Maestría en

Ciberseguridad

Trabajo de investigación previo a la obtención del título de

Magíster en Ciberseguridad

AUTORES:

EDGAR VINICIO TUPIZA GUALOTUÑA

GUILLERMO FRANCISCO QUIÑONEZ CASTRO

JONATHAN ALEXIS CUASQUER GARCIA

GEOVANNA BELÉN TORRES BONILLA

TUTORES:

Alejando Cortés

Iván Reyes

TEMA

Informe Técnico Pericial referente al desbloqueo, extracción, preservación, análisis, y materialización de datos almacenados en dispositivos móviles con Sistema Operativo Android.

Quito, (Julio – 2024)

Certificación de autoría

Nosotros, Edgar Vinicio Tupiza Gualotuña, Guillermo Francisco Quiñonez Castro, Jonathan Alexis Cuasquer García y Geovanna Belén Torres Bonilla, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador (UIDE), para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales

Firma del graduando
Edgar Vinicio Tupiza Gualotuña

Firma del graduando
Guillermo Francisco Quiñonez Castro

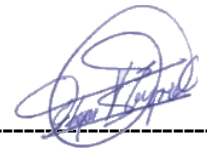
Firma del graduando
Jonathan Alexis Cuasquer Garcia

Firma del graduando
Geovanna Belén Torres Bonilla

Autorización de Derechos de Propiedad Intelectual

Nosotros, Edgar Vinicio Tupiza Gualotuña, Guillermo Francisco Quiñonez Castro, Jonathan Alexis Cuasquer Garcia y Geovanna Belén Torres Bonilla, en calidad de autores del trabajo de investigación titulado ***Informe Técnico Pericial referente al desbloqueo, extracción, preservación, análisis, y materialización de datos almacenados en dispositivos móviles con Sistema Operativo Android***, autorizamos a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que nos pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autores nos corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, (09 2024)



Firma del graduando
Edgar Vinicio Tupiza Gualotuña

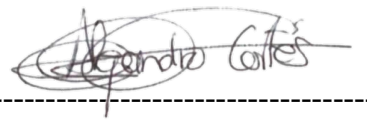
Firma del graduando
Guillermo Francisco Quiñonez Castro

Firma del graduando
Jonathan Alexis Cuasquer García

Firma del graduando
Geovanna Belén Torres Bonilla

Aprobación de dirección y coordinación del programa

Nosotros, Alejandro Cortés director EIG e Iván Reyes Coordinador UIDE, declaramos que: Edgar Vinicio Tupiza Gualotuña, Guillermo Francisco Quiñonez Castro, Jonathan Alexis Cuasquer García y Geovanna Belén Torres Bonilla, son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.



Alejandro Cortés
Director/a de la
Maestría en Ciberseguridad

Iván Reyes
Coordinador/a de la
Maestría en Ciberseguridad

DEDICATORIA

A nuestra familia querida, a cada uno por su amor incondicional como padres y acompañamiento constante, a nuestros hijos por ser nuestra motivación. Este logro es tanto nuestro como suyo, Gracias por siempre estar allí para nosotros y por tener fe en nosotros.

AGRADECIMIENTOS

A nuestros compañeros de tesis, profesores e instructores, nuestra más sincera gratitud. A nuestros compañeros por su colaboración, apoyo y compañía a lo largo de este largo y agotador viaje. A nuestros profesores e instructores por su supervisión, comprensión, tutorías y disposición para impartir su amplio conocimiento. Este logro se alcanza a través de los esfuerzos combinados y el compromiso de todos. Gracias por ser una parte esencial de este viaje académico.

RESUMEN

Para proteger la integridad de los dispositivos móviles y su contenido digital, es esencial contar con el equipamiento adecuado y garantizar que los dispositivos sigan siendo válidos como prueba judicial. Para ello, es indispensable determinar la metodología a aplicar, considerando el modelo, la versión del sistema operativo instalado y la marca del dispositivo, lo que permitirá aplicar diferentes tipos de extracción.

En la extracción lógica, el software forense envía solicitudes mediante comandos al teléfono, y este responde con datos desde su memoria. La extracción de sistemas de archivos extrae los archivos del sistema del dispositivo, los datos de usuario, de aplicaciones y algunos archivos ocultos o protegidos. La extracción física es la más invasiva, ya que realiza una copia bit a bit del contenido de la memoria flash del equipo, incluyendo el espacio sin asignar, y puede extraer información que haya sido borrada recientemente.

Palabras Claves: integridad, evidencia, judicial, metodología.

ABSTRACT

To safeguard the integrity of mobile devices and their digital information, it is crucial to have the right equipment in place and ensure that the devices maintain their validity as evidence in court proceedings. This involves establishing an appropriate methodology, taking into account the model, operating system version, and device brand, which will allow various types of extraction to be applied.

Logical extraction: In this method, forensic software sends commands to the phone, which responds by providing data from its memory.

File System Extraction: This process involves extracting files from the system, as well as user data, applications, and some hidden or protected files.

Physical extraction: This is the most intrusive method, as it makes a bit-by-bit copy of the contents of the device's flash memory, including unallocated space, and can recover information that has been recently deleted.

Keywords: integrity, evidence, judicial, methodology.

TABLA DE CONTENIDOS

Contenido

LISTA DE TABLAS

LISTA DE FIGURAS

CAPÍTULO 1:

Introducción

1.1. Planteamiento Del Problema E Importancia Del Estudio

La fiscalía general del Estado, entre sus cargos más importantes desea asegurar la justicia y salvaguardar el orden público por medio de la investigación y el enjuiciamiento de delitos. Es por esto que, en cumplimiento a su función, esta entidad va a los informes periciales de informática forense como herramientas esenciales y fundamentales en la investigación y el enjuiciamiento de delitos tecnológicos y cibernéticos. Estos dictámenes facilitan la recopilación, el análisis y la presentación de evidencias digitales, abarcando información de dispositivos electrónicos, redes y sistemas informáticos. Como un vínculo crucial entre el conocimiento técnico y la aplicación de la Ley.

El sacar información en dispositivos móviles a través de formas tradicionales y manuales crea un alto riesgo de manipulación de la evidencia, lo que compromete la autenticidad, integridad y fiabilidad de los datos, creando dudas sobre el valor de los hallazgos y afectando la credibilidad del informe técnico pericial, lo que causaría serias consecuencias en el ámbito judicial, afectando tanto a las partes implicadas como al sistema legal en su conjunto. Primero, un análisis incorrecto o una presentación defectuosa de la evidencia pueden tomarse decisiones equivocadas, como la liberación de un culpable o la condena de un inocente. Esta situación no solo perjudica a los afectados, sino también la confianza del público en la imparcialidad y la efectividad del sistema judicial, poniendo en duda su legitimidad y su capacidad para proporcionar justicia.

En tal virtud mediante el aumento del presente proyecto investigativo se obtendrá un informe técnico pericial, que use métodos internos de tratamiento de evidencia digital, herramientas forenses avanzadas y software forense especializado para el desbloqueo, sacar y analizar datos de dispositivos móviles con Sistema Operativo Android, logrando así la entrega de información precisa y confiable, significativo para casos de investigación delincuencial, que podrán ser presentados dentro de un tribunal.

1.2. Naturaleza o tipo de proyecto

Lo natural del proyecto se centra en el ámbito de la informática forense, con una claridad específica en aparatos móviles que operan con el sistema operativo Android. El propósito es desarrollar un procedimiento técnico y pericial que permita hacer una serie de actividades cruciales en investigaciones forenses digitales. Aquí se desglosa la naturaleza del proyecto basado en los objetivos proporcionados.

El procedimiento propuesto abarcará una serie de técnicas periciales avanzadas para la adquisición y análisis de información, y la preservación de evidencia, garantizando que se cumplan las mejores prácticas y protocolos establecidos en el ámbito de la informática forense. Este enfoque metódico no solo facilitará y protegerá la integridad de los datos en la recuperación de información crítica, que es vital para las investigaciones, sino que también a lo largo de todo el proceso investigativo, afirma que cada paso realizado sea verificable.

Asimismo, el proyecto de investigación se centrará en la integración de herramientas y software especializados que mejoren tanto la eficiencia como la efectividad del análisis forense. Estas tecnologías de vanguardia permitirán a los investigadores manejar grandes volúmenes de información de manera más efectiva y realizar análisis más profundos y significativos. El uso

de herramientas adecuadas no solo da calidad al proceso de recolección de datos, sino que también minimiza el riesgo de errores, lo que es crucial en el contexto legal.

Se dará especial importancia a la capacitación de los profesionales en el uso de estas herramientas, asegurando que estén debidamente preparados para enfrentar los retos que suponen los dispositivos móviles bajo el sistema operativo Android. Incluyendo no solo el manejo técnico de las herramientas, sino también una comprensión de las implicaciones legales y éticas que acompañan a la informática forense. Esto permitirá a los investigadores abordar cada caso con una perspectiva integral, considerando los aspectos técnicos y los legales.

Además, se aumentará el conocimiento en las áreas de tecnología, criminología y derecho, creando un marco que enriquecerá el proceso de investigación, la cual será fundamental para desarrollar un informe pericial adaptado a las necesidades cambiantes de las investigaciones forenses digitales, en especial, porque la tecnología avanza rápidamente.

1.3. Objetivos

1.3.1. Objetivo general

Desarrollar un informe Técnico Pericial que utilice métodos forenses para el proceso de desbloqueo, extracción, preservación, análisis, y materialización de la información almacenada en dispositivos móviles con Sistema Operativo Android.

1.3.2. Objetivos específicos

Analizar la compatibilidad de desbloqueo de dispositivos móviles mediante el uso de herramientas forenses, considerando la marca, modelo y versión sistema del operativo.

