      : 1
Creator                         : Adobe Illustrator(R) 24.0
AI Creator Version              : 24.2.3
For                             : bayardo,
Bounding Box                    : -281 -1212 885 411
AI Build Number                 : 521
AI Color Usage                  : Color
AI Ruler Units                  : Centimeters
AI Color Model                  : CMYK
AI Target Resolution            : 800
AI Num Layers                   : 1
Container Version               : 12
Creator Version                 : 24
```

Tabla 27. Adquisición de información de archivo PDF

UPSE	**Universidad Estatal Península de Santa Elena** **Facultad de Sistemas y Telecomunicaciones** **Carrera de Tecnologías de la Información**	

INFORME DE EXTRACCION	
Dispositivo	Samsung Galaxy A03s
Fecha	11/07/2023
Responsable:	ALEJANDRO ALEJANDRO ERICK JESÚS
Medio	CMD Windows 10 exiftool
Tipo de extracción	Extracción de metadatos
Objetivos:	Adquirir información de un archivo PPTX

Archivo:

Pruebas:

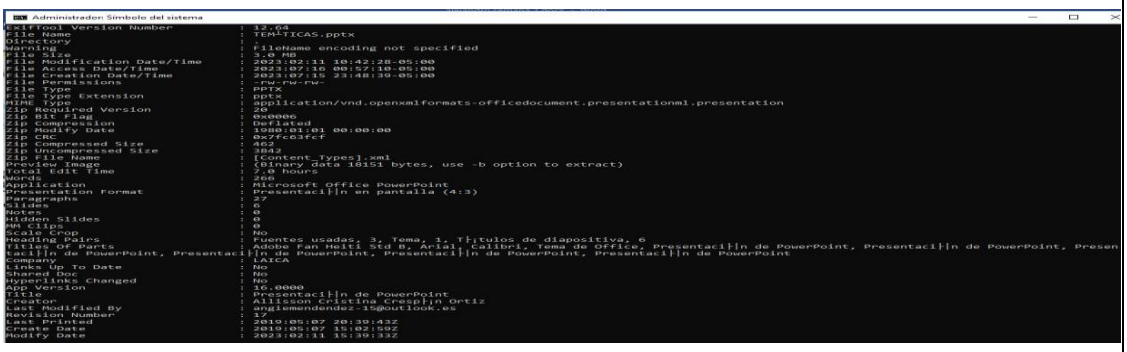


Tabla 28. Adquisición de información de archivo PPTX

Anexo 13. Análisis Meterpreter

METERPRETER

Meterpreter es una carga útil que permite la realización de tareas de forma remota en una computadora, siendo un software que se ejecuta a un nivel de máquina muy bajo, por lo que es difícil de detectar; Con la carga útil de Meterpreter, es posible conectarse a la cámara web y al teclado de la computadora infectada y tomar capturas de pantalla. Sin embargo, es importante recordar que el software no funciona igual en todos los sistemas operativos, ya que, la versión más completa de este programa es para Windows [9].

Extracción de datos en WhatsApp con Meterpreter

Como bien se ha sabido, en los dispositivos móviles la extracción de datos es un método que genera complicaciones al momento de tratar de manipularla, debido a esto, existen herramientas especializadas para su exportación a un equipo informático, esta información también se encuentra debidamente oculta haciendo que a simple vista no se pueda encontrar, Meterpreter ayudará a ejecutar esta información y con el proceso debido de su traslado en un ambiente Linux.

Una vez ejecutado el Meterpreter, se podrá acceder al equipo y las raíces para interpretar carpetas ocultas, de tal manera que, con este método pasa los permisos para poder ver esta misma información.

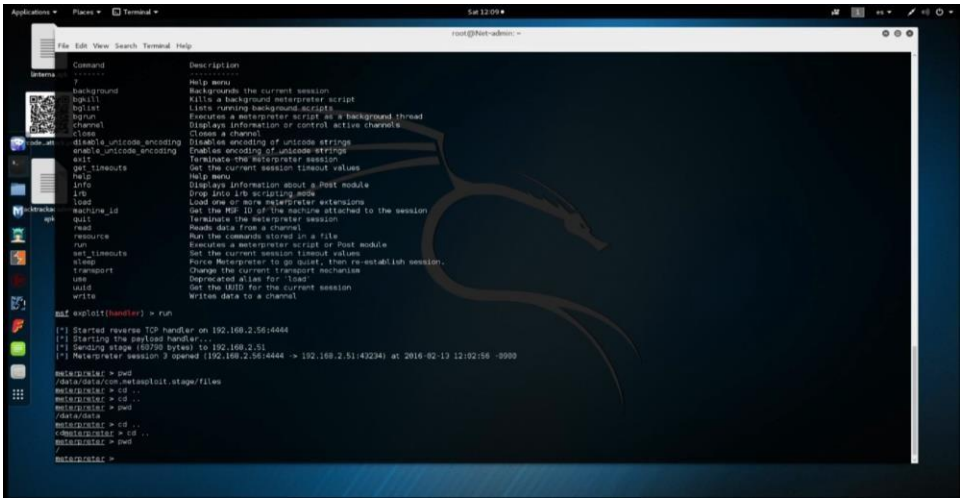


Figura 98. Ejecutar Meterpreter

Al entrar al equipo, podemos usar un código LS para ver la información del mismo.

