UNIB.E

UNIVERSIDAD IBEROAMERICANA DEL ECUADOR

FACULTAD DE COMUNICACIÓN Y TIC'S

CARRERA: INGENIERÍA EN SOFTWARE

TÍTULO

PROPUESTA DE MARCO DE TRABAJO DE ANÁLISIS FORENSE DE DISPOSITIVOS MÓVILES: EVALUACIÓN Y CONTRASTE DE HERRAMIENTAS DE SOFTWARE LIBRE

Trabajo de integración curricular para la obtención del título de Ingeniería de Software

Autores:

Marlon Joel Flores Núñez

Erika Pamela Garzón Quimbiurco

Tutor:

Msc. Carpio Harry

Quito, Ecuador

Febrero, 2025

DECLARACIÓN DE AUTORÍA Y AUTORIZACIÓN PARA LA DIFUSIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

1. Yo, **Garzón Quimbiurco Erika Pamela,** declaro en forma libre y voluntaria, que los criterios emitidos en el presente Trabajo de Integración Curricular, titulado: **"Propuesta de marco de trabajo de análisis forense de dispositivos móviles: evaluación y contraste de herramientas de software libre",** previo a la obtención del título profesional de **Ingeniería de Software**, así como también los contenidos, ideas, análisis, conclusiones y propuestas son exclusiva responsabilidad de mi persona, como autor/a.

2. Declaro, igualmente, tener pleno conocimiento de la obligación que tiene la Universidad Iberoamericana del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT, en formato digital una copia del referido Trabajo de Integración Curricular para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública, respetando los derechos de autor.

3. Autorizo, finalmente, a la Universidad Iberoamericana del Ecuador a difundir a través del sitio web de la Biblioteca de la UNIB.E (Repositorio Digital Institucional), el referido Trabajo de Integración Curricular, respetando las políticas de propiedad intelectual de la Universidad Iberoamericana del Ecuador.

Quito, DM., a los 13 días del mes de febrero de 2025

_____

Erika Pamela Garzón Quimbiurco

1722708979

DECLARACIÓN DE AUTORÍA Y AUTORIZACIÓN PARA LA DIFUSIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

1. Yo, **Marlon Joel Flores Núñez,** declaro en forma libre y voluntaria, que los criterios emitidos en el presente Trabajo de Integración Curricular, titulado: **"Propuesta de marco de trabajo de análisis forense de dispositivos móviles: evaluación y contraste de herramientas de software libre",** previo a la obtención del título profesional de **Ingeniería de Software**, así como también los contenidos, ideas, análisis, conclusiones y propuestas son exclusiva responsabilidad de mi persona, como autor/a.

2. Declaro, igualmente, tener pleno conocimiento de la obligación que tiene la Universidad Iberoamericana del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT, en formato digital una copia del referido Trabajo de Integración Curricular para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública, respetando los derechos de autor.

3. Autorizo, finalmente, a la Universidad Iberoamericana del Ecuador a difundir a través del sitio web de la Biblioteca de la UNIB.E (Repositorio Digital Institucional), el referido Trabajo de Integración Curricular, respetando las políticas de propiedad intelectual de la Universidad Iberoamericana del Ecuador.

Quito, DM., a los 13 días del mes de febrero de 2025.

Marlon Joel Flores Núñez

1729157261

AUTORIZACIÓN DE PRESENTACIÓN FINAL DEL TRABAJO DE INTEGRACIÓN CURRICULAR POR PARTE DEL TUTOR

Msc. Sandino Jaramillo Cartagena

Director(a) de la Carrera de Software

Presente. -

Yo, **Harry Carpio, Msc,** Tutor del Trabajo de Integración Curricular realizado por los estudiantes **ERIKA PAMELA GARZÓN QUIMBIURCO** y **MARLON JOEL FLORES NÚÑEZ** de la carrera de **SOFTWARE** informo haber revisado el presente documento titulado **PROPUESTA DE MARCO DE TRABAJO DE ANÁLISIS FORENSE DE DISPOSITIVOS MÓVILES: EVALUACIÓN Y CONTRASTE DE HERRAMIENTAS DE SOFTWARE LIBRE** el mismo que se encuentra elaborado conforme a lo establecido en el Reglamento de Titulación y el Manual de Estilo de la Universidad Iberoamericana del Ecuador, UNIB.E de Quito, por lo tanto, autorizo la entrega del Trabajo de Integración Curricular a la Unidad de Titulación para la presentación final ante el tribunal evaluador.

Firmado electrónicamente por:
HARRY ALBERTO
CARPIO SALVATIERRA

Atentamente,

Msc. Harry Carpio

Tutor

ACTA DE APROBACIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

UNIB.E
UNIVERSIDAD IBEROAMERICANA DEL ECUADOR

ACTA DE APROBACIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Facultad: Ciencias Administrativas, Servicios, Comunicación y Tecnología

Carrera: Software

Modalidad: Híbrida

Nivel: 3er nivel de Grado

En el Distrito Metropolitano de Quito a los treinta y un días de marzo del 2025 a las 09h00 ante el Tribunal de Presentación Oral, se presentó la señorita: **FLORES NUÑEZ MARLON JOEL**, titular de la cédula de ciudadanía No. **1729157261** a rendir la evaluación oral del Trabajo de Integración Curricular: "**PROPUESTA DE MARCO DE TRABAJO DE ANÁLISIS FORENSE DE DISPOSITIVOS MÓVILES: EVALUACIÓN Y CONTRASTE DE HERRAMIENTAS DE SOFTWARE LIBRE.**", previo a la obtención del Título de Ingeniera en Software. Luego de la exposición, la referida estudiante obtiene las calificaciones que a continuación se detallan:

	Calificación
Lectura del Trabajo de Integración Curricular	8,6 **/10**
Evaluación Oral del Trabajo de Integración Curricular	9,8 **/10**
Calificación Final del Trabajo de Integración Curricular	9,2 **/10**

Para constancia de lo actuado, los miembros del Tribunal de Presentación Oral del Trabajo de Integración Curricular, firman el presente documento en unidad de acto, a los treinta y un días de marzo del 2025 (31-03-2025).

Mgst. Andrea Guadalupe
DIRECTOR ACADÉMICO

UNIB.E
DIRECCIÓN ACADÉMICA

Mgst. Sandino Jaramillo
DIRECTOR DE LA CARRERA DE SOFTWARE

UNIB.E
SECRETARÍA ACADÉMICA
GRADO

Mgst. Harry Carpio
TUTOR

Mgst. Byron Moreno
LECTOR

UNIB.E

UNIVERSIDAD IBEROAMERICANA DEL ECUADOR

ACTA DE APROBACIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Facultad: Ciencias Administrativas, Servicios, Comunicación y Tecnología

Carrera: Software

Modalidad: Híbrida

Nivel: 3er nivel de Grado

En el Distrito Metropolitano de Quito a los treinta y un días de marzo del 2025 a las 09h00 ante el Tribunal de Presentación Oral, se presentó la señorita: **GARZON QUIMBIURCO ERIKA PAMELA**, titular de la cédula de ciudadanía No. **1722708979** a rendir la evaluación oral del Trabajo de Integración Curricular: **"PROPUESTA DE MARCO DE TRABAJO DE ANÁLISIS FORENSE DE DISPOSITIVOS MÓVILES: EVALUACIÓN Y CONTRASTE DE HERRAMIENTAS DE SOFTWARE LIBRE.**", previo a la obtención del Título de Ingeniera en Software. Luego de la exposición, la referida estudiante obtiene las calificaciones que a continuación se detallan:

	Calificación
Lectura del Trabajo de Integración Curricular	8,6 /10
Evaluación Oral del Trabajo de Integración Curricular	9,7 /10
Calificación Final del Trabajo de Integración Curricular	9,2 /10

Para constancia de lo actuado, los miembros del Tribunal de Presentación Oral del Trabajo de Integración Curricular, firman el presente documento en unidad de acto, a los treinta y un días de marzo del 2025 (31-03-2025).

Mgst. Andrea Guadalupe
DIRECTOR ACADÉMICO

UNIB.E DIRECCIÓN ACADÉMICA

Mgst. Sandino Jaramillo
DIRECTOR DE LA CARRERA DE SOFTWARE

UNIB.E SECRETARÍA ACADÉMICA GRADO

Mgst. Harry Carpio
TUTOR

Mgst. Byron Moreno
LECTOR

DEDICATORIA

El presente trabajo de titulación, dedico principalmente a Dios, quien me ha otorgado la fuerza y la sabiduría necesaria para alcanzar esta meta.

A mis padres, quienes han estado en mis malos y buenos momentos siempre apoyándome. Gracias infinitas a mi madre que me enseñó a ser una mujer fuerte, trabajadora, perseverante y a luchar hasta cumplir cada meta que me proponga; sus consejos y palabras de motivación me han recordado que con determinación y esfuerzo todo es posible. Y a toda mi familia, que siempre ha estado a mi lado, brindándome su amor y respaldo constante.

A mi esposo, cuyo apoyo incondicional ha sido esencial en cada momento de este trayecto; dándome cada día el ánimo y el impulso necesario para salir adelante y cumplir este gran objetivo ya que ha sido mi compañero en todas las etapas tanto académicas como personales; su apoyo ha sido invaluable para superar cada desafío y alcanzar mis objetivos que lo veo reflejado en este gran momento.

Erika Garzón

DEDICATORIA

Dedico este trabajo a mi familia a mi Padre y hermano que siempre estuvieron apoyándome desde un principio en esta etapa de mi vida los amo gracias a sus consejos hoy soy lo que soy un profesional de la República del Ecuador.

Marlon Flores

AGRADECIMIENTO

Siempre estaré agradecida en primer lugar con Dios por su guía y bendiciones que me han permitido alcanzar cada uno de mis objetivos personales y académicos.

A mis padres, quienes desde siempre me han enseñado a perseverar y nunca rendirme; su amor y palabras han sido fundamentales para mí, y le agradezco a Dios por ser mis padres.

A mi esposo, gracias por su amor, paciencia y aliento durante este largo y exigente trayecto, ha sido el impulso y la fuerza que me ha ayudado a seguir adelante y culminar esta meta con éxito.

Mi más sincero agradecimiento a todas aquellas personas que han creído en mí, incluyendo a mi familia, compañeros y colegas, quienes han contribuido significativamente en mi carrera profesional. Gracias por su total apoyo, que ha sido crucial para no abandonar mis sueños y llegar hasta aquí.

Erika Garzón

AGRADECIMIENTO

Agradezco infinitamente a mi tutor el Ing. Harry Carpio, al Ing. Sandino Jaramillo porque siempre estuvieron guiándonos en nuestro proyecto, a la Universidad Iberoamericana del Ecuador donde realice mis estudios y me nutrió de conocimientos que me servirán en mi crecimiento profesional y a Dios que siempre ilumino mi camino.

Marlon Flores

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

Erika Pamela Garzón Quimbiurco y Marlon Joel Flores Núñez. ***PROPUESTA DE MARCO DE TRABAJO DE ANÁLISIS FORENSE DE DISPOSITIVOS MÓVILES: EVALUACIÓN Y CONTRASTE DE HERRAMIENTAS DE SOFTWARE LIBRE.*** Carrera Ingeniería de Software. Universidad Iberoamericana del Ecuador. Quito Ecuador. 2025.

Resumen

El presente trabajo de titulación destaca la importancia de establecer un marco de trabajo estructurado para el análisis forense de dispositivos móviles utilizando herramientas de software libre, respondiendo a la creciente necesidad de métodos accesibles y eficaces para la adquisición, procesamiento y análisis de evidencia digital. A través de una revisión documental de 19 estudios científicos y técnicos, se identificaron herramientas clave y se evaluó su efectividad en comparación con soluciones comerciales. Esta investigación adoptó un enfoque cuantitativo, con un diseño no experimental de tipo documental y alcance exploratorio-descriptivo, utilizando fichas de análisis documental para la recolección de datos. A partir de este análisis, se diseñó un marco de trabajo forense basado en estándares como DFRWS e ISO/IEC 27037, integrando herramientas como CSI Linux, Magnet Acquire y Autopsy en un flujo de trabajo replicable y adaptable a distintos contextos forenses. Para validar su eficacia, el marco fue sometido a pruebas de concepto en entornos controlados, evidenciando su capacidad para extraer, analizar y presentar evidencia digital de manera confiable. Los resultados demostraron que las herramientas de software libre pueden ofrecer un desempeño comparable al de soluciones comerciales, siempre que los profesionales cuenten con la capacitación adecuada

Palabras Clave: Análisis forense, software libre, dispositivos móviles, Android, iOS.

INTRODUCCIÓN

Esta tesis, aborda de manera integral los aspectos teóricos, metodológicos y prácticos del análisis forense en dispositivos móviles, destacando la importancia de soluciones de software libre en este campo. Desde un enfoque cuantitativo, con un diseño no experimental, de nivel descriptivo y de tipo documental, se recopila información de fuentes secundarias como libros, artículos científicos, tesis y reportes técnicos. Para garantizar un análisis riguroso, se emplea una matriz de datos, permitiendo sistematizar la evaluación de la eficacia de las herramientas forenses estudiadas. El presente documento está dividido en cinco capítulos:

El capítulo I plantea el problema de principal de esta investigación, enfocado en la falta de conocimiento, confianza y difusión sobre herramientas de software libre en el análisis forense de dispositivos móviles en Ecuador. A pesar de la existencia de soluciones accesibles y avanzadas, su adopción sigue siendo limitada debido a la falta de estandarización y soporte técnico. Se justifica la investigación por la necesidad de fortalecer las capacidades forenses en la lucha contra delitos cibernéticos y aquellos en los que interviene la tecnología. Además, se establecen los objetivos específicos que guían el estudio.

El capítulo II presenta el marco teórico, explicando el papel del análisis forense de dispositivos móviles en la investigación criminal y su relevancia en delitos digitales. Se analizan las ventajas y desafíos del uso de herramientas de software libre, además de revisar estudios previos tanto a nivel internacional como en el contexto ecuatoriano. Esta revisión proporciona una base sólida para comprender la efectividad y aplicabilidad de estas herramientas en la práctica forense.

El capítulo III describe la metodología utilizada en la investigación. Se emplea un enfoque cuantitativo no experimental y documental, basado en el análisis de datos provenientes de fuentes secundarias como libros, tesis, artículos científicos, documentos técnicos. Las técnicas de recolección de datos incluyen el uso de guías de análisis documental y fichas de recolección de datos, así mismo se aplican técnicas de análisis estadístico descriptivo e inferencial para evaluar la efectividad y fiabilidad de las herramientas de software libre comparadas con las soluciones propietarias, además, se presentan los procedimientos para la clasificación, registro,

tabulación y codificación de los datos, asegurando una sistematización rigurosa de la información recopilada.

El Capítulo IV presenta el análisis de resultados obtenidos a partir de la revisión documental, evaluando las herramientas seleccionadas en términos de efectividad, compatibilidad y cumplimiento de estándares forenses. Se detalla la construcción del marco de trabajo forense, abordando sus fases clave: identificación, preservación, adquisición, procesamiento, análisis e informe.

Finalmente, el Capítulo V se exponen las conclusiones y recomendaciones derivadas del estudio, resaltando la viabilidad del uso de herramientas de software libre en el análisis forense digital en el Ecuador. En el cual se enfatiza la necesidad de capacitación y estandarización para potenciar su adopción y mejorar la eficacia de las investigaciones forenses.

CAPÍTULO I

EL PROBLEMA

En este capítulo, se explorarán las técnicas, metodologías y herramientas utilizadas para realizar análisis forenses en dispositivos móviles, se revisarán estudios previos y referentes teóricos pertinentes, con un enfoque particular en las herramientas de software libre y su aplicación en investigaciones forenses digital. Además, se analizarán los desafíos y oportunidades que estas herramientas presentan para entidades públicas y empresas privadas, permitiendo así establecer la base conceptual y teórica que sustentará el estudio de caso que se llevará a cabo para extraer, procesar y analizar datos de un dispositivo móvil.

Planteamiento del problema

En el entorno digital actual, los dispositivos móviles han evolucionado hasta convertirse en una parte integral de la vida cotidiana, almacenando una vasta cantidad de información personal y profesional. Esto ha convertido a los dispositivos móviles, en un objetivo principal de análisis para las entidades de ley e investigadores de incidentes y delitos informáticos lo que ha incrementado la necesidad de aplicación de técnicas, metodologías y herramientas forenses eficaces para realizar análisis en estos dispositivos. Según (Alemán Ariza, 2024), "el análisis forense digital en dispositivos móviles presenta muchos retos ligados al avance tecnológico de los dispositivos que son utilizados como fuente de evidencia y por las connotaciones legales referente a la privacidad (…)" (p. 45).

Las herramientas de software libre desempeñan un papel crucial en el análisis forense de dispositivos móviles, ofreciendo beneficios significativos en términos de accesibilidad, flexibilidad y costo, estas herramientas permiten a los investigadores forenses acceder y analizar datos almacenados en dispositivos móviles, facilitando la extracción de información relevante para investigaciones criminales y corporativas. Además, al ser de libres, estas herramientas pueden ser adaptadas y mejoradas continuamente por la comunidad, asegurando que estén actualizadas frente a las últimas tecnologías y amenazas. Según (Lorenzo, 2024), "Autopsy es una de las herramientas más utilizadas y recomendadas, ya que permite localizar muchos artefactos de los programas y complementos de código abierto, facilitando enormemente el análisis forense de sistemas informáticos".

A nivel mundial, el análisis forense de dispositivos móviles enfrenta desafíos significativos debido al rápido avance tecnológico y a las crecientes medidas de seguridad en estos dispositivos. La diversidad de marcas, modelos y sistemas operativos, junto con constantes actualizaciones de software, complica la extracción y el análisis de datos. Además, las implicaciones legales relacionadas con la privacidad añaden complejidad al proceso forense. Según (Alemán Ariza, 2024), "el análisis forense digital en dispositivos móviles presenta múltiples desafíos, no solo a nivel técnico, sino también en términos de cumplimiento legal y validación de evidencia en procesos judiciales (…)" (p. 52). Por lo tanto, es esencial que los profesionales se mantengan actualizados y continúen desarrollando metodologías y técnicas que aborden estas dificultades, garantizando así la integridad y validez de la evidencia digital obtenida.

En América Latina, la adopción de herramientas de software libre para el análisis forense digital ha sido variable. Aunque estas herramientas ofrecen beneficios en términos de accesibilidad y costo, su implementación se ve limitada por la falta de inversión en capacitación y en herramientas especializadas. Esto puede afectar la credibilidad de las pericias realizadas con software no licenciado. Según (Ferreyra, 2018) en su investigación titulada "*La investigación forense informática en América Latina* " es difícil que se realice la inversión en herramientas forenses, lo cual genera problemas cuando se trata de demostrar los resultados del proceso del análisis con software no licenciado en cabeza del organismo a cargo de la realización de la pericia (…)" (p. 52).

Por otro lado (Lázaro, 2024) destaca que el software libre no solo reduce costos operativos, sino que también fomenta la transparencia y flexibilidad en los procesos de análisis forense digital. La posibilidad de acceder al código fuente permite a los investigadores adaptar las herramientas a las necesidades específicas de cada caso, promoviendo así una mayor eficiencia en las investigaciones, sin embargo, también plantea desafíos, como la capacitación del personal y la disponibilidad de soporte técnico, los cuales pueden afectar la eficacia del análisis si no se abordan adecuadamente. De esta manera, el software libre representa un enfoque colaborativo y dinámico que fortalece tanto la práctica profesional como el desarrollo de metodologías innovadoras en el análisis forense digital.

En el contexto Ecuatoriano, la adopción de herramientas de software libre para el análisis forense digital enfrenta desafíos específicos. A pesar de políticas

gubernamentales que promueven el uso de software libre en entidades públicas desde 2008, su implementación en el ámbito forense ha sido limitada. La falta de capacitación adecuada y la preferencia por herramientas comerciales debido al soporte técnico especializado son barreras significativas para su adopción y aceptación.

En base lo anterior descrito según (Taylor, 2014) en su libro *Digital Forensics: A Primer for the First Responder* también destacan que “la falta de capacitación y el conocimiento insuficiente sobre herramientas de software libre son barreras significativas para su adopción en entornos forenses (…)” (p. 79).

A su vez Según (Echeverría Espinoza & Álvarez Vera, 2024), las herramientas de software libre para análisis forense digital han demostrado ser una alternativa viable a las soluciones comerciales, ofreciendo un alto nivel de eficacia y flexibilidad en diversas investigaciones. No obstante, "la preferencia por herramientas comerciales sigue siendo predominante debido al soporte técnico especializado y la garantía de calidad que ofrecen, lo que genera una barrera para la adopción de software libre en entornos forenses" (p. 72). Este sesgo hacia las herramientas comerciales puede limitar el aprovechamiento de estas herramientas libres, a pesar de sus beneficios en términos de accesibilidad y personalización.

En resumen, la falta de conocimiento de las diferentes herramientas de software libre, capacitación, la desconfianza en la fiabilidad de las herramientas de software libre y la insuficiente difusión de información sobre su uso en casos de éxito, son los principales desafíos que limitan la adopción, de estas herramientas en el análisis forense de dispositivos móviles. Esta investigación busca contribuir al desarrollo de la informática forense en Ecuador e incluso a nivel regional, proporcionando un marco de trabajo estructurado que promulgue la implementación y confiabilidad de herramientas de software libre en análisis forense digital, acoplándose a los procesos de adquisición, procesamiento y análisis de evidencia digital en investigaciones reales.

Por lo antes descrito, se plantea la siguiente interrogante de investigación ¿Cómo pueden las herramientas de software libre para el análisis forense digital de dispositivos móviles ser empleadas en los procesos y las capacidades de ciberseguridad en entidades públicas y privadas, asegurando la integridad, fiabilidad y validez de la evidencia digital obtenida en casos de estudio en Ecuador?

Objetivos de la investigación

Objetivo general

Proponer un marco de trabajo para el análisis forense digital de dispositivos móviles utilizando herramientas de software libre, que sea replicable y adaptable en diferentes escenarios, para investigadores forenses.

Objetivos específicos

1. Identificar las herramientas de software libre más relevantes para el análisis forense de dispositivos móviles mediante una revisión documental.
2. Examinar la efectividad de las herramientas de software libre en el contexto de las investigaciones realizadas por organismos públicos y privados, mediante el análisis documental de tesis, estudios, artículos científicos y reportes técnicos recopilados en una guía de análisis documental.
3. Diseñar un marco de trabajo que integre procesos de adquisición, procesamiento, análisis y presentación de evidencias digitales utilizando dichas herramientas adaptadas a las necesidades y realidades locales.
4. Evaluar el marco de trabajo mediante pruebas de concepto en entornos controlados.

Justificación e Impacto de la Investigación

A pesar de la amplia disponibilidad de herramientas de software libre para el análisis forense digital, su adopción en entidades públicas, privadas y pequeñas o medianas empresas sigue siendo limitada. Esto se debe, principalmente, a la falta de conocimiento, capacitación y confianza en su efectividad. Además, las soluciones comerciales representan un alto costo, lo que restringe su accesibilidad en muchos contextos. Esta investigación tiene como objetivo desarrollar un marco de trabajo estructurado que facilite y promueva el uso de herramientas de software libre en el análisis forense digital. A través de este modelo, los investigadores forenses podrán replicar los procesos de extracción, procesamiento y análisis de evidencia digital, garantizando su aplicabilidad en investigaciones reales con estas herramientas libres. Al basarse en un enfoque metodológico validado, esta investigación contribuirá a reducir las barreras de adopción y aceptación de estas herramientas, promoviendo así de esta manera su uso como una alternativa viable a las soluciones comerciales. Esto no solo disminuirá los costos asociados al análisis forense digital, sino que

también permitirá mejorar la eficiencia y efectividad en la recolección y procesamiento de evidencia en casos legales. Dado el crecimiento y la complejidad de los dispositivos móviles en el ámbito legal, resulta esencial fortalecer el acceso a herramientas libres, asegurando su implementación en entornos forenses y su integración en procesos institucionales. De esta manera, esta investigación aporta un marco de trabajo para fomentar la adopción y capacitación en el uso de herramientas de software libre, promoviendo su aplicación en el análisis forense digital a nivel académico, gubernamental y corporativo en el Ecuador.

Esta investigación es de gran relevancia por varios motivos:

- **Aporte social:** El avance en las capacidades de análisis forense digital de dispositivos móviles fortalecerá y mejorará el proceso de investigación de delitos en los cuales interviene la tecnología, mejorando significativamente los resultados de las investigaciones. Además, estas técnicas contribuirán a concienciar a la sociedad sobre la importancia de la seguridad digital y la protección de datos de la privacidad personal en el entorno digital.
- **Aporte científico:** El estudio propuesto contribuirá conocimiento científico al proporcionar una evaluación detallada y crítica de las herramientas seleccionadas (Magnet ACQUIRE, CSI-Linux, Avilla Forensics, Autopsy), identificando sus fortalezas y limitaciones. Esto ayudaría a los profesionales del análisis forense digital a seleccionar las herramientas más adecuadas según sus necesidades específicas, mejorando así la eficiencia y efectividad en la resolución de casos forenses digitales.
- **Aporte académico:** Servirá como un recurso educativo invaluable para instituciones académicas y profesionales, proporcionando un marco de trabajo detallado para investigaciones futuras. Será especialmente útil para estudiantes y especialistas en seguridad informática, ofreciendo orientación sobre las mejores prácticas y herramientas en el análisis forense de dispositivos móviles.
- **Aporte tecnológico:** Proporcionarán orientación para el desarrollo futuro de herramientas de software libre, adaptadas específicamente a las necesidades de las entidades encargadas de la investigación de delitos. Esto permitirá mejorar la eficiencia y efectividad de estas herramientas, asegurando que

estén alineadas con las demandas tecnológicas actuales y futuras en el ámbito forense digital.

Alcance de la investigación

El alcance de esta investigación se centra en identificar y contrastar herramientas de software libre para el análisis forense digital de dispositivos móviles, evaluando su efectividad y aplicabilidad en el contexto forense. Geográficamente, el estudio se enfoca en el análisis de fuentes documentales relevantes a nivel internacional y su aplicabilidad en el contexto ecuatoriano, considerando las necesidades y limitaciones de las entidades que realizan investigaciones forenses. El estudio abarca la población documental compuesta por artículos científicos, tesis académicas, documentos técnicos y revistas científicas que analizan y comparan herramientas de software libre y privativas en el análisis forense de dispositivos móviles. Se busca recopilar datos sobre su desempeño, ventajas, limitaciones y su aceptación en el ámbito forense.

Para abordar este estudio, se aplicarán técnicas de recolección y análisis de información documental, siguiendo una metodología cuantitativa, no experimental y de diseño documental. Se evaluará la efectividad de las soluciones de software libre en función de criterios como recuperación de datos, compatibilidad con sistemas operativos, facilidad de uso y cumplimiento de estándares forenses. El objetivo final es que los hallazgos de este estudio contribuyan a mejorar las capacidades mediante un marco de trabajo en el ámbito de la ciberseguridad, fortaleciendo la respuesta ante incidentes y delitos informáticos mediante la adopción de herramientas de software libre como alternativas viables y accesibles.

CAPITULO II

MARCO TEÓRICO

El marco teórico de esta investigación se centra en las técnicas y herramientas utilizadas para el análisis forense en dispositivos móviles, específicamente en el uso de software libre. Según (Enaidy, 2018), "*El marco teórico o marco referencial, es el conjunto de elementos conceptuales (teorías, leyes, principios, categorías, que se refieren de forma directa al problema de investigación focalizado y que define, explica y predice lógicamente los fenómenos del universo al que éste pertenece*"(pág. 12).

En este sentido, el análisis forense de dispositivos móviles se fundamenta en principios teóricos como la preservación de la evidencia digital, la integridad de los datos y el desarrollo de metodologías estandarizadas que garanticen la replicabilidad y confiabilidad de los procesos. Estas bases conceptuales aseguran que los datos extraídos puedan ser utilizados en contextos legales y académicos, consolidando la validez de la investigación forense.

El creciente uso de dispositivos móviles en la sociedad actual ha convertido a estos artefactos en repositorios de información de alto valor, tanto personal como profesional. Según (Alemán Ariza, 2024), "*el análisis forense digital en dispositivos móviles presenta muchos retos ligados al avance tecnológico de los dispositivos que son utilizados como fuente de evidencia (…)*" (p. 45). A partir de esta premisa, se establece la importancia de contar con herramientas tecnológicas que permitan realizar un análisis riguroso y adaptado a las particularidades de este tipo de dispositivos.

En particular, el uso de herramientas de software libre ha emergido como una alternativa clave dentro del análisis forense digital. Sepúlveda (Sepulveda, 2024) en su artículo "El Poder de las Herramientas de Código Abierto", "*las herramientas de código abierto en ciberseguridad ofrecen flexibilidad y transparencia, permitiendo a los profesionales adaptar y mejorar las soluciones según las necesidades específicas de cada investigación*". De esta manera, el software libre representa un enfoque colaborativo y dinámico que fortalece tanto la práctica profesional como la construcción teórica del análisis forense digital.

Este marco teórico, por lo tanto, articula conceptos interdisciplinarios provenientes de la informática, el derecho y las ciencias sociales, sentando las bases para una comprensión integral del análisis forense de dispositivos móviles y su aplicación en un contexto académico y profesional.

Antecedentes de la investigación

El análisis forense de dispositivos móviles es un campo de estudio que ha recibido considerable atención en los últimos años debido a la creciente prevalencia de dispositivos móviles y su uso en actividades delictivas, es por ello, que es necesario indagar en las investigaciones recientes que abordan este problema.

Siguiendo esta línea, en un estudio reciente, (Andrade Pesantez & Banegas Crespo, 2024) analizaron el uso de herramientas forenses en dispositivos móviles Android para la investigación de casos de ciber extorsión en el contexto latinoamericano, su investigación, basada en una revisión sistemática de literatura y en la aplicación de la norma ISO/IEC 27037:2012, destacó la importancia de adoptar estándares internacionales en análisis forense para garantizar la admisibilidad de la evidencia digital en procedimientos judiciales.

Los autores resaltan que en América Latina existen desafíos particulares en la aplicación de análisis forense digital, tales como la limitada disponibilidad de herramientas especializadas, la falta de capacitación técnica en instituciones públicas y privadas, y las restricciones presupuestarias que dificultan el acceso a soluciones comerciales. En este sentido, el estudio enfatiza que las herramientas de software libre representan una alternativa viable para fortalecer las capacidades forenses en la región, permitiendo a los investigadores acceder a tecnologías avanzadas sin incurrir en costos elevados.

Además, los resultados evidenciaron que el uso de herramientas de software libre facilita la replicabilidad y adaptación de metodologías a distintos contextos, promoviendo así su integración en laboratorios forenses y en investigaciones de delitos cibernéticos. Como conclusión, (Andrade Pesantez & Banegas Crespo, 2024) recomiendan la implementación de programas de capacitación y certificación en herramientas de software libre, con el fin de mejorar la efectividad y fiabilidad del análisis forense en dispositivos móviles dentro de América Latina.