Determinar el tipo de extracción de información forense, según el resultado del análisis de compatibilidad.

Analizar la información recuperada con software forense especializado en dispositivos móviles, para examinar datos previamente eliminados.

Seleccionar la información significativa, considerando parámetros de búsqueda definidos en una delegación fiscal para una investigación.

1.4. Justificación e importancia del trabajo de investigación

La presente investigación se justifica por las siguientes razones: Se utiliza software y equipamiento forense especializado, esencial para asegurar la exactitud y fiabilidad de la evidencia en procesos legales, permitiendo un análisis rápido y preciso que minimiza errores y falsos positivos, garantizando transparencia y credibilidad técnico-científica.

El informe técnico pericial generado con herramientas forenses avanzadas, para la extracción de información y análisis de datos en dispositivos móviles con sistema operativo Android, servirá como apoyo al sistema de justicia, convirtiéndose en una prueba crucial y de gran importancia en casos complejos, proporcionando evidencia admisible y objetiva que fundamenta decisiones informadas, en los procesos judiciales.

La aplicación de técnicas forenses innovadoras para sacar la información en telefonía móvil permitirá que las investigaciones sean exhaustivas y precisas, mejorando así la resolución de casos judiciales y prevención de errores en el desarrollo de informes técnico-periciales.

La utilización de normas ISO, en el desarrollo de la presente investigación asegurará la calidad, confiabilidad y credibilidad de los informes técnicos periciales, permitiendo que los resultados sean no a nuestra manera de pensar, sino verídicos y admisibles en los tribunales de justicia. Demostrando un enfoque científico en la integridad de la investigación, lo que es esencial para la justicia y la seguridad.

CAPÍTULO 2

Marco Teórico

2.1. Informe técnico pericial

Un informe técnico pericial es un documento elaborado por un perito, un experto en un área específica, como medicina, contabilidad, informática o ingeniería. Su propósito es proporcionar un análisis detallado y fundamentado sobre hechos o evidencias relevantes para un caso legal, actuando como apoyo en la toma de decisiones judiciales.

La función principal es ofrecer a las autoridades judiciales una interpretación clara y precisa de los aspectos técnicos relacionados con un caso, los cuales podrían resultar complicados o difíciles de entender. Por lo tanto, el informe debe ser rápido y riguroso, pero también redactado en un lenguaje claro y accesible, para que jueces, abogados y otros profesionales del sistema judicial puedan comprenderlo sin dificultad.

Los informes periciales deben cumplir con ciertos requisitos que garantizan su validez y utilidad en el proceso judicial. Esto incluye la obligación de presentar los hallazgos de manera estructurada, incluyendo elementos como la introducción del caso, la metodología empleada, los resultados obtenidos y las conclusiones a las que se ha llegado. Asimismo, se

enfatiza la importancia de documentar de manera exhaustiva cada paso del proceso, asegurando así la transparencia y la trazabilidad de la información presentada. (Ley de Enjuiciamiento Civil, 2015)

Extracción de Información de dispositivos móviles mediante la utilización de Software Forense. La extracción de información a través de software forense en dispositivos móviles es un proceso clave en el ámbito de las investigaciones digitales, especialmente debido a la creciente dependencia de estos dispositivos en la vida diaria. Con el aumento de datos personales almacenados en teléfonos inteligentes y tabletas, se vuelve cada vez más crucial realizar un análisis forense efectivo. Este procedimiento no solo consiste en recuperar informaciones disponibles, sino también en entender su contexto y significado dentro de un marco legal. La capacidad para recuperar datos eliminados, analizar aplicaciones y obtener metadatos puede ofrecer pruebas significativas que impacten en el resultado de un caso. Es vital que la recolección de estos datos sea precisa e íntegra para asegurar que la información recopilada sea admitida en los procedimientos judiciales.

Finalmente, la extracción de datos de dispositivos móviles debe realizarse en colaboración con las autoridades legales, respetando siempre las normativas sobre privacidad y protección de datos. Esto no solo refuerza la validez del trabajo realizado, sino que también ayuda a mantener la confianza del público en los procedimientos forenses. En conclusión, es fundamental integrar un enfoque ético, legal y técnico en la extracción de información forense para garantizar el éxito en el ámbito judicial y en la búsqueda de la verdad.

2.1.1. Software forense

El software forense se refiere a un conjunto de herramientas y aplicaciones diseñadas específicamente para la recuperación, análisis y preservación de datos en dispositivos electrónicos. Este tipo de software es fundamental en el ámbito de la ciberseguridad, las investigaciones criminales y el análisis de incidentes digitales. Proporciona a los expertos forenses la capacidad de acceder a información crítica que puede ser determinante para resolver delitos, como fraudes, acosos cibernéticos o accesos no autorizados. (Casey, E, 2011).

En la actualidad, hay diversos programas de software forense creados específicamente para la extracción de datos de dispositivos móviles. Estas herramientas son fundamentales para investigar incidentes cibernéticos y para la recolección de evidencias legales. A continuación, se detallan algunas de las herramientas más relevantes en este ámbito

2.1.2. Cellebrite UFED

Es uno de los softwares forenses más reconocidos en el ámbito de sacar la información de dispositivos móviles. Diseñado específicamente para investigadores y profesionales de la seguridad, este programa permite recuperar información de una amplia variedad de dispositivos y aplicaciones, incluyendo mensajes de texto, contactos, fotos, registros de llamadas y datos de aplicaciones. Su tecnología avanzada se destaca por la capacidad de sacar datos de dispositivos bloqueados y aquellos que han sido restaurados a su configuración de fábrica, lo que la convierte en una herramienta invaluable para la investigación forense.

2.1.3. Capacidades y Funcionalidades

Una de las principales ventajas de Cellebrite UFED es su versatilidad. El software es compatible con una extensa gama de dispositivos móviles, lo que incluye tanto teléfonos inteligentes como tabletas de diferentes marcas y modelos. Esta compatibilidad es crucial, dado que el ecosistema de dispositivos móviles es altamente diverso y en constante evolución.

Cellebrite UFED no solo se centra en la recuperación de datos accesibles; sino que también recupera información eliminada, lo que puede ser determinante en investigaciones donde se sospecha que se han borrado datos de manera intencionada. Además, el programa permite el análisis de datos en contexto, ayudando a los investigadores a comprender lo significativo de la información recuperada en relación con el caso en cuestión.

El software cuenta con una interfaz amigable que facilita el proceso de extracción y análisis, permitiendo que incluso aquellos que no son expertos en tecnología puedan utilizarlo de manera efectiva. A su vez, Cellebrite ofrece capacitación y soporte técnico, lo que refuerza su utilidad en entornos de investigación donde el tiempo y la precisión son esenciales.

2.1.4. Relevancia en Investigaciones Legales

Cellebrite UFED ha sido fundamental en numerosas investigaciones criminales, así como en casos de ciberseguridad, donde la recuperación de datos móviles es vital. La información extraída puede proporcionar evidencia crucial para juicios, investigaciones de delitos informáticos y en la recolección de pruebas en casos de fraude o acoso cibernético. La capacidad de acceder a datos que pueden haber sido intencionalmente eliminados es especialmente valiosa en este contexto.

Además, la tecnología de Cellebrite UFED permite la creación de informes detallados que presentan los hallazgos de manera clara y estructurada. Estos informes son esenciales en el ámbito judicial, ya que facilitan la comprensión de la evidencia por parte de jueces, abogados y otros actores del sistema legal. (Cellebrite, 2024)

2.2. El Physical Analyzer

Es una herramienta forense avanzada y altamente especializada, diseñada para la extracción y análisis de datos en dispositivos móviles. Este software se ha convertido en un recurso indispensable para investigadores forenses, ya que permite el acceso a una gama completa de información almacenada en dispositivos, incluyendo áreas que pueden no ser fácilmente accesibles mediante métodos convencionales de análisis.

Una de las características más destacadas del Physical Analyzer es su capacidad para recuperar datos que han sido eliminados. Muchos usuarios creen que al borrar información se elimina permanentemente, pero este software puede acceder a fragmentos de datos que permanecen en la memoria del dispositivo, lo que puede ser crucial en investigaciones donde las pruebas digitales son determinantes.

Además, el Physical Analyzer permite la extracción de datos desde diferentes sistemas operativos y tipos de dispositivos, ofreciendo versatilidad en su aplicación. Desde teléfonos inteligentes hasta tabletas, esta herramienta puede manejar diversas plataformas, facilitando la recopilación de información crítica que incluye no solo mensajes de texto y registros de llamadas, sino también datos de aplicaciones, fotos, videos y más.

El software también proporciona un análisis detallado de la estructura de archivos y bases de datos, lo que permite a los investigadores entender mejor cómo se organizan y

almacenan los datos en el dispositivo. Esto es útil en casos complejos donde la organización de la información puede ofrecer pistas sobre el comportamiento del usuario o el contexto de un delito. (Cellebrite, 2024a).

2.2.1. XRY

Es una herramienta destacada en el campo de la extracción forense de datos de dispositivos móviles, reconocida por su especialización en el análisis de plataformas móviles. Esta herramienta permite a los investigadores acceder a una amplia gama de dispositivos, facilitando la recuperación de información crítica de aplicaciones y otros datos almacenados. XRY se ha convertido en una opción preferida para aquellos que trabajan en la intersección de la tecnología y la ley, gracias a su capacidad para manejar diferentes sistemas operativos y tipos de dispositivos.