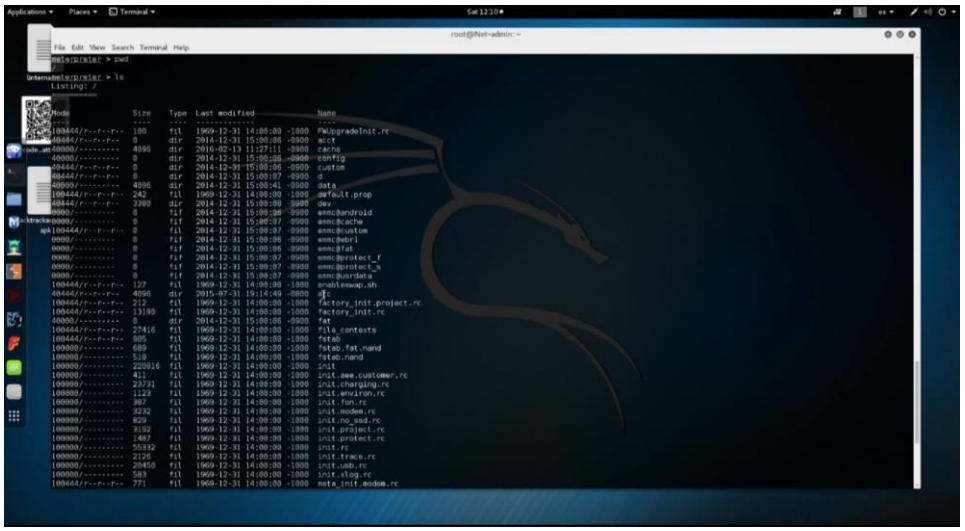


Figura 99. Código LS

Según las raíces de este tipo de tecnología, se basa en guardar la información Android en el apartado del Sdcard para hacer las indagaciones debidas.

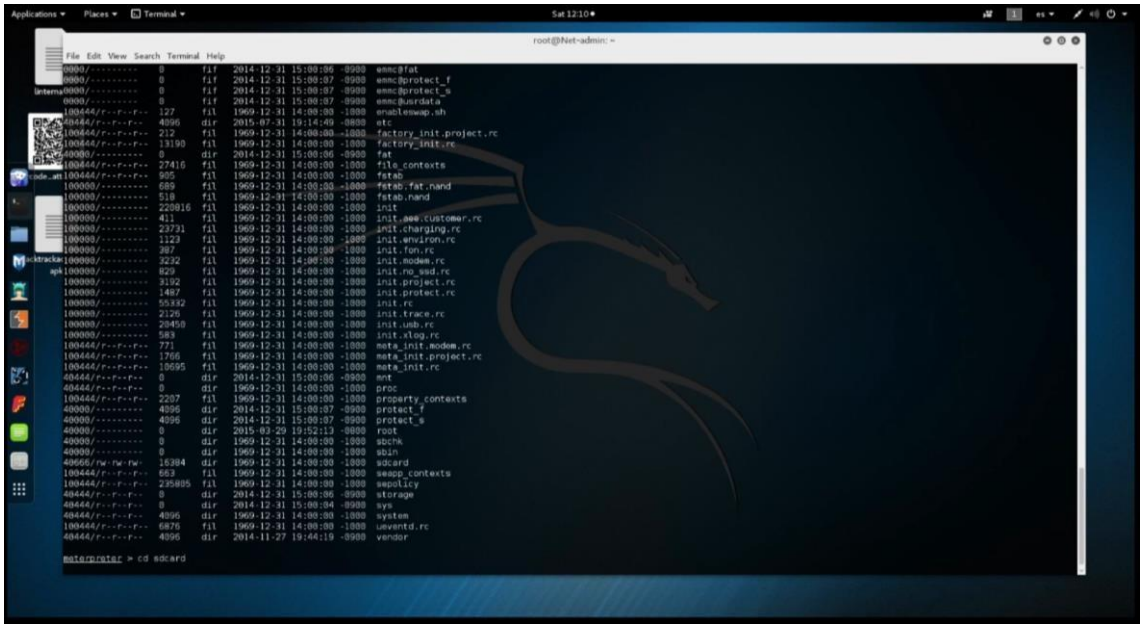


Figura 100. Guardar información Android

En este apartado, también se recomienda brindar un LS para su debida visualización de la información, aquí ya se pueden ver las aplicaciones, algunas desconocidas como conocidas, por ejemplo, WhatsApp.

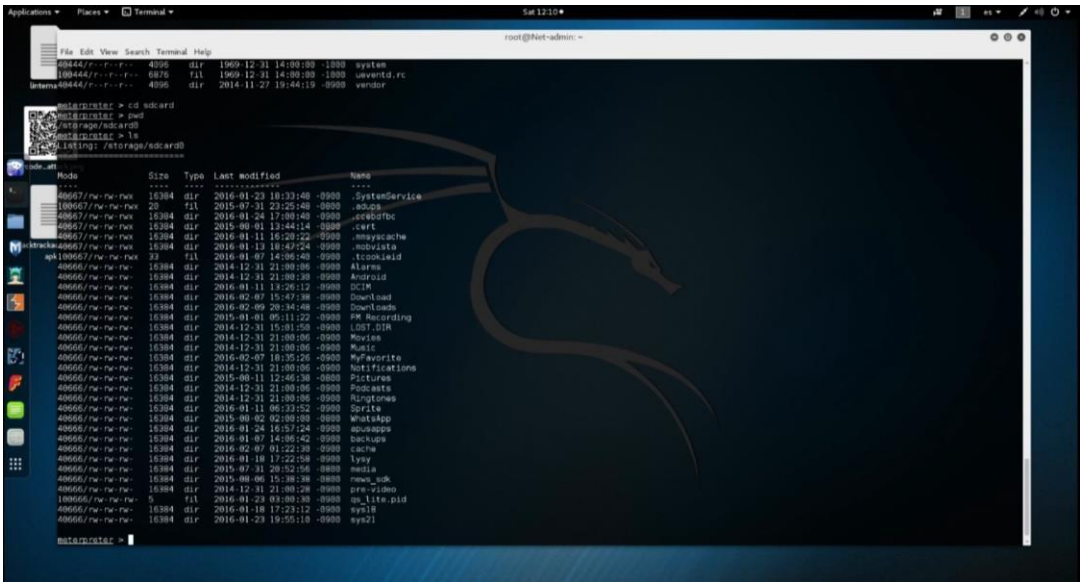


Figura 101. Brindar LS

Siguiendo el protocolo que se brindó en la documentación, las aplicaciones almacenan su información oculta en carpetas como Lost, pero principalmente en la carpeta DCIM, la cual es la que indagaremos en este trabajo.