En el contexto ecuatoriano (Grijalva Lima & Loarte Cajamarca, 2017), en su investigación "*Modelo para el análisis forense y la legalización de evidencia digital*

atípica en procesos judiciales en Ecuador", analizaron la aplicación y efectividad de las herramientas de software libre en el análisis forense de dispositivos móviles dentro de Ecuador. Utilizaron un enfoque cualitativo y cuantitativo para evaluar la adaptabilidad de estas herramientas en instituciones ecuatorianas. Los resultados indicaron que, a pesar de la disponibilidad de avanzadas herramientas de software libre, muchas entidades públicas y privadas en Ecuador no han logrado adaptarse completamente a su uso debido a la falta de capacitación. Concluyeron que es crucial implementar programas de formación y actualización para maximizar el potencial de estas herramientas en las investigaciones forenses locales.

Los antecedentes revisados ofrecen una base sólida para esta investigación, resaltando la importancia de las herramientas de software libre en el análisis forense de dispositivos móviles y su aplicabilidad en diversos contextos. Los estudios realizados por (Grijalva Lima & Loarte Cajamarca, 2017) señala que la falta de capacitación es una barrera clave para su implementación en Ecuador, lo que refuerza la necesidad de desarrollar estrategias que faciliten su adopción. En este contexto, el presente estudio tiene como objetivo profundizar en la evaluación de herramientas forenses de software libre y proponer un marco de trabajo que optimice su uso en entornos forenses, especialmente en Ecuador. A partir de la información recopilada, se analizarán metodologías existentes, desafíos técnicos y mejores prácticas que permitan integrar efectivamente estas herramientas en investigaciones forenses. De esta manera, la investigación contribuirá al fortalecimiento del análisis forense digital, promoviendo el uso de soluciones accesibles y eficientes tanto a nivel local como internacional.

Bases teóricas

Análisis forense

El análisis forense se refiere al proceso de identificación, preservación, colección, examen, análisis y presentación de evidencia digital, de manera que sea admisible en un tribunal de justicia, este proceso es esencial para extraer evidencias digitales de dispositivos móviles como smartphones y tabletas, que se utilizan cada vez más en actividades delictivas. Según (Badman & Forrest, 2024), "*el análisis forense digital es el proceso de recopilación y análisis de pruebas digitales de una manera que mantenga su integridad y admisibilidad en los tribunales*".

El software libre ha demostrado ser una alternativa viable en el campo del análisis forense. Según (Fernández, 2022) señala que las herramientas libres también pueden ser viables al momento de extraer información y a su vez analizar la misma de los dispositivos móviles, permitiendo a los investigadores adaptar y personalizar las herramientas según sus necesidades. La flexibilidad del software libre es particularmente útil en contextos donde los recursos financieros son limitados. La flexibilidad del software libre es particularmente útil en contextos donde los recursos financieros son limitados, sin embargo, (Hay & Nance, 2016) advierten que, aunque el software libre puede ser eficaz, su adopción requiere una comprensión adecuada de su funcionamiento y una capacitación apropiada para maximizar su utilidad en investigaciones forenses.

Según el artículo publicado por (Mag, 2024)"Análisis Forense Digital: ¿Cómo se realiza? Herramientas y técnicas", la adopción de herramientas de software libre en el análisis forense digital puede ser eficaz, pero requiere una comprensión adecuada de su funcionamiento y una capacitación apropiada para maximizar su utilidad en investigaciones forenses.

A pesar de las ventajas, la implementación de herramientas de software libr20e en el análisis forense presenta desafíos, de acuerdo con (Finneran & Sutton, 2020) en su estudio detalla que uno de los principales desafíos es la falta de estandarización y el soporte técnico limitado en comparación con las herramientas comerciales, además, la comunidad de software libre debe garantizar la integridad y la seguridad del software para evitar comprometer la validez de las pruebas forenses.

En el informe elaborado por (Palmer, 2001) menciona que las metodologías forenses establecen los pasos y procedimientos a seguir en un análisis forense, una de las metodologías más reconocidas es la de *Digital Forensic Research Workshop* (DFRWS), que define seis fases principales: identificación, preservación, colección, examen, análisis y presentación. A continuación, se describen las fases:

- **Identificación:** implica la detección y documentación de un incidente de seguridad, se recopila información preliminar para comprender la naturaleza y el alcance del incidente, en esta etapa, es crucial responder a preguntas clave como: ¿Quién?, ¿Qué?, ¿Cuándo?, ¿Dónde?, ¿Por qué?, ¿Cómo?
- **Preservación:** el objetivo principal es garantizar que la evidencia digital recopilada no se altere, dañe o destruya. Se deben seguir procedimientos

adecuados para mantener la integridad de la evidencia y se recomienda crear copias exactas de la información original, y trabajar sobre estas copias para evitar cualquier modificación de los datos originales.

- **Colección:** se recopilan todos los datos relevantes del incidente, utilizando herramientas y técnicas forenses apropiadas. Es importante mantener la cadena de custodia de la evidencia, documentando cada paso del proceso de recolección.
- **Examen:** implica una revisión exhaustiva de la evidencia digital recopilada, para ello se utilizan herramientas de software especializadas para extraer información relevante, como archivos ocultos, eliminados o corruptos. El estudio de la línea de tiempo, logs de accesos y una descarga de la memoria RAM puede ser útil para la mayoría de las pericias.
- **Análisis:** se analizan los datos extraídos durante el examen para identificar patrones, relaciones y otra información relevante para la investigación, para ello se deben usar metodologías estructuradas para analizar la información y evaluar la criticidad del incidente.
- **Presentación:** al final se prepara un informe detallado que documenta todas las acciones realizadas durante el análisis forense. El informe debe presentar los hallazgos de manera clara, concisa y respaldada por la evidencia recopilada, para esto se recomienda incluir un informe ejecutivo con los datos más importantes y un informe técnico con mayor detalle y precisión.

Además de la metodología DFRWS, existen otras metodologías en el campo del análisis forense digital, como el Modelo Avanzado de Análisis Forense (ADFM) y la Metodología de Investigación Forense Digital (DFIM).

El ADFM es una metodología que amplía las fases tradicionales del análisis forense digital, incorporando etapas adicionales para abordar desafíos contemporáneos; es especialmente útil en investigaciones complejas que requieren una planificación meticulosa y una gestión de riesgos detallada. Aunque las fases específicas pueden variar según la fuente, generalmente incluyen:

- **Planeación:** desarrollo de una estrategia detallada para la investigación, definiendo objetivos, recursos necesarios y cronogramas.
- **Gestión de riesgos:** identificación y mitigación de posibles riesgos que puedan afectar la integridad de la evidencia o el éxito de la investigación.

- **Validación y verificación:** asegurar que las herramientas y técnicas utilizadas sean apropiadas y funcionen correctamente, garantizando la fiabilidad de los resultados.
- **Revisión Post-Investigación:** evaluación de todo el proceso una vez finalizado, identificando lecciones aprendidas y áreas de mejora para futuras investigaciones.

La DFIM es un enfoque que enfatiza la adaptabilidad y flexibilidad en el proceso de investigación forense digital; es adecuada para organizaciones que buscan un enfoque dinámico y adaptable, permitiendo respuestas rápidas y efectivas a incidentes de seguridad. Sus fases suelen incluir:

- **Preparación:** establecimiento de políticas y procedimientos antes de que ocurra un incidente, asegurando que el equipo esté listo para responder de manera efectiva.
- **Detección e Investigación inicial:** identificación de incidentes potenciales y evaluación preliminar para determinar la necesidad de una investigación forense completa.
- **Respuesta contenida:** acciones inmediatas para contener el incidente y prevenir una mayor pérdida o corrupción de datos.
- **Recuperación:** restauración de sistemas y datos a su estado operativo normal después de la investigación.
- **Lecciones aprendidas:** análisis posterior al incidente para mejorar las respuestas futuras y actualizar las políticas y procedimientos según sea necesario.

A continuación, se presenta una comparación de estas metodologías:

Tabla 1. *Comparativa entre metodologías de análisis forense*

	ESTRUCTURA	FLEXIBILIDAD	ADAPTABILIDAD
DFRWS	Ofrece un enfoque lineal y secuencial. Sigue una estructura más rígida.	Menos flexibilidad debido a su naturaleza estructurada.	Ampliamente aceptada en diversas investigaciones forenses digitales.
ADFM	Enfoque modular que permite ajustes según el caso.	Alta flexibilidad, permite la adaptación y personalización de procedimientos.	Preferida en casos complejos que requiere una planificación detallada.
DFIM	Incorpora etapas adicionales que abordan aspectos como la gestión de riesgos, la preparación previa al incidente.	Destaca por su adaptabilidad, permitiendo ajustes en función de la naturaleza del incidente y las necesidades específicas de la organización.	Ideal para entornos que demandan respuestas rápidas y flexibles.

Nota: Datos construidos a partir de la comparativa entre metodologías.

El análisis forense de dispositivos móviles es el proceso sistemático de recolección, preservación, análisis de datos almacenados en dispositivos móviles como teléfonos inteligentes y tabletas. Esta disciplina es crucial en la actualidad debido a la proliferación de dispositivos móviles y su papel central en la comunicación, transacciones financieras y almacenamiento de información personal y profesional. Permite a los investigadores forenses recuperar evidencia digital de relevancia en investigaciones criminales, casos legales, incidentes de seguridad cibernética y en la reconstrucción de eventos digitales, garantizando la integridad de la evidencia y el cumplimiento de normativas legales y éticas vigentes. El análisis forense de dispositivos móviles presenta características y retos únicos debido a la diversidad de sistemas operativos, la rápida evolución tecnológica y la naturaleza volátil de la memoria.

Según (Ariza, 2024) en su estudio Análisis forense digital en dispositivos móviles, "*El análisis forense de dispositivos móviles enfrenta desafíos como la diversidad de marcas y modelos, sistemas de archivos, actualizaciones, procesadores, versiones de sistemas operativos, estado físico, tecnologías de encriptación y regulaciones de privacidad, complicando la extracción y análisis de datos*"

Esta cita es relevante porque enfatiza los desafíos técnicos y operativos que enfrentan los investigadores forenses al trabajar con dispositivos móviles, tales como la diversidad de sistemas operativos, la encriptación y la falta de estandarización en los procedimientos de análisis. Estos factores dificultan la extracción y preservación de evidencia digital, lo que subraya la necesidad de desarrollar marcos metodológicos

adaptativos y herramientas especializadas. En este sentido, la implementación de estrategias basadas en software libre se presenta como una alternativa viable para optimizar el acceso y la eficiencia en las investigaciones forenses, permitiendo una mayor flexibilidad y reducción de costos en entornos con limitaciones presupuestarias.

Herramientas especializadas en análisis forense

Existe una diversidad de herramientas especializadas tanto comerciales como libres para el análisis forense de dispositivos móviles, herramientas que permiten la extracción, procesamiento y análisis de datos de dispositivos de manera rápida y garantizando en todo momento integridad y fiabilidad de la información obtenida. Estas herramientas ofrecen opciones avanzadas como la decodificación de aplicaciones, información cifrada, así como la recuperación de datos eliminados para su análisis.

Por lo expuesto, las herramientas forenses han revolucionado el campo del análisis forense de dispositivos móviles debido a las diferentes bondades que ofrecen a los analistas en este campo, por lo que, en los siguientes apartados se detallas las herramientas más conocidas y utilizadas actualmente en este ámbito.

Herramientas Comerciales:

- **XRY de MSAB:** conocida como una de las herramientas más potentes a nivel global para la extracción y análisis de datos en dispositivos móviles, especialmente en contextos judiciales.
- **Oxygen Forensic Detective:** reconocida por su capacidad avanzada para la extracción de datos desde dispositivos móviles y aplicaciones en la nube, proporciona herramientas específicas para analizar redes Wi-Fi, contraseñas almacenadas y archivos multimedia. Es valorada en contextos judiciales por su capacidad de generar reportes detallados de evidencia digital.
- **Magnet AXIOM:** destacada por su capacidad para realizar un análisis exhaustivo de dispositivos móviles, computadoras y datos almacenados en la nube. Es conocida por su enfoque integral, permitiendo correlacionar datos entre múltiples dispositivos, lo que facilita la reconstrucción de eventos en investigaciones complejas. Su interfaz intuitiva y capacidad la convierten en una herramienta popular entre los analistas forenses.

- **UFED de CELLEBRITE:** es probablemente la herramienta más conocida en el mundo del análisis forense digital de dispositivos móviles, es utilizada en su mayoría por las fuerzas del orden para investigaciones e inteligencia, una de sus grandes desventajas es el costo para su adquisición.
- **MOBILedit:** es una de las herramientas de análisis forense de dispositivos móviles y dispositivos IoT más conocidas por su facilidad de uso y bajo costo en comparación a las anteriormente descritas.

Herramientas Libres:

- **Tsurugi Linux:** valorada por ser una distribución de Linux optimizada para investigaciones forenses y análisis de datos móviles, proporcionando un conjunto completo de herramientas de código abierto.
- **CSI Linux:** esta distribución se destacó por su orientación específica hacia la seguridad y la investigación forense, ofreciendo un entorno confiable para realizar análisis forense detallados.
- **Avilla Forensics:** herramienta de extracción y análisis forense móvil de acceso libre, creada por Daniel Avilla, un oficial de la policía de Sao Paulo, para ayudar a investigadores forenses a recopilar y analizar información de dispositivos móviles utilizando herramientas de software libre.
- **Magnet Acquire:** es una herramienta liberada de manera gratuita por Magnet Forensics, la cual permite adquirir de manera rápida y fácil imágenes forenses de cualquier dispositivo, disco duro y medio extraíble iOS o Android.
- **ADB (Android Debug Bridge):** es una herramienta de línea de comandos de código abierto que permite comunicarse con dispositivos con sistema operativo Android a través de una Shell, es la herramienta base para las comunicaciones de herramientas forenses para la extracción de datos.
- **Libimobiledevice:** herramienta multiplataforma de software libre y código abierto escrita en C que permite comunicarse con dispositivos iOS de forma nativa para la extracción y/o adquisición de datos.
- **DB Browser for SQLite:** es una herramienta gráfica de código abierto que permite a los investigadores forenses realizar búsquedas en bases de datos SQLite extraídas de dispositivos móviles Android y/o iOS.

- **ALEAPP (Android Logs Events & Protobuf Parser):** herramienta multiplataforma de código abierto especializada en el análisis forense de dispositivos móviles con sistema operativo Android.
- **iLeAPP (iOS Logs, Events, And Properties Parser):** herramienta multiplataforma de código abierto especializada en el análisis forense de dispositivos móviles con sistema operativo iOS.
- **Andriller:** conjunto de herramientas que permite la extracción y decodificación de datos de dispositivos Android, soportando varios métodos de extracción de datos.
- **AFLogical:** herramienta de recolección de datos para dispositivos Android que permite la extracción de una amplia variedad de datos, incluidos contactos, registros de llamadas y mensajes.
- **Autopsy:** destacada como la principal plataforma de análisis forense digital de código abierto, modular y de uso frecuente en escenarios forenses. Se reconoce por su facilidad de uso y adaptabilidad a diferentes tipos de casos.

Según los autores (Foo & Al-Sabaawi, 2019), en su estudio, enfatizan que herramientas como AccessData FTK Imager y Kali Linux VM son efectivas para la extracción y análisis de datos forenses, aunque requieren una preparación cuidadosa para garantizar la integridad de los datos procesados (*A Comparison Study of Android Mobile Forensics for Retrieving Files System*). Según (Lázaro, 2024) en su artículo El papel del software libre en la ciberseguridad: beneficios, desafíos y herramientas clave, "*el software libre es una alternativa viable en el análisis forense digital por su flexibilidad y reducción de costos, pero su implementación enfrenta desafíos en capacitación y soporte técnico, que pueden afectar la eficacia de las investigaciones si no se abordan correctamente*".

A continuación, se presenta la comparación de estas herramientas:

Tabla 2. *Comparativa entre herramientas de software libre*

Herramienta		Curva de Aprendizaje	Entorno de ejecución	Compatibilidad Android / iOS	Tipo de Adquisición	Documentación	Generación automática de HASH
Adquisición	**CSI Linux**	Media, requiere conocimiento de Linux	Multiplataforma (Windows, Linux Mac)	Android, iOS.	Lógica Física	Documentación Oficial	Si
	Magnet Acquire	Baja, interfaz intuitiva y fácil de usar.	Windows.	Android, iOS.	Lógica Física	Documentación oficial	Si
	AFLogical	Baja, interfaz sencilla y fácil de usar.	Linux	Android.	Lógica	Documentación básica, disponible en foros y comunidades.	No.
	ADB	Alta, requiere manejo de comandos Linux	Multiplataforma	Android	Lógica Física	Documentación oficial	No
Procesamiento y análisis	**Avilla Forensics**	Media, requiere conocimientos previos	Windows y Linux.	Android, iOS.	Lógica	Documentación limitada pero muy completa, dependiente de la comunidad.	Si
	iLEAPP	Media, requiere conocimientos previos	Multiplataforma	iOS	N/A	Limitada, depende de la comunidad	No
	ALEAPP	Media, requiere conocimientos previos	Multiplataforma	Android	N/A	Limitada, depende de la comunidad	No
	Autopsy	Baja	Multiplataforma	Android iOS	N/A	Documentación extensa y comunidad activa.	Si

Nota: Datos construidos a partir de la evaluación de herramientas comerciales.

Las herramientas forenses de software libre son alternativas viables a las soluciones comerciales, permitiendo la adquisición y análisis de datos sin costos elevados. Gracias a su transparencia, flexibilidad y compatibilidad multiplataforma, se convierten en opciones estratégicas para investigadores forenses con presupuestos limitados o necesidades específicas de personalización.

Tabla 3. *Comparativa entre herramientas comerciales*

Herramienta comercial	Curva de aprendizaje	Multiplataforma	Compatibilidad con Android/iOS	Tipo de adquisición	Documentación	Facilidad de uso
Oxygen Forensics	Alta, requiere conocimientos avanzados en análisis forense.	No, solo disponible en Windows.	Sí, compatible con Android e iOS, permite extracción avanzada de datos.	Extracción lógica, física y en la nube.	Documentación extensa y soporte técnico especializado.	Moderada, interfaz gráfica intuitiva, pero con múltiples opciones avanzadas.
XRY	Media-Alta, requiere capacitación técnica.	No, solo disponible en Windows.	Sí, compatible con Android e iOS, especializado en extracción segura de datos.	Extracción física y lógica, soporte para dispositivos cifrados.	Documentación detallada, soporte técnico especializado.	Moderada, interfaz optimizada, pero con funciones avanzadas que requieren experiencia.
Magnet AXIOM	Media-Alta, interfaz amigable, pero con herramientas avanzadas.	No, solo disponible en Windows.	Sí, compatible con Android e iOS, permite extracción y análisis detallado.	Extracción y análisis de datos de dispositivos móviles, computadoras y la nube.	Excelente documentación, comunidad activa y soporte técnico.	Excelente documentación, comunidad activa y soporte técnico.

Nota: Datos construidos a partir de la comparativa de herramientas.

Las herramientas privativas como Oxygen Forensics, Magnet AXIOM y XRY sobresalen por su capacidad de extracción avanzada y compatibilidad con dispositivos cifrados. Sin embargo, su elevado costo y la dependencia de licencias restringen su accesibilidad, lo que las hace menos atractivas en comparación con las herramientas de software libre.

Tabla 4. *Comparativa entre herramientas comerciales y software libre*

Herramienta	Extracción de datos	Análisis de datos	Soporte para Android	Soporte para iOS	Multiplataforma (Windows/Linux/macOS)	Interfaz gráfica	Tipo de herramienta
CSI Linux	x	x	x		x	x	Software libre
Magnet Acquire	x		x	x	x	x	Software libre
AFLogical	x		x		x		Software libre
Avilla Forensics	x	x	x	x	x	x	Software libre
Autopsy		x	x	x	x	x	Software libre
Oxygen Forensics	x	x	x	x		x	Comercial
XRY	x	x	x	x	x	x	Comercial
Magnet AXIOM	x	x	x	x	x	x	Comercial

Nota: Datos construidos a partir de la evaluación de herramientas.

Fundamentación legal

Para llevar a cabo investigaciones forenses en dispositivos móviles en Ecuador, es fundamental considerar el marco legal que protege los derechos y privacidad de las personas y regula la gestión de la evidencia digital. Este marco legal se articula en varias normativas nacionales e internacionales que se desarrollan a continuación:

Constitución de la República del Ecuador

Referente a datos personales y derecho al debido proceso la Constitución de la República del Ecuador (Ediciones Legales EDLE S.A, 2008) indica lo siguiente:

> Es la norma suprema y establece los derechos fundamentales, incluyendo el derecho a la protección de datos personales en la Constitución de la República del Ecuador (2021) Artículo 66, numeral 19 y el debido proceso (Artículo 76). Estos derechos constitucionales deben ser respetado en cualquier actividad, así como en el proceso de un análisis forense, asegurando que se protejan los derechos y libertades fundamentales de los individuos, tal como se describen a continuación:
> - **Artículo 66:** "Se garantiza el derecho a la privacidad y la protección de datos de carácter personal. Toda intervención en la vida privada y en los datos de las personas, así como el acceso a los sistemas de información, se efectuará con respeto a estos derechos y, en muchos casos, requiere autorización del titular o una orden judicial."
> - **Artículo 76:** "Toda persona tiene derecho a un debido proceso en todas las fases de la investigación y del juicio. Esto incluye la garantía de que la evidencia digital obtenida durante el proceso de investigación se maneje con el debido respeto a los derechos y garantías procesales."

Código Orgánico Integral Penal (COIP)

Vigente desde el 2014, es la principal normativa penal en Ecuador. Regula los delitos informáticos y sanciona conductas delictivas relacionadas con la tecnología (Artículo 178, 208, 229, 230, 231, 232, 233, 234, entre otros) (Ediciones Legales EDLE S.A, 21), menciona lo siguiente:

> Es un código que debe cumplirse de manera obligatoria en el análisis forense digital, asegurando y garantizando la protección de derechos. Por ejemplo, el artículo 178 penaliza la violación a la intimidad, mientras que el artículo 232 regula el acceso no consentido a sistemas informáticos. Estas disposiciones subrayan la importancia de que cualquier análisis forense de dispositivos móviles sea realizado de manera que no infrinja los derechos de privacidad y protección de datos personales y se realice con la debida autorización judicial, garantizando la legitimidad de la recolección de evidencia.

Ley orgánica de protección de datos personales (LOPDP)

Publicada en 2021 (Ediciones Legales EDLE S.A., 26), establece que:

> Las normas para la recolección, manejo, almacenamiento y protección de datos personales en Ecuador, esta ley es fundamental para garantizar la privacidad y la protección de los datos personales durante el proceso de análisis forense. Cualquier análisis forense de dispositivos móviles debe cumplir con las disposiciones de esta ley, asegurando que los datos personales sean manejados de forma legal y respetando los derechos de los individuos.

Ley de comercio electrónico, firmas electrónicas y mensajes de datos (LCEFEMD)

Esta ley promulgada en el 2002 establece un:

> Marco legal para el uso y la validez de los documentos electrónicos, firmas digitales y mensajes de datos. En particular, esta
> ley define la validez y la admisibilidad de la evidencia digital en procedimientos judiciales y administrativos. El marco de trabajo de análisis forense debe asegurar que la evidencia digital recolectada cumpla con los requisitos de integridad y autenticidad establecidos por esta ley, garantizando su admisibilidad en procesos legales.

Resoluciones de creación de unidades especializadas en ciberdelitos en Ecuador

En Ecuador, la creciente amenaza de los ciberdelitos ha llevado a la implementación de unidades especializadas para combatir estos crímenes, que trabajan en estrecha colaboración para proteger a los ciudadanos en el entorno digital y garantizar el cumplimiento de la legislación ecuatoriana en materia de delitos informáticos (Resolución No. 34-FGE-2022, 2022). Por lo que destaca la creación de las unidades:

- Creación de la Unidad de Ciberdelitos de la Policía Nacional del Ecuador
  El Acuerdo Ministerial No. 1369-2019 emitido por el Ministerio del Interior en 2019 establece la creación de la Unidad de Investigación de Ciberdelitos de la Policía Nacional. Esta unidad se encarga de investigar, prevenir y combatir los delitos informáticos, como el fraude electrónico, el robo de datos, la extorsión en línea, el ciberacoso, y el uso indebido de la información en las redes sociales.
- Creación de la Fiscalía Especializada en Ciberdelitos
  La Resolución 034-FGE-2022 es una respuesta institucional de la Fiscalía ante el incremento de los delitos informáticos en Ecuador, reflejando la necesidad de contar con una estructura legal y técnica que permita enfrentar estos crímenes de manera efectiva. Con la implementación de esta unidad especializada, la fiscalía general del Estado busca mejorar la protección de los ciudadanos en el entorno digital y garantizar que los delitos informáticos sean investigados y procesados adecuadamente, este tipo de medidas responde a la realidad de un mundo cada vez más interconectado, donde los ciberdelitos son una amenaza constante y requieren de una preparación y capacidad institucional acorde a las nuevas tecnologías.
- Cooperación entre la Policía Nacional y la Fiscalía
  Ambas entidades la Policía Nacional y la fiscalía general del Estado, colaboran estrechamente en la lucha contra los ciberdelitos. La Unidad de Ciberdelitos de la Policía Nacional se encarga de la investigación y recopilación de pruebas digitales en campo, bajo la dirección de la Fiscalía Especializada de Ciberdelitos, la cual lleva adelante la persecución penal de los responsables, asegurando que se cumpla la legislación ecuatoriana en materia de delitos informáticos.

Tratados Internacionales

(Aboso, 2022) Ecuador ha reconocido la importancia de la seguridad de la información en un mundo cada vez más digitalizado y conectado, por lo que menciona lo siguiente:

> A medida que las amenazas cibernéticas aumentan, el país ha tomado medidas para establecer un marco legal y participar en tratados internacionales que fortalezcan la seguridad de la información y la ciberseguridad de los ciudadanos y de las instituciones.
> La participación de Ecuador en convenios como el de Budapest y la implementación de normativas de protección de datos son pasos significativos hacia la creación de un entorno digital seguro y resilientes.

Convenio de Budapest sobre ciberdelincuencia

El convenio de Budapest, también conocido como convenio sobre la Ciberdelincuencia según (Consejo de Europa, 2021), señala lo siguiente:

> Es el primer tratado internacional que aborda la investigación de delitos cometidos en internet y otros sistemas informáticos, cuyo principal objetivo es establecer una política penal común entre sus países miembros para le investigación de estos delitos y el manejo y gestión de la evidencia digital. Ecuador desde diciembre del 2024 es oficialmente miembro de este convenio.

CAPÍTULO III

MARCO METODOLÓGICO

A lo largo de este capítulo, se detallarán los pasos metodológicos que se seguirán para seleccionar, evaluar y aplicar herramientas de software libre en el análisis forense digital, estableciendo un enfoque sistemático que garantice la efectividad y la validez del marco de trabajo propuesto. Primero se describe la naturaleza de la investigación la población y la muestra con los criterios de inclusión y exclusión asumidos, las técnicas e instrumentos de recolección de información, la técnica de análisis de resultado y la metodología del producto.

Naturaleza de la Investigación

Enfoque de la investigación

El presente estudio se ubica en el paradigma positivista con un enfoque cuantitativo, el cual se basa en la objetividad y la posibilidad de medir y analizar los fenómenos o variables mediante datos numéricos. Según (Amsler, Casco, & Roatta, 2017), en su informe “Limitaciones de las actuales herramientas de análisis digital forense para dispositivos móviles", el objetivo del trabajo fue realizar una comparación cualitativa y cuantitativa de diferentes herramientas de adquisición de evidencia digital en dispositivos móviles" (p. 1), este enfoque es adecuado para evaluar la eficacia de las herramientas de software libre utilizadas en el análisis forense de dispositivos móviles, proporcionando resultados cuantificables y objetivos.

Nivel de la investigación

El nivel de la investigación es exploratorio-descriptivo, ya que busca, por un lado, explorar un fenómeno poco estudiado y, por otro lado, describir detalladamente sus características, usos y desafíos en relación con las herramientas de software libre utilizadas en el análisis forense de dispositivos móviles en el Ecuador, según (Beltrán tapia, 2021), los estudios exploratorios se enfocan en examinar fenómenos poco investigados, mientras que los estudios descriptivos buscan detallar las características específicas del objeto de estudio. La fase exploratoria del estudio se centra en identificar y comprender las diversas herramientas y técnicas utilizadas en el análisis forense de dispositivos móviles, esta fase es esencial para proporcionar una visión general del estado actual de las herramientas de software libre en el campo

forense, especialmente en el contexto ecuatoriano. Durante esta fase, se revisarán documentos técnicos, estudios de caso y publicaciones académicas recientes para obtener una comprensión profunda de las herramientas disponibles y sus aplicaciones prácticas. Según el artículo "*Investigación exploratoria: qué es, características, ejemplo*" publicado en (Concepto, 2024), "*una investigación exploratoria es un tipo de investigación que se lleva a cabo cuando se quiere estudiar un tema nuevo o del que existe poca información. También sirve cuando un objeto de estudio no está del todo definido y los especialistas necesitan conocer mejor el fenómeno*". Este enfoque permite al investigador familiarizarse con fenómenos desconocidos, identificar variables relevantes y establecer hipótesis para estudios posteriores.

Nivel descriptivo

La fase descriptiva se enfoca en detallar las características específicas, los usos prácticos y los desafíos asociados con las herramientas de software libre en el análisis forense digital de dispositivos móviles. En esta fase, se recopilará información de diversas fuentes secundarias, incluyendo tesis, documentos técnicos, artículos de revistas científicas y reportes de investigaciones anteriores. Esta metodología permite obtener una visión detallada y completa del uso de las herramientas de software libre en contextos reales, sin la necesidad de aplicar encuestas directas a los profesionales del área. (Yin, 2018) señala que "*el diseño descriptivo es crucial para proporcionar una imagen precisa y detallada del fenómeno estudiado, lo cual es fundamental para comprender las dinámicas y contextos específicos en los que se utilizan las herramientas forenses* (…)" (p. 56).

Diseño de la investigación

El diseño de la investigación es **No Experimental-Transversal**, este tipo de diseño no manipula variables independientes y se limita a observar y analizar el fenómeno tal como ocurre en su entorno natural y en un solo momento. De acuerdo con (Hernández Sampieri, Fernández Collado, & Baptista Lucio, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4ta ed.), 2014), el diseño no experimental se utiliza cuando las variables no pueden ser controladas deliberadamente por el investigador, mientras que un diseño transversal recolecta datos en un único momento, permitiendo describir variables y analizar su incidencia e interrelación.

Tipo de investigación

En este proyecto, el tipo de investigación se centrará en la investigación documental, la cual se define como "*la recolección y análisis de datos provenientes de documentos existentes, tales como libros, artículos científicos, informes técnicos y otros materiales escritos, sin manipular o controlar variable alguna. El investigador obtiene la información a partir de estas fuentes secundarias, proporcionando una comprensión profunda y contextualizada del fenómeno estudiado*", (Martínez Corona, Palacios Almón, & Oliva Garza, 2023). Detallan que, la autenticidad, credibilidad, representatividad y significado de los documentos son criterios esenciales para asegurar la validez de la información obtenida en una investigación documental.