2.2.2. Capacidades de Análisis Avanzado

Una de las características más notables de XRY es su capacidad avanzada para analizar datos específicos de aplicaciones. Esto incluye no solo la recuperación de datos básicos, como mensajes y registros de llamadas, sino también la extracción de información detallada de aplicaciones de mensajería, redes sociales y otras plataformas digitales. Esta funcionalidad es crucial en investigaciones que requieren un enfoque meticuloso, donde los detalles pueden marcar la diferencia en la resolución de un caso.

El software de XRY permite a los expertos forenses obtener datos que de otro modo podrían ser difíciles de acceder, incluyendo datos eliminados. Además, su interfaz intuitiva facilita el trabajo de los investigadores, quienes pueden realizar análisis complejos sin necesidad de contar con un amplio conocimiento técnico.

2.2.3. Importancia en Investigaciones Legales

XRY ha demostrado ser una herramienta invaluable en diversas investigaciones legales, desde delitos informáticos hasta casos de acoso. La capacidad de acceder a información almacenada en aplicaciones y otros datos que pueden haber sido eliminados puede ser decisiva para la recopilación de pruebas en un juicio. Los informes generados por XRY son claros y estructurados, lo que facilita su uso en entornos judiciales. (MSAB, 2024).

2.2.4. GrayKey

Graykey es una herramienta avanzada en el campo de la extracción forense de datos de dispositivos móviles, diseñada en especial para ayudar a investigadores y fuerzas del orden en el acceso a información de teléfonos inteligentes, particularmente aquellos que operan con sistemas iOS. Desarrollada por la empresa Grayshift, Graykey ha ganado reconocimiento por su capacidad para eludir las medidas de seguridad que protegen los datos de los dispositivos, lo que la convierte en un recurso invaluable en la lucha contra la criminalidad digital.

2.2.4.1. Capacidades y Funcionalidades

Una de las cosas más destacadas de Graykey es su volumen para desbloquear dispositivos iOS y sacar información, incluso de lo que ha sido bloqueados. Utilizando un enfoque técnico sofisticado, Graykey puede recuperar datos como mensajes de texto, contactos, fotos, registros de llamadas y datos de aplicaciones, dando a los investigadores un acceso completo a la información guardada en el dispositivo.

Graykey opera por medio de la conexión física del dispositivo a la herramienta, lo que permite realizar un análisis profundo de los datos. Esta capacidad de recuperación es muy

valiosa en investigaciones criminales, donde la información de un dispositivo puede ser crucial para establecer vínculos entre sospechosos y delitos. (Magnet Forensics, 2024)

2.2.4.2. Normas ISO

Las normas ISO relevantes para sacar la información de aparatos móviles con software forense son importantes para asegurar la calidad y la confiabilidad de los casos involucrados en la investigación digital. Estas normas establecen un marco de referencia que guía a los profesionales forenses en la implementación de prácticas consistentes y efectivas, lo que es crucial en un campo donde la precisión y la integridad de la información son esenciales.

La adopción de estas normas contribuye y ayuda a mejorar la calidad del trabajo forense, y a fortalecer la confianza en los resultados obtenidos. En un ambiente donde las pruebas digitales pueden ser determinantes en la resolución de casos legales, seguir directrices estandarizadas asegura que la información tomada sea tratada de manera adecuada, restando el riesgo de contaminación o pérdida de datos.

Estas normas, promueven la operabilidad intermedia entre diferentes herramientas y sistemas, lo que permite a los investigadores utilizar una variedad de software forense sin comprometer la calidad de los resultados. También fomentan la capacitación y el desarrollo profesional continuo, asegurando que los especialistas en forense se actualicen con las mejores prácticas y tecnologías emergentes.

2.3.1. Normas ISO para el Tratamiento de Evidencia Digital

Las normas ISO son importantes para definir directrices y procedimientos estandarizados en el manejo de evidencia digital, garantizando la integridad y calidad de los datos a lo largo de todas las etapas de recolección, análisis y presentación en entornos legales. Estas directrices dan paso a los profesionales forenses a gestionar la evidencia de forma coherente y confiable, lo cual es vital para asegurar la validez de los hallazgos en investigaciones legales.

2.3. Principales Normas ISO

2.3.1. ISO/IEC 27037:2012

Esta norma es esencial para la identificación, recolección, adquisición y preservación de evidencia digital en el contexto de investigaciones forenses. Establece procedimientos claros que guían a los investigadores en la gestión adecuada de la evidencia desde el instante en que se junta, garantizando que se sigan prácticas que disminuyan el riesgo de contaminación, alteración o pérdida de información.

Además, la norma enfatiza lo importante de documentar cada proceso, lo que no solo ayuda a mantener la cadena de custodia de la evidencia, sino que asegura que los hallazgos sean válidos y admisibles en un entorno judicial. Esto es crucial en un campo donde la precisión y la integridad de los datos son importantes para la resolución de casos legales. La implementación de ISO/IEC 27037:2012, mejora la calidad del trabajo forense, y fortalece la confianza en los resultados, contribuyendo a la credibilidad de las investigaciones. (ISO/IEC 27043:2015)

2.3.2. Cuadro comparativo de los Software Forense

Una vez recogida toda la información en relación al software forense para el desbloqueo, extracción y análisis de información; Cellebryte UFED, GRAYKEY y XRY, se procede a realizar un cuadro comparativo donde se expone los principales puntos fundamentales que caracterizan a cada uno, ver tabla 1.

Tabla 1

Comparación de los Software forense para extracción de información.

Característica	Cellebrite UFED	Graykey	XRY
Logotipo			
Plataformas Soportadas	iOS, Android, Windows Mobile	Principalmente iOS	iOS, Android, Windows Mobile
Tipos de Datos Accesibles	Mensajes, contactos, fotos, registros de llamadas, datos de aplicaciones	Mensajes, fotos, contactos, registros de llamadas, datos de aplicaciones	Mensajes, fotos, contactos, registros de llamadas, datos de aplicaciones

Recuperación de Datos Eliminados	Sí	Sí	Sí
Desbloqueo de Dispositivos	Sí, incluyendo dispositivos bloqueados	Sí, utilizando técnicas avanzadas	Sí, con capacidades para desbloqueo eficaz
Interfaz de Usuario	Intuitiva y fácil de usar	Interfaz especializada en análisis forense	Interfaz amigable, optimizada para investigadores
Documentación y Reporte	Informes claros y estructurados	Informes detallados, adecuados para soporte legal	Informes claros y bien organizados

Aplicaciones en Investigación	Amplio uso en fuerzas del orden y seguridad	Principalmente en investigaciones criminales	Utilizado por investigadores y fuerzas del orden
Actualizaciones y Soporte	Actualizaciones frecuentes y soporte técnico	Actualizaciones regulares y soporte continuo	Soporte constante y actualizaciones de software

2.4. Dispositivos Móviles Android

2.4.1. Introducción al Sistema Operativo Android

El sistema operativo Android es una plataforma basada en Linux que ha sido diseñada para dispositivos móviles, como teléfonos inteligentes y tabletas. Desde que salió en 2008, ha cambiado rápido y se ha consolidado como el sistema operativo más utilizado a nivel mundial, alcanzando una cuota de mercado superior al 70% (Statista, 2023). Su flexibilidad y capacidad de personalización ha sido la clave en su adopción masiva. Android permite a los usuarios adaptar sus dispositivos a sus gustos individuales, lo que ha aumentado un ecosistema vibrante de aplicaciones y servicios.

2.4.2. Historia y Desarrollo de Android

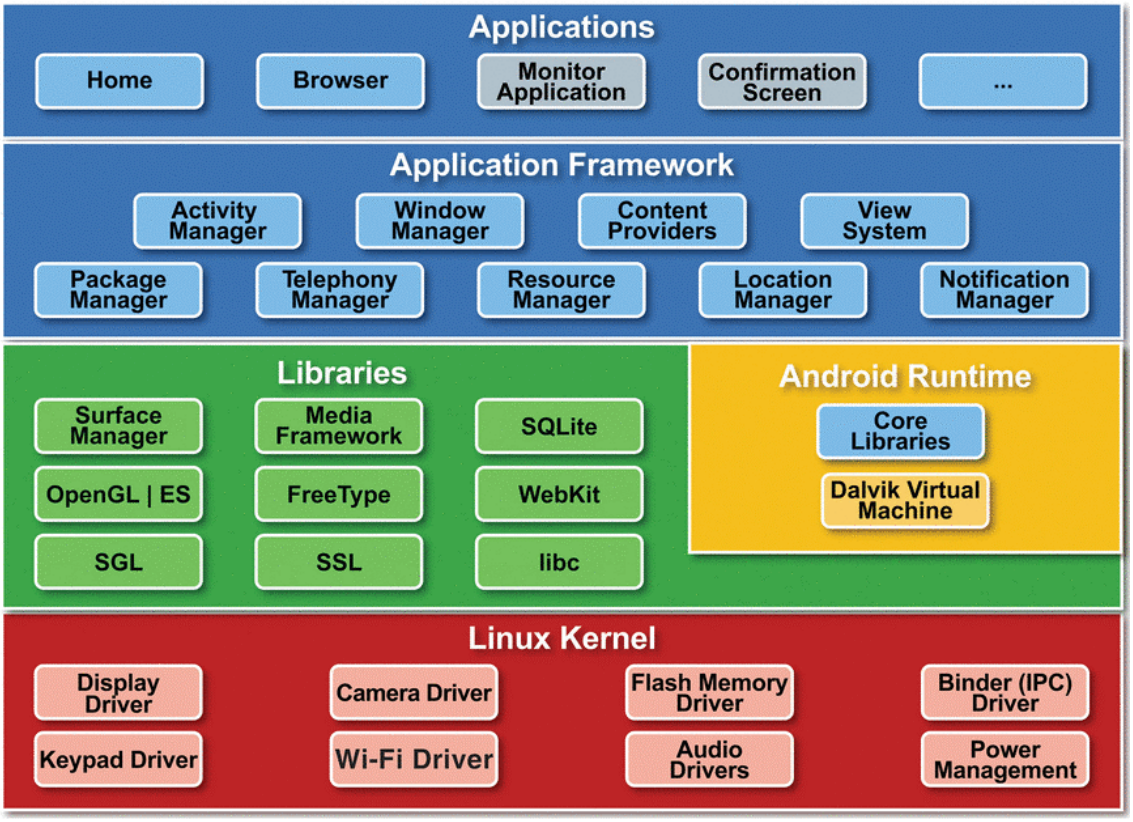
El aumento de Android inició en 2003 por la empresa Android Inc., que fue conseguido por Google en 2005. La primera versión, Android 1.0, entro al mercado en septiembre de 2008, fue el comienzo de una nueva era en la tecnología móvil. Con cada actualización, Android ha mejorado en términos de usabilidad, rendimiento y seguridad. Las versiones recientes, como Android 12 y 13, han agregado cualidades avanzadas, incluyendo una mayor personalización de la interfaz e instrumento de privacidad mejoradas, reflejando una respuesta a las necesidades de los usuarios y las tendencias del mercado (Google, 2023).