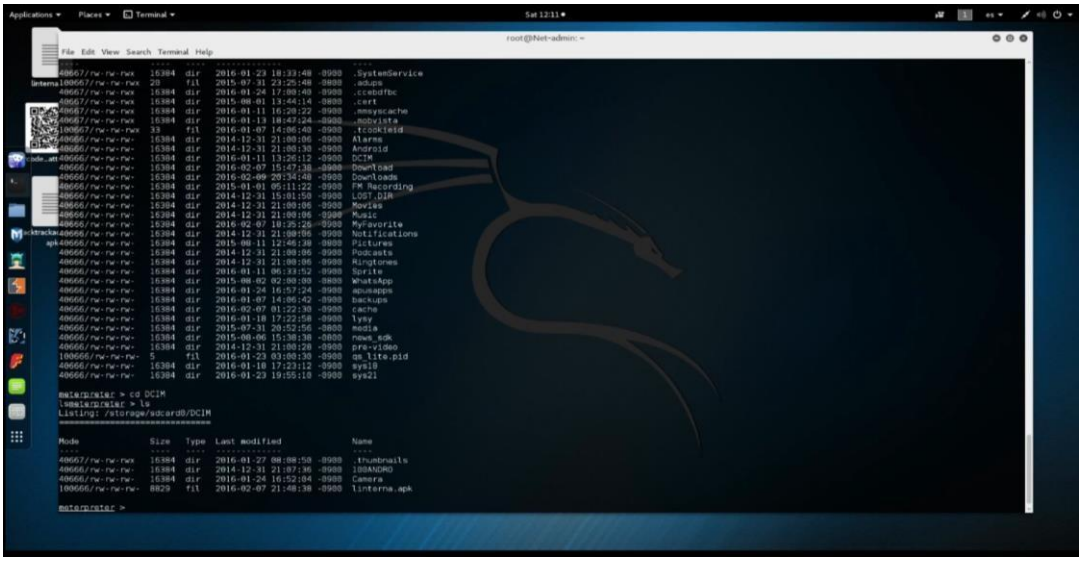


Figura 102. Almacenamiento de información oculta

Accediendo a este espacio, ya se pueden visualizar archivos, tales como: thumbmails, 180Andro, Camera y la linterna; para realizar un pequeño ejemplo, se ingresará a la parte

de la camera para ver qué información nos arroja, en esta situación mostró imágenes tomadas por la cámara.

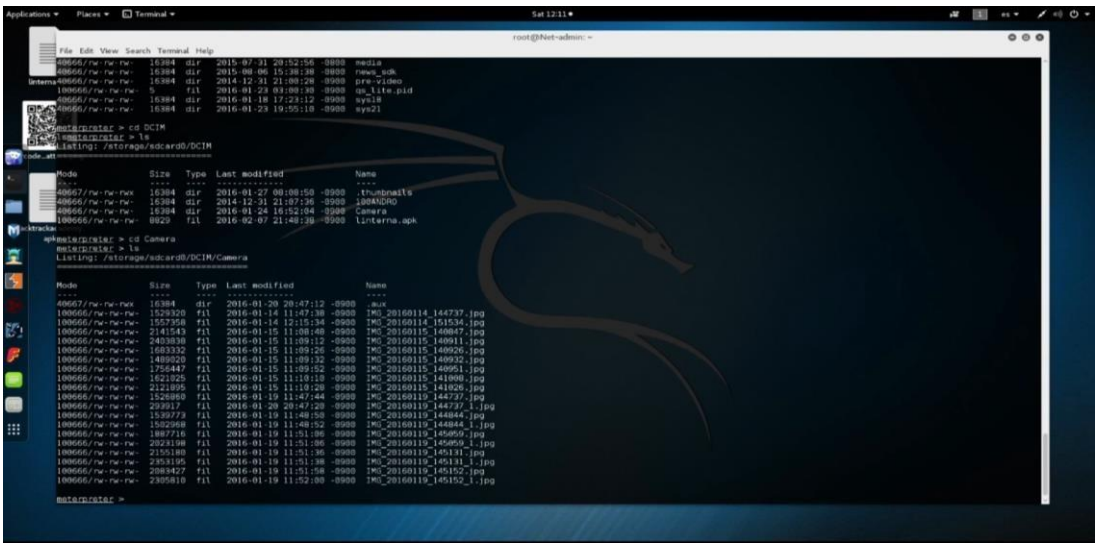


Figura 103. Visualización de archivos

Una vez ubicados estos archivos, se procederá a realizar una copia mediante descarga usando un código en general: download/storage/sdcard0/DCIM/Camera/(nombre del archivo).

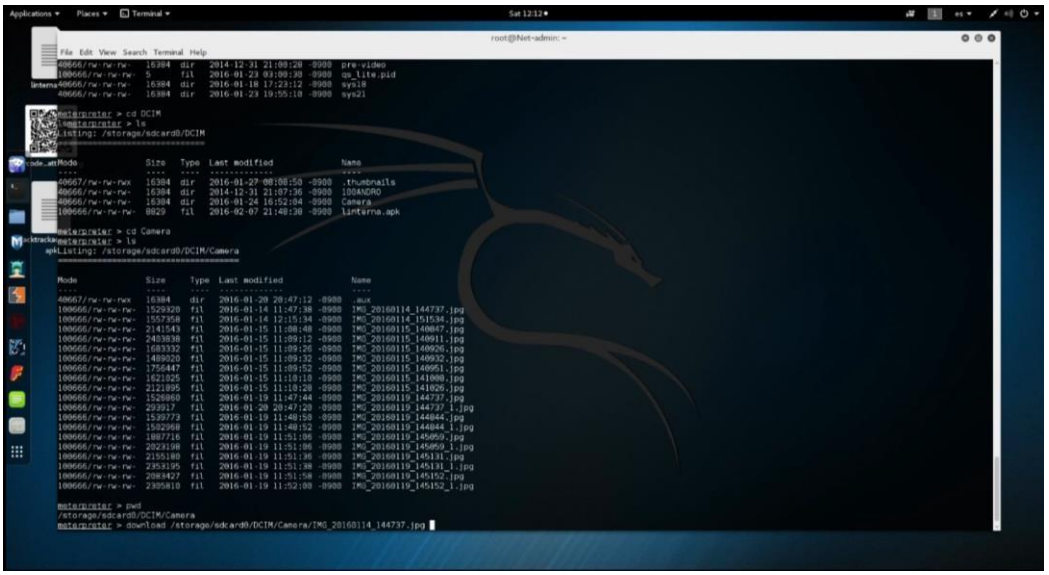


Figura 104. Realización de copia

Se debe por recomendación tratar de mantener el equipo cargado al tope para no presentar fallas de conectividad al momento del traslado.