En este sentido, el presente estudio corresponde a una investigación documental, debido a que los datos fueron recolectados a partir de una variedad de fuentes secundarias, estas fuentes incluyen tesis, artículos científicos y documentos técnicos relevantes que proporcionan detalles sobre las herramientas de software libre utilizadas en el análisis forense digital de dispositivos móviles. Este enfoque permite una comprensión exhaustiva y objetiva del uso de herramientas de software libre en el análisis forense, sin alterar las condiciones existentes, proporcionando una base sólida y bien documentada para el análisis y las conclusiones del estudio.

Población y muestra

Ventura (Ventura León, 2017), señala que la población se refiere al conjunto completo de elementos que poseen las características que se desean estudiar, mientras que la muestra es un subconjunto de esa población, seleccionado para representar al conjunto total. Una comprensión precisa de estos términos es esencial para el diseño metodológico y la interpretación de los resultados en los estudios, ya que una definición inadecuada puede conducir a conclusiones erróneas o no generalizables, además, el autor destaca la necesidad de describir adecuadamente la población accesible y el tipo de muestreo utilizado, ya que esto influye directamente en la validez de las inferencias realizadas a partir de los datos obtenidos.

Por su parte, la muestra es un subconjunto de la población de estudio según (Hernández Sampieri & Mendoza Torres, Metodología de la investigación. Rutas cuantitativa cualitativa y mixta-libre, 2018)

En base a estos autores la población documental de esta investigación incluyó artículos científicos, tesis académicas, reportes técnicos y normativas internacionales

que tratan sobre metodologías forenses aplicadas a dispositivos móviles, con énfasis en herramientas de software libre. Para la búsqueda de información, se consultaron las siguientes bases de datos y repositorios:

- IEEE Xplore
- SpringerLink
- ScienceDirect
- ACM Digital Library
- Dialnet
- Google Scholar
- Repositorios de universidades con facultades de ingeniería informática y ciberseguridad

Inicialmente, se identificaron 180 documentos a partir de búsquedas avanzadas con palabras clave como "*mobile forensics*", "*free forensic tools*", "*digital forensic methodologies*", "*herramientas forenses de código abierto*" y "*análisis forense en dispositivos móviles*".

Tras aplicar un proceso de filtrado riguroso, basado en criterios de inclusión y exclusión previamente definidos, se seleccionaron 32 documentos para revisión detallada. Posteriormente, luego de una evaluación más estricta sobre la pertinencia y calidad metodológica, se estableció una muestra final de 19 documentos que fundamentan esta investigación, los mismos que cumplen con los criterios de inclusión acorde al tema de la investigación.

Criterios de inclusión y exclusión

Para garantizar la validez y pertinencia de la información recopilada, se establecieron los siguientes criterios:

Criterios de inclusión

- Publicaciones relacionadas con el análisis forense de dispositivos móviles.
- Documentos que aborden el uso y comparación de herramientas de software libre.
- Estudios publicados en los últimos 5 años (desde 2019 en adelante).
- Documentos provenientes de revistas científicas, repositorios universitarios y entidades especializadas en ciberseguridad.
- Normativas internacionales aplicables al análisis forense digital, que incluyan procedimientos con software libre.

Criterios de exclusión

- Documentos con un enfoque exclusivo en herramientas comerciales sin comparación con software libre.
- Estudios que no aborden específicamente el análisis forense en dispositivos móviles.
- Publicaciones con información desactualizada, es decir, documentos previos a 2019.
- Normativas o estándares que no guarden relación con software libre o análisis forense digital.
- Documentos que no presenten una metodología replicable o cuyos resultados no sean verificables.
- Fuentes sin respaldo académico o institucional confiable, como blogs o artículos de opinión sin validación científica.
- Investigaciones que no contengan pruebas empíricas o estudios de caso aplicables al análisis forense digital.

Tabla 5. *Proceso de filtrado documental*

Fase	Cantidad de documentos	Acción realizada
Búsqueda inicial	180	Resultados obtenidos en bases de datos científicas (IEEE Xplore - SpringerLink - ScienceDirect - ACM Digital Library - Dialnet - Google Scholar - Repositorios de universidades) con palabras clave específicas.
Filtrado por relevancia temática	120	Se excluyeron 60 documentos que no abordaban específicamente herramientas de software libre o análisis forense en dispositivos móviles.
Revisión por año de publicación	95	Se eliminaron 25 documentos publicados antes de 2019.
Evaluación de la calidad metodológica	32	Se excluyeron 63 documentos que no contenían una metodología replicable o cuyos resultados no eran verificables.
Selección final	19	Documentos seleccionados por su relevancia y aporte directo a la investigación.

Nota: Datos construidos a partir del análisis documental revisado.

La muestra específica de esta investigación incluye:

- Tesis universitarias: Investigaciones académicas recientes relacionadas con el análisis forense de dispositivos móviles y el uso de herramientas de software

libre, estas tesis proporcionan estudios de casos detallados, metodologías aplicadas y resultados obtenidos en contextos similares.

- Artículos científicos: Publicaciones en revistas científicas indexadas que abordan el desarrollo, aplicación y evaluación de herramientas de software libre para el análisis forense, estos artículos ofrecen perspectivas teóricas y empíricas, así como comparaciones entre diferentes herramientas.
- Documentos técnicos: Informes y manuales técnicos publicados por organismos de seguridad y empresas especializadas en forense digital, estos documentos incluyen guías de uso, análisis de rendimiento y estudios de implementación práctica de herramientas de software libre.

Después del riguroso proceso de selección, se consolidó una muestra final de 19 documentos que cumplen con los estándares de calidad y pertinencia científica, estos documentos incluyen:

- 9 artículos científicos
- 5 tesis académicas
- 3 reportes técnicos
- 2 normativas internacionales

Los documentos seleccionados cumplieron con los siguientes estándares de selección:

- Relación directa con el análisis forense de dispositivos móviles y herramientas de software libre.
- Contenido aplicable a investigaciones en entornos públicos y privados.
- Publicaciones dentro del rango 2019 - 2024.
- Información alineada con tecnologías y metodologías forenses contemporáneas.
- Uso de metodologías científicas replicables.
- Evaluación comparativa de herramientas forenses.
- Inclusión de pruebas empíricas o estudios de caso.
- Publicaciones en revistas indexadas o artículos científicos.
- Tesis respaldadas por universidades reconocidas.
- Normativas internacionales con reconocimiento en la comunidad forense.
- Evaluación de herramientas en escenarios reales o simulados.

- Propuestas metodológicas para la implementación de software libre en análisis forense.
- Aportes significativos a la comunidad forense y de ciberseguridad.

La consolidación de esta muestra documental asegura que la investigación se fundamenta en evidencia científica y técnica de alta calidad, proporcionando una base sólida para el análisis y la propuesta de un marco de trabajo forense basado en herramientas de software libre.

Técnicas e instrumentos de recolección de datos

La técnica de recolección de datos aplicada en la presente investigación quedó determinada por el análisis documental, el cual posibilitó la obtención de datos fundamentales para el estudio del uso de herramientas de software libre en el análisis forense de dispositivos móviles. El análisis documental se basa en la revisión y examen crítico de documentos relevantes, tales como tesis, artículos científicos e informes técnicos.

Esta técnica permite recopilar información detallada y contextualizada sin la necesidad de interactuar directamente con los sujetos del estudio, proporcionando una base sólida y bien fundamentada para el análisis y las conclusiones de la investigación.

Instrumento de recolección de datos

Los instrumentos de recolección de datos en una investigación documental están diseñados para recopilar información precisa y relevante de diversas fuentes secundarias. En el contexto de esta investigación, los instrumentos utilizados incluyen guías de análisis documental y fichas de recolección de datos, estos instrumentos permiten sistematizar y organizar la información extraída de documentos escritos, asegurando que los datos recopilados sean consistentes y útiles para el análisis.

Fichas de recolección de datos

Las fichas de recolección de datos son utilizadas para registrar la información relevante de cada documento analizado, estas fichas permiten organizar los datos de manera estructurada, facilitando el proceso de análisis y comparación. Cada ficha incluye campos para el título del documento, autor, año de publicación, tipo de documento, resumen de contenido y principales hallazgos, según (Reyes, 2015), "*la*

creación de las fichas debe ser un trabajo creador, de análisis crítico o bien de síntesis" (p. 7), enfatizando la importancia de un enfoque analítico en su elaboración.

Guía de análisis documental

La guía de análisis documental es un instrumento esencial para evaluar, organizar y analizar la información obtenida de diversas fuentes secundarias, esta guía incluye criterios específicos para la selección y evaluación de documentos, como título, autores, año, país, base de datos, documentos o links de referencia y los resultados relevantes para la investigación. Según (Martínez Corona, Palacios Almón, & Oliva Garza, 2023), "*el análisis documental es un proceso que permite al investigador comprender y analizar las definiciones y conceptos alrededor de un tema de investigación*" (p. 1).

Tabla 6. *Guía de análisis documental*

Nº	Título	Autor(es)	Año	País	DB	Documento (links)	Resultados Relevantes

Estos instrumentos son cruciales para garantizar que la información recopilada sea precisa, coherente y relevante para los objetivos de la investigación, al utilizar fichas de recolección de datos y guías de análisis documental, se asegura una metodología robusta y sistemática que respalda la validez de los resultados.

Técnicas de análisis de los datos

Según (Martínez Corona, Palacios Almón, & Oliva Garza, 2023), "*un análisis documental, se reconoce como un procedimiento científico y obedece a un proceso que se caracteriza por ser sistemático para indagar, recolectar, organizar, analizar e interpretar información alrededor de un tema* (…)" (p. 1). En el enfoque cuantitativo, se prioriza la medición y los cálculos estadísticos. Para esta investigación documental, que incluye el análisis de cumplimento de aplicaciones de software libre y la comparación con software comercial, para lo cual, se emplearán las siguientes técnicas de análisis de datos cuantitativos:

- **Clasificación y registro**

Los datos recopilados de las fuentes documentales serán clasificados y registrados en fichas de recolección de datos, cada ficha incluirá información detallada sobre el documento, tales como el título, autor, año de publicación, tipo de documento, y un resumen de los principales hallazgos, esta clasificación facilita la organización y el acceso a la información relevante para el análisis posterior.

- **Tabulación**

Los datos serán tabulados para identificar patrones y frecuencias. Las tablas permitirán organizar los datos numéricos de manera sistemática, facilitando el cálculo de estadísticas descriptivas identificadas en los documentos revisados.

- **Análisis estadístico**

Se aplicarán técnicas de análisis estadístico descriptivo para resumir y describir las características principales de los datos recopilados. Esto incluirá:

    - **Frecuencia absoluta y frecuencia porcentual:** Para medir la aparición de temas específicos dentro de los documentos, se calculará la frecuencia de uso de herramientas de software libre versus herramientas comerciales, así como la frecuencia de aparición de ciertos atributos de confiabilidad en las herramientas analizadas.

Estándares para el manejo de evidencia digital y análisis forense

La metodología propuesta para la presente tesis, la cual se denomina “análisis forense de dispositivos móviles: utilizando de herramientas de software libre” está acorde lo establecido en las normas y estándares internacionales como el RFC 3227, ISO IEC 27037-2012, ISO IEC 27041-2015, ISO IEC 27042-2015, ISO IEC 27043-2015, NIST.IR.8354, NIST.IR.8387 y NIST.IR.8428, las mismas que se describen a continuación:

- **RFC 3227**

El documento RFC 3227, establece recomendaciones generales para la recolección y preservación de evidencia digital volátil. Aunque ha sido superado por normas más recientes como ISO/IEC 27037, sigue siendo relevante al proporcionar un marco

inicial sobre el manejo adecuado de evidencias digitales dentro del proceso de análisis forense.

- **ISO/IEC 27037:2012**

La norma ISO/IEC 27037:2012 establece directrices para la identificación, recolección, adquisición y preservación de evidencia digital, la cual se centra en garantizar la integridad y la cadena de custodia de las evidencias para su admisibilidad en procesos judiciales. Cumpliendo los siguientes puntos:

  - **Identificación:** localización los de las potenciales fuentes de información.
  - **Recolección:** recolección de elementos físicos que almacenen contenido digital.
  - **Adquisición:** extraer la evidencia digital, utilización de técnicas digitales forenses y herramientas especializadas en el área.
  - **Preservación:** garantizar la integridad de la evidencia digital.

Además, la norma estable el cumplimiento de los siguientes principios:

  - **Relevancia:** asegurar que la evidencia sea pertinente al caso a investigar.
  - **Confiabilidad:** garantizar que la evidencia se maneje de manera que su integridad no sea comprometida.
  - **Suficiencia:** asegurar que la cantidad de evidencia recolectada sea adecuada para respaldar las conclusiones.

- **ISO/IEC 27041:2015**

La norma ISO/IEC 27041:2015 proporciona directrices para documentar el proceso de análisis forense. Se enfoca en asegurar que los métodos utilizados para el análisis sean reproducibles y verificables, lo que es concluyente para validar los resultados obtenidos durante una investigación digital.

- **ISO/IEC 27042:2015**

La norma ISO/IEC 27042:2015 establece las directrices para el análisis e interpretación de la evidencia digital. Ofrece un marco que guía a los investigadores

en la evaluación de la validez y relevancia de las evidencias recolectadas, asegurando que se apliquen buenas prácticas durante el análisis.

- **ISO/IEC 27043:2015**

La norma ISO/IEC 27043:2015 integra las directrices mencionadas anteriormente y proporciona un enfoque holístico para las investigaciones forenses digitales, además esta norma establece un modelo que combina todos los aspectos del manejo de evidencias digitales desde su recolección hasta su análisis, enfatizando la necesidad de un enfoque documentado acorde los estándares internacionales.

- **Documentos NIST (National Institute of Standards and Technology)**

Adicional a las normas ISO/IEC, los documentos del NIST también son fundamentales ya que complementan el proceso del análisis forense digital, permitiendo establecer marcos de trabajo estandarizados bajo las mejores prácticas y estándares internacionales acorde el siguiente detalle:

  - **NIST.IR.8354:** Proporciona un marco para la gestión de incidentes relacionados con la ciberseguridad, destacando la aplicación de técnicas de investigaciones digitales forenses.
  - **NIST.IR.8387:** Se enfoca en la identificación y preservación de evidencia digital en el contexto de incidentes de ciberseguridad, ofreciendo directrices específicas para los responsables de manejo de evidencias digitales.
  - **NIST.IR.8428:** Se centra en establecer un marco de trabajo que aplique las mejores prácticas para la preservación de evidencia digital durante investigaciones forenses.

SWGDE (Scientific Working Group on Digital Evidence)

Se centra en establecer estándares y mejores prácticas para la recolección, adquisición y preservación de la evidencia digital forense de dispositivos móviles, asegurando su integridad y validez en investigaciones criminales.

Por lo expuesto, y acorde lo detallado en las normas ISO y los documentos RFC, NIST y SWGDE, estos estándares son fundamentales para establecer marcos de trabajo y procedimientos estandarizados en el manejo de evidencia digital y análisis

forense, esto debido a que proporcionan un marco robusto que asegura la integridad, relevancia y admisibilidad de las evidencias en contextos legales y empresariales, lo cual es crucial para el éxito de las investigaciones forenses digitales.

La adopción de estos estándares permite mejorar la calidad probatoria y fortalecer la confianza en los procesos judiciales relacionados con delitos informáticos, por lo tanto, en las siguientes ilustraciones se establece el procedimiento recomendando para el análisis forense digital de dispositivos móviles.

Metodología del producto

La metodología utilizada para desarrollar el marco de trabajo propuesto en esta investigación está basada en un enfoque documental y no experimental, considerando las características específicas del análisis forense de dispositivos móviles y el uso de herramientas de software libre. Este marco sigue una estructura flexible y replicable que permite la sistematización y optimización de los procesos forenses.

Elección de la Metodología

Para el diseño del marco de trabajo, se adoptó un enfoque inspirado en las metodologías iterativas y basadas en fases, similar a las prácticas ágiles en el ámbito de la ingeniería de software. Aunque esta investigación es documental, se priorizó una estructura modular que incluye las siguientes etapas claves:

- **Revisión documental:** Se realizó una recopilación exhaustiva de información de artículos científicos, reportes técnicos y tesis para identificar las herramientas de software libre más relevantes y las prácticas forenses recomendadas, esta etapa permitió determinar los procesos básicos de adquisición, procesamiento y análisis de evidencias digitales.
- **Procedimiento de investigación:** Basado en la revisión documental, se diseñó un flujo de trabajo dividido en las siguientes fases:

Ilustración 1. Proceso para el análisis forense digital de dispositivos móviles

1. **Identificación:** es la primera fase dentro del proceso del análisis forense de dispositivos móviles, su objetivo principal es localizar, reconocer y documentar los posibles indicios que contengan evidencia digital acorde el objeto de la investigación.
2. **Preservación:** esta es la segunda fase del manejo de evidencia digital dentro de un proceso de análisis forense de dispositivos móviles y consiste en garantizar en todo momento la integridad de los datos recolectados para que puedan ser utilizados en una investigación sin alteración, perdida o contaminación.
3. **Adquisición:** esta fase se enfoca en obtener una copia exacta de los datos de un dispositivo, asegurando su integridad y autenticidad, para lo cual, se utilizan herramientas especializadas como Magnet Acquire, CSI Linux, Avilla Forensics, Así mismo, se recomienda utilizar códigos hash para su validación.
4. **Procesamiento y análisis:** en esta fase, usaremos herramientas especializadas como Autopsy para procesar, indexar, organizar y analizar los datos adquiridos, filtrando la información relevante mediante búsquedas y etiquetas para facilitar un análisis conciso y detallado de las evidencias, identificando patrones y respondiendo a las preguntas clave del caso.
5. **Informe:** es la fase final del proceso de análisis forense digital de dispositivos móviles y consiste en la documentación y presentación de resultados y/o hallazgos obtenidos durante toda la investigación. Su objetivo es presentar de manera clara y precisa la evidencia analizada garantizando su validez, para lo cual, nos apoyaremos también en la generación de reportes que nos brindan las herramientas como

Autopsy, ya que la misma nos permite exportar en formatos legibles y organizado lo encontrado en la etapa del análisis.

Validación del marco de trabajo: para el cumplimiento y validación del marco de trabajó, se realizó pruebas de concepto en un entorno controlado, simulando escenarios forenses con dispositivos móviles reales que contienen datos estructurados y no estructurados, para lo cual, las herramientas utilizadas fueron evaluadas en términos de efectividad, curva de aprendizaje, multiplataforma, tipo de adquisición, documentación disponible de las herramientas.

Adaptaciones metodológicas

El enfoque que hemos adoptado engloba un marco de trabajo iterativo, donde las fases se revisan y ajustan continuamente según los resultados obtenidos en cada etapa. Esto garantiza:

- **Flexibilidad:** Permite adaptar el marco a diferentes herramientas y contextos locales.
- **Escalabilidad:** El flujo de trabajo puede ampliarse para cubrir necesidades específicas en investigaciones de mayor complejidad.
- **Estandarización:** Sigue estándares internacionales de buenas prácticas, como los propuestos por NIST y DFRWS.

Fases del marco de trabajo

- **Planeación:**
  1. Definición de objetivos específicos para el análisis forense.
  2. Selección de herramientas de software libre según el tipo de evidencia a analizar.
- **Implementación:**
  1. Configuración del entorno de análisis y adquisición de datos.
  2. Ejecución de pruebas controladas para validar los procesos.
- **Evaluación:**
  1. Análisis de los resultados obtenidos.
  2. Ajustes al marco de trabajo según los problemas identificados durante las pruebas.

- **Documentación:**
    1. Creación de guía práctica para replicar el marco de trabajo.
    2. Redacción de informes finales con los hallazgos y las recomendaciones.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

En este capítulo se presentan los resultados obtenidos a partir de la revisión documental realizado sobre herramientas especializadas de software libre aplicadas al análisis forense digital de dispositivos móviles. Se describe el proceso de evaluación de dichas herramientas, basado en criterios de efectividad, compatibilidad y cumplimiento de estándares forenses, siguiendo los lineamientos establecidos en la metodología de investigación documental.

Resultados de la investigación

Se detalla la construcción del marco de trabajo propuesto, incluyendo las fases de identificación, preservación, adquisición, procesamiento, análisis y presentación de resultados (Informe) de la evidencia digital analizada. Se analizan los hallazgos obtenidos a través de la aplicación del marco de trabajo, en estudios de caso y se contrastan con enfoques previos, destacando las ventajas y limitaciones de la adopción de herramientas de software libre en investigaciones forenses digitales.

Análisis de resultados

1. ***Identificación de herramientas de software libre para análisis forense de dispositivos móviles***

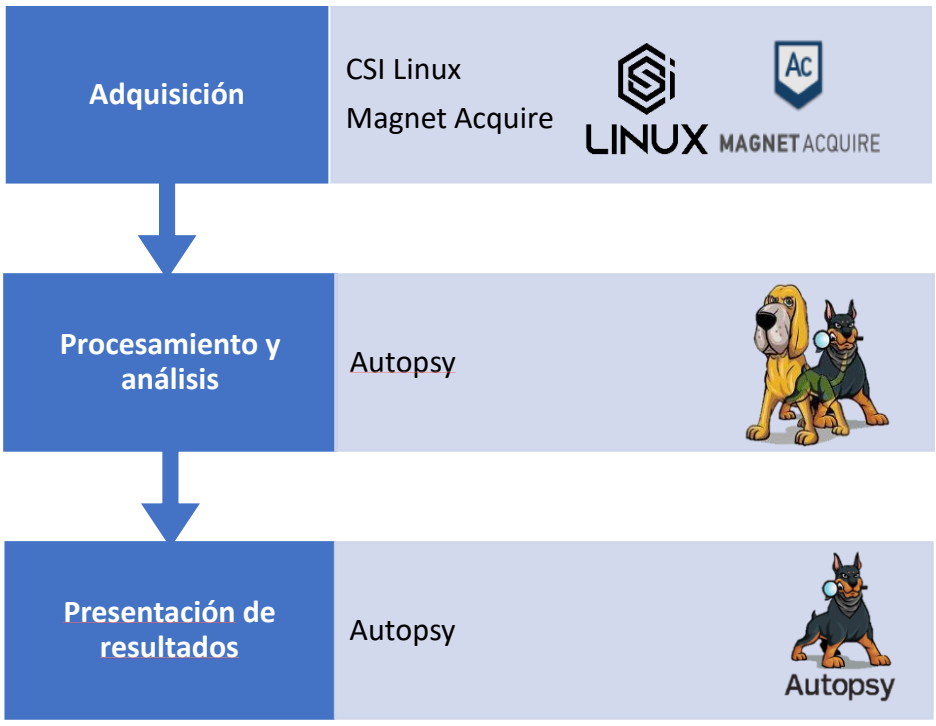
Para cumplir con el primer objetivo de la investigación, que es identificar las herramientas de software libre más relevantes para el análisis forense de dispositivos móviles mediante una revisión documental, se realizó un análisis detallado del universo documental compuesto por 9 artículos científicos, 5 tesis académicas, 3 reportes técnicos y 2 normativas internacionales, obteniendo como resultado las herramientas detalladas en la siguiente ilustración.

	Adquisición	CSI Linux Magnet Acquire AFLogica ADB
	Procesamiento y análisis	Avilla Forensics iLEAPP ALEAPP Autopsy

Ilustración 2. *Herramientas libres para el análisis forense de dispositivos móviles*

2. **Examinación de efectividad de herramientas de software libre para análisis forense de dispositivos móviles mediante análisis documental.**

Posterior a la realización del análisis documental y ejecución de pruebas de concepto en entornos controlados con dispositivos reales, se obtuvo como resultados que las herramientas que se detallan en la siguiente Ilustración, son las que mejor resultados se obtienen.



3. Diseño del marco de trabajo que integra, adquisición, procesamiento, análisis y presentación de evidencias digitales

Para la evaluación del marco de trabajo integral se toma como referencia, la metodología propuesta y detallada en la Ilustración 1. "*Proceso para el análisis forense digital de dispositivos móviles*", la cual detalla el proceso a seguir para el análisis forense de dispositivos móviles, acorde los siguientes puntos:

- Identificación
- Preservación
- Adquisición
- Procesamiento y análisis
- Informe

Por lo expuesto, el marco de trabajo propuesto está encaminado a cumplir con los puntos en mención, para lo cual, en los siguientes apartados se expone la activada a realizar en cada fase.

3.1 Fase de Identificación

La actividad de identificación de dispositivos móviles es un paso crucial en la investigación forense digital, ya que permite determinar la presencia, tipo y posible relevancia de los dispositivos electrónicos que puedan contener evidencia.

Una vez asegurada la escena, se procede a la identificación y documentación de los dispositivos móviles presentes, acorde se detalla en la siguiente Ilustración.

Ilustración 3. Identificación dispositivos móviles

De cada dispositivo identificado debe generar un registro de como mínimo los siguientes detalles:

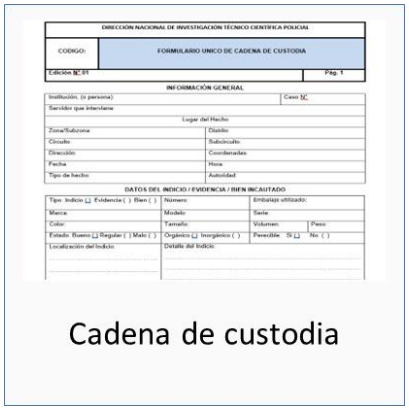
- Marca y modelo del dispositivo
- Número de serie e IMEI (si es visible)
- Estado del dispositivo (encendido, apagado, dañado, bloqueado)
- Ubicación exacta en la escena
- Posibles conexiones a redes o dispositivos cercanos

Para mayore detalle del proceso, se adjunta como Anexo 1 Formulario de verificación de dispositivos móviles.

3.2 Fase de Preservación

La preservación de la evidencia digital constituye una fase fundamental y delicada en la investigación forense, ya que esta puede ser fácilmente manipulada. Para garantizar que la evidencia sea válida en una investigación corporativa o penal, es esencial que los investigadores la salvaguarden y mantengan en su estado original, sin alteraciones, preservando su validez y confiabilidad en todo momento, esta fase requiere una meticulosa documentación de cada acción realizada, desde la

recolección hasta la transferencia, registrando aspectos como la fecha, la hora y los datos de la persona que maneja la evidencia (cadena de custodia). Además, las evidencias deben almacenarse en contenedores apropiados y debidamente etiquetados, como bolsas de Faraday, bolsas antiestáticas, o papel aluminio, y se debe utilizar etiquetas de identificación únicas para asegurar la protección y el seguimiento de la evidencia en todo momento, tal como se puede visualizar en la Ilustración 4. El adecuado manejo y mantenimiento de estos registros es vital para la admisión de la evidencia en un tribunal, ya que cualquier deficiencia en su conservación podría poner en duda su integridad.



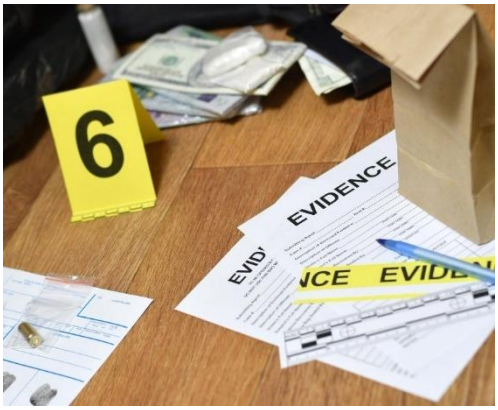


Ilustración 4. Proceso de preservación de la evidencia

3.3 Fase de Adquisición

La fase de adquisición de evidencia en dispositivos móviles es un componente esencial en el análisis forense digital, ya que implica la recolección de datos de manera que se preserve su integridad y se garantice su legalidad, para ellos se debe tomar en cuenta los siguientes aspectos.

3.3.1 Elección del método de extracción de información

Previo a la elección de método de extracción, uno de los procesos que nos permitirá elegir el mejor método de adquisición de la información de los dispositivos móviles, es la expuesta en la ilustración 3, misma que nos dará todas las aristas necesarias para elegir entre una adquisición física, lógica o manual.

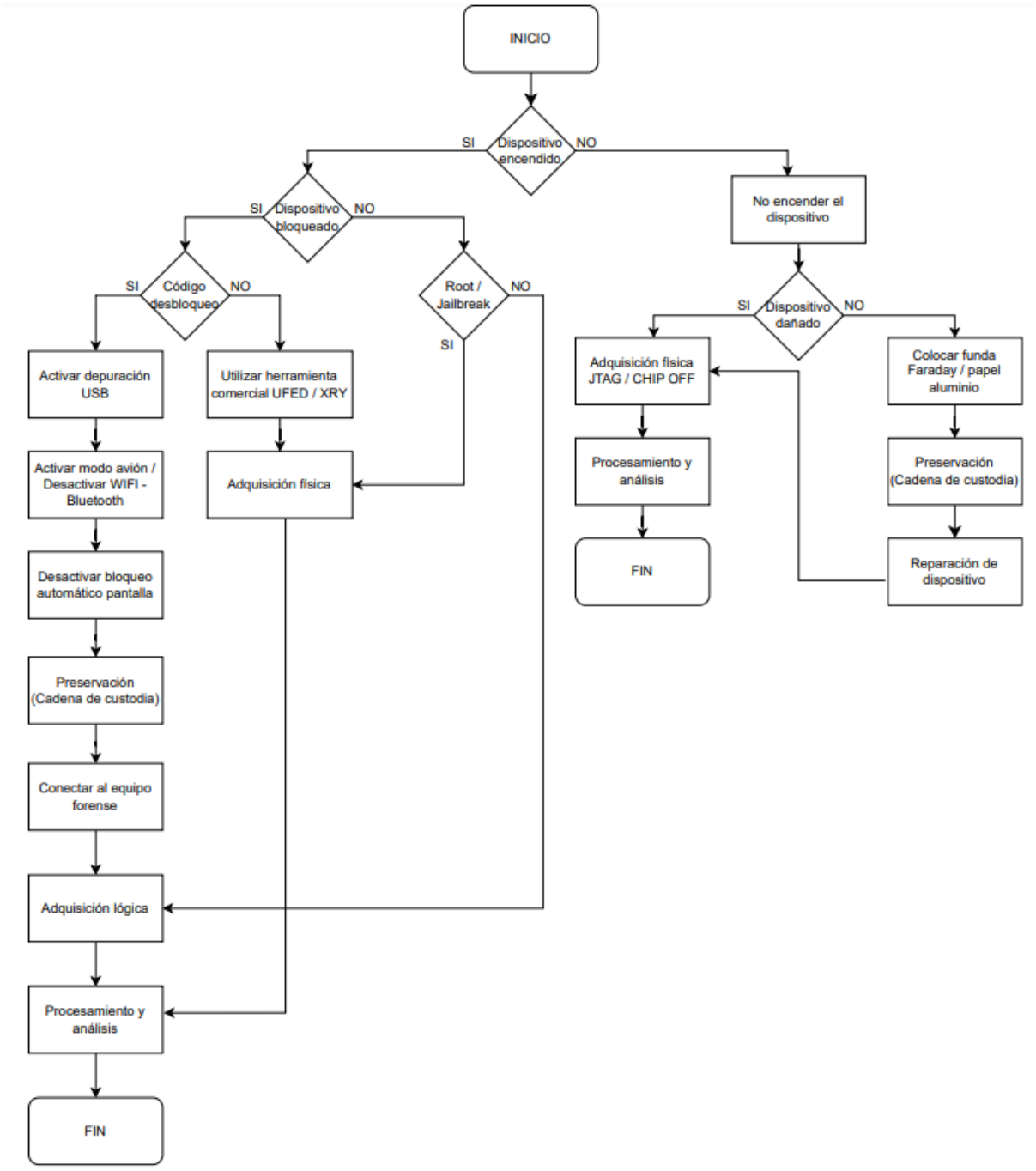


Ilustración 5. Proceso para la adquisición

Una vez identificad esta primera parte, en la Ilustración 6 se detalla los métodos utilizados dentro del proceso de adquisición y/o extracción de información de dispositivos móviles, la elección del método de extracción dependerá de casa caso en particular.