2.4.3. Arquitectura de Android

La arquitectura de Android indicada en la figura 2 se compone de varias capas interrelacionadas que trabajan en conjunto para proporcionar al usuario una experiencia fluida y eficiente.

Figura 1

Estructura Android



Nota. Adaptado de (Rodríguez et al., 2016)

Enseguida se explica cada estructura del sistema operativo Android, iniciando desde los aspectos más relevantes:

Núcleo Linux: Esta capa Dispone y ordena la base para la gestión de recursos, la seguridad y la comunicación entre el hardware y el software del dispositivo.

Bibliotecas: Android incluye un conjunto de bibliotecas C/C++ que da funciones esenciales, como la gestión de gráficos, el acceso a bases de datos y la reproducción de multimedia. La biblioteca SQLite es importante, ya que permite a las aplicaciones almacenar y gestionar documentos de manera eficiente.

Marco de Aplicaciones: Esta capa ofrece un conjunto de API que permite a los desarrolladores crear aplicaciones utilizando lenguajes como Java y Kotlin. El marco de aplicaciones facilita la interacción entre diferentes aplicaciones y componentes del sistema.

Aplicaciones: Los usuarios pueden instalar y ejecutar una amplia gama de aplicaciones, disponibles a través de la Google Play Store. Esta diversidad de aplicaciones abarca desde juegos hasta herramientas de productividad, enriqueciendo la experiencia del usuario.

2.4.4. Características Clave del Sistema

Android se destaca por su interfaz personalizable, que permite a los usuarios modificar su experiencia a través de widgets, temas y configuraciones. La capacidad de personalizar la interfaz es uno de los principales atractivos del sistema, ya que permite a los usuarios adaptarlo a sus preferencias y necesidades individuales. Además, Android soporta la multitarea, permitiendo a los usuarios ejecutar múltiples aplicaciones simultáneamente, lo que mejora la productividad y la usabilidad.

La integración de servicios de Google, como Google Assistant, Google Maps y Google Drive, también es una característica destacada que añade valor a la experiencia del usuario. Estas integraciones permiten un acceso más sencillo y fluido a información y servicios relevantes, mejorando la funcionalidad del dispositivo.

2.4.5. Seguridad en Android

La seguridad en Android se aborda a través de múltiples capas, que incluyen el sandboxing de aplicaciones, el cifrado de datos y la autenticación biométrica. El sandboxing garantiza que cada aplicación funcione aislada, lo que hace que el riesgo sea menor, a que un software malicioso acceda a datos sensibles. Sin embargo, la fragmentación del sistema operativo puede dificultar la implementación de actualizaciones de seguridad, representando un desafío constante para las personas y desarrolladores (Smith, 2023). Las actualizaciones periódicas son cruciales para mantener la integridad y la seguridad del sistema, y es importante que los usuarios se mantengan informados sobre las actualizaciones disponibles.

2.4.6. Tendencias Actuales y Futuras

Las tendencias actuales y futuras en el desarrollo de Android incluyen la integración de inteligencia artificial y aprendizaje automático, que están transformando la forma en que los usuarios interactúan con sus dispositivos. Estas tecnologías permiten, por ejemplo, un mejor reconocimiento de voz y una personalización más profunda de las aplicaciones.

La adopción de la tecnología 5G promete mejorar la conectividad y el rendimiento de los dispositivos Android, dando experiencias más ricas y dinámicas. Además, la expansión hacia el Internet de las Cosas (IoT) está creando nuevas oportunidades para la innovación en el ecosistema Android, permitiendo que dispositivos inteligentes se comuniquen y trabajen juntos de manera más efectiva (Johnson, 2023).

2.4.7. Impacto Social y Económico

Android ha transformado la forma en que las personas se comunican, trabajan y acceden a información. Su accesibilidad ha permitido que millones de usuarios en todo el mundo se beneficien de la tecnología móvil, impulsando a la inclusión digital y al crecimiento económico a través de la creación de nuevas aplicaciones y servicios. La democratización de la tecnología móvil ha facilitado el emprender e innovarse en diversas áreas, desde la educación hasta el comercio, contribuyendo así al desarrollo económico global.

CAPÍTULO 3

Diseño metodológico

3.1. Diseño / Tipo de investigación

3.1.1. Enfoque de investigación

El proyecto actual, denominado " Informe Técnico Pericial referente al desbloqueo, extracción, preservación, análisis, y materialización de datos almacenados en dispositivos móviles con Sistema Operativo Android", emplea un enfoque de investigación mixta, combinando métodos cuantitativos y cualitativos para recoger, analizar y unir datos, con el objetivo de aprovechar las fortalezas de cada enfoque.

3.2. Tipos de investigación

3.2.1. Investigación bibliográfica.

Esta investigación tiene diversas fuentes de información nacionales e internacionales, para recoger, seleccionar y analizar datos, lo que servirá como fundamento clave para la documentación y contextualización del desarrollo del informe técnico pericial.

3.2.2. Investigación Descriptiva.

Se toma en consideración la investigación descriptiva debido a que no solo consiste en sacar y procesar los datos por medio de software forense, sino que se aplicará un análisis de datos relevante para casos de investigación de delitos. Con dicha investigación, se conseguirá examinar las características del presente tema, definirlo y formular hipótesis sobre el caso que se esté investigando.

3.3. Metodologías de Desarrollo.

En cuanto al desarrollo del Informe Técnico Pericial, es conveniente que sea claro, objetivo y fundamente de manera técnico-científica los hallazgos claves y relevantes para una investigación iterativo e incremental.

Considerando este antecedente se tomó en cuenta las siguientes metodologías:

3.3.1. SCRUM

Una metodología de desarrollo ágil que se destaca por su enfoque incremental y por trabajar en iteraciones, lo que facilita la gestión eficaz del proyecto, es Scrum. Este marco proporciona una adecuada administración de tareas, así como la asignación de recursos y roles, lo que contribuye a obtener mejores resultados en menor tiempo.

Al implementar Scrum, el cliente está involucrado en cada etapa del desarrollo, recibiendo retroalimentación en cada iteración, lo que permite ajustar los requisitos según las necesidades emergentes. Por estas razones, esta metodología fomenta un trabajo eficiente para realizar entregas parciales del producto final y requiere reuniones frecuentes para retroalimentar y perfeccionar los entregables funcionales.

Roles de Scrum

Product Owner. – una persona actúa como la voz del cliente, funcionando como un representante que comunica y traduce al equipo los requisitos deseados por el cliente. Este rol suele estar asociado al product backlog, que recoge las funcionalidades del sistema.

Scrum master. - responsable de guiar al equipo de desarrollo es quien se encarga de apoyar y asegurar que se sigan adecuadamente todos los aspectos de la metodología.

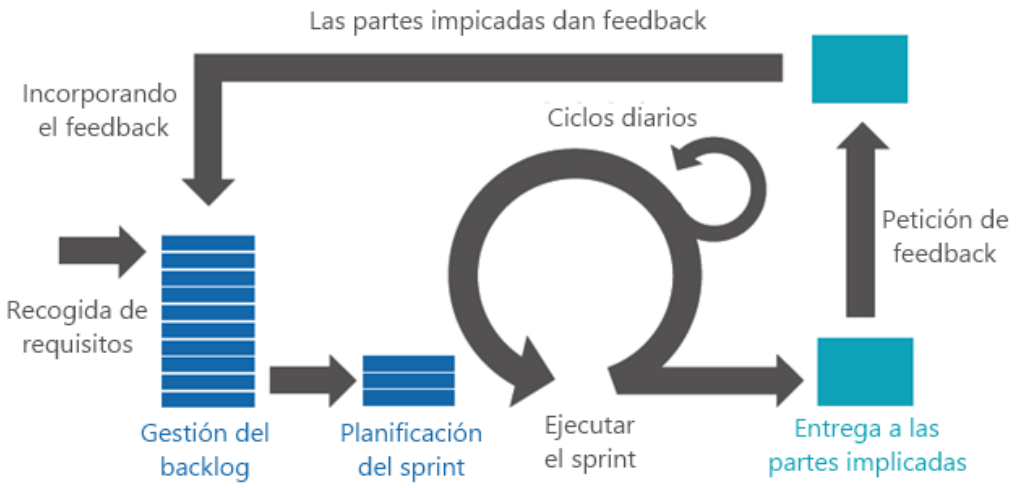
Scrum team. - Se refiere a la cantidad de individuos que integrarán un equipo de desarrollo profesional, incluyendo analistas, diseñadores, programadores y testers. Este número varía según el alcance y el tamaño del proyecto, siendo común que los equipos estén compuestos por entre 2 y 9 personas.