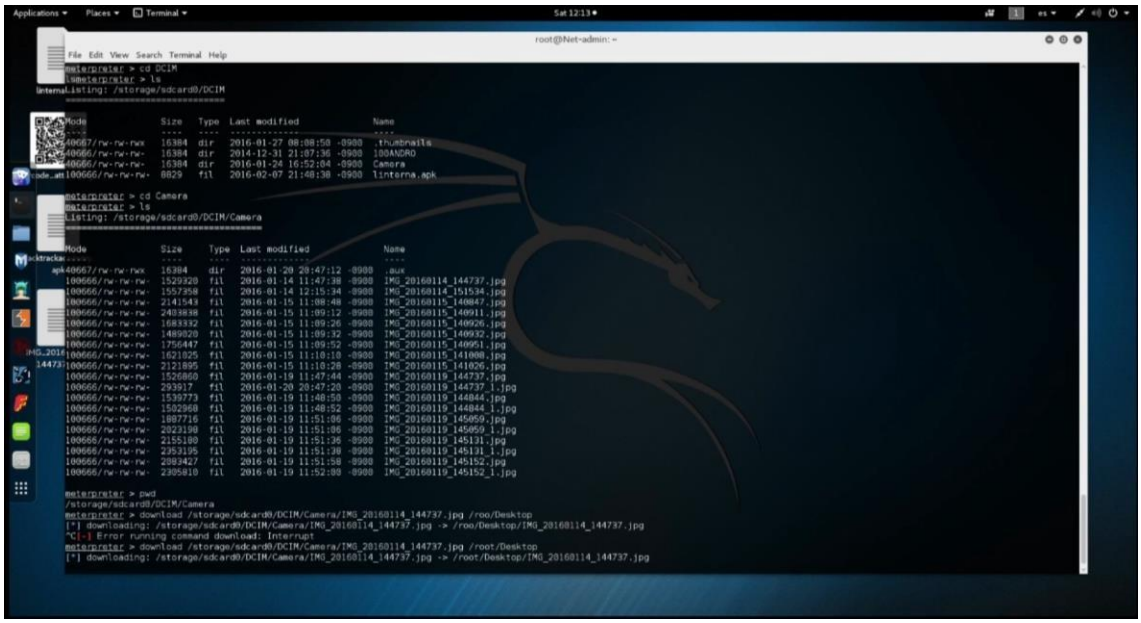


Figura 105. Mantener el equipo cargado

En teoría, se realiza este proceso para las diferentes aplicaciones que interactúan con el dispositivo; En esta parte se utilizará WhatsApp, por ser una herramienta de redes sociales con varias seguridades.

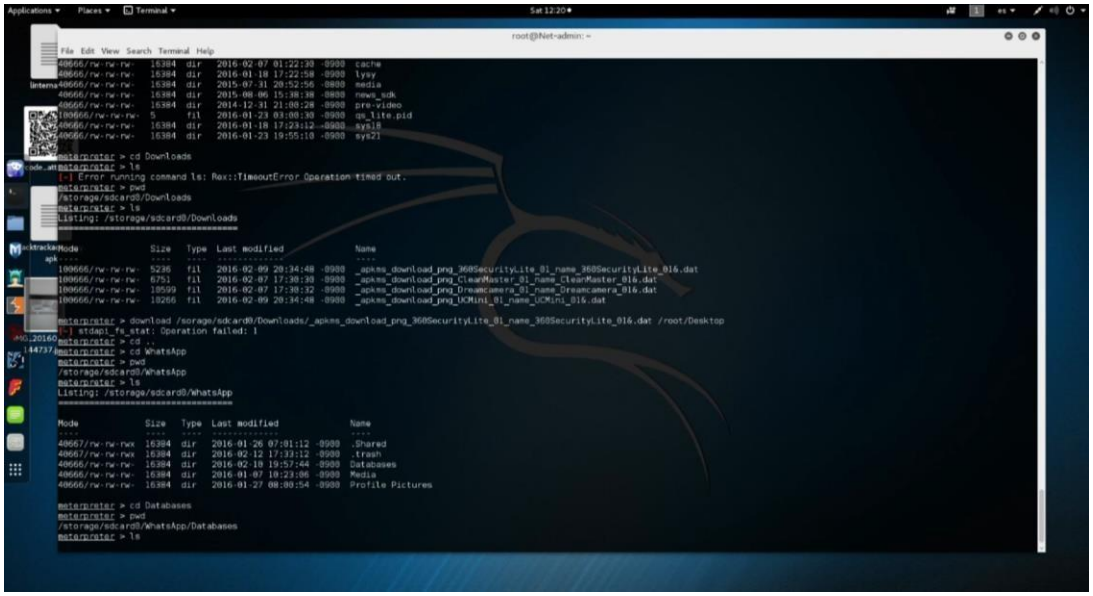


Figura 106. WhatsApp

Al ver la información que contiene este aplicativo, se encontró la carpeta de la base de datos (Databases), en la cual se identifican 3 archivos encriptados bajo la extensión. crypt8.