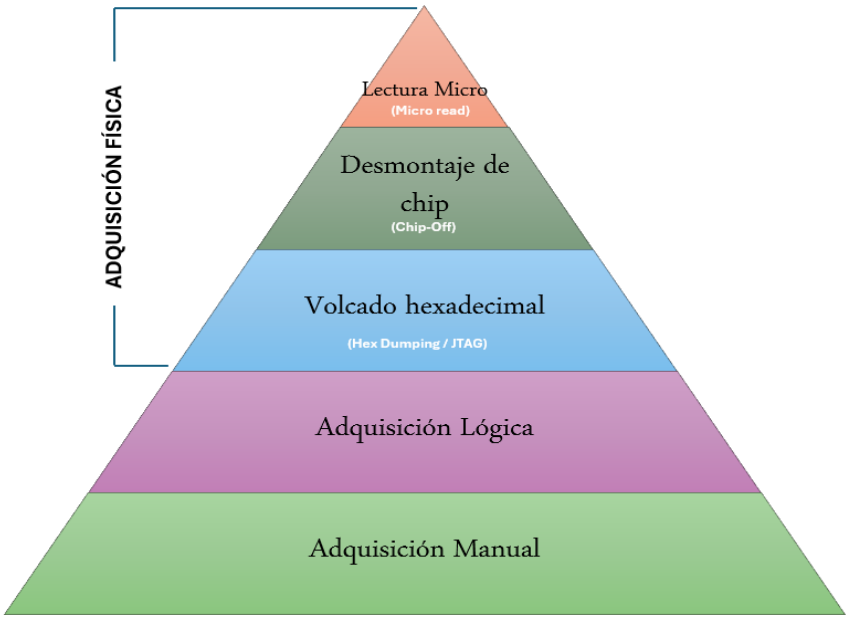


Ilustración 6. Métodos de extracción de información

Existen 3 métodos distintos para la extracción de información de dispositivos móviles, las cuales son: extracción física (*Hex Dump/JTAG, Chip-off, Micro Read*), extracción lógica y extracción manual, acorde el siguiente detalle:

- **Manual:** el especialista forense analizar el dispositivo directamente, o realiza fijaciones fotográficas con herramientas como: XRY Camera o UFED Camera para su preservación.
- **Lógica:** esta técnica necesita establecer conexión entre el dispositivo y el software forense, puede ser a través de un cable USB, Bluetooth, infrarrojos o RJ-45. Es soportada por un gran número de herramientas como UFED, XRY, entre otras.
- **Hex Dump/JTAG**: es una copia bit a bit del contenido, requiere que el equipo se conecte a los puertos de acceso de prueba del equipo (TAP). El resultado es un archivo binario que requiere de un perfil técnico que pueda interpretarlo.
- **Chip-off:** consiste en extraer los chips de memoria del teléfono, el nivel de dificultad de este procedimiento es elevado, cualquier error puede ocasionar la pérdida definitiva de los datos.
- **Micro Read:** este proceso implica interpretar los datos del chip de memoria, se debe utilizar un microscopio de alta potencia para analizar las puertas físicas de los chips, leer las puertas binarias y convertirlas en ASCII.

A la hora de seleccionar el método más adecuado, se debe tener en cuenta algunos aspectos, por ejemplo: el nivel de exhaustividad requerido, la limitación de tiempo para realizar la adquisición, tipo de información a obtener: información volátil, información previamente eliminada, información de aplicaciones de terceros, entre otros, acorde el siguiente detalle:

Debido a las características de seguridad inherentes a los dispositivos móviles, extraer los datos no siempre es sencillo. El método de extracción se decide en gran medida dependiendo del sistema operativo, la marca, el modelo y la herramienta utilizada para dicho proceso (Skulkin, Tindall, & Tamma, 2018). En la ilustración 6 se identifican los métodos de adquisición acorde la información a extraer.

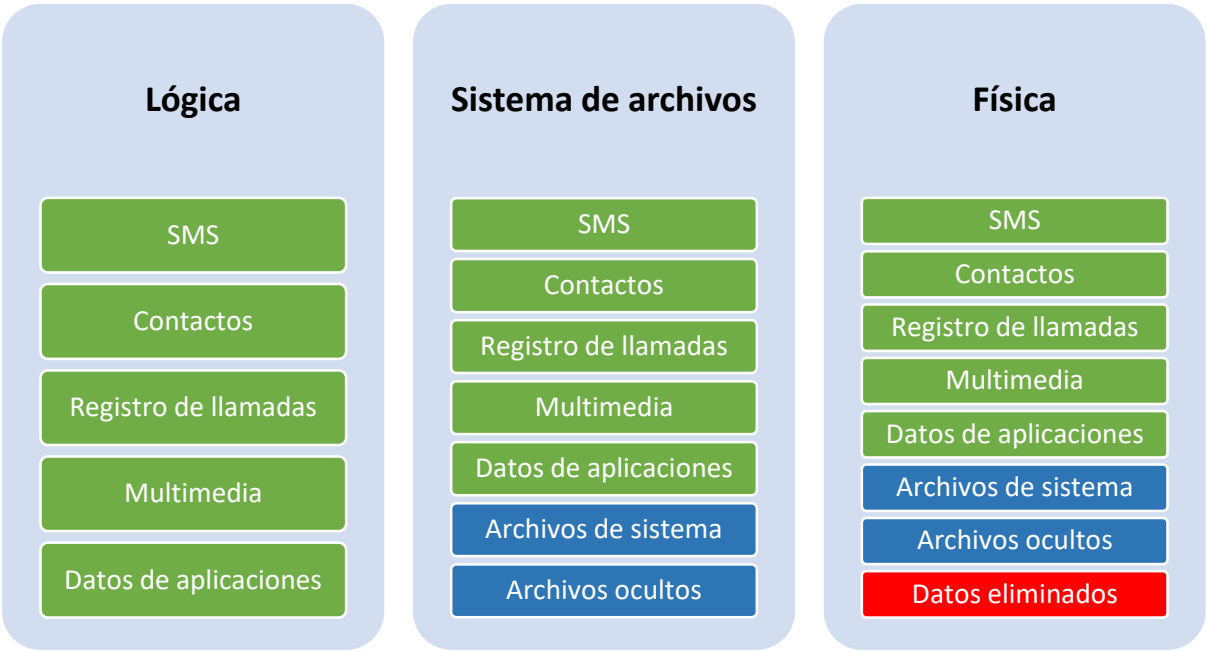


Ilustración 7. Adquisición de información de dispositivos móviles, acorde el método de extracción

Adquisición Manual

Este método de adquisición es un método de recolección de evidencias digitales de un dispositivo móvil sin utilizar herramientas automatizadas, se basa en la inspección visual y documentación manual a través de fijaciones fotográficas de la información disponible en el dispositivo.

Adquisición Lógica

Este método recupera archivos presentes en el sistema de archivos de un dispositivo móvil, como mensajes de texto, historial de llamadas e imágenes. Utiliza las API del fabricante para sincronizar el contenido del dispositivo móvil con una computadora,

obteniendo registros de llamadas, SMS, MMS, historial del navegador, contactos, metadatos de archivos multimedia, datos de ubicación, actividad de Internet, lista de aplicaciones instaladas y datos de aplicaciones de redes sociales.

Este método puede ayudar a recuperar contenido eliminado almacenado en archivos SQLite, archivos ocultos, registros del sistema y proporciona un volumen intermedio de datos en comparación con la extracción lógica estándar.

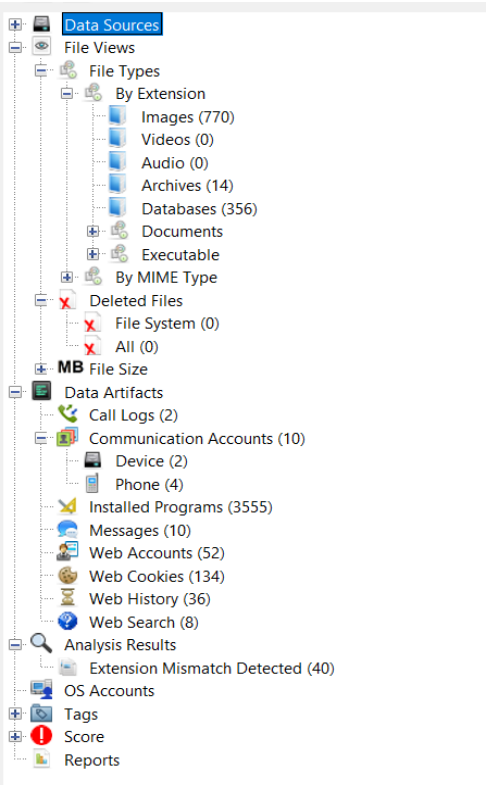
Adquisición Física

Implica hacer una copia bit por bit de un dispositivo de almacenamiento flash completo, equivalente a una imagen completa de un disco duro. Los datos extraídos con este método suelen estar en forma de datos brutos (como un volcado hexadecimal) que luego se pueden analizar más a fondo para obtener información del sistema de archivos o datos legibles por humanos. Para Android, la viabilidad de las extracciones físicas depende del modelo del dispositivo y si ha sido "rooteado", para iOS que el dispositivo tenga accesos prolijeados o tenga “jailbreak”.

Finalmente, dentro del proceso de adquisición

3.3.2 Elección de la Información almacenada en los dispositivos móviles a ser extraída.

A través de la extracción forense de datos de dispositivos móviles, se puede obtener gran cantidad de información, estos datos se pueden encontrar en varias ubicaciones: por ejemplo, la tarjeta SIM, la tarjeta de almacenamiento externa y la memoria del teléfono, además, el proveedor de servicios también almacena información relacionada con las comunicaciones. En esta tesis nos centraremos en adquirir los datos de la memoria de un teléfono, aunque las herramientas también permiten recuperar información borrada durante la adquisición forense, esto depende mucho del modelo y sistema operativo de los dispositivos móviles, en general los siguientes datos son comunes en todos los modelos de teléfonos:



- Libreta de dirección (Contactos)
- Calendarios
- Registros e historial de llamadas
- Mensajes de texto – SMS
- Redes sociales (Facebook, WhatsApp, X, viber, LinkedIn, Google)
- Archivos multimedia (fotos, videos)
- Correos electrónicos
- Documentos
- Mapas / GPS
- Historial de navegación
- Ficheros eliminados
- **SIM:** Código de identificación del chip
- **IMEI:** identificador único de cada dispositivo móvil
- **Celda:** Es el espacio de cobertura de telefonía celular

Ilustración 8. Información almacenada en dispositivos móviles

3.4 Fase de Procesamiento y análisis

Una vez ejecutado el método de extracción que cumpla con los requerimientos específicos de la investigación, el siguiente paso crucial es la elección de la herramienta adecuada para ejecutar el proceso. Es fundamental que la herramienta elegida esté alineada con las necesidades del trabajo, permitiendo un procesamiento preciso y eficiente de los datos.

En esta fase se utiliza la herramienta Autopsy, la mista que permite realizar un procesamiento adecuando acorde las mejores prácticas y estándares a nivel internacional.

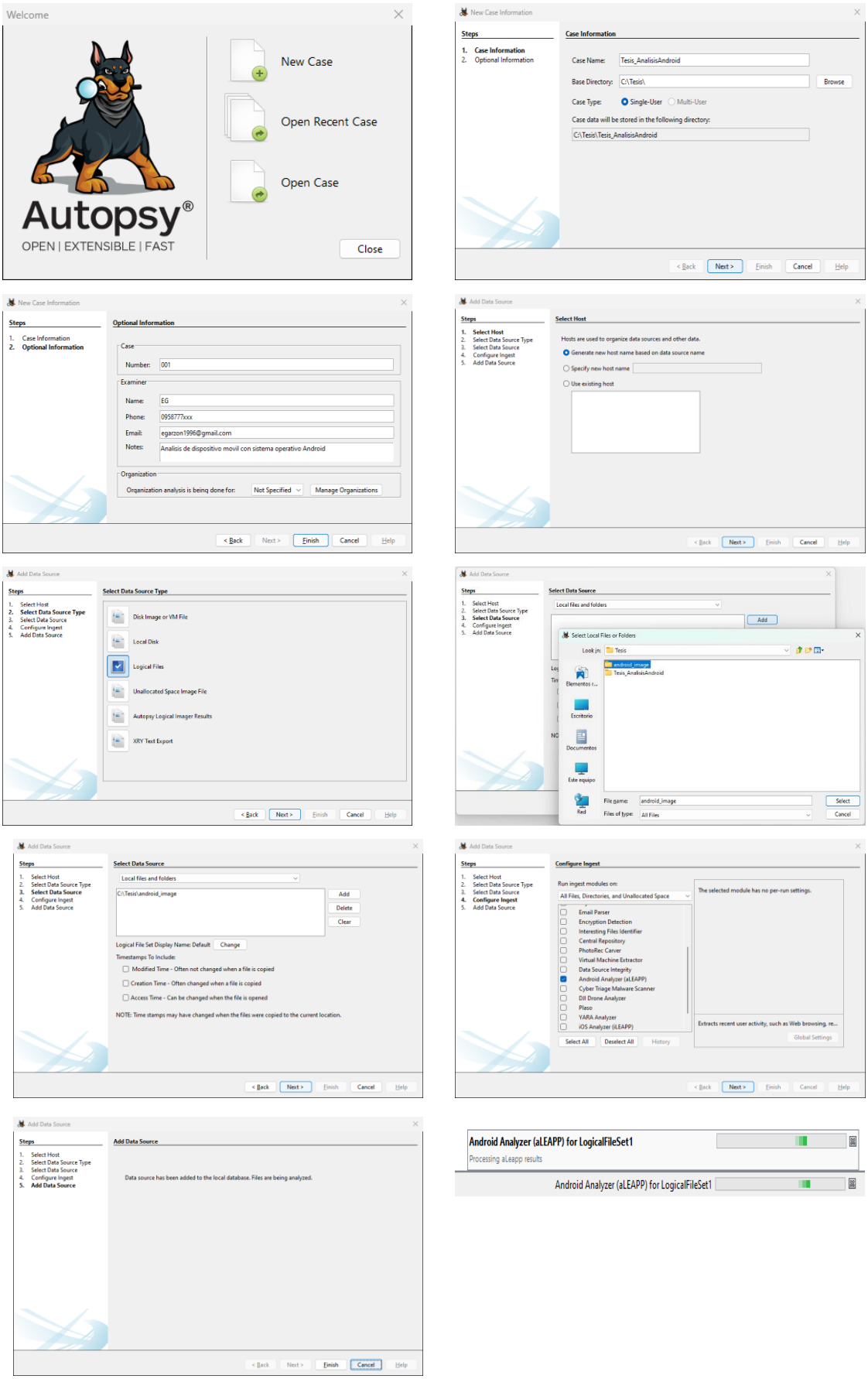


Ilustración 9. Procesamiento de una imagen forense de un dispositivo Android

Esta herramienta permite procesar e indexar la información la información de tal manera que el analista que está llevando la investigación puede realizar el análisis de manera adecuada, fácil y precisa.

3.5 Fase de Informe (Presentación de resultados)

Finalmente, y no menos importante viene el proceso de presentación de resultados, los mismos que deben ser claros, precisos y concisos, de igual manera para la presentación de resultados, Autopsy nos permite generar reportes del análisis realizado, el cual debe ser adjuntado al informe que se presenta de todo el proceso investigativo del análisis forense digital de un dispositivo móvil, en la Ilustración X, se puede visualizar como se generan estos reportes.

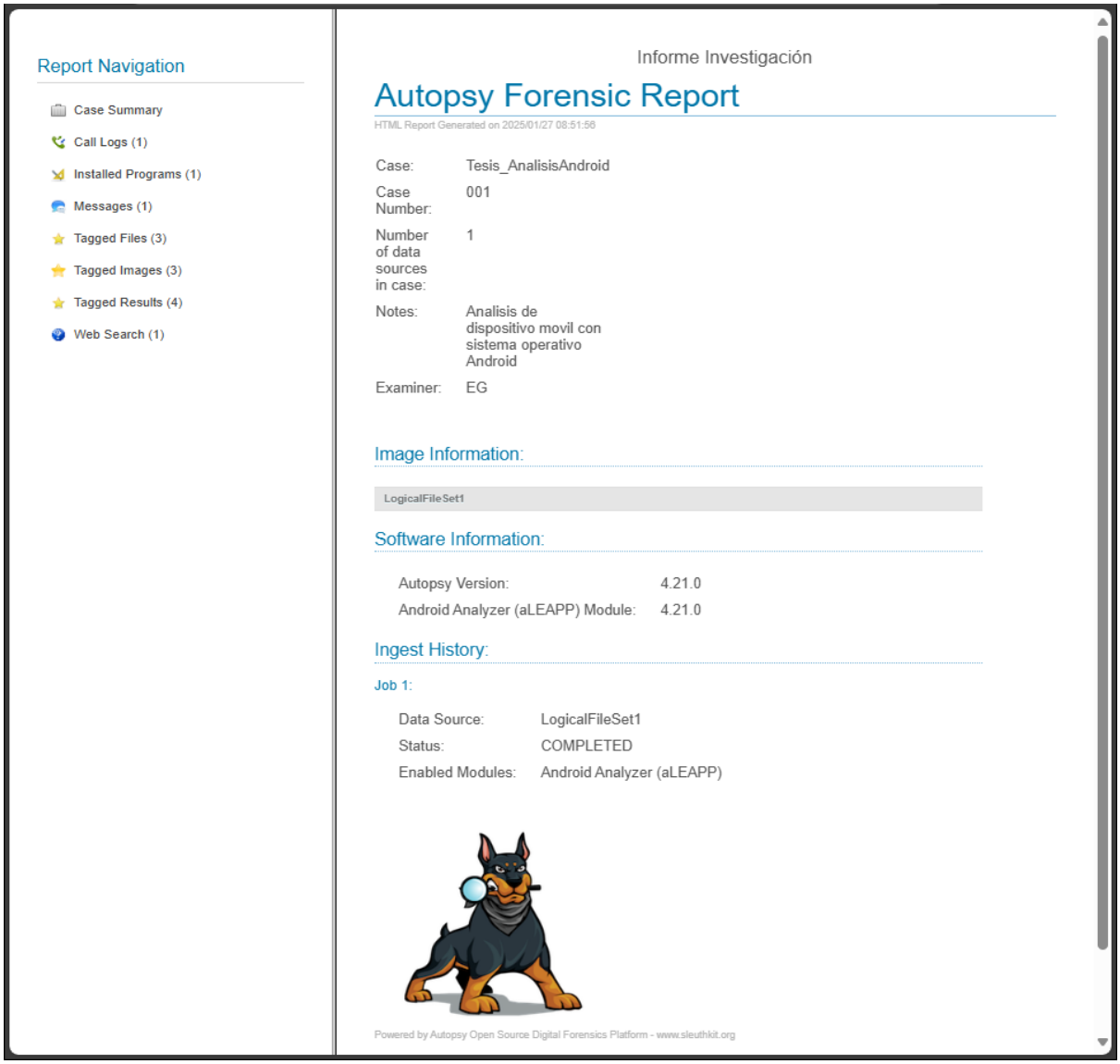


Ilustración 10. Reporte con la herramienta Autopsy

4. Evaluación del marco de trabajo mediante pruebas de concepto en entornos controlados

Laboratorio de análisis forense de dispositivos móviles

En los siguientes apartados se detallarán las fases para el proceso de análisis forense de dispositivos móviles basado en un caso práctico.

Preparación de la investigación

Esta fase preliminar comienza cuando se recibe una solicitud de análisis forense de un dispositivo móvil, la cual da inicios a la preparación de todos los ambientes, herramientas, documentos y formularios necesarios para documentar todo el proceso incluyendo su respectiva cadena de custodia de ser una causa legal, la cual involucra información del dueño del dispositivo, marca y modelo del dispositivo, el propósito del análisis, la información que requiere el solicitante, entre otras acciones.

A partir de los detalles presentados por el solicitante, es importante tener claro el objetivo de cada análisis forense a realizar, esto es fundamental para que se cumpla con el objetivo del análisis.

4.1 Identificación

Esta fase tiene como objetivo principal identificar el o los dispositivos móviles a los cuales se les realizará el análisis forense digital. En primera instancia se identifica el dispositivo, al cual se va a realizar el análisis forense, logrando obtener los datos esenciales para poder continuar con la ejecución de las siguientes fases, la identificación la podemos realizar acorde lo detallado en la Ilustración 9.

Ilustración 11. Identificación del dispositivo

De la identificación del dispositivo móvil, se logró obtener los siguientes datos generales:

- **Marca:** Samsung
- **Modelo:** Galaxy S21
- **IMEI:** 3555218130451XX
- **Estado:** Encendido
- **Número de teléfono:** 098123987X

4.2 Preservación

Aislamiento de dispositivos

Una vez que ya se cuenta con el dispositivo, uno de los pasos más importantes previa a la adquisición es aislar preservar el mismo para evitar perdida de datos, así mismo es importante tener en cuenta de que, si el dispositivo se encuentra bloqueado y si se tiene la posibilidad, solicitar la clave o desbloqueo para adquirir la mayor cantidad de datos. Si el dispositivo se encuentra desbloqueado se recomienda realizar las configuraciones respectivas para tener un mayor acceso al mismo, esto acorde lo detallados en las siguientes secuencias de ilustraciones.

- **Bloqueo de comunicaciones inalámbricas**

Este paso consiste en activar el modo avión del dispositivo móvil, para lo cual en primera instancia se debe bloquear las comunicaciones inalámbricas incluyendo WiFi y Bluetooth para prevenir que ningún dato sea modificado o eliminado a través de comunicaciones externas, acorde se detalla en el Collage de la Ilustración 10.

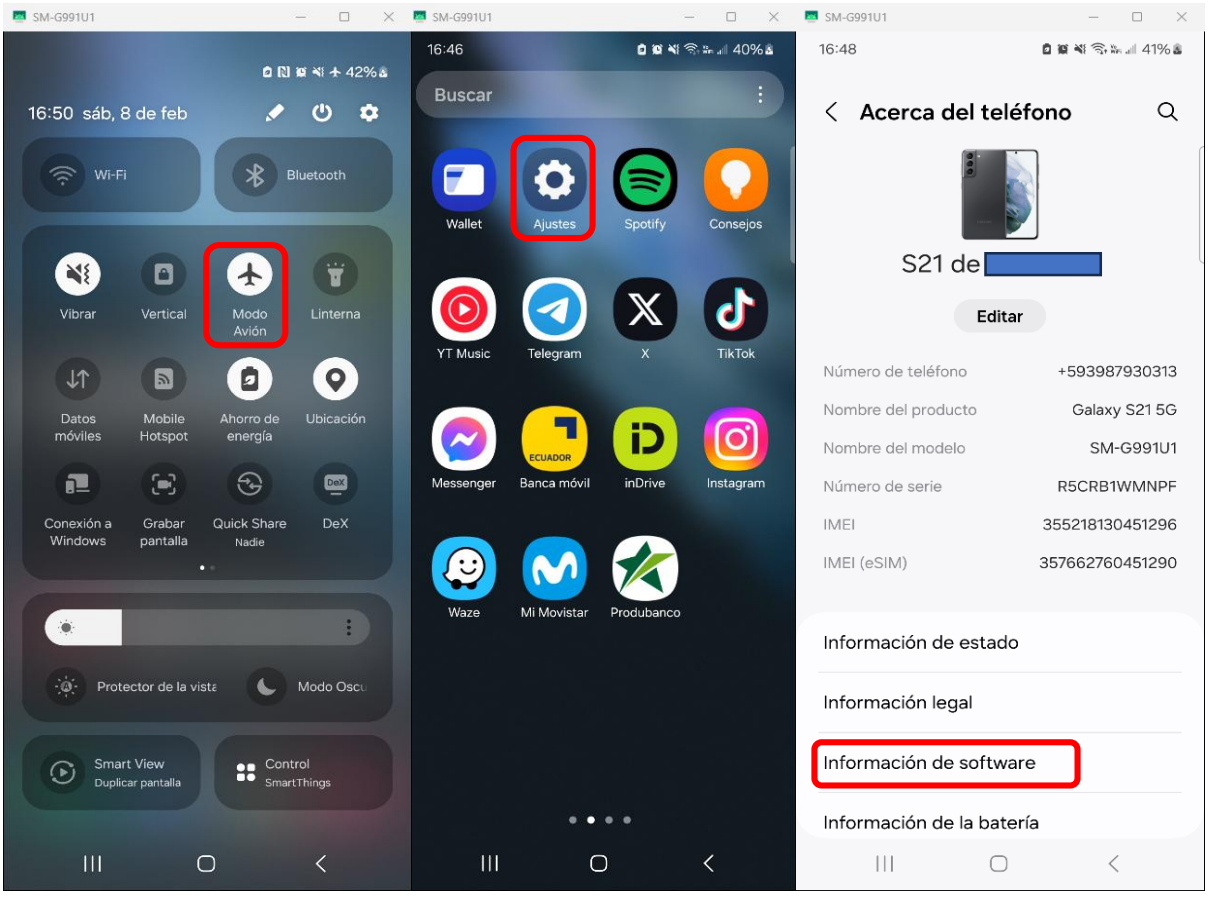


Ilustración 12. Pasos para la depuración USB

- **Habilitación de la depuración USB**

En la ilustración 11, se visual el proceso para activar la “Depuración USB” del dispositivo móvil, para lo cual se debe ejecutar las siguientes acciones: en la opción “Número de compilación” se debe dar 7 veces clic para activar el modo “Opciones de desarrollador”, una vez activo, regresamos a las opciones de ajustes y nos dirigimos a la sección final donde se encontrará el modo activado, en la misma interfaz se muestra la opción “Depuración por USB” que normalmente se encuentra desactivada; se procede a realizar la activación.

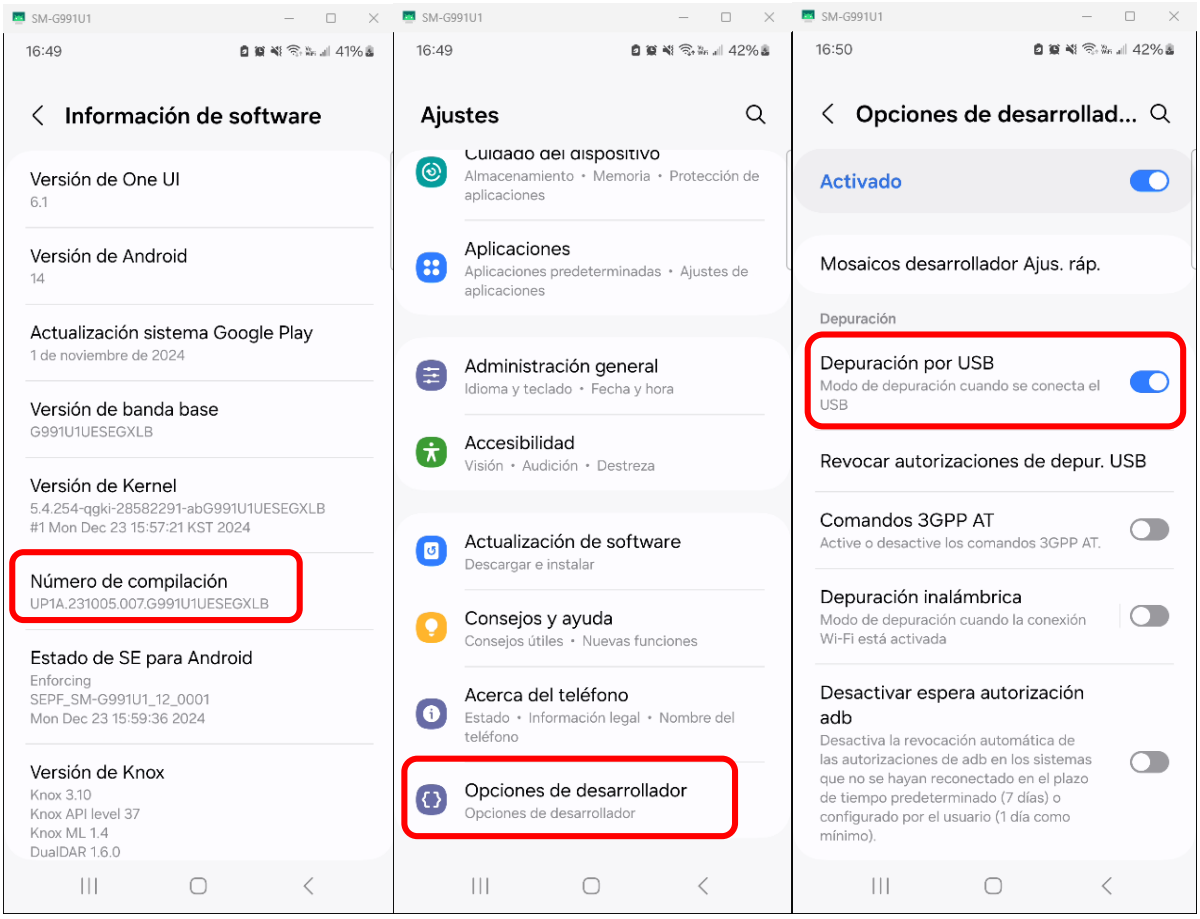


Ilustración 13. Pasos finales depuración USB

Se debe tener en cuenta que, en esta fase, si el análisis forense implica un proceso judicial, se debe contar con la autorización de la autoridad competente, y se debe ejecutar todo el proceso de aseguramiento y preservación incluyendo el levantamiento de la cadena de custodia. De ser un proceso administrativo continuaremos con la siguiente fase.

4.3 Adquisición

Durante esta etapa, se emplean herramientas y técnicas especializadas para obtener una copia exacta de la información, asegurando que no se altere en ningún momento la data. Así mismo, se hace uso de diversas herramientas de software libre que facilitan la adquisición y/o extracción de los datos de manera efectiva del dispositivo móvil, respetando los estándares de calidad y confiabilidad necesarios en el proceso forense. En esta fase y en este laboratorio se efectúa la adquisición lógica de información de un dispositivo móvil con dos herramientas diferentes:

Adquisición de imagen forense en dispositivos Android con la herramienta Magnet ACQUIRE

Una vez conectado el dispositivo donde se encuentra la herramienta forense instalada, ejecutamos la herramienta, la misma que debe detectar el dispositivo móvil a extraer acode se visualiza en la Ilustración 14.