Roles auxiliares

Stakeholders. – Son los clientes que permiten la realización de un proyecto. A continuación, la figura 18 ilustra el funcionamiento de la metodología Scrum.

Figura 2

Funcionamiento Scrum



Nota. Adaptado de (Buele Obando & Rengifo Pozo, 2015)

Artefactos

La metodología Scrum tiene la siguiente documentación como artefactos:

Product Backlog. – Es un documento que incluye una descripción de cada requisito funcional y el feedback obtenido en cada reunión con el interesado o stakeholder.

Sprint Backlog. – Es un documento que detalla las especificaciones sobre cómo se desarrollará cada requisito. Es importante señalar que cada sprint debe tener un tiempo máximo de 16 horas laborables; de lo contrario, se dividirá en dos sprints más cortos.

Burn down chart. - documento que presenta de manera gráfica y detalla la cantidad de tareas pendientes desde el inicio hasta el final de cada sprint.

Después de dar a conocer cada aspecto relacionado con la metodología de desarrollo ágil, es importante señalar que Scrum no impone un límite en la cantidad de miembros que pueden formar un equipo de desarrollo. Lo esencial es seguir cada procedimiento para gestionar el desarrollo de cualquier sistema informático. Por esta razón, el autor de este trabajo de titulación adoptará todos los roles y artefactos de Scrum.

3.4. Diseño de la propuesta

3.4.1. Población y Muestra.

Debido a las características mencionadas en el desarrollo del presente trabajo de titulación, no es necesario definir una población ni una muestra.

3.4.2. Recolección de información.

En este proceso se lleva a cabo la recopilación y análisis de datos, lo que implica reunir toda la información relevante para el diseño de un informe técnico científico pericial de dispositivitos, mediante libros, normas ISO internacionales y artículos científicos e internet.

3.4.3. Procesamiento y análisis de información.

3.4.3.1. Investigación en fuentes de datos e información confiables.

Revisión exhaustiva de la información recopilada, donde se lleva a cabo un filtrado de datos obsoletos o irrelevantes para la investigación.

3.4.3.2. Análisis cualitativo y cuantitativo de la información recabada.

Determinación de modelos apropiados que faciliten la ejecución eficiente del presente trabajo de titulación.

3.4.4. Desarrollo de la propuesta.

• Determinación de las herramientas y software forense a usar para el desarrollo.

• Recopilación, identificación y análisis de los datos e información generada por los diferentes softwares forenses.

• Revisión exhaustiva de la información recolectada, asegurando la veracidad y pertinencia de los datos.

• Elaboración del documento, siguiendo los procesos del tratamiento correcto de evidencia digital y la estructura definida, aplicando los principios éticos y normativas legales, garantizando la confidencialidad de la información y el respeto a los derechos de las partes implicadas.

3.5. Desarrollo de la experticia de extracción de información en dispositivos móviles.

La presente investigación, hace referencia a la experticia informática que, da inicio, con la identificación de evidencia digital donde los intervinientes fiscalía y policía nacional realizan un allanamiento a un inmueble, verificando la existencia de evidencia digital, donde se realiza el levantamiento de diez (11) teléfonos celulares. Siguiendo la respectiva cadena de custodia, estos indicios son ingresados a la Jefatura Zonal de Criminalística de la Policía Nacional, asignándoles la cadena de custodia “2024-0001”, de cual el fiscal encargado de la presente investigación solicita se designe dos peritos del Departamento de Informática Forense a fin de que realicen la extracción de Información.

3.5.1. Objeto pericial:

Realizar la APERTURA, EXHIBICIÓN, EXAEN, EXTRACCIÓN, ANÁLISIS Y MATERIALIZACIÓN de la información de los dispositivos móviles 9ingresados en cadena de custodia Nro. 2024-0001.

3.5.2. Metodología

Para el desarrollo de esta actividad pericial requerida por Fiscalía, se ha considerado la metodología de normalización establecida por la ISO / IEC 27037:2012, la cual determina los procesos de recopilación de evidencias y su almacenamiento in situ, información técnica que ha permitido desarrollar un proceso metodológico de trabajo pericial en base a las siguientes etapas:

- Identificación.
- Adquisición.
- Preservación.
- Análisis
- Presentación (materialización) del contenido digital.

3.6. Proceso utilizado para la extracción y análisis de la información almacenada en los dispositivos de telefonía móvil con Sistema Operativo Android.

3.6.1. Verificación del Estado del Dispositivo

Comprobar el modelo y versión de Android: Es fundamental conocer el modelo exacto del teléfono Android y la versión del sistema operativo. UFED, XRY y GRAYKEY, tienen soporte para una amplia variedad de dispositivos y versiones de Android, pero algunas versiones pueden requerir configuraciones específicas o tener limitaciones.

Revisión del estado físico: Inspeccionar el dispositivo para asegurarse de que esté en buenas condiciones y que no tenga daños visibles que puedan afectar su funcionamiento (pantalla rota, humedad, etc.).

3.6.2. Desbloqueo del Dispositivo

El teléfono móvil debe estar desbloqueado para poder realizar la extracción de datos. En algunos casos, esto puede implicar realizar un desbloqueo de seguridad, lo cual depende del nivel de protección configurado en el dispositivo.

Si el dispositivo está bloqueado con PIN, patrón o contraseña: UFED, XRY y GRAYKEY, pueden intentar obtener acceso utilizando un proceso de bypass si el dispositivo permite este tipo de desbloqueo.

Si se conoce el PIN o la contraseña, estos deben ser proporcionados al software forense durante el proceso de extracción.

Si el dispositivo está bloqueado con biometría (huella dactilar o reconocimiento facial): El software forense, puede no ser capaz de desbloquear el dispositivo directamente a través de biometría, pero la herramienta puede hacer un intento de obtener el hash de la huella dactilar o utilizar técnicas avanzadas de bypass si el dispositivo es compatible.

3.6.3. Desactivar el Bloqueo Automático de Pantalla

Es importante desactivar el bloqueo de pantalla para evitar que el dispositivo se bloquee automáticamente durante el proceso de extracción. Esto puede evitar interrupciones en la conexión entre el software forense y el dispositivo.

3.6.4. Configuración de Opciones de Desarrollo en el Teléfono Android

Para permitir que el software forense acceda al dispositivo Android y pueda realizar la extracción lógica o física, el teléfono debe estar configurado correctamente. Esto incluye la habilitación de ciertas opciones en el sistema operativo Android.

Activar las Opciones de Desarrollador

Para acceder a las opciones de desarrollo y habilitar la depuración USB, sigue estos pasos:

Acceder a las opciones de desarrollador: Entra a "Ajustes" > "Acerca del teléfono".

Busca la opción "Número de compilación" y toca sobre ella varias veces (generalmente 7 veces) hasta que se active el modo de Desarrollador.

Habilitar la depuración USB: Una vez activado el modo de desarrollador, ve a Ajustes > Opciones de desarrollador (puede aparecer como "Sistema" > "Avanzado" en algunos dispositivos).

Habilita la opción "Depuración USB". Esta opción permitirá que UFED se comunique con el dispositivo a través de un cable USB.

Permitir el acceso de USB para depuración:

Conecta el dispositivo Android a un ordenador mediante el cable USB.

Aparecerá una ventana emergente en el dispositivo que pregunta si deseas permitir la depuración USB. Acepta y marca la opción "Siempre permitir desde esta computadora" para asegurar que el dispositivo sea reconocido por UFED.

3.6.5. Desactivar las Restricciones de Seguridad (si es posible)

En algunos casos, el dispositivo Android puede tener configuraciones de seguridad adicionales, como Protección de Activación o Protección contra Restablecimiento de Fábrica. Estas deben desactivarse antes de realizar la extracción, especialmente si el dispositivo se encuentra cifrado o tiene alguna restricción de acceso.

Desactivar bloqueos de seguridad avanzados: Si el dispositivo utiliza algún tipo de gestor de contraseñas o aplicaciones de seguridad adicionales, es recomendable desactivarlas temporalmente para evitar que interfieran con la extracción de datos.

Desactivar el cifrado completo de disco: Algunos dispositivos Android más recientes tienen habilitado un cifrado completo del dispositivo. El software forense puede tener problemas para acceder a estos dispositivos si no se encuentra disponible una clave de cifrado o si no se puede realizar un bypass exitoso.

3.6.6. Conexión del Teléfono a UFED y Selección de Método de Extracción

Conectar el Dispositivo a UFED: Utilizando el cable USB adecuado, conecta el dispositivo Android al software o equipo forense.

Verificar la conexión: Asegúrate de que el dispositivo sea detectado correctamente por el software forense. Si el dispositivo está conectado correctamente, debería reconocerlo automáticamente y mostrar detalles sobre el modelo y la versión de Android.

3.6.7. Seleccionar el Método de Extracción en UFED, XRY y GRAYKEY.

Existe varias opciones para extraer los datos del dispositivo Android, dependiendo de las capacidades del dispositivo y de la protección que tenga configurada.

Extracción Lógica: Esta opción extrae los datos accesibles desde el sistema operativo del dispositivo (sin manipular la memoria interna de manera profunda).

El software podrá recuperar los registros de llamadas, mensajes (SMS/MMS), contactos, archivos multimedia, aplicaciones, y datos de ubicación.

Extracción Física: Si el dispositivo no está demasiado protegido (es decir, no está cifrado de manera completa), se puede realizar una extracción física, que implica una copia bit a bit de la memoria interna del dispositivo, recuperando todos los datos, incluyendo los archivos eliminados.