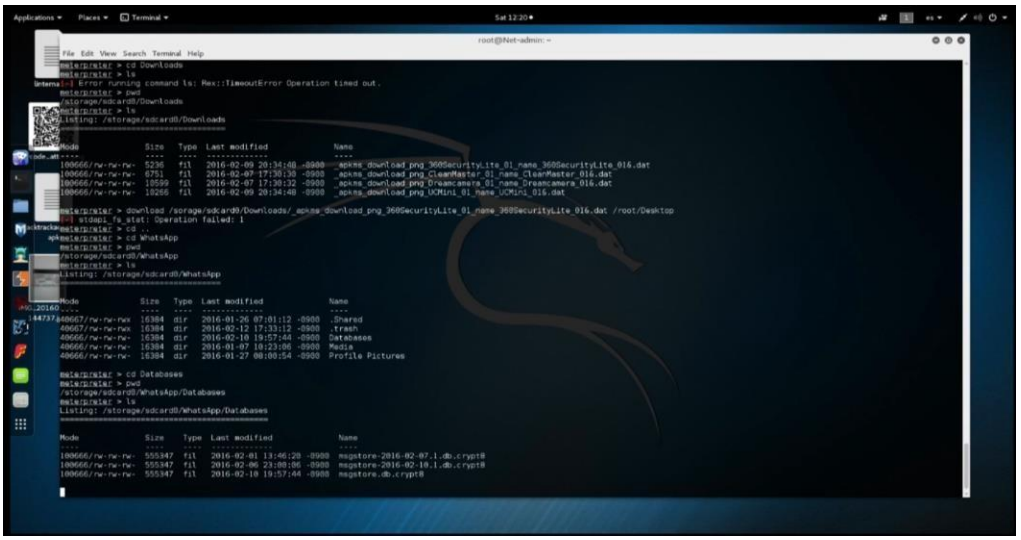


Figura 107. Carpeta de la base de datos

Una vez hallados estos archivos, se realiza el mismo proceso para el copiado en la PC, obteniendo el resultado esperado en este análisis de vulnerabilidad forense; estos datos se podrán desencriptar en páginas especializadas a este fin brindando un historial de chat.

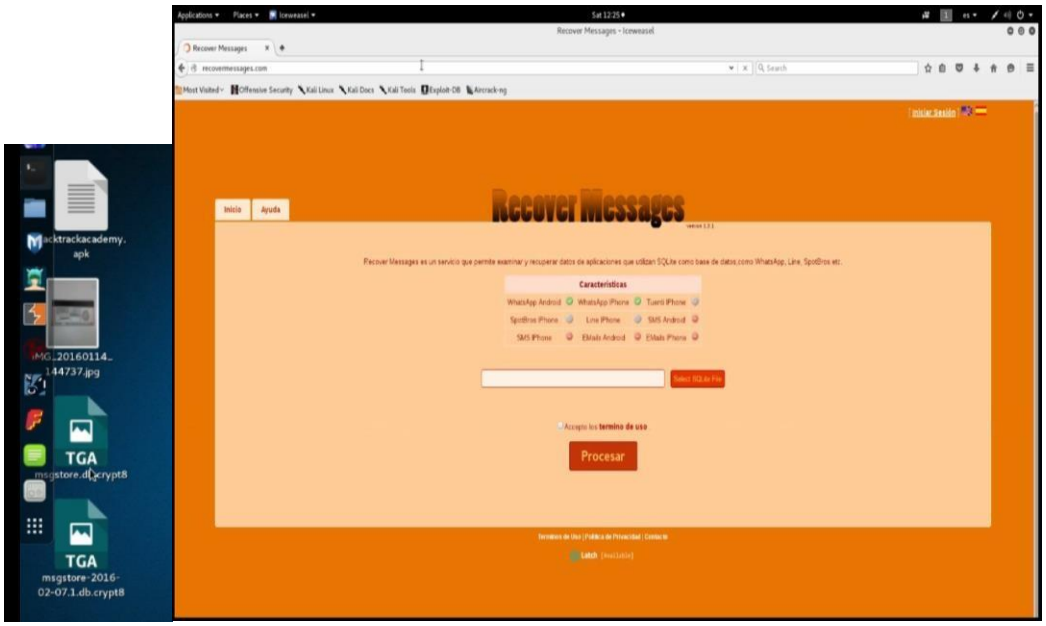


Figura 108. Copia en la PC

Extracción de datos en Dropbox con Meterpreter

Dropbox es una plataforma de colaboración y almacenamiento de archivos en línea que brinda a los usuarios una forma conveniente y segura de almacenar, compartir y acceder a documentos, fotos, videos y otro contenido digital. Es una solución de almacenamiento en la nube que se sincroniza en todos sus dispositivos (laptops, computadoras de escritorio, tabletas, teléfonos), para que pueda acceder a su contenido desde cualquier lugar. Dropbox también ofrece funciones avanzadas, como colaboración en equipo, control de versiones, eliminación remota y varias medidas de seguridad para garantizar que sus datos estén siempre seguros.

Entre los datos relacionados que se pueden extraer desde el equipo móvil en esta aplicación, son datos ocultos que quedan como una firma de datos para información oculta que se encuentra internamente en la base de datos de la misma.

Para ver la carpeta que se aloja en el Dropbox, se ingresa a la parte denominada com.dropbox.android para extraer la información, estas acciones dan como resultado tres archivos asset_cache, cache y files.