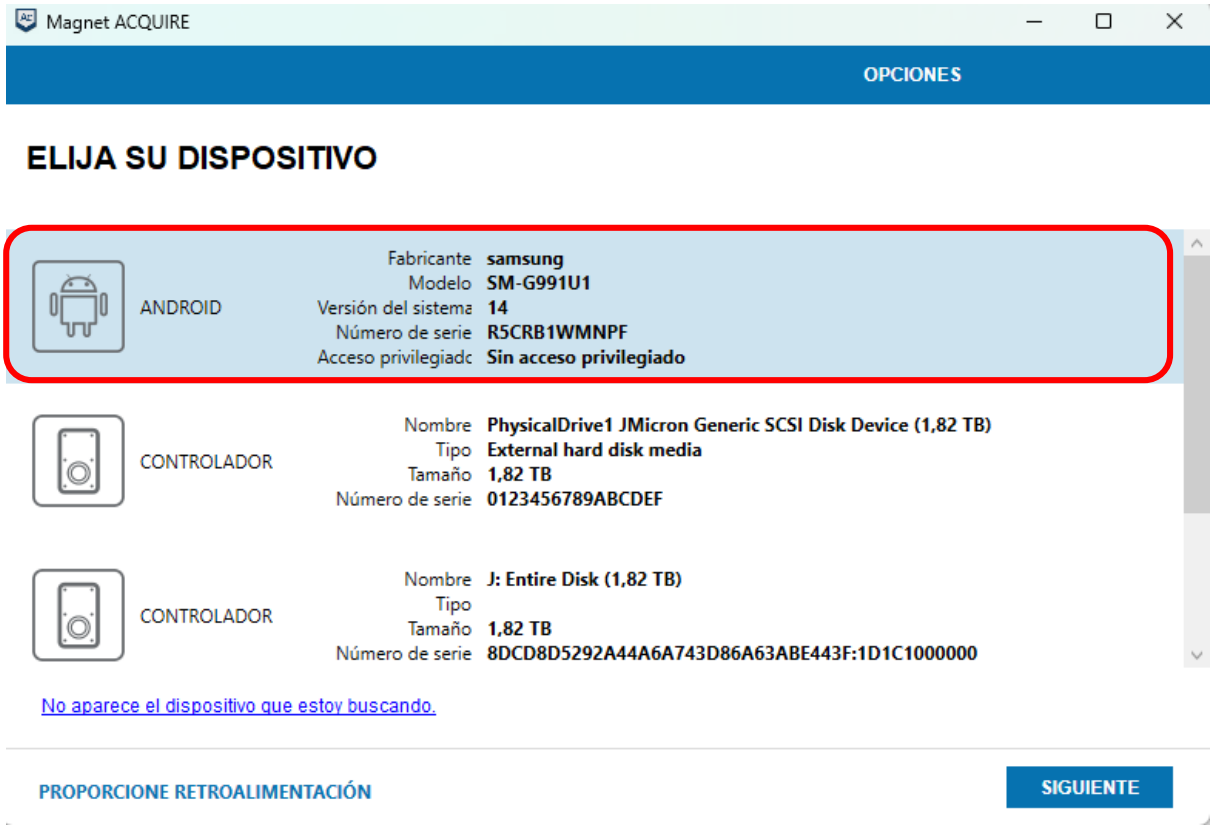


Ilustración 14. Selección o elección del dispositivo móvil a extraer

Posteriormente, se procede a seleccionar la opción “Tipo de imagen”, para la adquisición de la imagen forense como se muestra en la ilustración 13.

Ilustración 15. Selección del tipo de imagen a extraer

Continuando con el proceso, se configura el directorio en donde se almacenará la evidencia extraída, esto se realiza en la opción “Crear la carpeta de evidencias” como se muestra en la ilustración 16, donde se almacenará la imagen obtenida.

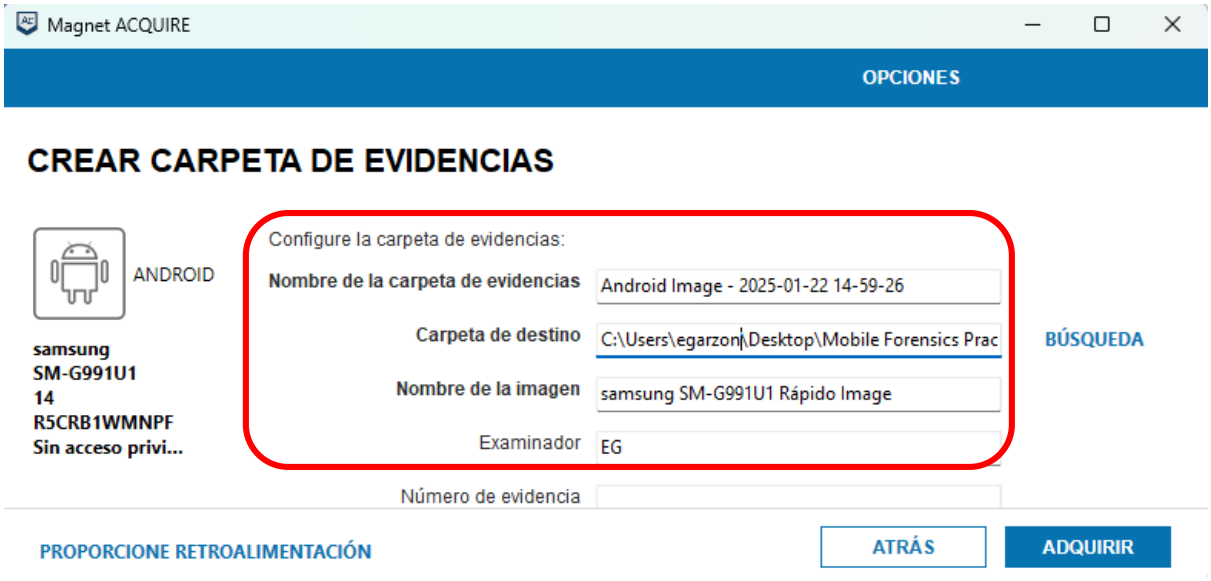


Ilustración 16. Creación de carpeta de evidencias

Una vez configurada la ruta y nombre con el que se guardará la imagen, se procede con la adquisición, como podemos visualizar en la ilustración 17.

En este punto es importante tener en cuenta que el dispositivo móvil debe estar configurado para que la pantalla no se bloquee y desactivado las diferentes opciones de bloqueo (patrón, pin, contraseña).

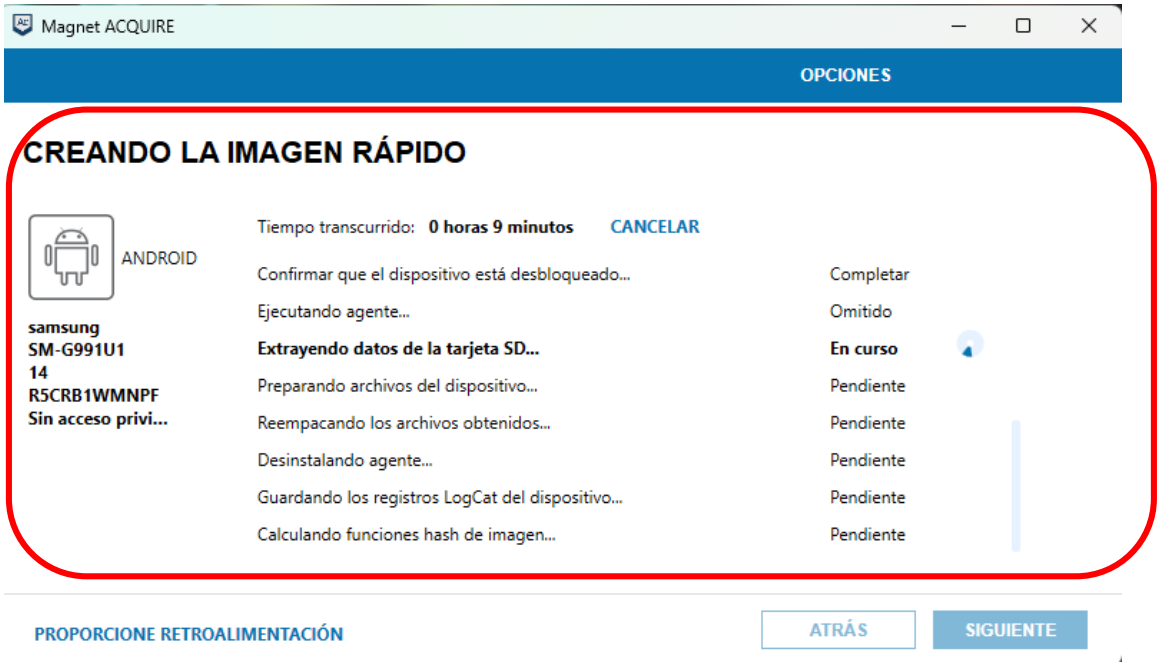


Ilustración 17. Creación de la imagen forense

Finalmente, el software forense nos muestra un breve resumen con la extracción y generación de la imagen del dispositivo móvil, como se puede visualizar en las ilustraciones 18 y 19.

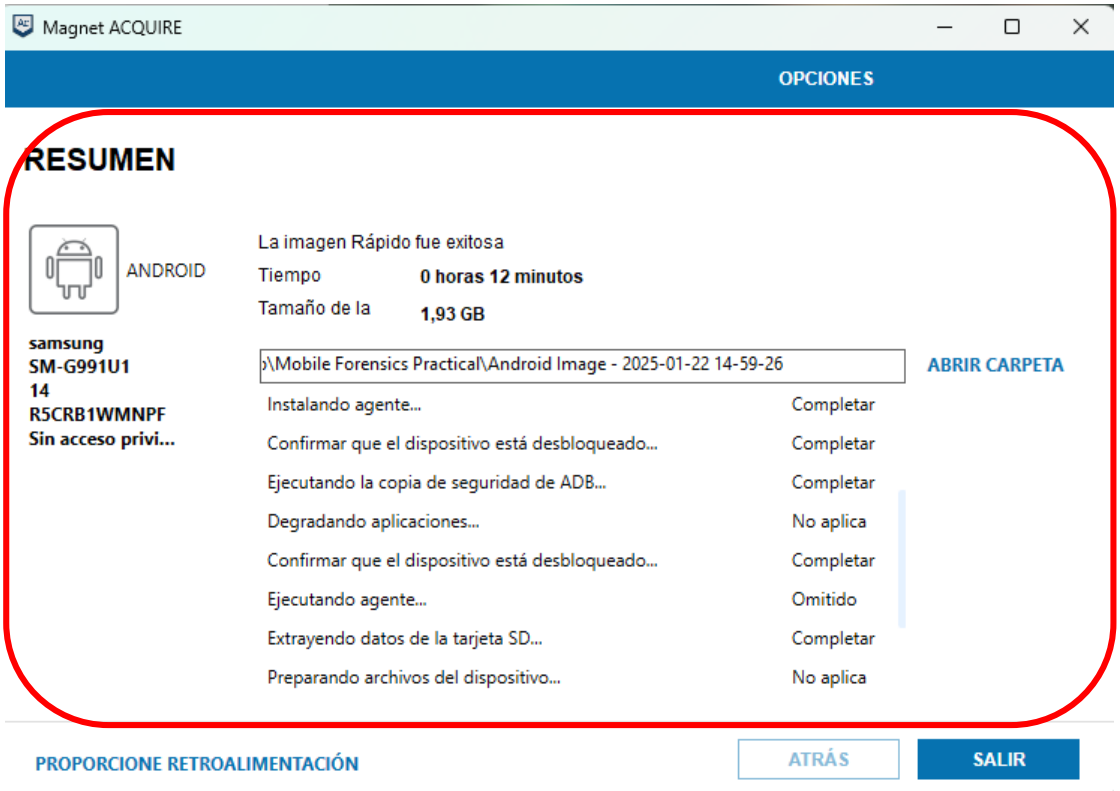


Ilustración 18. Resumen de la adquisición de la imagen forense

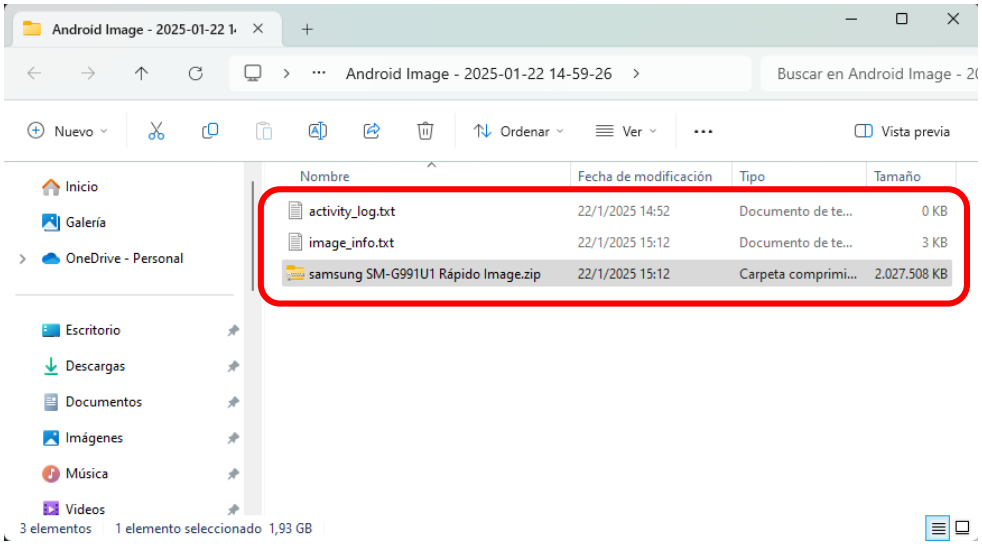


Ilustración 19. Ruta donde se encuentra la evidencia digital

Adquisición de imagen forense en dispositivos Android con la herramienta CSI Linux

Al igual que la adquisición con Magnet Acquire, en el sistema CSI Linux se realizan los mismos pasos previos como: depuración USB, habilitación modo avión, desbloqueo de la pantalla, desbloqueo de métodos de seguridad y creación del caso. Por lo tanto, para iniciar el proceso de adquisición con la herramienta CSI Linux en la ilustración 20 y 21 podemos ver las opciones para iniciar con la adquisición de un dispositivo móvil con Sistema Operativo Android.

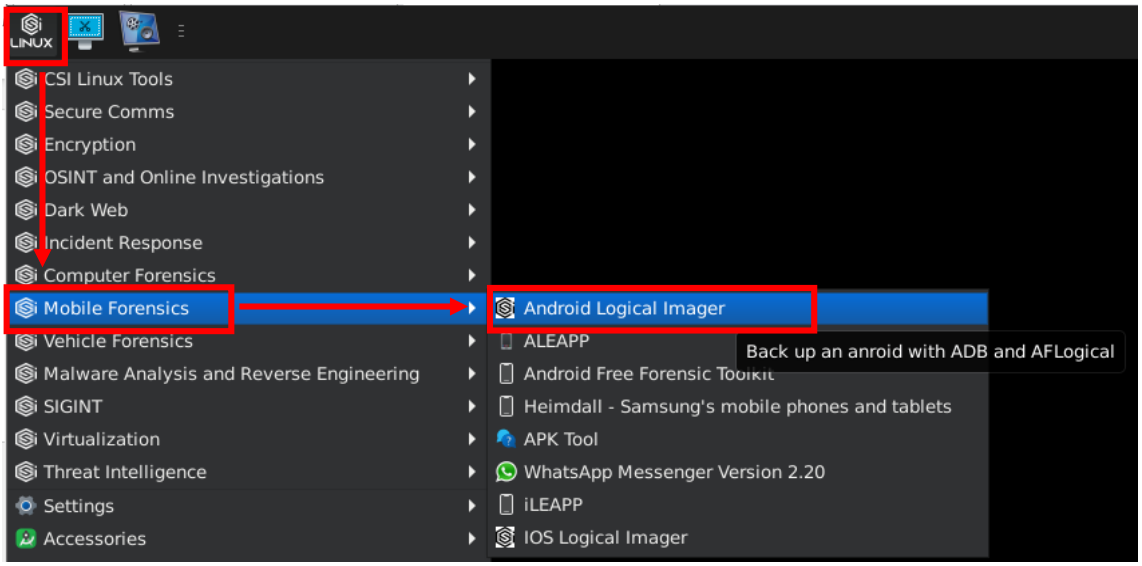


Ilustración 20. Adquisición con la herramienta CSI-Linux con un SO Android

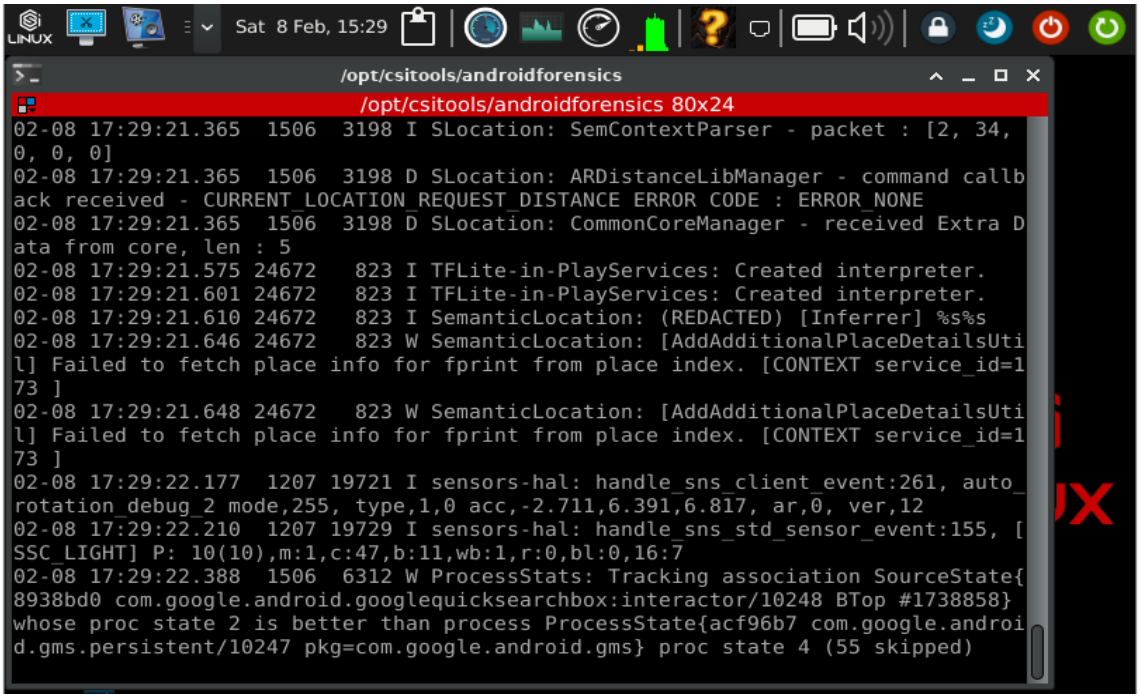


Ilustración 21. Proceso de adquisición con CSI-Linux

Una vez finalizado el proceso de adquisición se puede visualizar en las ilustraciones 22 y 23 la creación de directorios y la generación de imagen producto de la extracción del dispositivo móvil Android.

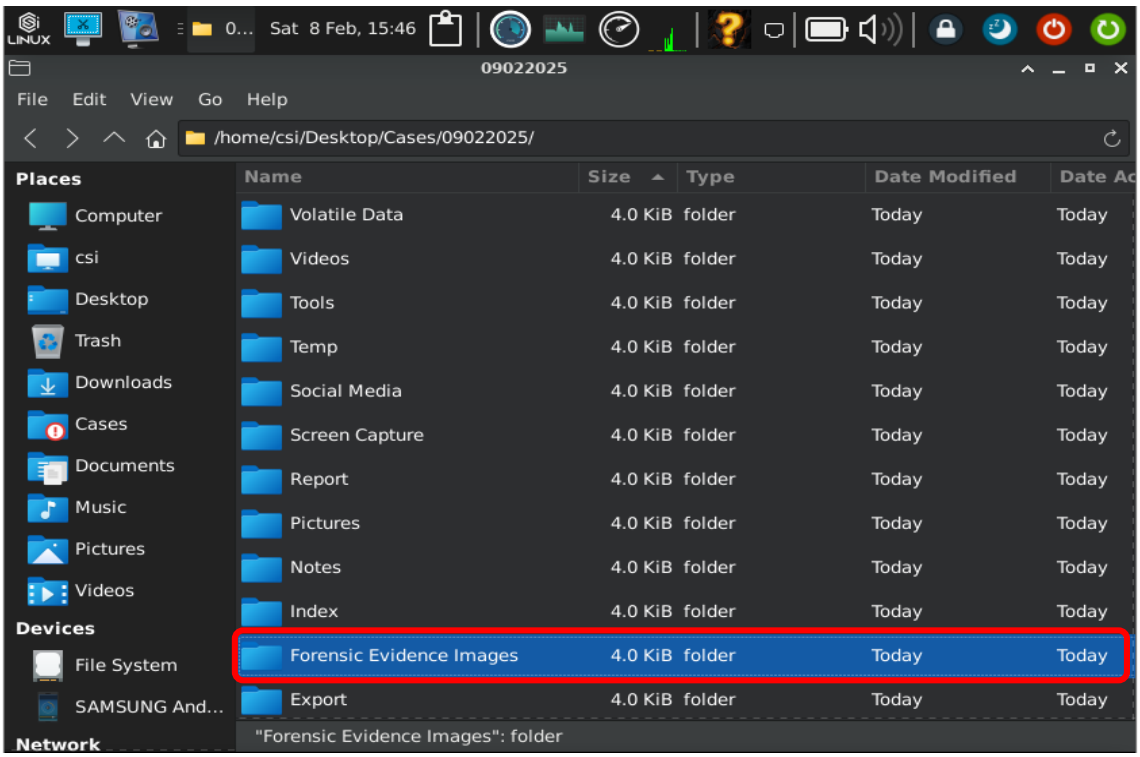


Ilustración 22. Creación de directorios de la imagen forense

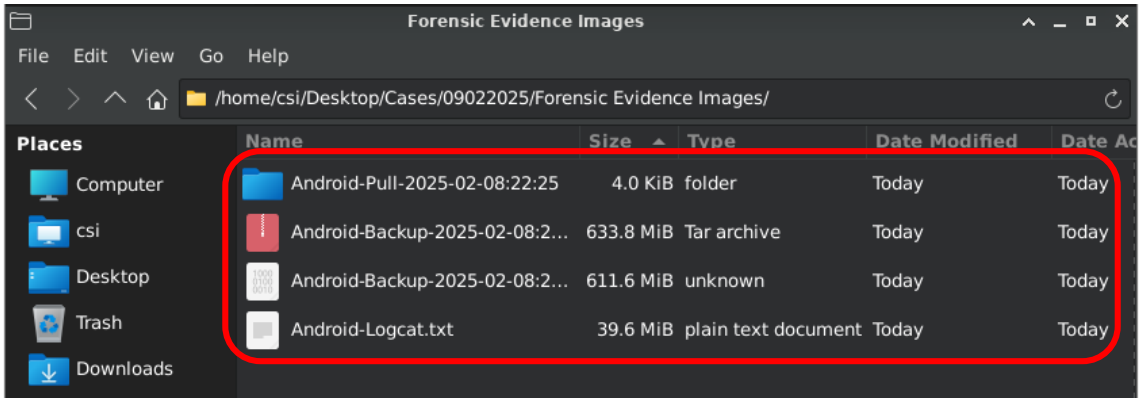


Ilustración 23. Generación de la imagen forense del dispositivo móvil

Finalmente, se puede visualizar en la ilustración 24 los hashes generados de la extracción mismos que permiten validar en todo momento la integridad del proceso.

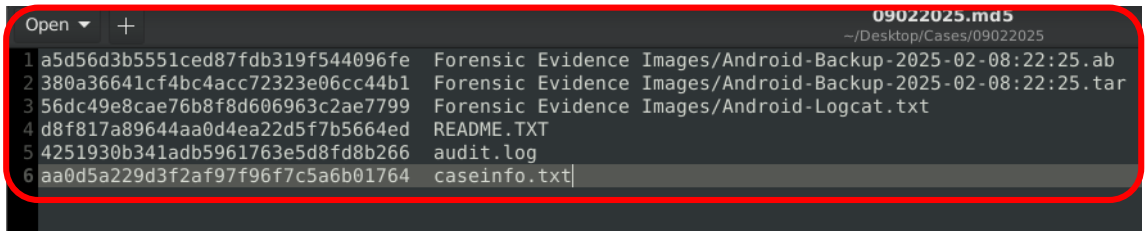


Ilustración 24. Hashes de la extracción de la imagen forense

Adquisición de imagen forense en dispositivos iOS con la herramienta CSI-Linux

En la ilustración 25 se visualiza el proceso para la extracción lógica de un dispositivo móvil con sistema Operativo iOS. La cual se sigue los mismos pasos que permitieron generar la adquisición de una imagen con un dispositivo Android.

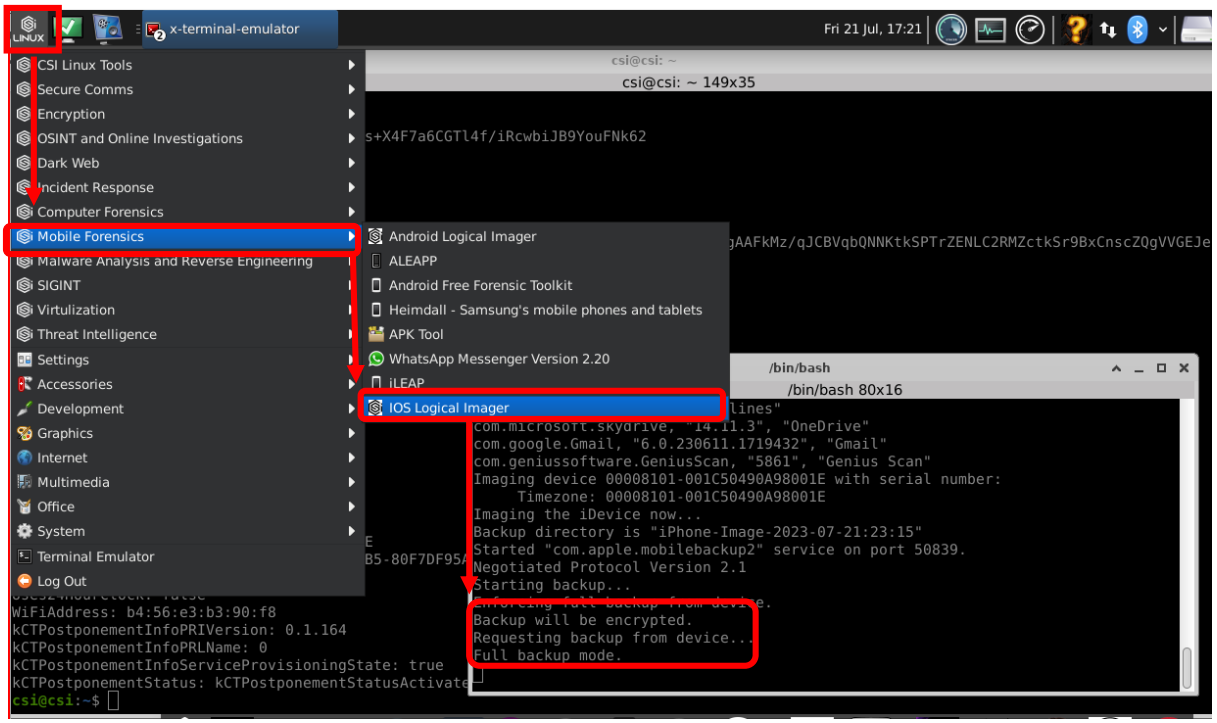


Ilustración 25. Adquisición con la herramienta CSI-Linux con un SO iOS

4.4 Procesamiento y análisis

En la fase de procesamiento y análisis de dispositivos móviles se emplea el software de análisis forense Autopsy. Inicialmente, se carga la adquisición de datos extraída mediante MAGNET ACQUIRE, CSI Linux o cualquier otro método que permita obtener una imagen forense, garantizando la integridad de los datos. El primer paso para el procesamiento y análisis consiste en iniciar el Software especializado de análisis forenses **Autopsy**, posterior se procede a crear un nuevo caso e ingresar información relevante, como el nombre del caso y la ruta donde se almacenará la evidencia procesada, tal como se muestra en las ilustraciones 26 y 27.

Ilustración 26. Interfaz inicial Autopsy

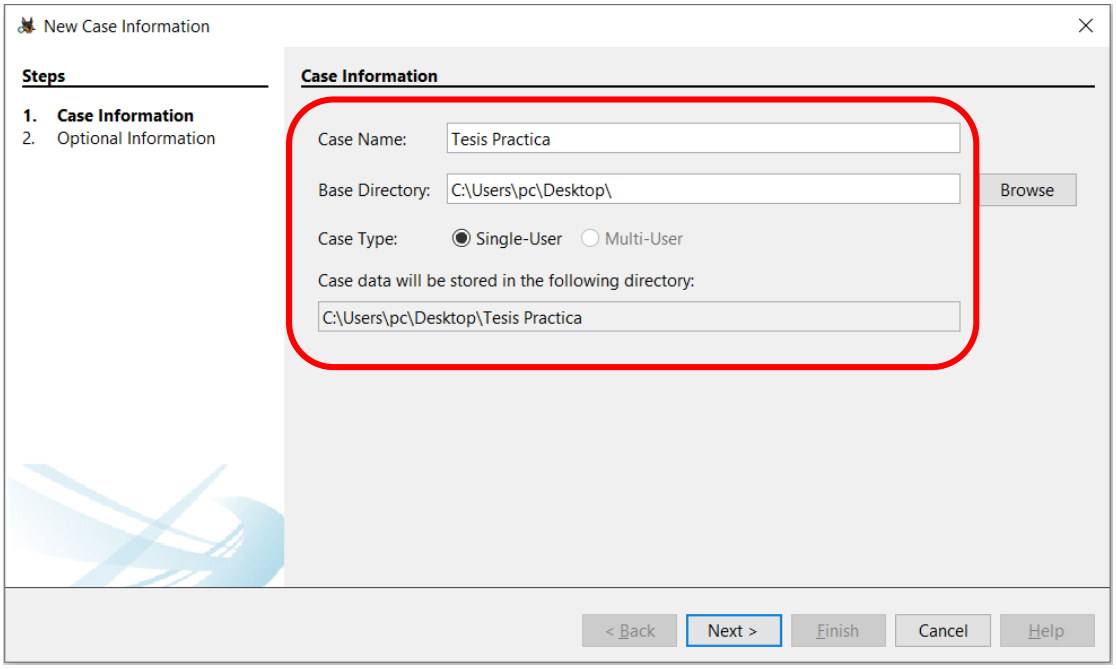


Ilustración 27. Información del caso

Como siguiente paso, es fundamental registrar datos detallados del examinador forense, esto incluye cualquier información relevante que pueda ser necesaria para documentar quién está realizando el análisis y para garantizar la cadena de custodia de la evidencia. Este paso es crucial para mantener la integridad y transparencia del proceso forense.