Extracción de Backups (si corresponde): Si el dispositivo tiene datos almacenados en un backup en la nube, como Google Drive, puede extraer estos datos, siempre que se tenga acceso a la cuenta de Google asociada.

3.6.8. Iniciar la Extracción de Datos

Una vez seleccionado el método de extracción, inicia el proceso y sigue las instrucciones que aparezcan en el software forense para llevar a cabo la extracción.

3.7. Verificación de la Integridad de los Datos y Generación del Informe

3.7.1. Verificación Post-Extracción

Una vez finalizado el proceso de extracción, se mostrará un informe detallado sobre los datos recuperados. Es importante revisar que toda la información relevante haya sido extraída correctamente.

3.7.2. Generación de Informe

El software forense generará un informe forense en formato PDF, CSV, XML, o UFDR Este informe debe contener todos los detalles sobre los datos extraídos, incluyendo:

- Registros de llamadas
- Mensajes (SMS/MMS)
- Archivos multimedia (fotos, videos, audios)
- Información de aplicaciones
- Datos de ubicación

3.7.3. Elementos Recibidos.

ONCE (11) dispositivos móviles de telefonía celular, cuyas identificaciones técnicas se describen en la siguiente tabla de datos:

3.8. Extracción y análisis con el software forense UFED.

Tabla 2

Dispositivo móvil etiquetado como ELEMENTO E1.

ELEMENTO E1	
TELEFONO CELULAR	**TARJETA SIM (CHIPS)**

MARCA:	XIAOMI	**COMPAÑÍA 1:**	CLARO
		SERIE:	895930100082915632
COLOR:	VERDE	**COMPAÑÍA 2:**	NO POSEE
MODELO:	23117RA68G	**SERIE:**	NO POSEE
IMEI:	863357065380362	**TARJETA DE MEMORIA**	
	863357065380370		
ESTUCHE:	NO POSEE	**MARCA:**	KINGSTON
MODO AVIÓN:	ACTIVADO	**CAPACIDAD:**	16 GB
BATERIA:	INTERNA	**ETIQUETADO**	NINGUNO

OBSERVACIONES: El teléfono celular se encuentra en regular estado de conservación y funcionamiento, el pin de desbloqueo fue proporcionado por el propietario

Componente del dispositivo

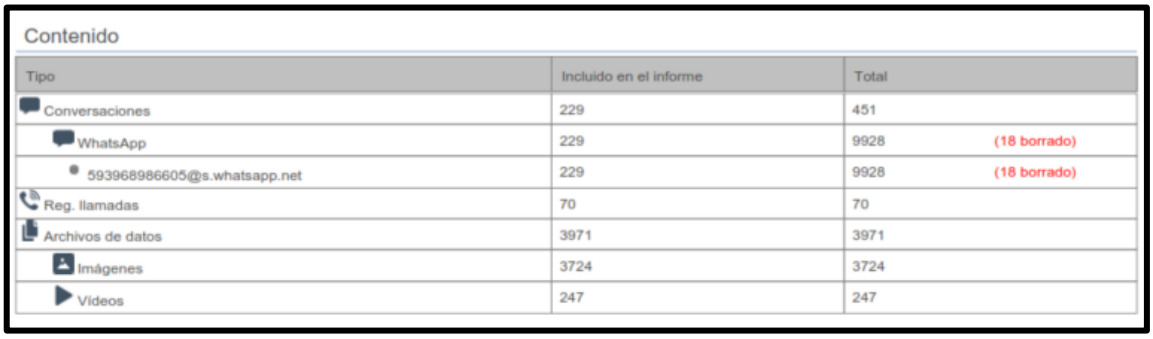
Numeraciones físicas

3.8.1. Análisis y preservación de la información digital del ELEMENTO E1.

Mediante el instrumental técnico forense UFED versión “7.68.0.809” se ha desarrollado la adquisición lógica avanzada de los datos almacenados en el dispositivo de telefonía celular de interés pericial, considerando, los criterios de búsqueda relacionados con el TRAFICO ILÍCITO DE SUSTANCIAS CATALOGADAS SUJETAS A FISCALIZACIÓN, se generó un reporte en formato con extensión .pdf y html denominado “E1”, comprendido por mil cuatrocientas sesenta y tres (1463) páginas, contenido digital asociada a la presente investigación, datos que está relacionado con: mensajería instantánea tipo chat bajo el aplicativo WhatsApp, cuentas de usuario y registro de llamadas.

Figura 3

Contenido generado ELEMENTO E1.



Contenido

Tipo	Incluido en el informe	Total	
Conversaciones	229	451	
WhatsApp	229	9928	(18 borrado)
593968986605@s.whatsapp.net	229	9928	(18 borrado)
Reg. llamadas	70	70	
Archivos de datos	3971	3971	
Imágenes	3724	3724	
Vídeos	247	247	

Tabla 3

Dispositivo móvil etiquetado como ELEMENTO E2.

ELEMENTO E2

TELEFONO CELULAR		**TARJETA SIM (CHIPS)**	
MARCA:	TECNO	**COMPAÑÍA 1:**	CLARO
		SERIE:	895930100099792729

COLOR:	BLANCO	**COMPAÑÍA 2:**	TUENTI
MODELO:	TECNOKI7	**SERIE:**	8959300550511009938
IMEI LOGICO:	354531262931161	**TARJETA DE MEMORIA**	
	354531262931179		
ESTUCHE:	SI POSEE	**MARCA:**	NO POSEE
MODO AVIÓN:	ACTIVADO	**CAPACIDAD:**	NO POSEE
BATERIA:	INTERNA	**ETIQUETADO**	NINGUNO

OBSERVACIONES: El teléfono celular se encuentra en regular estado de conservación y funcionamiento.

Componente del dispositivo

Numeraciones físicas

3.8.2. Análisis y preservación de la información digital del ELEMENTO E2.

Mediante el instrumental técnico forense UFED versión "7.68.0.809" se ha desarrollado la adquisición lógica avanzada de los datos almacenados en el dispositivo de telefonía celular de interés pericial detallado en el acápite 3.2, considerando, los criterios de búsqueda relacionados con el presunto delito de ASESINATO, se generó un reporte en formato con extensión .pdf y html

denominado “E2”, comprendido de cuarenta y siete (47) páginas, contenido digital asociada a la presente investigación, datos que está relacionado con contenido multimedia relacionado con imágenes y mensajería instantánea tipo chat bajo el aplicativo WhatsApp.

Figura 4

Contenido generado ELEMENTO E2.

Contenido

Tipo	Incluido en el informe	Total	
Conversaciones	2	249	(5 borrado)
WhatsApp	2	210	(5 borrado)
593987890115@s.whatsapp.net	2	210	(5 borrado)
Dispositivos	6	6	
Usuarios del dispositivo	1	1	
Archivos de datos	3	50196	
Imágenes	3	50196	

Tabla 4

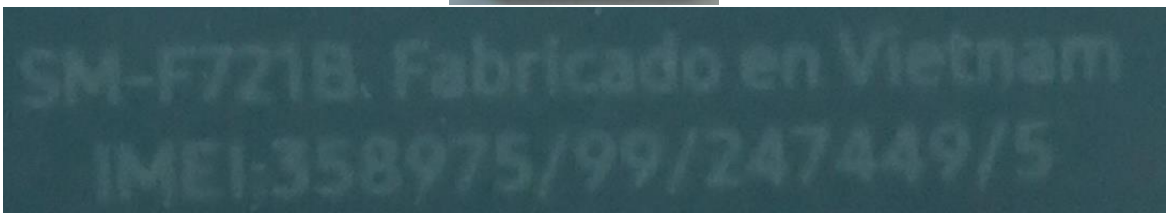
Dispositivo móvil etiquetado como ELEMENTO E3.

ELEMENTO E3

TELEFONO CELULAR		**TARJETA SIM (CHIPS)**	
MARCA:	SAMSUNG	**COMPAÑÍA 1:**	CLARO
		SERIE:	895930100097455939
COLOR:	NEGRO	**COMPAÑÍA 2:**	NO POSEE
MODELO:	SM-F721B	**SERIE:**	NO POSEE
IMEI LOGICO:	358975992474495	**TARJETA DE MEMORIA**	
	359697852474493		
ESTUCHE:	NO POSEE	**MARCA:**	NO POSEE
MODO AVIÓN:	ACTIVADO	**CAPACIDAD:**	NO POSEE

BATERIA: INTERNA **ETIQUETADO** NINGUNO

OBSERVACIONES: El teléfono celular se encuentra en regular estado de conservación y funcionamiento, posee trizada la tapa posterior



Componente del dispositivo Numeraciones físicas

3.8.3. Análisis y preservación de la información digital del ELEMENTO E3.

Mediante el instrumental técnico forense UFED versión “7.68.0.809” se ha desarrollado la adquisición lógica avanzada de los datos almacenados en el dispositivo de telefonía celular de interés pericial detallado en el acápite 3.3, considerando, los criterios de búsqueda relacionados

con el presunto delito de ASESINATO, se generó un reporte en formato con extensión .pdf y html denominado “E3”, comprendido de treinta y cuatro (34) páginas, contenido digital asociada a la presente investigación, datos que está relacionado con mensajería instantánea tipo chat bajo el aplicativo WhatsApp y cuentas de usuario.

Figura 5

Contenido generado ELEMENTO E3.

Contenido

Tipo	Incluido en el informe	Total
Conversaciones	3	399 (8 borrado)
WhatsApp	3	319 (4 borrado)
593991045440@s.whatsapp.net	3	319 (4 borrado)
Cuentas de usuario	26	26
Usuarios del dispositivo	1	1

Tabla 5

Dispositivo móvil etiquetado como ELEMENTO E4.