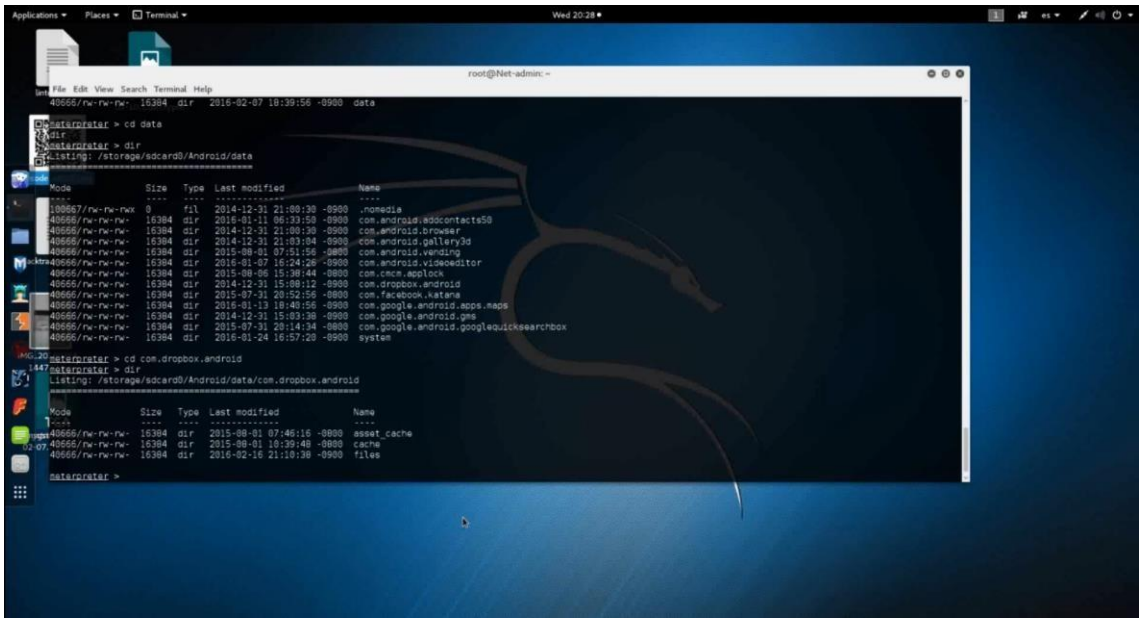


Figura 109. Extracción de datos en Dropbox

Se pudo visualizar la información de la carpeta files, en la cual se pudo extraer datos, como: imagen y 3 archivos ocultos.

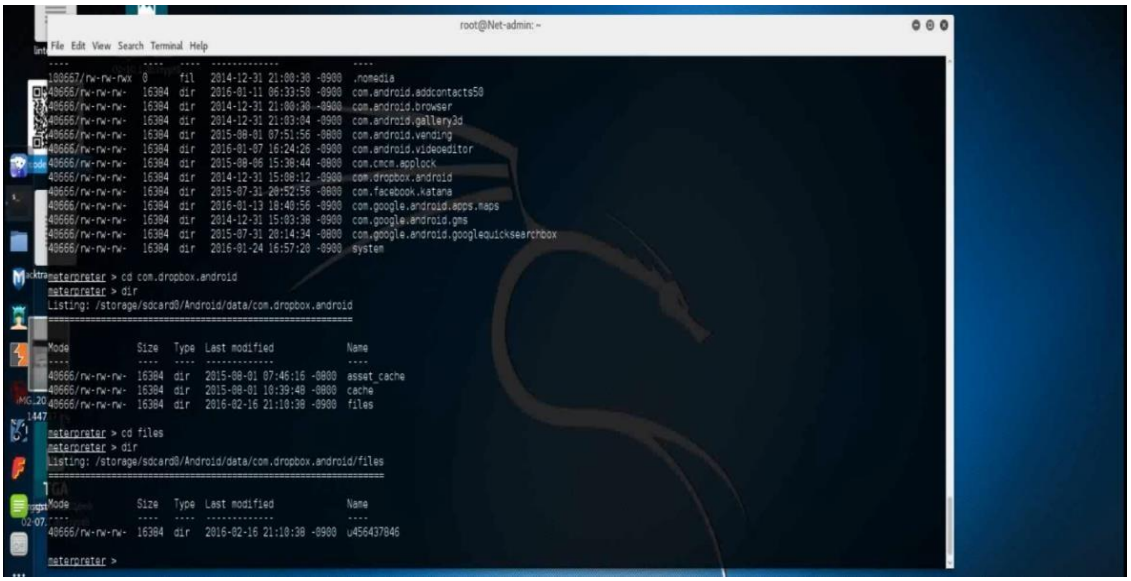


Figura 110. Visualizar información de carpeta files

Los archivos encontrados fueron un documento de PowerPoint, un documento de Word y una imagen en formato png.

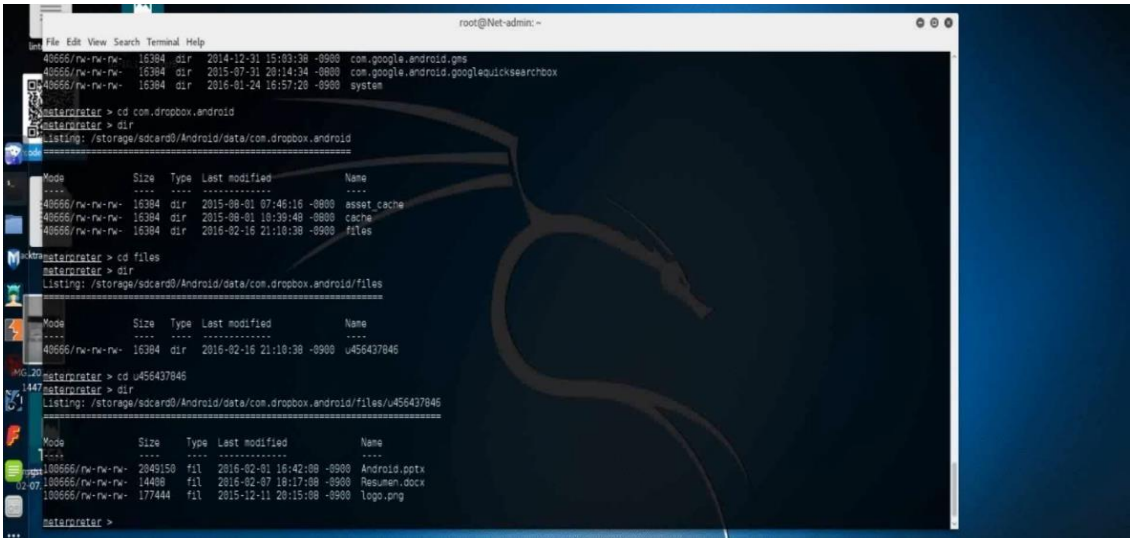


Figura 111: Archivos hallados

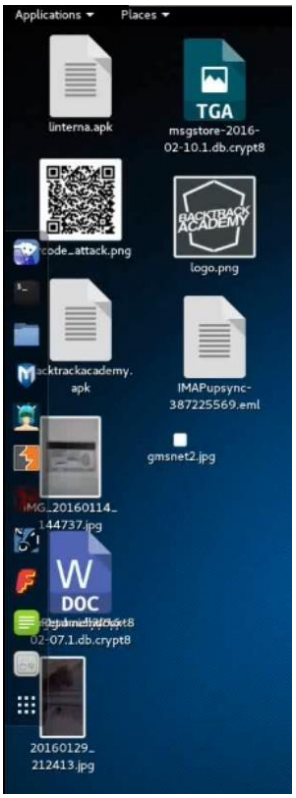


Figura 112. Archivos encontrados

Reporte referente al tercer ataque de extracción de información

UPSE	**Universidad Estatal Península de Santa Elena** **Facultad de Sistemas y Telecomunicaciones** **Carrera de Tecnologías de la Información**	
INFORME DE EXTRACCION		
Dispositivo	Samsung Galaxy A03s	
Fecha	28/07/2023	
Responsable:	ALEJANDRO ALEJANDRO ERICK JESÚS	
Medio	Terminal Kali Linux	

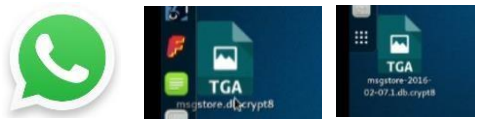
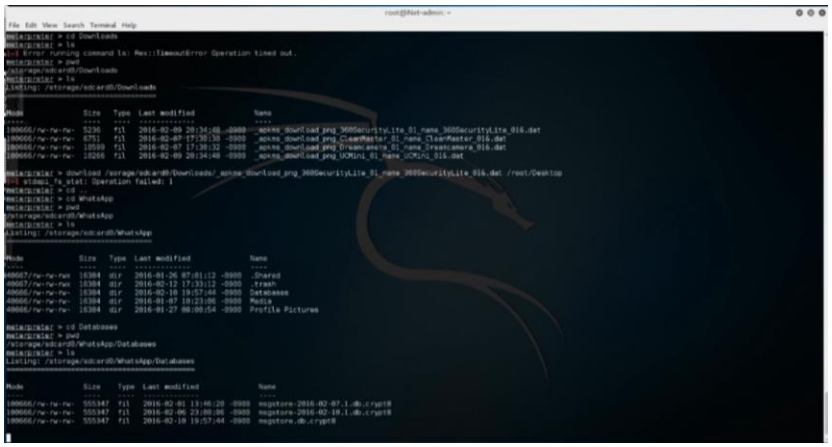