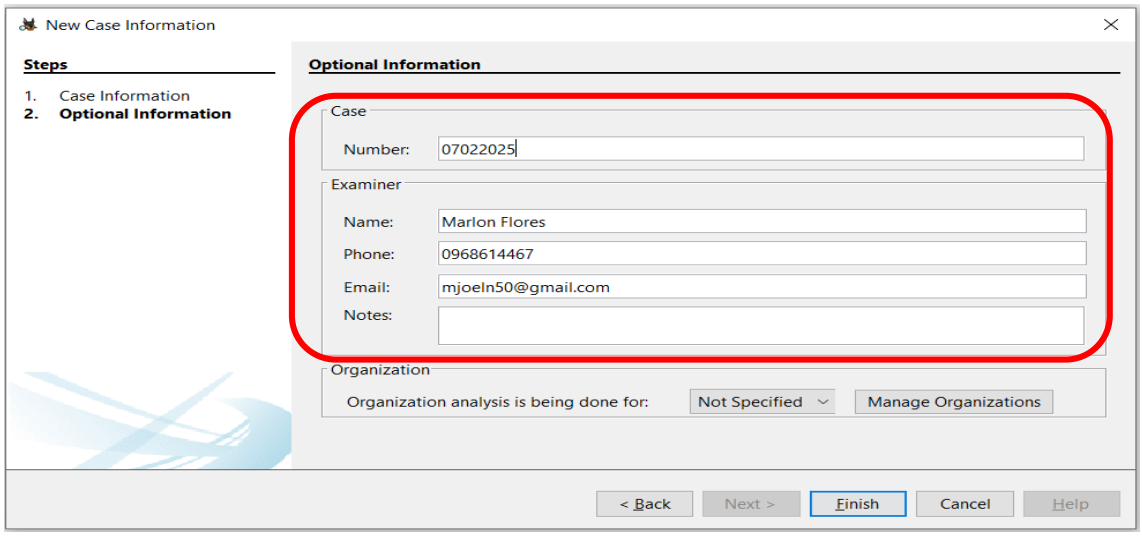


Ilustración 28. Datos del experto

Una vez completado el registro de la información del caso, se procede a seleccionar la fuente de datos a procesar. En esta investigación, se utilizará la opción “Logical Files”, que permite cargar la imagen forense previamente generada a partir de la extracción lógica de los datos forenses del dispositivo móvil.

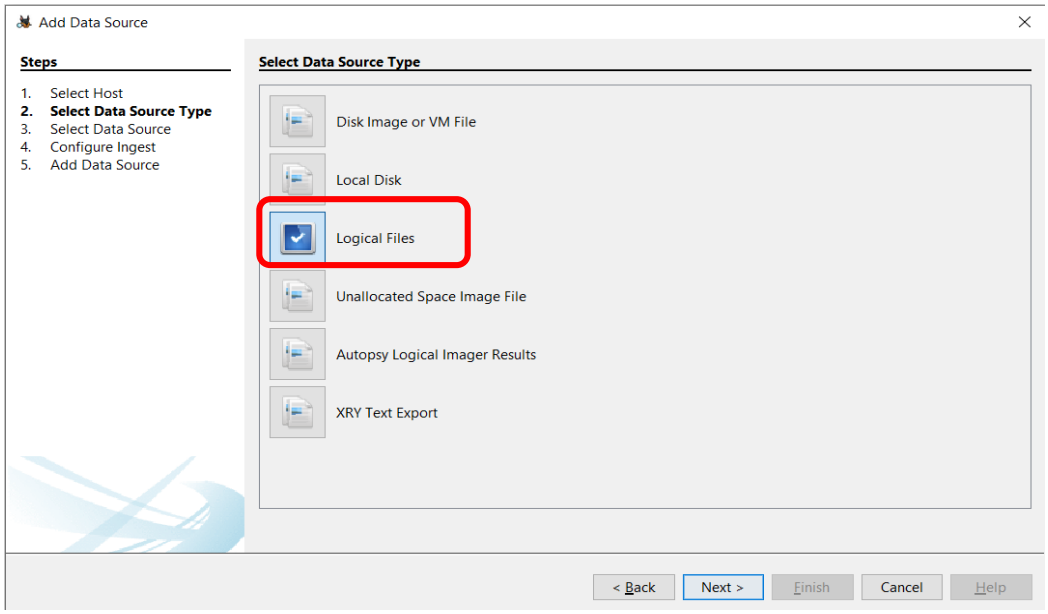


Ilustración 29. selección fuente de datos

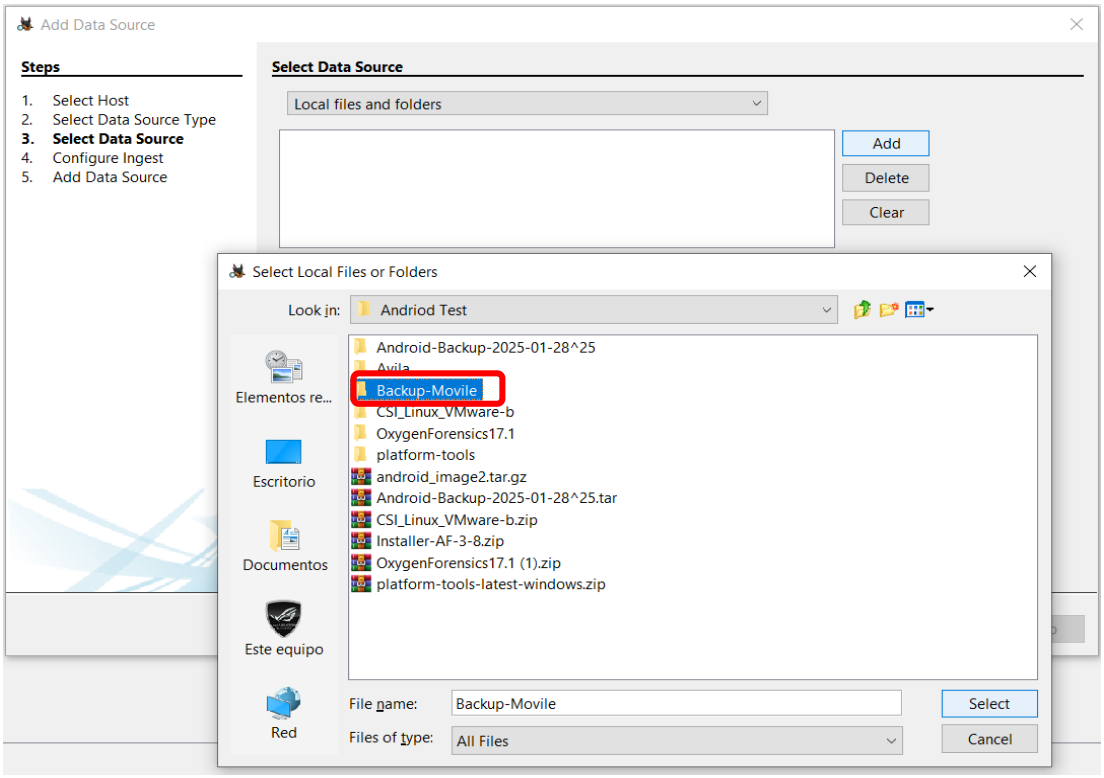


Ilustración 30. Selección de la imagen forense a procesar

Como siguiente paso, se debe configurar la ingesta y seleccionar los módulos de análisis que se utilizar y serán necesarios para procesar e indexar la información acorde el objetivo de la investigación y la fuente de origen, en este caso la imagen del sistema operativo Android.

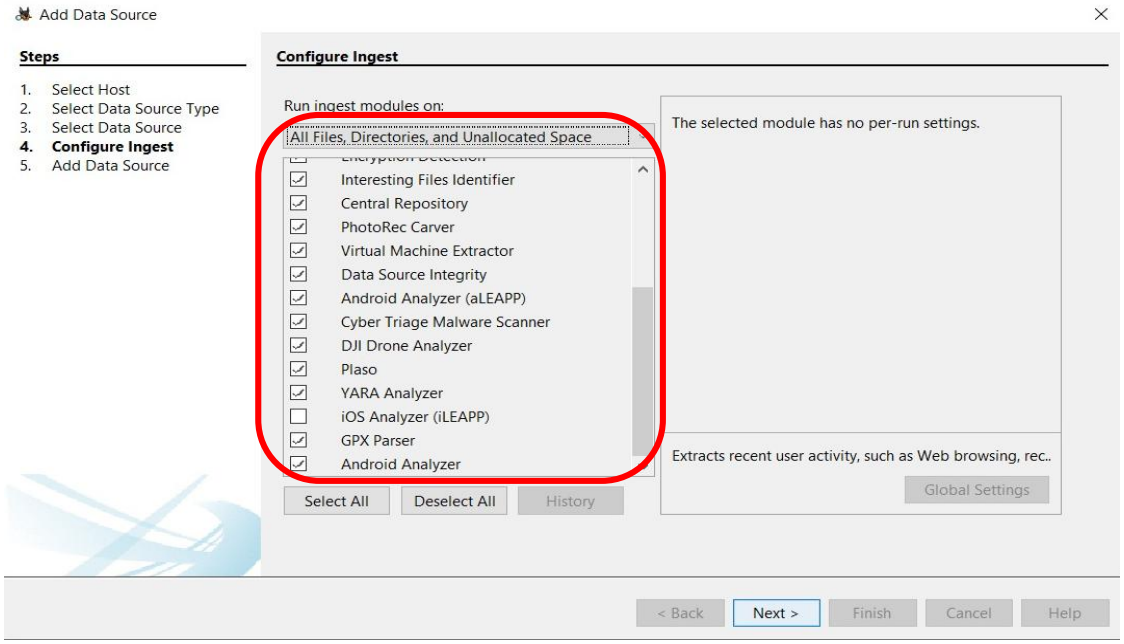


Ilustración 31. Módulos de análisis de evidencia digital

En este laboratorio, al estar procesando una imagen con sistema operativo Android, seleccionamos las opciones de “Android Analyzer (aLEAPP)” y “Embedded File Extractor” principalmente, para que la indexación de la imagen forense del dispositivo móvil previamente adquirida se realice de manera exhaustiva, Tras la selección de los módulos, el software inicia su análisis, cuya duración dependerá de la cantidad de datos contenidos en la imagen, como se muestra en la ilustración 32.

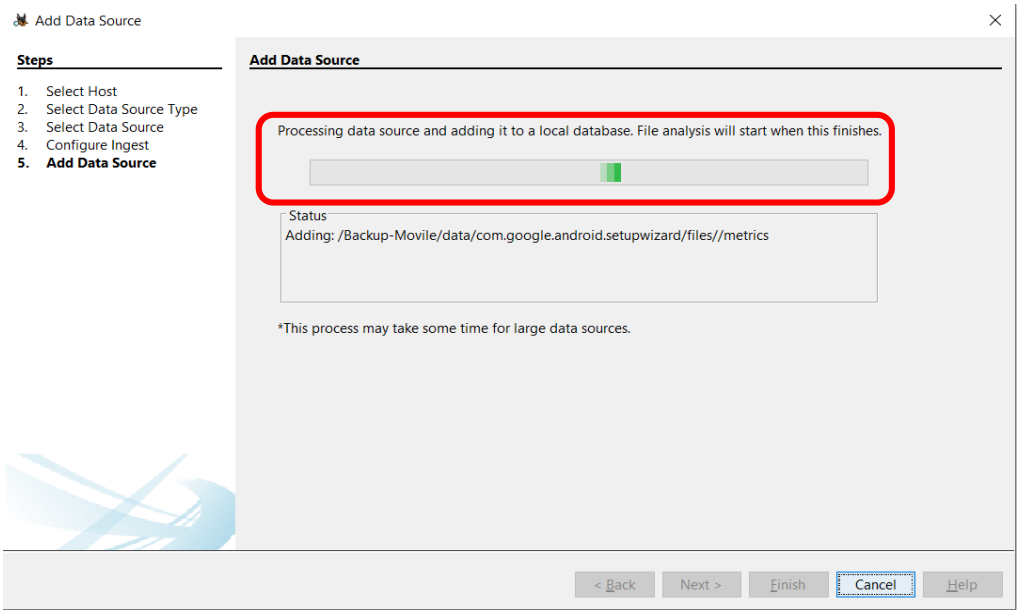


Ilustración 32. Procesamiento de la data adquirida

Una vez finalizado el procesamiento de los datos, Autopsy genera un árbol de evidencias, categorizando por carpetas. A continuación, se realiza un resumen de la evidencia procesada en Autopsy. En la ilustración 33 se puede visualizar la carpeta de imágenes que contiene 643 elementos, 14 archivos con diferentes extensiones y 356 bases de datos, además se identifican 2 registros de llamadas, 10 cuentas de usuario utilizadas en diversas aplicaciones de mensajería o redes sociales, y datos del dispositivo analizado como el IMEI o el nombre del equipo.

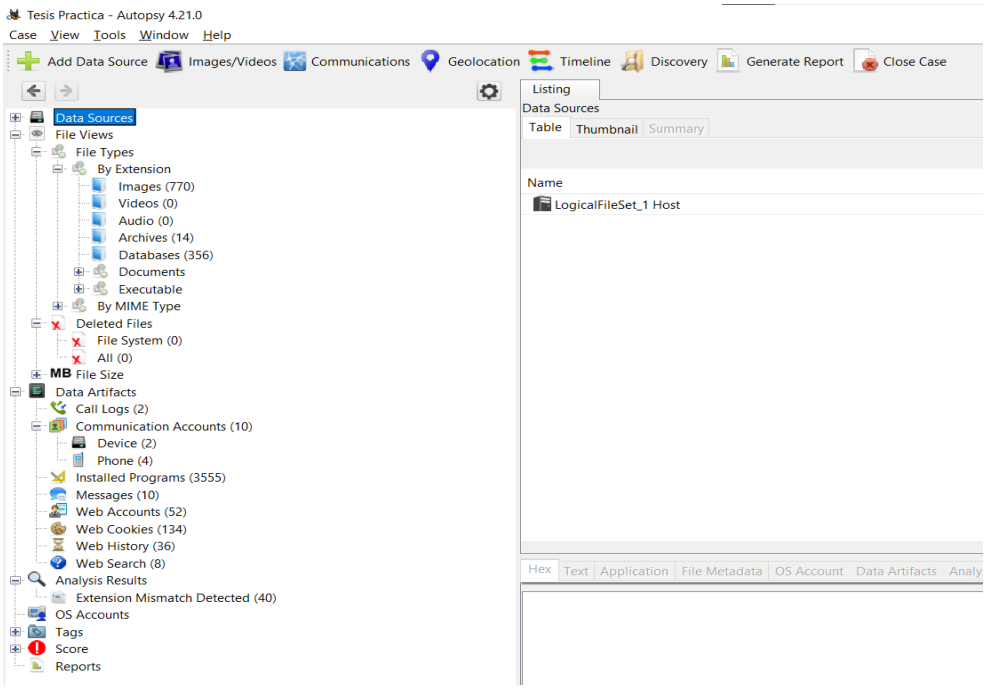


Ilustración 33. resultados de los datos analizados

Gracias a la versatilidad de la herramienta se puede identificar los detalles o contenido de la evidencia obtenida, en texto plano como se muestra en la ilustración 34.

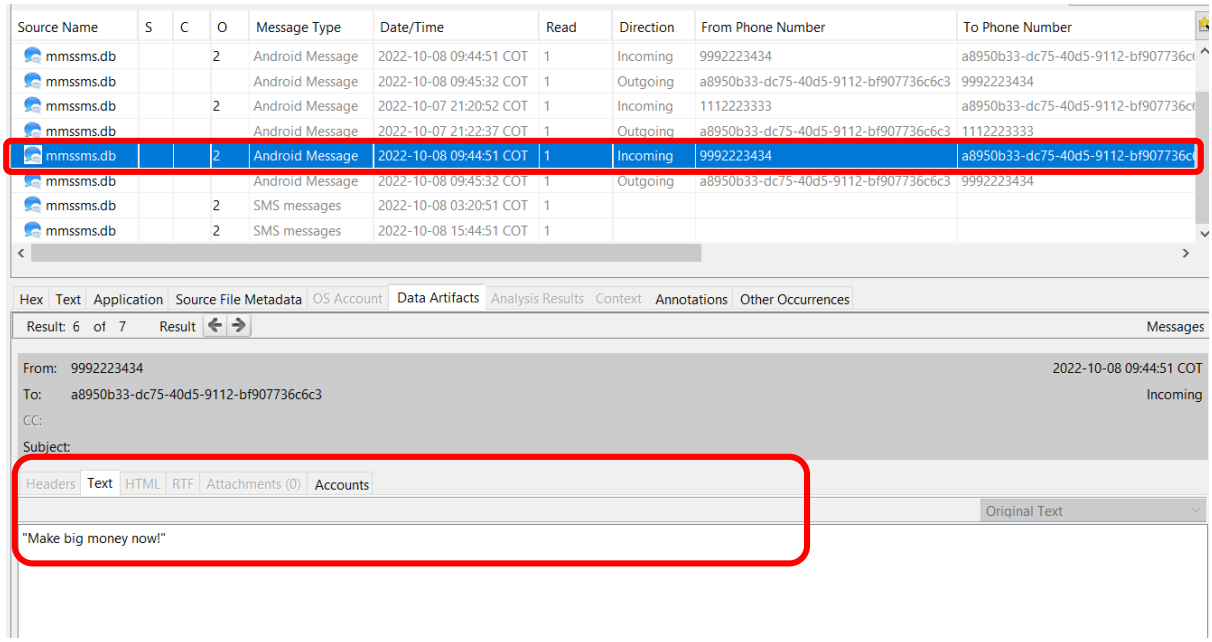


Ilustración 34. Contenido de la evidencia obtenida

Si el examinador encuentra información relevante para la investigación, procede a etiquetarla siguiendo el procedimiento mostrado en las ilustraciones 35 y 36. Para este ejemplo, se consideran las secciones más comunes para encontrar evidencia en un dispositivo durante el análisis forense. Una vez identificada la evidencia, el

examinador tiene la posibilidad etiquetar por categorías los indicios encontrados acorde el objeto de la investigación.

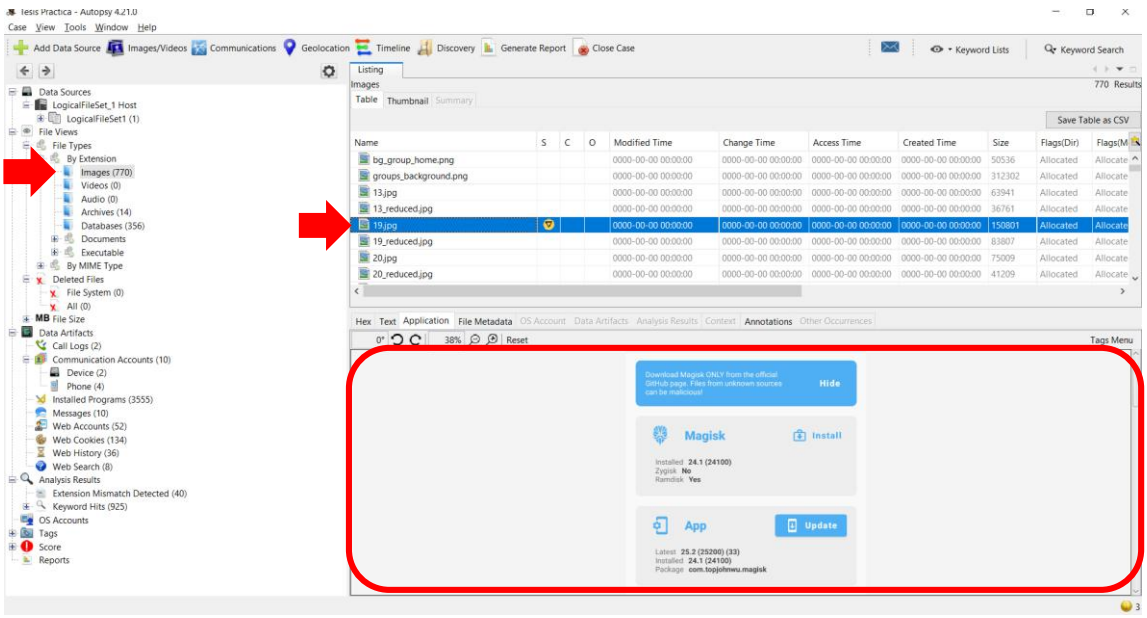


Ilustración 35. Identificación evidencia digital

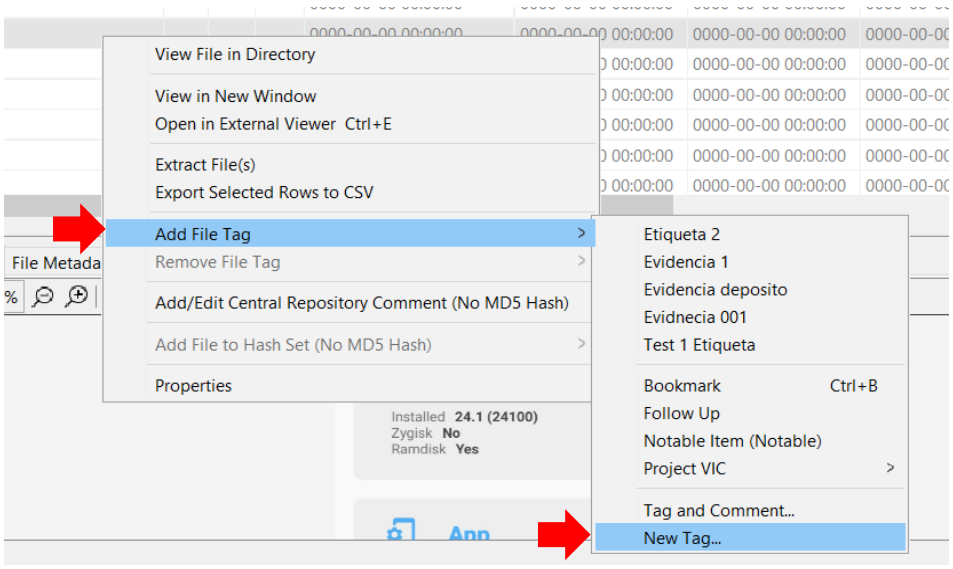


Ilustración 36. insertar etiqueta a la información relevante

De ser necesario para el examinador, el software también permite la creación de nuevas etiquetas como se visualiza en la Ilustración 37.

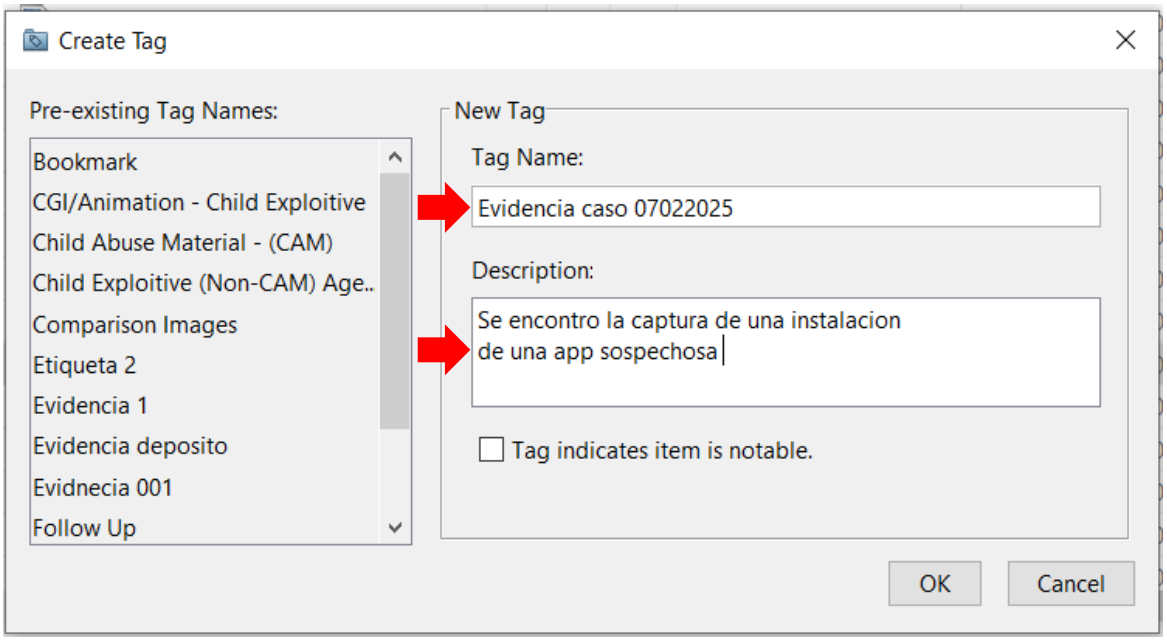


Ilustración 37. Creación de etiquetas

Una vez creada la etiqueta correspondiente, el software lo identificará con un ícono como se muestra en la ilustración 38.

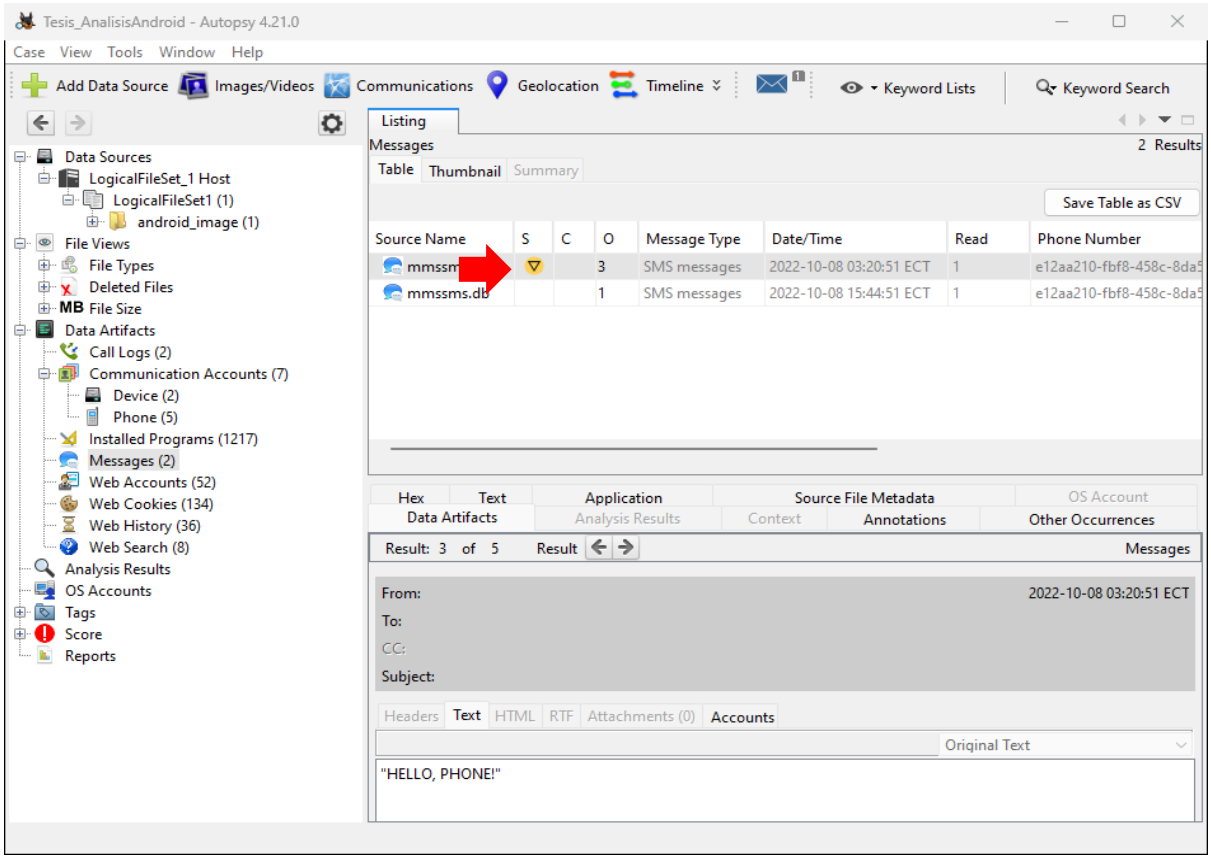


Ilustración 38. Etiquetado de la evidencia relevante

Una de las opciones más interesantes de esta herramienta forense es la poder trabajar con líneas de tiempo, estas líneas de tiempo nos pueden permitir en gran medida tener un visión mucho más amplia y rápido de los procesos o acciones ejecutadas en el dispositivo en el tiempo.

Esta opción se encuentra en la pestaña "Timeline" y permite identifican hallazgos importantes y patrones sospechosos de actividad que pueden aportar como evidencia probatoria ejecutadas en una secuencia de tiempo, como se identifica en la Ilustración 39.

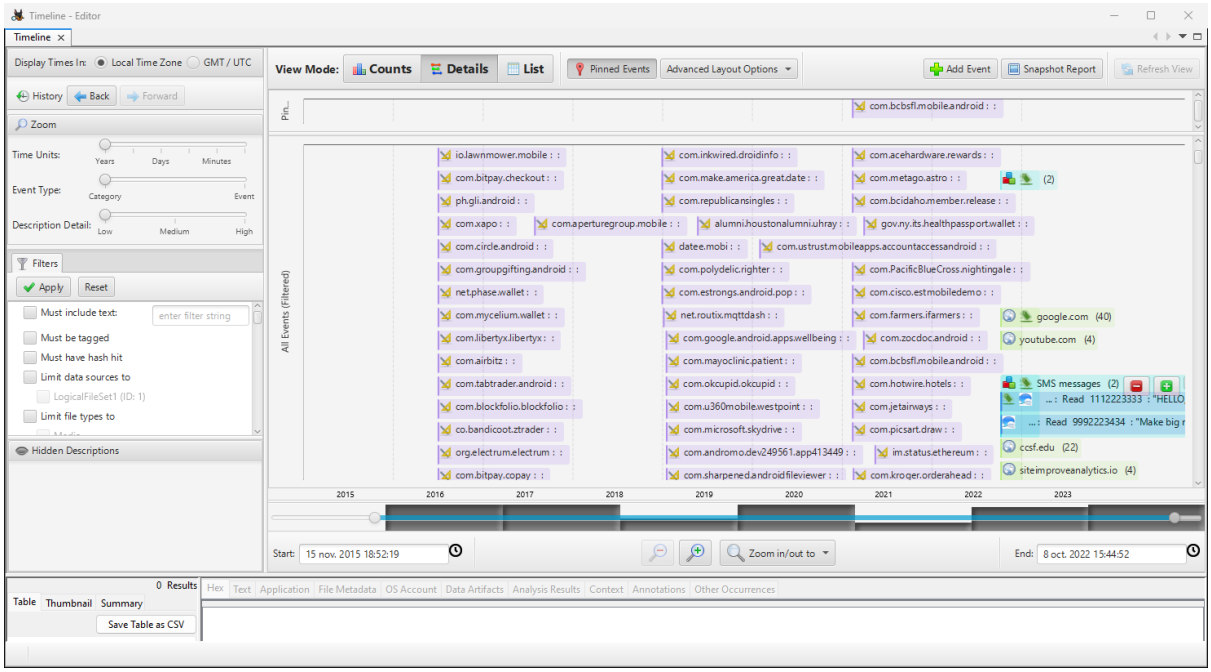


Ilustración 39. Línea de tiempo de la recopilación de evidencias

Otra sección muy interesante y primordial en el análisis forense es la sección **"Web"** de Autopsy, es esencial ya que permite examinar las actividades en línea de un usuario. Esta sección se subdivide en varias categorías que permiten una revisión detallada de los artefactos web almacenados en el sistema. A continuación, se describen las principales subcategorías como se muestra en la ilustración 40.