ELEMENTO E4

TELÉFONO CELULAR – ELEMENTO 1		**TARJETA SIM 1 (CHIP)**	
MARCA:	SAMSUNG	**COMPAÑÍA:**	MOVISTAR
COLOR:	NEGRO	**SERIE:**	8959300420558547408
MODELO:	SMA037M/DS	**COLOR:**	BLANCO
IMEI FISICO1:	352550/42/999019/3	**TARJETA DE MEMORIA**	
IMEI FISICO2:	356627/90/999019/4		
IMEI LOGICO 1:	352550429990193/01	**MARCA:**	NO APLICA
IMEI LOGICO 2:	356627909990194/01		
BATERIA:	INTERNA	**CAPACIDAD:**	NO APLICA
MODO AVIÓN:	ACTIVADO	**ETIQUETADO:**	NO APLICA

OBSERVACIONES: NINGUNA

Componente del dispositivo

Numeraciones físicas

3.8.4. Análisis y preservación de la información digital del ELEMENTO E4.

Mediante el instrumental técnico forense UFED versión "7.68.0.809" se ha desarrollado la adquisición lógica avanzada de los datos almacenados en el dispositivo de telefonía celular de interés pericial detallado en el acápite 3.3, considerando, los criterios de búsqueda relacionados con el presunto delito de TRAFICO ILÍCITO DE SUSTANCIAS CATALOGADAS SUJETAS A FISCALIZACION, se generó un reporte en formato con extensión .pdf y html denominado "E5", comprendido de dieciséis (16) páginas, contenido digital asociada a la presente investigación, datos que está relacionado con mensajería instantánea tipo chat bajo el aplicativo WhatsApp y cuentas de usuario.

Figura 6

Contenido generado ELEMENTO E4.

Contenido

Tipo	Incluido en el informe	Total	
Conversaciones	2	795	(17 borrado)
WhatsApp Business	2	795	(17 borrado)
593999986068@s.whatsapp.net	2	795	(17 borrado)
Cuentas de usuario	1	1	

Tabla 6

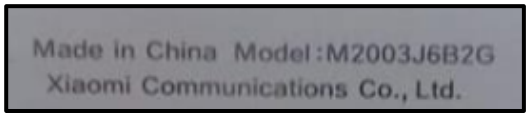
Dispositivo móvil etiquetado como ELEMENTO E5.

ELEMENTO E5

TELEFONO CELULAR		**TARJETA SIM (CHIPS)**	
MARCA:	XIAOMI	**COMPAÑÍA 1:**	NO POSEE
		SERIE:	NO POSEE
COLOR:	BLANCO	**COMPAÑÍA 2:**	NO POSEE
MODELO:	M2003J6B2G	**SERIE:**	NO POSEE
IMEI LOGICO:	862532056140196	**TARJETA DE MEMORIA**	
	862532056140204		
ESTUCHE:	NO POSEE	**MARCA:**	NO POSEE
MODO AVIÓN:	ACTIVADO	**CAPACIDAD:**	NO POSEE
BATERIA:	INTERNA	**ETIQUETADO**	NINGUNO

OBSERVACIONES: El teléfono celular se encuentra en regular estado de conservación y funcionamiento.

Componente del dispositivo



Numeraciones físicas

3.8.5. Análisis y preservación de la información digital del ELEMENTO E5.

Mediante el instrumental técnico forense UFED versión "7.68.0.809" se ha desarrollado la adquisición lógica avanzada de los datos almacenados en el dispositivo de telefonía celular de interés pericial, considerando, los criterios de búsqueda del delito de EXTORSIÓN, se generó un reporte en formato con extensión **.pdf** y **html** denominado **"E5"**, comprendido por cuarenta y cinco (45) páginas, contenido digital asociada a la presente investigación, datos que está relacionado con: mensajería instantánea tipo chat bajo el aplicativo WhatsApp, cuentas de usuario y registro de llamadas.

Figura 7

Contenido generado ELEMENTO E5.

Contenido

Tipo	Incluido en el informe	Total	
Conversaciones	2	526	(3 borrado)
WhatsApp	2	400	(2 borrado)
593992741483@s.whatsapp.net	2	400	(2 borrado)
Cuentas de usuario	18	18	
Dispositivos	1	1	
Reg. llamadas	36	312	

Tabla 7

Dispositivo móvil etiquetado como ELEMENTO E6.

ELEMENTO E6

TELEFONO CELULAR		**TARJETA SIM (CHIPS)**	
MARCA:	XIAOMI	**COMPAÑÍA 1:**	NO POSEE
		SERIE:	NO POSEE
COLOR:	CELESTE	**COMPAÑÍA 2:**	NO POSEE
MODELO:	22101317C	**SERIE:**	NO POSEE
IMEI LOGICO:	867271067186725	**TARJETA DE MEMORIA**	
	867271067186733		
ESTUCHE:	NO POSEE	**MARCA:**	NO POSEE
MODO AVIÓN:	ACTIVADO	**CAPACIDAD:**	NO POSEE
BATERIA:	INTERNA	**ETIQUETADO**	NINGUNO

OBSERVACIONES: El teléfono celular se encuentra en regular estado de conservación y funcionamiento.

Componente del dispositivo

Numeraciones físicas

3.8.6. Análisis y preservación de la información digital del ELEMENTO E6.

Mediante el instrumental técnico forense UFED versión "7.68.0.809" se ha desarrollado la adquisición lógica avanzada de los datos almacenados en el dispositivo de telefonía celular de interés pericial, considerando, los criterios de búsqueda del delito de EXTORSIÓN, se generó un reporte en formato con extensión **.pdf** y **html** denominado **"E6"**, comprendido de ocho (08) páginas, contenido digital asociada a la presente investigación, datos que está relacionado con: mensajería instantánea tipo chat bajo el aplicativo WhatsApp, cuentas de usuario y registro de llamadas.

Figura 8

Contenido generado ELEMENTO E6.

Contenido

Tipo	Incluido en el informe	Total
Cuentas de usuario	1	1
Usuarios del dispositivo	1	1
Archivos de datos	41	4110
Imágenes	31	4100
Videos	10	10

Tabla 8

Dispositivo móvil etiquetado como ELEMENTO E7.

ELEMENTO E7

TELEFONO CELULAR		**TARJETA SIM (CHIPS)**	
MARCA:	SAMSUNG	**COMPAÑÍA 1:**	MOVISTAR
		SERIE:	8959300520555569329
COLOR:	CELESTE	**COMPAÑÍA 2:**	NO POSEE
MODELO:	SM-A715F/DS	**SERIE:**	NO POSEE
IMEI LOGICO:	352635112087413	**TARJETA DE MEMORIA**	
	352636112087411		
ESTUCHE:	NO POSEE	**MARCA:**	NO POSEE
MODO AVIÓN:	ACTIVADO	**CAPACIDAD:**	NO POSEE
BATERIA:	INTERNA	**ETIQUETADO**	NINGUNO

OBSERVACIONES: El teléfono celular se encuentra en regular estado de conservación y funcionamiento.

Componente del dispositivo

Numeraciones físicas

3.8.7. Análisis y preservación de la información digital del ELEMENTO E7.

Mediante el instrumental técnico forense UFED versión "7.68.0.809" se ha desarrollado la adquisición lógica avanzada de los datos almacenados en el dispositivo de telefonía celular de interés pericial, considerando, los criterios de búsqueda del delito de EXTORSIÓN, se generó un reporte en formato con extensión **.pdf** y **html** denominado **"E7"**, comprendido por cuarenta y nueve (49) páginas, contenido digital asociada a la presente investigación, datos que está relacionado con: mensajería instantánea tipo chat bajo el aplicativo WhatsApp, cuentas de usuario y registro de llamadas.

Figura 9

Contenido generado ELEMENTO E7.

Contenido

Tipo	Incluido en el informe	Total	
Conversaciones	4	882	(4 borrado)
WhatsApp Business	4	874	(4 borrado)
593991456292@s.whatsapp.net	4	874	(4 borrado)
Cuentas de usuario	27	27	
Dispositivos	2	2	
Archivos de datos	62	17709	(1 borrado)
Imágenes	62	17709	(1 borrado)

3.9. Extracción y análisis con el software forense XRY

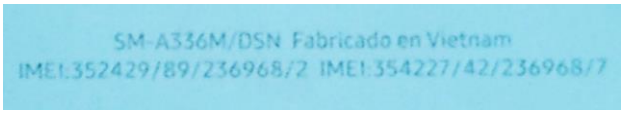
Tabla 9

Dispositivo móvil etiquetado como ELEMENTO E8.

ELEMENTO E8

TELEFONO CELULAR		**TARJETA SIM (CHIP)**	
MARCA:	SAMSUNG	**COMPAÑÍA:**	CLARO
COLOR:	CELESTE	**SERIE:**	895930100104889801
MODELO:	SM-A336M/DSN	**COLOR:**	BLANCO - ROJO
IMEI FISICO 1:	352429892369682	**TARJETA DE MEMORIA**	
IMEI FISICO 2:	354227422369687		
IMEI LÓGICO1:	352429892369682	**MARCA:**	NO POSEE
IMEI LÓGICO2:	354227422369687		
BATERIA:	INTERNA	**CAPACIDAD:**	NO APLICA
MODO AVIÓN:	ACTIVADO	**ETIQUETADO:**	NO APLICA
OBSERVACIONES:	SIN NOVEDAD.		

Componente del dispositivo



Numeraciones Físicas

3.9.1. Análisis y preservación de la información digital del ELEMENTO E8.

Se realiza la extracción “lógica” con la utilización del software forense XRY versión “10.7.1”, como resultado de los filtros de búsqueda relacionada al delito de TRÁFICO ILÍCITO DE SUSTANCIAS CATALOGADAS SUJETAS A FISCALIZACIÓN, se generó un reporte en formato con extensión .pdf denominado “E8”, conteniendo cuatro (04) páginas, con sus respectivos anexos multimedia.