Tipo de extracción	Extracción de datos reservados en el root.
Objetivos:	Adquirir información de aplicativo WhatsApp
Archivo:	
Pruebas:	

Tabla 29. Adquisición de información encriptada de WhatsApp

UPSE	**Universidad Estatal Península de Santa Elena** **Facultad de Sistemas y Telecomunicaciones** **Carrera de Tecnologías de la Información**	
INFORME DE EXTRACCION		
Dispositivo	Samsung Galaxy A03s	
Fecha	28/07/2023	
Responsable:	ALEJANDRO ALEJANDRO ERICK JESÚS	

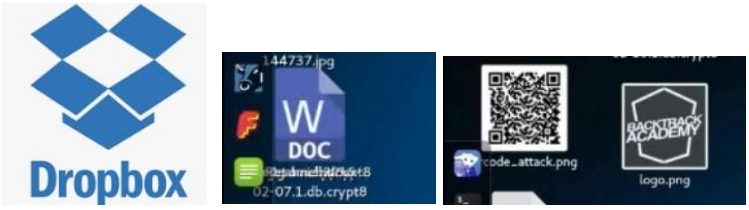
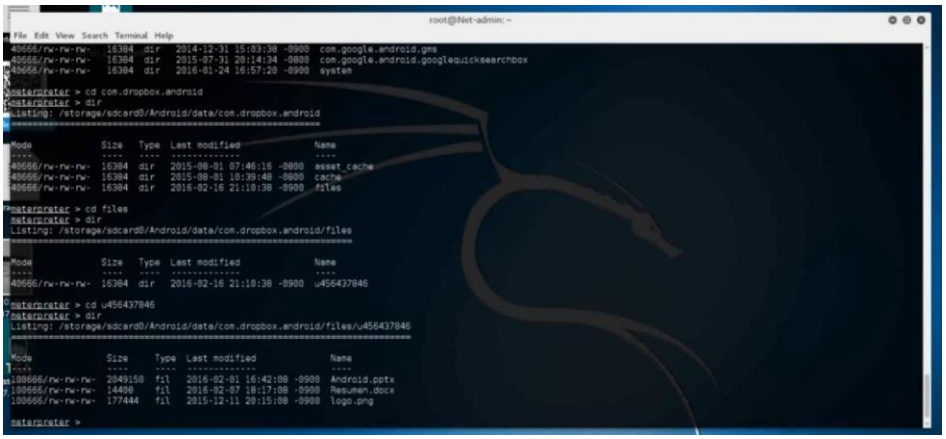
Medio	Terminal Kali Linux
Tipo de extracción	Extracción de datos reservados en el root.
Objetivos:	Adquirir información de aplicativo WhatsApp
Archivo:	
Pruebas:	

Tabla 30. Adquisición de información de Dropbox

Anexo 14. Reportes Generales

El uso generalizado de dispositivos móviles los ha convertido activamente en una herramienta más de nuestro trabajo, ya que a menudo alojan mensajes comerciales importantes o valiosos que, si se interceptan, pueden plantear graves problemas de seguridad.