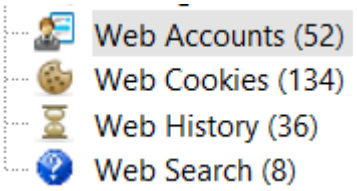


Ilustración 40. Sección web

4.5 Informe

En el contexto del análisis forense de dispositivos móviles, la redacción del informe debe seguir pautas estrictas que garanticen su validez legal y técnica. El informe debe estar escrito en lenguaje objetivo, comprensible y basado en hechos comprobables, proporcionando una respuesta concisa al objetivo de la investigación producto del análisis forense, esto mientras mantiene todos los detalles técnicos complejos en una sección de apéndices para facilitar la comprensión por parte de personas no técnicas.

Así mismo, el informe debe incluir la metodología utilizada, las herramientas empleadas y mantener una documentación clara incluido el manejo de cadena de custodia, considerando que, dependiendo de la jurisdicción, este documento podría ser suficiente por sí solo en un tribunal o requerir la presencia de quien realizó el análisis forense como testigo experto o perito para explicar los hallazgos.

Finalmente, es importante destacar y resaltar que Autopsy también ofrece la capacidad de crear un reporte detallado con todos los hallazgos encontrados por el analista, el cual se convierte en un documento oficial dentro de la investigación, ya que, tras completar el análisis de las evidencias, se requiere presentar los hallazgos, este reporte generado con Autopsy, puede ser parte del informe gerencial expuesto por el analista, ya que cubre al 100 por ciento los resultados técnicos y las evidencias digitales producto del análisis forense.

Para crear el reporte en cuestión se debe seguir los pasos como se muestra en la Ilustración 41:

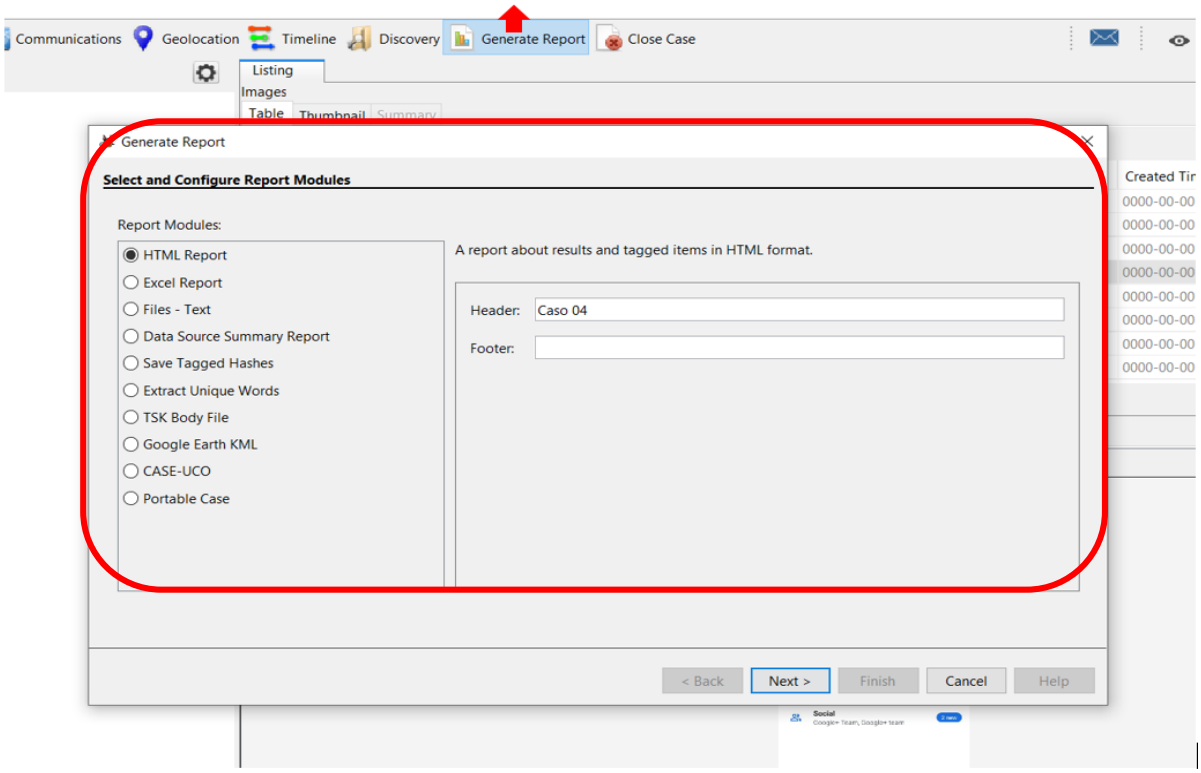


Ilustración 41. Creación del reporte

Justo antes de la creación del reporte forense se puede observar las etiquetas asignadas previamente a la investigación como se muestra en la ilustración 42.

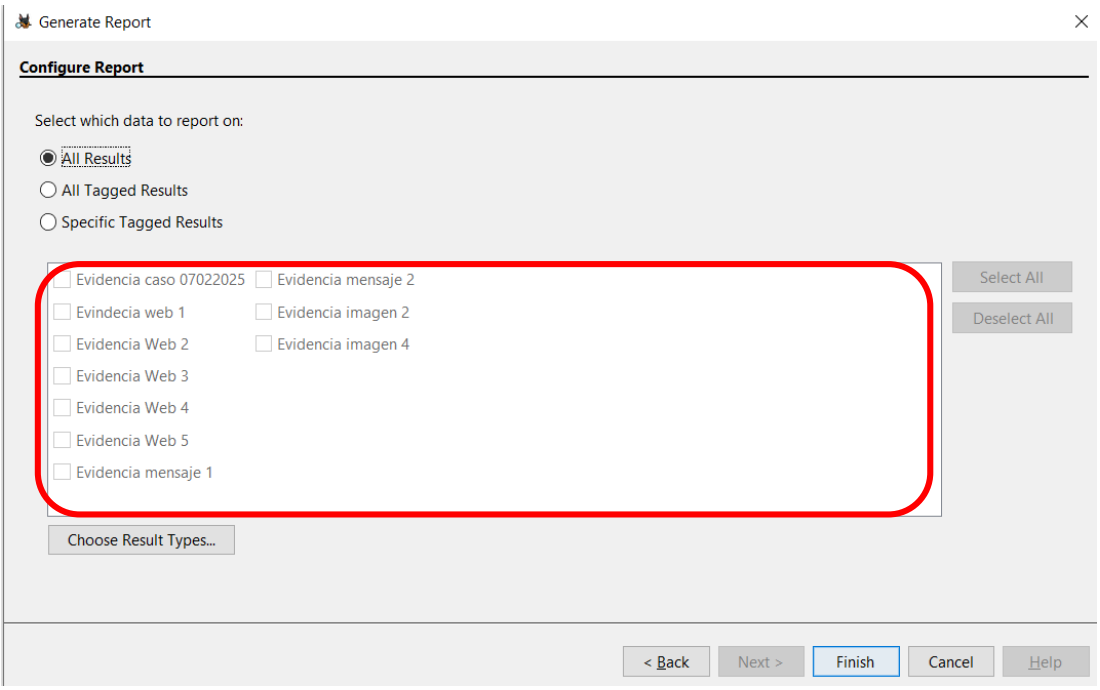


Ilustración 42. Resumen de etiquetas

Una vez finalizados los pasos previos a la generación del reporte, el programa completará el proceso creando una URL, como se muestra en la ilustración 43 la misma que permite acceder directamente al reporte generado.

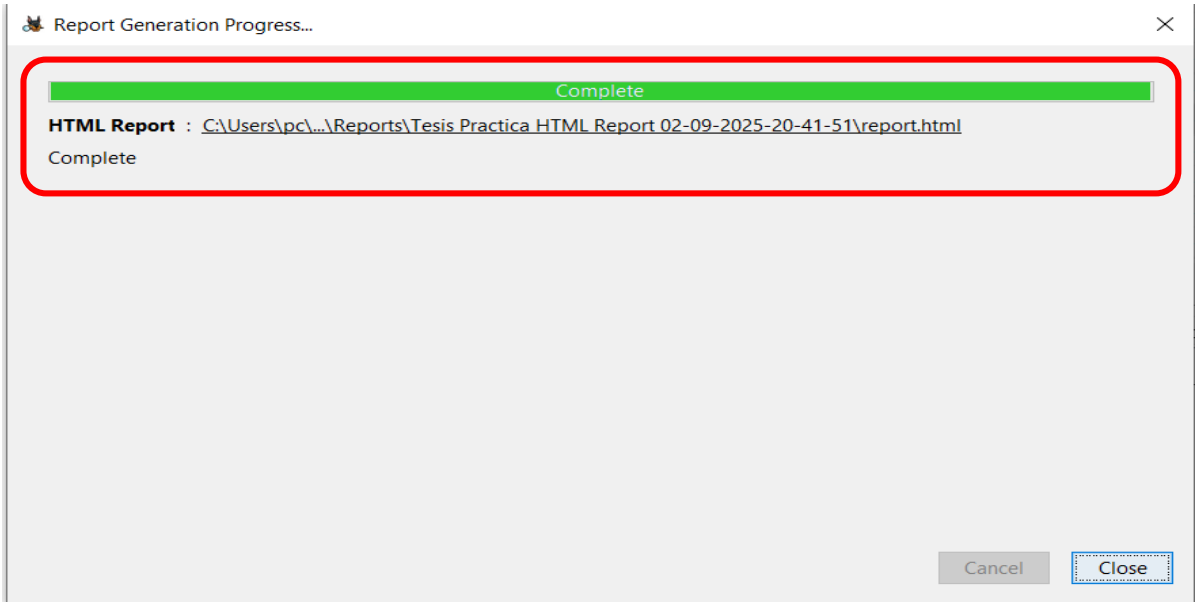


Ilustración 43. Creación URL del reporte generado

Al acceder a la URL, podremos visualizar el reporte que contiene toda la información destacada: detalles del caso, información técnica del dispositivo y datos sobre los módulos analíticos utilizados, tal como se muestra en las ilustraciones 44.

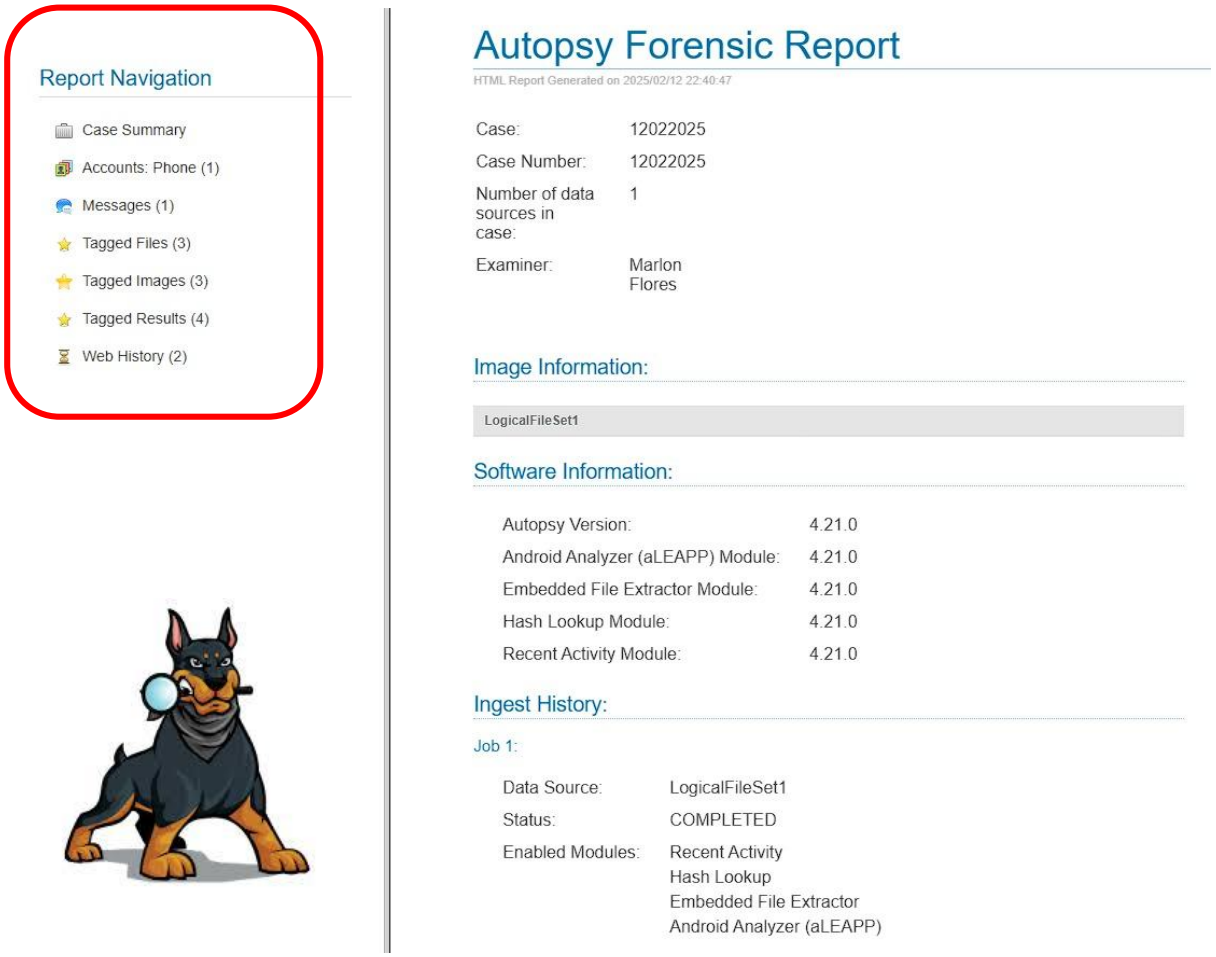


Ilustración 44. Reporte de evidencias con Autopsy

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

En este capítulo se presentan las conclusiones a las que llego finalizada la investigación, las mismas que se encuentran acorde los objetivos planteados, así como una serie de recomendaciones para futuras investigaciones en el ámbito del análisis forense digital de dispositivos móviles mediante herramientas de software libre.

Conclusiones

- Mediante la revisión documental de estudios científicos y reportes técnicos, se identificaron herramientas de software libre altamente relevantes para el análisis forense de dispositivos móviles. Entre las más destacadas se encuentran CSI Linux, Magnet Acquire, Avilla Forensics y Autopsy, las cuales han demostrado su utilidad en diferentes etapas del proceso forense. La identificación de estas herramientas permitió consolidar una base tecnológica accesible y adaptable a distintos entornos investigativos, facilitando su adopción en instituciones con recursos limitados.

- Se realizó un análisis comparativo basado en la documentación científica disponible, permitiendo examinar la efectividad de las herramientas de software libre en investigaciones forenses realizadas por organismos públicos y privados. Se evidenció que CSI Linux proporciona un entorno especializado para la investigación forense digital, Magnet Acquire facilita la extracción de información sin alterar la integridad de la evidencia, y Autopsy destaca por su capacidad de análisis modular. Aunque las herramientas comerciales como Oxygen Forensics y Magnet AXIOM ofrecen soporte técnico más avanzado, las soluciones de código abierto presentan una alternativa viable y accesible.

- Se desarrolló un marco de trabajo estructurado que integra procesos de Identificación, adquisición, procesamiento, análisis y presentación de evidencias digitales, basándose en metodologías forenses reconocidas como las ISO/IEC 27037, ISO/IEC 27042 DFRWS, NIST y RFC. Este marco establece directrices claras y específicas para la selección y aplicación de herramientas especializadas, garantizando la validez y replicabilidad del

análisis forense. La propuesta representa una contribución significativa al campo forense, proporcionando un esquema adaptable a distintas instituciones y escenarios investigativos.

- La validación del marco de trabajo se realizó mediante pruebas de concepto en entornos controlados y con dispositivos reales, evaluando su aplicabilidad en distintos escenarios forenses. Autopsy se destacó en la recuperación de registros de llamadas, mensajes y navegación web, CSI Linux proporcionó un entorno especializado con múltiples herramientas preconfiguradas, y Magnet Acquire demostró su eficiencia en la extracción de datos sin comprometer la evidencia. Los resultados confirmaron que el marco de trabajo es funcional y adaptable, aunque su implementación efectiva requiere capacitación técnica para garantizar la correcta aplicación de los procedimientos forenses.

Recomendaciones

- Dado que se identificaron herramientas de software libre como CSI Linux, Magnet Acquire, AFLogical, Avilla Forensics y Autopsy, se recomienda a instituciones y profesionales forenses implementar estrategias de adopción que incluyan capacitaciones técnicas y pruebas en entornos controlados, esto permitirá maximizar el potencial de estas herramientas en la investigación de delitos digitales, promoviendo su uso como una alternativa viable a las soluciones comerciales.

- Debido a que la investigación demostró que herramientas como CSI Linux, Magnet Acquire y Autopsy son altamente efectivas, se recomienda que las entidades forenses realicen pruebas periódicas de rendimiento y comparaciones con herramientas comerciales para identificar oportunidades de mejora y garantizar su fiabilidad en investigaciones criminales. Adicionalmente, se sugiere documentar cada caso de uso para generar una base de datos de experiencias y mejores prácticas en el campo forense.

- El marco de trabajo diseñado en esta investigación proporciona un esquema replicable y adaptable para la adquisición, procesamiento, análisis y presentación de evidencias digitales. Para mejorar su implementación, se recomienda desarrollar protocolos estandarizados para cada etapa del proceso forense y asegurar su alineación con normativas internacionales como ISO/IEC

27037. Así mismo, se sugiere la creación de guías detalladas y manuales de aplicación para facilitar su adopción por parte de profesionales y entidades forenses.

- Si bien la evaluación del marco de trabajo se realizó en entornos controlados con herramientas de software libre previamente seleccionadas, se recomienda su validación en casos reales dentro de investigaciones forenses oficiales, además, se sugiere explorar la integración de nuevas herramientas y metodologías emergentes que puedan fortalecer el proceso de análisis digital.

BIBLIOGRAFÍA

(20 de 10 de 2008). Obtenido de Ediciones Legales EDLE S.A: https://www.fielweb.com/Index.aspx?rn=93455&nid=1#norma/1

(2021). Obtenido de Consejo de Europa: https://www.coe.int/en/web/cybercrime/the-budapest-convention

(2025 de 02 de 21). Obtenido de Ediciones Legales EDLE S.A: https://www.fielweb.com/Index.aspx?35&nid=1070225#norma/1070225

(2021 de 05 de 26). Obtenido de Ediciones Legales EDLE S.A.: https://www.fielweb.com/Index.aspx?rn=46602&nid=1162059#norma/1162059

Aboso, G. E. (2022). *Ciberdelitos: Análisis doctrinario y jurisprudencial.* elDial. com.

Alemán Ariza, A. (2024). Análisis forense digital en dispositivos móviles. *Revista Cathedra*, 1(21), 45–64.

Amsler, G., Casco, M. E., & Roatta, S. (2017). Limitaciones de las actuales herramientas de análisis digital forense para dispositivos móvile. *46jaiio.sadio.org.ar*, 1.

Andrade Pesantez, D. J., & Banegas Crespo, D. A. (2024). *Análisis Forense en Dispositivos Móviles Android para Casos de Ciberextorsión, Revisión Sistemática de Literatura.* Cuenca: UNIVERSIDAD CATÓLICA DE CUENCA.

Ariza, A. A. (2024). Análisis forense digital en dispositivos móviles. *Universidad Metropolitana de Educación, Ciencia y Tecnología*.

Badman, A., & Forrest, A. (16 de 02 de 2024). *IBM.com.* Obtenido de https://www.ibm.com/mx-es/topics/digital-forensics

Beltrán tapia, K. W. (2021). MODELO PARA ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID. *PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR*, 40.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet.* Academic Press.

Concepto, E. (2024). *Concepto.de*. Obtenido de https://concepto.de/investigacion-exploratoria/

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4ta ed.).* SAGE Publications.

Echeverría Espinoza, E., & Álvarez Vera, M. (2024). Análisis de técnicas y herramientas forenses para la investigación de delitos informáticos y su perspectiva legal en el Ecuador. Una revisión sistemática. *593 Digital Publisher CEIT*, 9(6), 644-652.

Ecuador, A. N. (2008). *Constitucion de la republica del Ecuador.*

Enaidy, R. N. (2018). Trabajo de investigación. Teoría,. *https://www.aacademica.org*, 12.

Fernández, D. R. (2022). PRUEBA DE CONCEPTO PARA EXTRAER INFORMACIÓN CON HERRAMIENTAS DE ANALISIS FORENSE OPEN-SOURCE EN DISPOSITIVOS ANDROID. *Pontificia Universidad*

Católica del Ecuador. Obtenido de https://repositorio.puce.edu.ec/server/api/core/bitstreams/a39b3e86-e2f5-4443-b90d-d19690c1e4a4/content

Ferreyra, E. (2018). La investigación forense informática en América Latina. En *La investigación forense informática en América Latina* (pág. 29).

Finneran, C., & Sutton, M. (2020). Challenges in implementing open source tools for digital forensics. *International Journal of Cyber Forensics and Advanced Threats*, 6(1), 21-35.

Foo, E., & Al-Sabaawi, A. (2019). A Comparison Study of Android Mobile Forensics for Retrieving Files System. *eprints.qut.edu.au*.

Garfinkel, S. C. (2010). *Digital forensics with open source tools.* Syngress.

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

Harris, C. W. (2014). *Computer forensics: Investigating electronic crime.* Cengage Learning.

Hay, B., & Nance, S. (2016). The role of open source software in digital forensics. *Journal of Digital Forensics, Security and Law*, 11(2), 45-47.

Hernández Sampieri, R., & Mendoza Torres, C. P. (2018). *Metodología de la investigación. Rutas cuantitativa cualitativa y mixta-libre.* Bogotá: McGraw-Hill Education.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4ta ed.).* McGraw-Hill Education.

Jurado, D., & Acuña, U. (2011). *Guía metodológica sobre las técnicas y herramientas de software libre, aplicadas a la informática forense.* Colombia: Universidad Autónoma de Bucaramanga.

Lázaro, A. d. (08 de 12 de 2024). *lazarusalliance.com*. Obtenido de Lazarus Alliance Inc.: https://lazarusalliance.com/es/the-role-of-open-source-software-in-cybersecurity-benefits-challenges-and-key-tools/

Lorenzo, J. A. (26 de 07 de 2024). *RedesZone*. Obtenido de redeszone.net: https://www.redeszone.net/tutoriales/seguridad/mejores-herramientas-gratuitas-informatica-forense/

Mag, I. M. (2024). *Análisis forense digital ¿Cómo se realiza? Herramientas, pasos y las mejores prácticas.* Ciudad de Mexico: network-digixem-360.

Martínez Corona, J., Palacios Almón, G. E., & Oliva Garza, D. B. (2023). GUÍA PARA LA REVISIÓN Y EL ANÁLISIS DOCUMENTAL: PROPUESTA DESDE EL ENFOQUE INVESTIGATIVO. *raximhai.uaim.edu.mx*, 1.

Palmer, G. (2001). *Digital Forensics Research Workshop (DFRWS).* Obtenido de http://www.dfrws.org/2001/dfrws-rm-final.pdf

Resolución No. 34-FGE-2022. (2022). Obtenido de https://www.fiscalia.gob.ec/transparencia/2022/julio/a3/RESOLUCION-034-FGE-2022.pdf

Reyes, A. C. (2015). Recolección de datos: Ficha. *repositorios - Universidad de San Carlos de Guatemala*, 7.

Seigfried, M. K. (2004). The future of computer forensics: A needs analysis survey. *Computers & Security*, 62. Obtenido de https://doi.org/10.1016/j.cose.2004.01.003.

Sepulveda, M. (2024). El Poder de las Herramientas de Código Abierto. *Ciberseguridad.club*.

Skulkin, O., Tindall, D., & Tamma, R. (2018). *Analyze Android devices with the latest forensic tools and.* Mumbai: Packt Publishing.

StatCounter. (2024). *StatCounter*. Obtenido de https://gs.statcounter.com/vendor-market-share/mobile/ecuador#monthly-202401-202412

Taylor, R. e. (2014). *Digital forensics: A primer for the first responder.* Taylor & Francis.

Ventura León, J. L. (2017). ¿Población o muestra?: Una diferencia necesaria. *redalyc.org*, 648.

Yin, R. K. (2018). *Case study research and applications Design and methods.* Thousand Oaks, CA: SAGE Publications.

ANEXOS

LISTA DE VERIFICACIÓN DE INCAUTACIÓN DE DISPOSITIVOS MÓVILES

NOMBRE DE LA AGENCIA:

NOMBRE DEL INVESTIGADOR:

FECHA Y HORA:

UBICACIÓN:

1. ESTADO DEL DISPOSITIVO MÓVIL	**NOTAS**
Verificar estado del dispositivo: ENCENDIDO ☐ APAGADO ☐ Primero, verifique la condición del dispositivo móvil. Si el dispositivo está ENCENDIDO, entonces los contenidos de la pantalla deben ser documentados y/o fotografiados. Si el dispositivo está APAGADO, déjelo APAGADO. ENCENDER el dispositivo podría alterar la evidencia en el dispositivo. Minimice la interacción con el dispositivo, salvo que sea absolutamente necesario. Las fechas/horas de los registros podrían verse afectadas por verlos en el teléfono. Los registros podrían ser modificados o eliminados accidentalmente. El estado de leído/no leído de los correos electrónicos y mensajes de texto podría verse afectado. Documente el estado del dispositivo móvil en la sección de Notas.	

2. BLOQUEAR LA COMUNICACIÓN INALÁMBRICA	**NOTAS**
Comunicación inalámbrica bloqueada: SÍ ☐ NO ☐ Los dispositivos móviles se comunican a través de ondas de radio. Bloquee TODAS las comunicaciones inalámbricas (incluyendo WiFi y Bluetooth) para prevenir que ningún dato sea modificado a través de comunicaciones externas. Los dispositivos móviles con capacidades inalámbricas pueden ser bloqueados poniéndolos en Modo Avión / de Vuelo, envolviéndolo en al menos 5 capas de papel aluminio, o sacando la batería. Documente el método usado para bloquear las comunicaciones inalámbricas del dispositivo móvil en la sección de Notas. No almacene dispositivos móviles en el mismo contenedor. Los cables de alimentación y de datos conectados a un dispositivo móvil pueden actuar como antena alternativa para comunicaciones inalámbricas.	

3. CÓDIGO DE ACCESO	**NOTAS**
Código de Acceso / PIN del Dispositivo Móvil:_____ Obtenga el Código de Acceso / PIN del sujeto. Documente en el espacio de arriba. Los dispositivos podrían bloquearse automáticamente (por ejemplo, tras inactividad por 2 minutos) y denegar el acceso al teléfono, incluyendo el acceso a través de cables de datos. Considere deshabilitar el Código de Acceso / PIN y apagar la opción de auto-bloqueo y cualquier temporizador de inactividad. Documente cualquier cambio hecho al dispositivo móvil en la sección de Notas.	

4. DOCUMENTACIÓN/COMENTARIOS	**NOTAS**
Documente la siguiente información de identificación para el dispositivo móvil: FABRICANTE:_____ MODELO:_____ NÚMERO DE SERIE: _____ NÚMERO DE TELÉFONO: _____ PROPIETARIO:_____ Documente cualquier información de identificación adicional (IMEI, MEID, ICCID) en la sección de Notas.	

5. INCAUTACIÓN DE ARTÍCULOS RELACIONADOS	**NOTAS**
Considere incautar cables asociados al dispositivo móvil. Algunos dispositivos móviles tienen cables únicos / inusuales para la comunicación de datos. Estos cables podrían ser necesitados más adelante para encender / adquirir datos del dispositivo móvil. Adicionalmente, considere incautar cualquier tarjeta de memoria o tarjeta SIM que pueda estar asociada con el dispositivo móvil. Tome en cuenta que los estuches de transporte pueden contener información valiosa o evidencia (tal como contraseñas o tarjetas de memoria).	

6. SELLE LA EVIDENCIA	**NOTAS**
A los artículos incautados se les debe asignar un número de identificación de evidencia único, sellado, con iniciales, y con la fecha usando las técnicas estandarizadas de manejo de evidencia. Si el dispositivo móvil tiene capacidades inalámbricas, debe ser bloqueado de la red inalámbrica (*tal como se describe arriba*). Todos los dispositivos deben ser colocados en un contenedor del tamaño apropiado que prevenga que los botones o pantallas táctiles sean presionados inadvertidamente.	