Los siguientes informes generalizan los ataques realizados durante este estudio:

Ataque 1

HACKING ETICO			
REPORTE DE EVALUACIÓN DE VULNERABILIDADES EN DISPOSITIVOS MOVILES			
DATOS DEL EXPERIMENTO			
Título del experimento:	Extraccion de informacion	**Realizado por:**	Erick Alejandro
No. Prueba:	A-01	**Fecha inicio:**	13/7/2023
Tipo prueba:	Laboratorio	**Fecha fin:**	13/7/2023
DETALLES DEL EXPERIMENTO			
Objetivo del experimento:	Extraer informacion del dispositivo movil mediante SO	**Fase:**	Adquisición de evidencia
Nivel complejidad prueba:	Medio	**Tiempo ejecución:**	6 horas y 30 minutos
HERRAMIENTAS APLICADAS			
Hardware:	Computadora Celular	**Virtualización:**	Sentoku
Software:	SE hacking	**Redes:**	Enlace de datos
DISEÑO DEL EXPERIMENTO			
Procedimientos:		**Descripción del procedimiento:**	
1. Instalacion de SO 2. Proceso de creacion de la APK 3. Proceso de extracion 4. Pruebas		Anexo 1. Instalacion Anexo 2. Proceso Anexo 3. Puebas	
Resultados esperados:		**Resultados obtenidos:**	
1. Adquirir información del equipo CallLog Calls 2. Adquirir información del equipo Contactos 3. Adquirir información del equipo SMS		1. Adquirir información del equipo CallLog Calls 2. Adquirir información del equipo Contactos 3. Adquirir información del equipo SMS	
Conclusiones:			Validado ■ Invalidado □ No concluyente □
El sistema operativo que se utilizo para este trabajo tiene un limite de uso hacia ciertos dispositivos que en la actualidad estan en existenacia, ya que su ultima actualizacion trabaja hasta con Android 8 mediante este ataque se pudo capturar diversos datos del disipositivo el cual por medio de una apk que el sistema creo os permitio extraer mensajes, contactos , log e informacion correspondienta a las actividades interna del dispositivo en custodia			

Figura 113: Ataque 1

Ataque 2

HACKING ETICO			
REPORTE DE EVALUACIÓN DE VULNERABILIDADES EN DISPOSITIVOS MOVILES			
DATOS DEL EXPERIMENTO			
Título del experimento:	Extraccion de informacion	**Realizado por:**	Erick Alejandro
No. Prueba:	A-02	**Fecha inicio:**	18/7/2023
Tipo prueba:	Laboratorio	**Fecha fin:**	18/7/2023
DETALLES DEL EXPERIMENTO			
Objetivo del experimento:	Extraer informacion de metadatos de los archivos mediante programa	**Fase:**	Adquisición de evidencia metadatos
Nivel complejidad prueba:	Medio	**Tiempo ejecución:**	4 horas y 30 minutos
HERRAMIENTAS APLICADAS			
Hardware:	Computadora	**Virtualización:**	CMD
Software:	Exiftool	**Redes:**	Ninguno
DISEÑO DEL EXPERIMENTO			
Procedimientos:		**Descripción del procedimiento:**	
1. Instalacion del programa 4. Procedimientos y pruebas		Anexo 9. Instalacion Anexo 10. Pruebas	
Resultados esperados:		**Resultados obtenidos:**	
1. Adquirir diferentes archivos del dispositivo 2. Ejecutar los metadatos por CMD en exiftool 3. Analizar la informacion de los metadatos		1. Adquirir diferentes archivos del dispositivo 2. Ejecutar los metadatos por CMD en exiftool 3. Analizar la informacion de los metadatos	
Conclusiones:			Validado ■ Invalidado ☐ No concluyente ☐
En el analisis obtenidos de los metadatos adquirido se pudo analizar tres tipos de archivos JPG, MP4 y documentos demostrando que entre los archivos de video se realizaron diferentes ediciones y cambios mediante programas de codificacion y edicion de la familia Adobe. Entre los datos obtenidos en este ataque tambien se visuaizo varios combios en cierto aspecto tanto en imagenes como en video dando por entender que se pudo haber realizado montajes en los archivos para poder realizar algun robo o delito mediante delincuencia informatica.			

Figura 114: Ataque 2

Ataque 3

HACKING ETICO			
REPORTE DE EVALUACIÓN DE VULNERABILIDADES EN DISPOSITIVOS MOVILES			
DATOS DEL EXPERIMENTO			
Título del experimento:	Extraccion de informacion	**Realizado por:**	Erick Alejandro
No. Prueba:	A-03	**Fecha inicio:**	25/7/2023
Tipo prueba:	Laboratorio	**Fecha fin:**	25/7/2023
DETALLES DEL EXPERIMENTO			
Objetivo del experimento:	Extraer informacion de datos reservados en el root	**Fase:**	Adquirir información de aplicativo WhatsApp y dropbox
Nivel complejidad prueba:	Medio	**Tiempo ejecución:**	4 horas y 30 minutos
HERRAMIENTAS APLICADAS			
Hardware:	Computadora celular	**Virtualización:**	Kali Linux
Software:	Linux	**Redes:**	Ninguno
DISEÑO DEL EXPERIMENTO			
Procedimientos:		**Descripción del procedimiento:**	
1. Instalacion de SO 2. Proceso de extracion 3. Pruebas		Anexo 11. Instalacion Anexo 12. Proceso Anexo 13. Puebas	
Resultados esperados:		**Resultados obtenidos:**	
1. Adquirir información del WhatsApp - Dropbox 2. Extraer archivos requeridos 3. Analizar archivos		1. Adquirir información del WhatsApp - Dropbox 2. Extraer archivos requeridos 3. Analizar archivos	
Conclusiones:			Validado ■ Invalidado ☐ No concluyente ☐
extracion de datos mediante meterpreter para extraer datos resguardado por root en aplicaciones como whatsApp o Dropbox dando como resutados extracciones exitotas y guardando los archivos en el computador para luego ser analizados. En el aplicativo Whatsapp se pudo obtener informacion relevante como los archivos compactados de los historiales de chat y documentacion multimedia y en el Dropbox archivos relevantes a documentacion variada , audio y video.			

Figura 115: Ataque 3