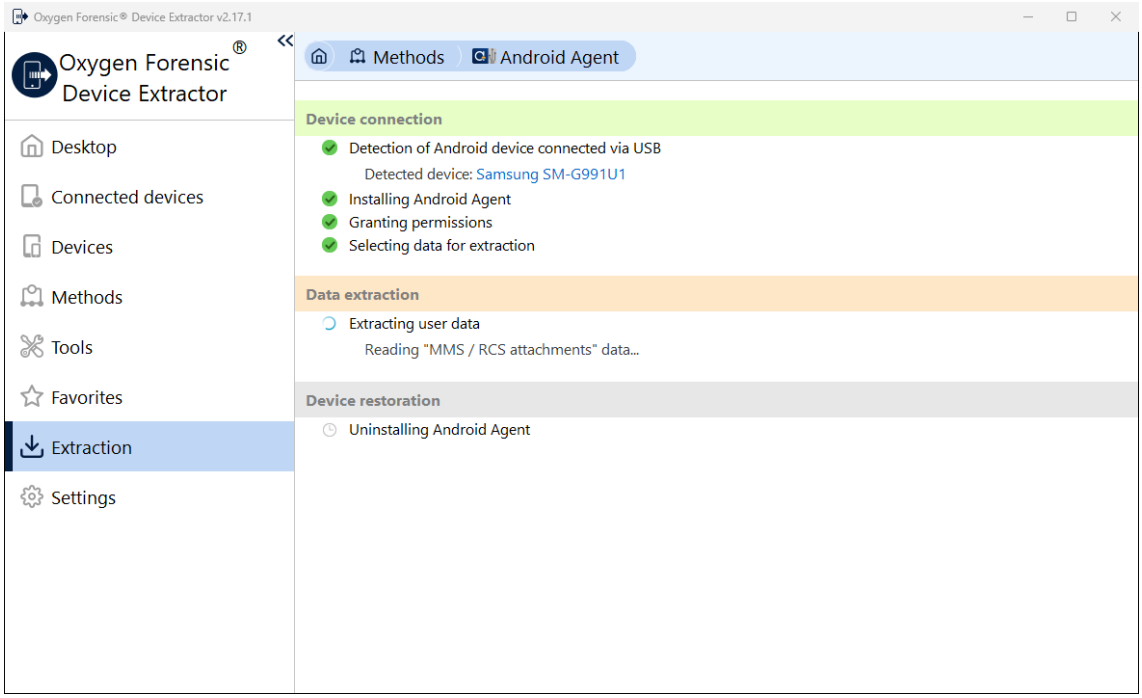


Ilustración 45. Adquisición lógica de un dispositivo Android con la herramienta Oxygen Forensic

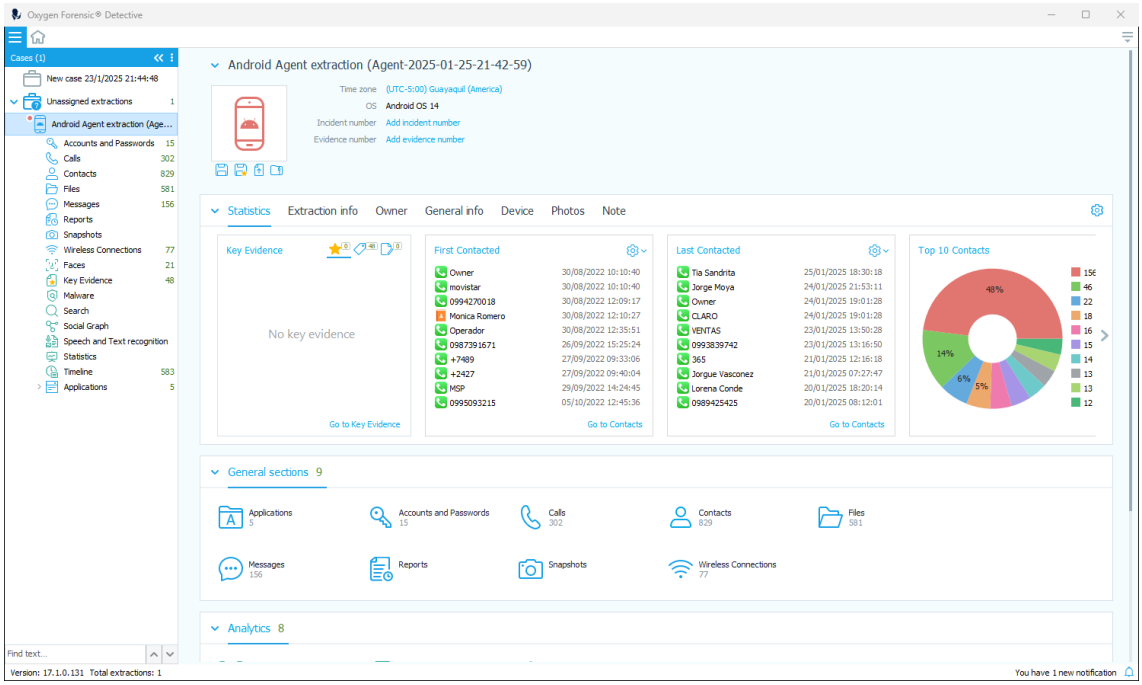


Ilustración 46. Procesamiento de resultados con Oxygen Forensic

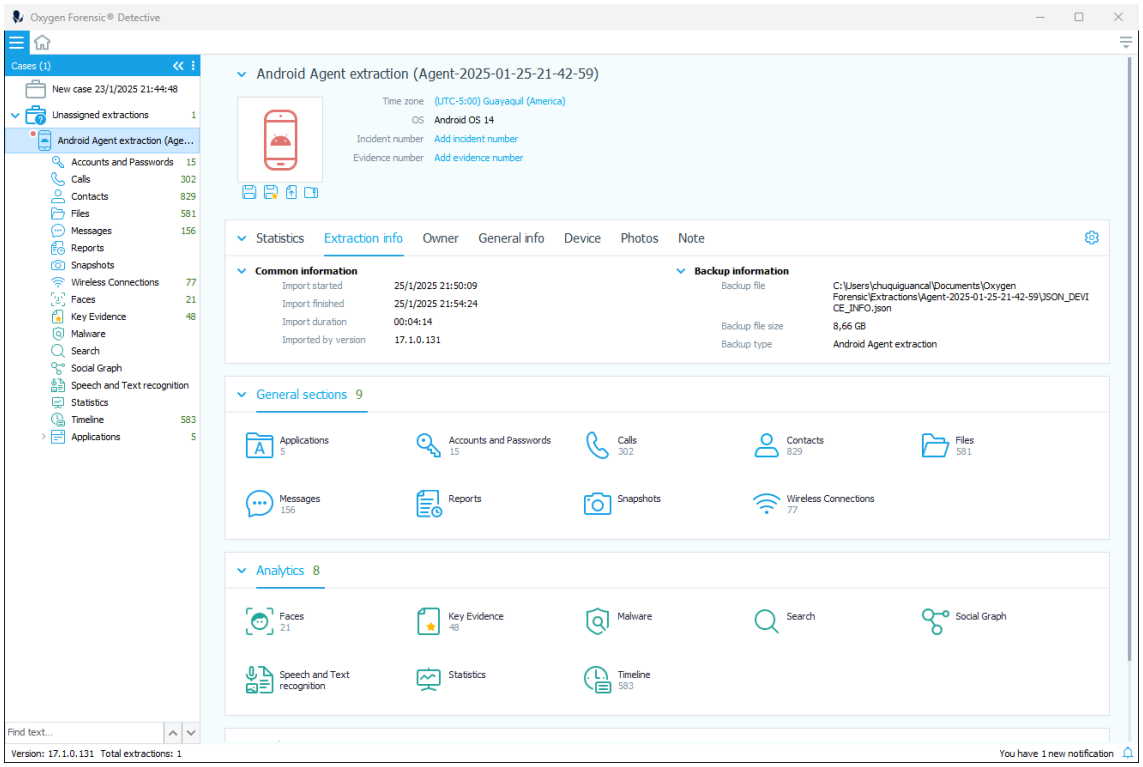


Ilustración 47. Resultados del procesamiento de datos

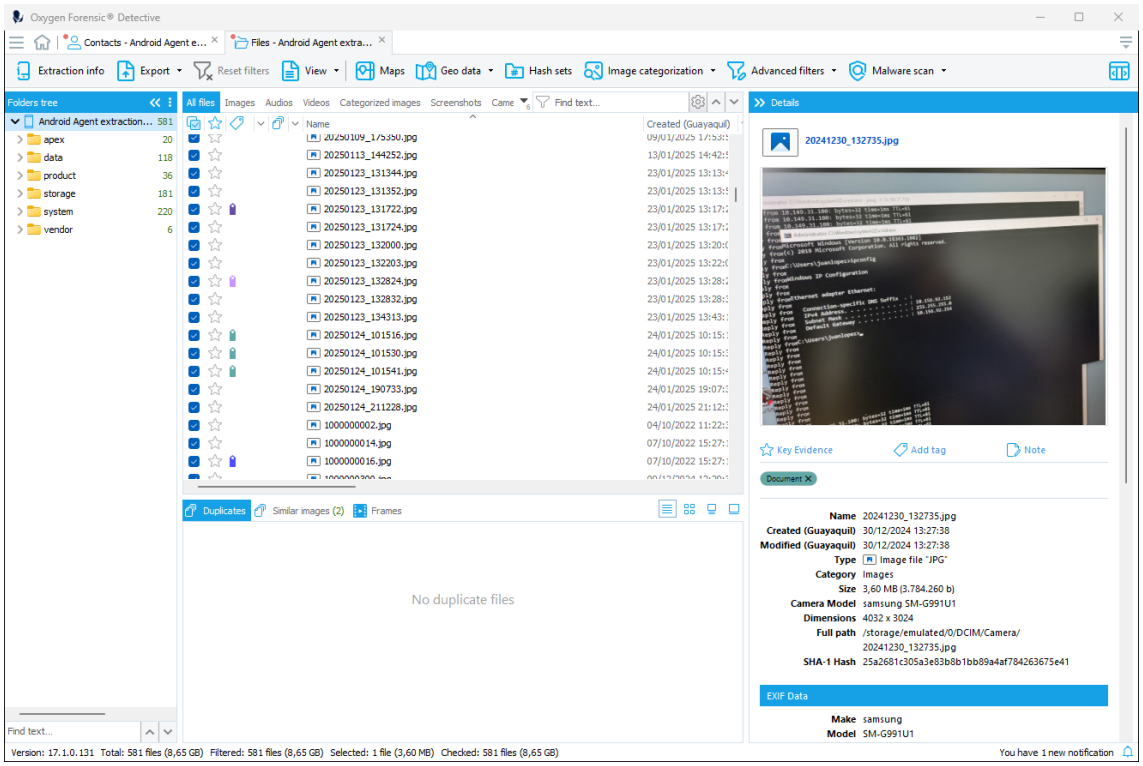


Ilustración 48. Resultados del procesamiento de datos

Tabla 7. Estadística delitos informáticos en Ecuador

Tipo penal	2022	2023	2024
ACCESO NO CONSENTIDO A UN SISTEMA INFORMÁTICO, TELEMÁTICO O DE TELECOMUNICACIONES	355	486	978
APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS	3.138	3.449	3.697
ATAQUE A LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS	200	175	252
COMERCIALIZACIÓN DE PORNOGRAFÍA CON UTILIZACIÓN DE NIÑAS, NIÑOS O ADOLESCENTES	20	38	27
COMERCIALIZACIÓN ILÍCITA DE TERMINALES MÓVILES	1	33	13
CONTACTO CON FINALIDAD SEXUAL CON MENORES DE DIECIOCHO AÑOS POR MEDIOS ELECTRÓNICOS	183	173	123
DELITOS CONTRA LA INFORMACIÓN PÚBLICA RESERVADA LEGALMENTE	5	5	6
FALSIFICACIÓN INFORMÁTICA	24	68	116
INTERCEPTACIÓN ILEGAL DE DATOS	79	61	69
OFERTA DE SERVICIOS SEXUALES CON MENORES DE DIECIOCHO AÑOS POR MEDIOS ELECTRÓNICOS	18	15	11
PORNOGRAFÍA CON UTILIZACIÓN DE NIÑAS, NIÑOS O ADOLESCENTES	109	142	127
REPROGRAMACIÓN O MODIFICACIÓN DE INFORMACIÓN DE EQUIPOS TERMINALES MÓVILES	8	3	4
REVELACIÓN ILEGAL DE BASE DE DATOS	63	29	45
TRANSFERENCIA ELECTRÓNICA DE ACTIVO PATRIMONIAL	117	166	169
VIOLACIÓN A LA INTIMIDAD	1.722	1.684	1.748
Total NDDs	**28.717**	**30.269**	**32.015**

Fuente: Fiscalía General del Estado 2024

Dispositivos móviles más vendidos en Ecuador entre enero a diciembre de 2024 **(StatCounter, 2024)**

Tabla 8. *Dispositivos móviles más vendidos en Ecuador 2024*

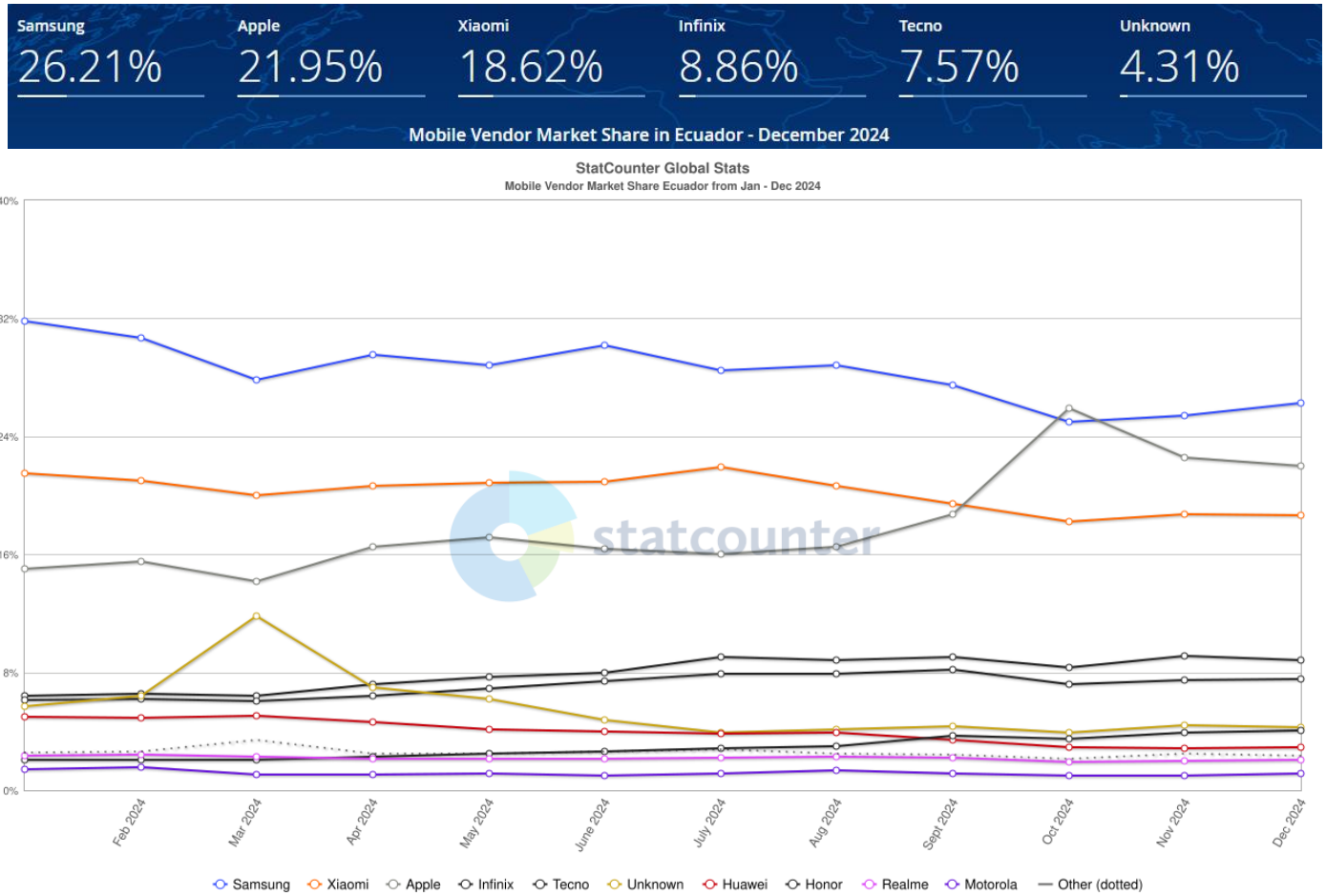


Tabla 9. *Guía de análisis documental*

N.º	*Título*	Autor(es)	Año	País	DB	Documento (Links)	Resultados Relevantes	Metodología empleada	Palabras clave	Impacto práctico	Relevancia en Ecuador
1	*Forensic Analysis of Instant Messenger Applications on Android Devices*	Aditya Mahajan, M. S. Dahiya, H. P. Sanghvi	2013	Internacional	arXiv	https://arxiv.org/pdf/1304.4915	Este estudio analiza cómo las aplicaciones de mensajería instantánea en Android pueden contener evidencia clave como mensajes, chats y archivos multimedia.	Pruebas experimentales en dispositivos Android con aplicaciones populares de mensajería.	Android forensics, instant messaging	Útil para investigaciones de ciberdelitos relacionadas con comunicaciones electrónicas.	Alta relevancia, dado el uso masivo de Android y aplicaciones de mensajería en Ecuador.
2	*Probar la Eficacia de CSI Linux en el Análisis Forense de un Caso de Fuga de Información*	Parra Suzaño, D.J.	2022	Bolivia	Repositorio Digital de la Universidad Mayor de San Simón	ddigital.umss.edu	Evalúa la eficacia de la distribución CSI Linux en la investigación forense de un caso simulado de fuga de información, demostrando su utilidad en la recolección y análisis de evidencia digital.	Estudio de caso con aplicación práctica de CSI Linux en un entorno controlado para simular una fuga de información y posterior análisis forense.	CSI Linux, análisis forense, fuga de información, seguridad informática	Proporciona una evaluación práctica de CSI Linux, ofreciendo insights sobre su aplicabilidad y eficacia en casos reales de fuga de información.	Aunque el estudio se realizó en Bolivia, los hallazgos pueden ser relevantes para profesionales forenses en Ecuador, dado que CSI Linux es una herramienta de código abierto accesible a nivel global.
3	*Conceptual Evidence Collection and Analysis Methodology for Android Devices*	Ben Martini, Kim-Kwang Raymond Choo	2015	Internacional	arXiv	https://arxiv.org/pdf/1506.05527	Analiza siete aplicaciones populares en Android y describe los artefactos forenses relevantes que generan. Proporciona una metodología sólida para su recolección y análisis.	Investigación teórica con pruebas experimentales en un entorno controlado.	Evidence analysis, Android devices	Metodología práctica y útil para investigaciones enfocadas en recuperación de datos de aplicaciones sociales.	Alta relevancia, dado el uso extensivo de aplicaciones sociales en investigaciones locales en Ecuador.
4	*Forensic Analysis of Third-Party Location Applications in Android and iOS*	Jason Bays, Umit Karabiyik	2022	Internacional	arXiv	https://arxiv.org/pdf/1907.00074	Analiza aplicaciones de ubicación de terceros en Android y iOS, mostrando cómo extraer y analizar información relevante como registros de ubicación y eventos asociados.	Análisis práctico utilizando técnicas de extracción en ambas plataformas (Android e iOS).	Location apps, geolocation forensics	Esencial para investigaciones relacionadas con rastreo de ubicaciones y reconstrucción de eventos.	Alta relevancia, dado el interés en temas de geolocalización en investigaciones en Ecuador.

5	*Performance of Android Forensics Data Recovery Tools*	Bernard Ogazi-Onyemaechi, Ali Dehghantanha, Kim-Kwang Raymond Choo	2017	Internacional	arXiv	https://arxiv.org/pdf/1709.05144	Evaluación comparativa de herramientas forenses a través de experimentos controlados.	Enfocado solo en recuperación de datos eliminados; no evalúa otros tipos de análisis como extracción en vivo o artefactos específicos.	Data recovery, forensic tools	Útil para seleccionar herramientas específicas en investigaciones centradas en recuperación de datos borrados.	Alta relevancia, considerando el frecuente uso de dispositivos Android en Ecuador.
6	*Digital Investigation Techniques: A NIST Scientific Foundation Review*	James R. Lyle -Barbara Guttman -John M. Butler -Kelly Sauerwein -Christina Reed -Corrine	2022	Internacional	Scholar	https://www.nist.gov/publications/digital-investigation-techniques-nist-scientific-foundation-review	Explica técnicas profesionales para investigación forense digital y extracción de datos.		NIST, investigación forense, extracción de datos	Aplicaciones en procedimientos forenses profesionales	
7	*Guidelines on Mobile Device Forensics*	Ayers, R., Jansen, W., Moenner, L., & Delaitre, A.		EE.UU.	NIST	Report	Proporciona lineamientos clave para estructurar un marco metodológico aplicable al análisis forense documental.	Revisión documental y análisis de normativa	Análisis forense, dispositivos móviles, directrices forenses	Aplicable en la definición de estándares para análisis forense en dispositivos móviles	Puede servir como base para adaptar procedimientos forenses en Analiza cómo los datos almacenados en la nube pueden ser recuperados y examinados en el contexto de una investigación forense digital.Ecuador
8	*ForensicVM: Developing a Virtualisation Plugin for Autopsy Software: Challenges and Solutions in Acquiring Digital Evidence from Virtualised Forensic Images*	Mourinho, N.G.A.A.	2024	Portugal	Repositorio do Instituto Politécnico de Beja	content	Desarrolla un plugin de virtualización para Autopsy, abordando desafíos y soluciones en la adquisición de evidencia digital de imágenes forenses virtualizadas.	Desarrollo de software y evaluación práctica	Autopsy, virtualización, imágenes forenses, adquisición de evidencia	Mejora la capacidad de Autopsy para manejar imágenes forenses virtualizadas, facilitando el análisis de entornos virtuales en investigaciones digitales.	Proporciona una herramienta avanzada que puede ser adoptada por profesionales forenses en Ecuador para mejorar la eficiencia en el análisis de evidencia digital en entornos virtualizados.
9	*Digital Forensics Research: The Next 10 Years*	Garfinkel, S. L.	2020	EE.UU.	ScienceDirect	Digital forensics research: The next 10 years - ScienceDirect	Examina tendencias futuras en el análisis forense digital, resaltando la importancia del software libre en la disciplina.	Revisión bibliográfica	Software libre, futuro de la forensia digital, tendencias tecnológicas	Permite prever avances en herramientas de software libre	Puede influir en la adopción de software libre en la investigación forense local

10	*Manejo de la evidencia digital con visión en normas internacionales aplicables por los primeros interventores y peritos forenses en Ecuador*	Fernando Mauricio De la Torre Muñoz Alejandro Xavier Puertas Realpe Christian Eduardo Burbano Peña	2024	Ecuador	Repositorio ISUPOL	https://innovacionysaber.isupol.edu.ec/index.php/innovacion/article/view/280	Explica cómo manejar la evidencia digital conforme a normas internacionales y su aplicación en Ecuador.	Análisis, normativas	Evidencia digital, normas internacionales, Ecuador		El estudio nos indica de cómo llevar o preservar la evidencia digital en los acasos respectivos , el estudio se hizo con normas internacionales y su aplicabilidad fue en Ecuador
11	*Análisis forense digital en dispositivos móviles*	Alemán Ariza, A.	2024	Panamá	Revista Cathedra	Análisis forense digital en dispositivos móviles | Revista Cathedra	El estudio aborda los desafíos que presenta el análisis forense digital en dispositivos móviles debido al constante avance tecnológico y las implicaciones legales relacionadas con la privacidad. Se enfatiza la necesidad de que los analistas forenses se mantengan actualizados para realizar extracciones exitosas de información, respetando las normas que rigen el manejo de evidencia digital y garantizando la integridad de la información obtenida.	Revisión documental y análisis de las normativas vigentes en el manejo de evidencia digital, junto con una discusión sobre las técnicas de extracción en diferentes sistemas operativos móviles.	Informática forense, análisis forense digital, dispositivo móvil, copia forense, sistemas operativos móviles, extracción Android, extracción iOS.	Proporciona una visión actualizada de los retos y mejores prácticas en el análisis forense de dispositivos móviles, sirviendo como referencia para profesionales en el campo.	Aunque el estudio se centra en el contexto panameño, los desafíos y recomendaciones presentados son aplicables a nivel global, incluyendo Ecuador, donde el uso de dispositivos móviles es prevalente y las consideraciones legales son similares.
12	*Comparative Study of Mobile Forensics Tools: Autopsy, Belkasoft X and Magnet Axiom*	Mehta, J., Bhadania, Y., Shah, P., & Patel, D.	2024	India	IEEE Xplore	Comparative Study of Mobile Forensics Tools: Autopsy, Belkasoft X and Magnet Axiom | IEEE Conference Publication | IEEE Xplore	Este estudio compara las herramientas forenses móviles Autopsy, Belkasoft X y Magnet Axiom en términos de eficiencia, precisión y facilidad de uso. Los resultados indican que,	Evaluación experimental de las tres herramientas utilizando un conjunto de datos estandarizado para medir su rendimiento en diversas	Análisis forense móvil, Autopsy, Belkasoft X, Magnet Axiom, comparación de herramienta	Proporciona información valiosa para los profesionales forenses en la selección de herramientas adecuadas según las necesidades específicas de sus investigaciones.	Aunque el estudio se realizó en India, las conclusiones son aplicables a nivel global, incluyendo Ecuador, ya que las herramientas evaluadas son utilizadas internacionalmente.

							aunque todas las herramientas tienen sus fortalezas, Magnet Axiom destaca en la recuperación de datos eliminados, mientras que Autopsy es valorada por ser una solución de código abierto.	métricas clave.			
13	*Forensic Investigation: Apple Devices Acquisition & Analysis*	Shukla, P., & Pratap, A.	2022	India	Journal of Cyber Security and Digital Forensics	jcsdf.nfsu.ac.in/assets/dl/%2817-24%29 Forensic Investigation Apple Devices Acquisition %26 Analysis.pdf	Este estudio aborda los desafíos en la adquisición y análisis forense de dispositivos Apple, destacando las características de seguridad que dificultan la investigación. Se presentan métodos de adquisición y análisis utilizando herramientas de código abierto, proporcionando una guía práctica para investigadores forenses.	Revisión de la arquitectura de iOS y macOS, análisis de los modos de operación y procesos de arranque, y aplicación de técnicas de adquisición como el uso de jailbreak y herramientas como 3uTools, checkra1n, iLEAPP, Belkasoft Evidence Center X y Sumuri Recon Lab.	Dispositivos Apple, adquisición forense, análisis forense, iOS, macOS, herramientas de código abierto.	Ofrece una guía práctica para la adquisición y análisis de dispositivos Apple, lo que es valioso para profesionales forenses que enfrentan desafíos debido a las robustas características de seguridad de estos dispositivos.	Aunque el estudio se realizó en India, los métodos y herramientas discutidos son aplicables a nivel global, incluyendo Ecuador, donde la prevalencia de dispositivos Apple requiere técnicas especializadas para su análisis forense.
14	*Análisis de dispositivos móviles con las herramientas del sistema operativo Tsurugi de casos derivados de la oficina técnica de la Unidad de Violencia Carcelén*	Tipanta Díaz, K. M.	2023	Ecuador	Repositorio de la Universidad Técnica de Cotopax	Análisis de dispositivos móviles con las herramientas del sistema operativo Tsurugi de casos derivados de la oficina técnica de la Unidad de Violencia Carcelén "Casa de Justicia".	Este estudio evalúa la eficacia del sistema operativo Tsurugi y sus herramientas en el análisis forense de dispositivos móviles en casos reales gestionados por la Unidad de Violencia Carcelén. Los resultados indican que Tsurugi proporciona un conjunto robusto de herramientas que facilitan la extracción y	Aplicación práctica de las herramientas de Tsurugi en casos reales, con documentación detallada de los procedimientos de extracción y análisis de datos, y evaluación de la eficacia de las herramientas utilizadas.	Análisis forense, dispositivos móviles, Tsurugi, extracción de datos, violencia de género	Proporciona una evaluación práctica de Tsurugi en un contexto real, ofreciendo insights sobre su aplicabilidad y eficacia en investigaciones forenses de dispositivos móviles.	Al ser un estudio realizado en Ecuador, los hallazgos son directamente relevantes para las prácticas forenses locales, especialmente en casos relacionados con violencia de género.

							análisis de datos relevantes para investigaciones forenses.				
15	*How to do a forensic analysis of Android 11 artifacts*	Delija, D., Sudec, D., Sirovatka, G., & Žagar, M.	2022	Croacia	IEEE Xplore	How to do a forensic analysis of Android 11 artifacts | IEEE Conference Publication | IEEE Xplore	Este estudio compara los resultados obtenidos utilizando varias herramientas forenses en dispositivos con el sistema operativo Android 11.	Evaluación comparativa de herramientas forenses aplicadas a dispositivos Android 11, analizando su eficacia en la extracción y análisis de artefactos específicos del sistema operativo.	Análisis forense, Android 11, herramientas forenses, artefactos digitales.	Análisis forense, Android 11, herramientas forenses, artefactos digitales.	Aunque el estudio se realizó en Croacia, los hallazgos son aplicables a nivel global, incluyendo Ecuador, donde el uso de dispositivos Android es prevalente.
16	*Análisis forense digital: extracción de información de dispositivos*	Pradhan, A., y Dei, B.	India	2023	Taylor y Francis	https://www.taylorfrancis.com/books/edit/10.1201/9781003471103/advancements-cyber-crime-investigations-modern-data-analytics-shishir-kumar-shandilya-devangana-sujay-gupta?refId=730f4525-579a-4049-b69f-c97fc5c3ac6f&context=ubx	Este capítulo aborda las técnicas de ciberseguridad y normas internacionales	Revisión de técnicas de adquisición de datos, análisis de sistemas de archivos y métodos para superar obstáculos comunes en la extracción de datos de dispositivos digitales.	Informática forense, extracción de datos, dispositivos digitales, integridad de la evidencia.		Aunque el estudio se realizó en India, las técnicas y metodologías discutidas son aplicables a nivel global, incluyendo Ecuador, donde la correcta extracción de información de dispositivos digitales es crucial en investigaciones forenses.
17	*Herramientas forenses para navegadores web: Autopsy BHE y análisis de red*	Adamu, H., Ahmad, AA, Hassan, A. y otros	Nigeria	2021	Ent. J.Res. Innovación. Aplicación.	https://d1wqtxts1xzle7.cloudfront.net/108463630/103-107-libre.pdf?1701892371=&response-content-disposition=inline%3B+filename%3DWeb_Browser_Forensic_Tools_Autopsy_BHE_a.pdf&Expires=1739306789&Si	Este estudio analiza el uso de herramientas forenses, específicamente Autopsy y Browser History Examiner (BHE), en la investigación de actividades en navegadores web. Se destaca la eficacia de estas herramientas en la recuperación y	Evaluación práctica de Autopsia y BHE en entornos controlados, con análisis de casos de estudio que simulan actividades sospechosas en navegadores web.	Informática forense, navegadores web, Autopsy, Browser History Examiner, análisis de red.	Proporciona a los profesionales forenses métodos efectivos para extraer y analizar datos de navegación web, lo que es crucial en investigaciones relacionadas con actividades en línea.	Aunque el estudio se realizó en Nigeria, las herramientas y metodologías discutidas son aplicables a nivel global, incluyendo Ecuador, donde el análisis de datos de navegación web es relevante en investigaciones forenses.

						gnature=MIKJM-ILoxXfDw3OEDTWdAdRba8~rz94cClrWYl7k0UrlhkmmTpJcOm5~hWsaWANXNad8FHK5tr~2pPxC57Jlfw4gnlMPq~xN14gTZe7-AXoXrv6-RQK6CLxPXVQyjlY84vNGoLk5KYR3xgmOwtspNRV3g3olBCZK8s12kPefkCDjhskCor6ygyop5kCl0Caf58YM8o5aqzaNS0Y1NRFxPTiWb5R9CUElvCAtSkxNu40LDqqgEQ42a8GfBPQnF78b-KfbbCtYqVjKcRfLi-86iVTWTF3pBiP5aLVAMsVOLXaQQdEj1-~YDFKTmD6JgudWSfDF5ipKAwJlK--Q5tUsQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA	análisis de datos de navegación, así como en la interpretación de patrones de comportamiento del usuario en línea.			
18	*Android Chat Application Forensic Process Improvement & XRY Support*	Djagilev, V.	2017	Estonia	CORE.ac.uk	https://core.ac.uk/download/pdf/237085076.pdf	El estudio propone mejoras en los procesos forenses aplicados a aplicaciones de mensajería en Android y evalúa la capacidad de XRY para extraer y analizar estos datos. Se identificaron limitaciones en la extracción de datos encriptados y se sugirieron optimizaciones para mejorar la	Evaluación experimental con herramientas forenses, pruebas de extracción de datos con XRY y comparación con otras soluciones.	Informática forense, XRY, aplicaciones de mensajería, análisis de datos móviles.	Permite mejorar los procedimientos de recuperación de datos	En Ecuador, donde el uso de aplicaciones de mensajería es alto, la mejora en los procesos de extracción de datos facilita investigaciones forenses y refuerza la capacidad de análisis digital.

							recuperación de información					
19	*Data Acquisition Techniques in Mobile Forensics*	Sathe, S.C., & Dongre, N.M.	2018	India	EEE Xplore	https://ieeexplore.ieee.org/abstract/document/8399079	Se presenta una revisión de las técnicas más utilizadas en la adquisición de datos en dispositivos móviles, incluyendo métodos físicos y lógicos. También se evalúa el impacto de los sistemas de cifrado en la recuperación de datos.	Revisión de literatura y análisis experimental de herramientas de adquisición forense.	Análisis forense, adquisición de datos, dispositivos móviles, cifrado de datos.	Facilita la selección de técnicas de adquisición adecuadas según el tipo de dispositivo y nivel de seguridad, mejorando la eficacia en investigaciones forenses.	En Ecuador, la adquisición efectiva de datos es clave para fortalecer investigaciones de delitos digitales y mejorar la admisibilidad de evidencia en procesos judiciales.