Figura 10

Contenido generado ELEMENTO E8.

Tabla 10

Dispositivo móvil etiquetado como ELEMENTO E9.

ELEMENTO E9

TELÉFONO CELULAR		TARJETA SIM (CHIP)	
MARCA:	INFINIX	**COMPAÑÍA:**	NO POSEE
COLOR:	AZUL	**SERIE:**	NO APLICA
MODELO:	X678B	**COLOR:**	NO APLICA
IMEI FISICO 1:	353299481313485	**TARJETA DE MEMORIA**	
IMEI FISICO 2:	353299481313493		
IMEI LÓGICO:	NO APLICA	**MARCA:**	NO POSEE
BATERIA:	INTERNA	**CAPACIDAD:**	NO APLICA
MODO AVIÓN:	ACTIVADO	**ETIQUETADO:**	NO APLICA
OBSERVACIONES:	SIN NOVEDAD.		

Componente del dispositivo

Numeraciones Físicas

3.9.2. Análisis y preservación de la información digital del ELEMENTO E9.

Se realiza la extracción “lógica” con la utilización del software forense XRY versión “10.7.1”, como resultado de los filtros de búsqueda relacionada al delito de TRÁFICO ILÍCITO DE SUSTANCIAS CATALOGADAS SUJETAS A FISCALIZACIÓN, se generó dos reportes en formato con extensión .pdf denominado “E9”, conteniendo veintiocho (28) páginas y “E9_Informemessenger”, conteniendo trecientos cuarenta y cinco (345) páginas.

Figura 11

Contenido generado ELEMENTO E9.

Contenido

3.10. Desbloqueo mediante el software forense GRAYKEY

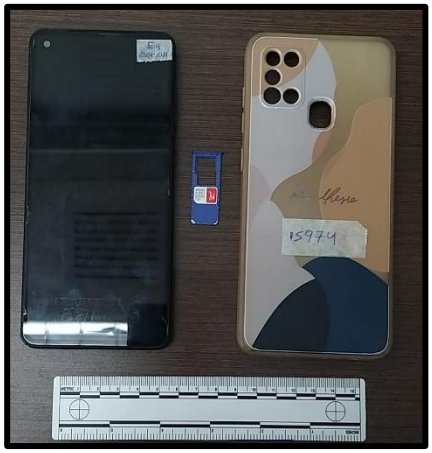
Tabla 11

Dispositivo móvil etiquetado como ELEMENTO E10.

ELEMENTO E10

TELÉFONO CELULAR		**TARJETA SIM (CHIP)**	
MARCA:	SAMSUNG	**COMPAÑÍA:**	CLARO
		SERIE:	895930100105505757
MODELO:	SM-A217M	**COMPAÑÍA:**	NO APLICA
ESTUCHE	SI	**SERIE:**	NO APLICA
IMEI	354712/52/019148/9	**TARJETA DE MEMORIA**	
IMEI	NO APLICA	**MARCA:**	NO APLICA
CAPACIDAD	NO APLICA	**CAPACIDAD:**	NO APLICA
MODO AVIÓN	QUEDA ACTIVADO	**ETIQUETADO CELULAR**	NO APLICA

OBSERVACIONES: DISPOSITIVO BLOQUEADO.

Componente del dispositivo	Observación
	

El dispositivo móvil antes descrito se encuentra bloqueado, con la finalidad de realizar la extracción de información se utilizó el software forense GRAYKEY, versión 1.24.2.29241656.

Tabla 12

Dispositivo móvil etiquetado como ELEMENTO E10.

ELEMENTO 10

Código de acceso encontrado	159874

3.10.1. Análisis y preservación de la información digital del ELEMENTO E10.

Se realiza la extracción “lógica” con la utilización de diferentes técnicas forenses y Se realiza la extracción “lógica” con la utilización de diferentes técnicas forenses y mediante la utilización del software forense UFED, versión: 7.68, del dispositivo móvil, descrito en el acápite 2.4, como resultado de los filtros de relacionada con el delito DELINCUENCIA ORGANIZADA, se generó un reporte bajo la extensión .pdf denominado “E10”, conteniendo nueve (09) paginas, con sus respectivos anexos multimedia.

Figura 12

Contenido generado ELEMENTO E10.

Contenido

Tipo	Incluido en el informe	Total	
Contactos	3	7953	(27 borrado)
Cuentas de usuario	36	36	
Reg. llamadas	20	726	(5 borrado)
Usuarios del dispositivo	1	1	
Archivos de datos	5	56180	
Imágenes	5	56180	

Tabla 13

Dispositivo móvil etiquetado como ELEMENTO E11.

ELEMENTO 11

TELÉFONO CELULAR		**TARJETA SIM (CHIP)**	
MARCA:	XIOMI REDMI	**COMPAÑÍA:**	MOVISTAR
		SERIE:	8959300520577221230
MODELO:	M2004J19C	**COMPAÑÍA:**	MOVISTAR
ESTUCHE	NO	**SERIE:**	8959300320539318954
IMEI FÍSICO	NO VISIBLE	**TARJETA DE MEMORIA**	
IMEI LÓGICO 1	863927054072525	**MARCA:**	NO APLICA
IMEI LÓGICO 2	863927054072533		
CAPACIDAD	NO APLICA	**CAPACIDAD:**	NO APLICA
MODO AVIÓN	QUEDA ACTIVADO	**ETIQUETADO CELULAR**	NO APLICA

OBSERVACIONES: NINGUNO

Componente del dispositivo	Observación
	

El dispositivo móvil antes descrito se encuentra bloqueado, con la finalidad de realizar la extracción de información se utilizó el software forense GRAYKEY, versión 1.24.2.29241656.

Tabla 14

Dispositivo móvil etiquetado como ELEMENTO E11.

ELEMENTO 11

Código de acceso encontrado	14789

3.10.2. Análisis y preservación de la información digital del ELEMENTO E11.

Se realiza la extracción “lógica” con la utilización de diferentes técnicas forenses y Se realiza la extracción “lógica” con la utilización de diferentes técnicas forenses y mediante la utilización del software forense UFED, versión: 7.68, del dispositivo móvil, descrito en el acápite 2.4, como resultado de los filtros de relacionada con el delito DELINCUENCIA ORGANIZADA, se generó un reporte bajo la extensión .pdf denominado “E11”, conteniendo treinta y dos (32) paginas, con sus respectivos anexos multimedia.

Figura 13

Contenido generado ELEMENTO E11

Contenido

Tipo	Incluido en el informe	Total
Contactos	7	6117 (7 borrado)
Conversaciones	4 (1 borrado)	1045 (29 borrado)
WhatsApp	4 (1 borrado)	242 (25 borrado)
593979421305@s.whatsapp.net	4 (1 borrado)	242 (25 borrado)
Cuentas de usuario	25 (1 borrado)	25 (1 borrado)
Reg. llamadas	35	4438 (38 borrado)
Archivos de datos	14	45795
Imágenes	8	41114
Vídeos	6	4681

CAPÍTULO 4

4.1. Presentación y discusión de resultados

4.1.1. Resultados

Tabla 15

Resultado de recolección de datos

No.	Delito	Marca del dispositivo	Modelo	Software Forense utilizado	Tipo de Extracción
1	TRAFICO ILÍCITO DE SUSTANCIAS CATALOGADAS SUJETAS A FISCALIZACIÓN.	XIAOMI	23117RA68G	UFED	Full File System
2	ASESINATO	TECNO	TECNOKI7	UFED	Full File System
3	ASESINATO	SAMSUNG	SM-F721B	UFED	Full File System
4	TRAFICO ILÍCITO DE SUSTANCIAS CATALOGADAS SUJETAS A FISCALIZACION	SAMSUNG	SMA037M/DS	UFED	Full File System
5	EXTORSIÓN	XIAOMI	M2003J6B2G	UFED	Full File System
6	EXTORSIÓN	XIAOMI	22101317C	UFED	Full File System
7	EXTORSIÓN	SAMSUNG	SM-A715F/DS	UFED	Full File System
8	TRÁFICO ILÍCITO DE SUSTANCIAS CATALOGADAS SUJETAS A FISCALIZACIÓN	SAMSUNG	SM-A336M/DSN	XRY	Full File System
9	TRÁFICO ILÍCITO DE SUSTANCIAS CATALOGADAS SUJETAS A FISCALIZACIÓN	INFINIX	X678B	GRAYKEY/ UFED	Full File System
10	DELINCUENCIA ORGANIZADA	SAMSUNG	SM-A217M	GRAYKEY/ UFED	Full File System
11	DELINCUENCIA ORGANIZADA	XIOMI REDMI	M2004J19C	GRAYKEY/ UFED	Full File System

4.1.2. Análisis general de resultados

Una vez realizado el proceso forense, se recuperó una variedad de datos de los dispositivos móviles, los cuales fueron fundamentales para la reconstrucción de las actividades y patrones de comportamiento de los usuarios durante el periodo de interés. A continuación, se detallan los principales hallazgos organizados por categoría y dispositivo:

4.1.3. Registros de Llamadas

Se logró recuperar registros detallados de llamadas realizadas, recibidas y perdidas, los cuales incluían información crucial como:

Fecha y hora exacta de cada llamada permitiendo establecer cronologías.

Duración de las llamadas, lo que permitió identificar llamadas más significativas o recurrentes.

Números telefónicos implicados en las llamadas, permitiendo la correlación de contactos y la identificación de relaciones clave dentro del contexto de la investigación.

La recuperación de registros de llamadas permitió reconstruir la actividad telefónica de los usuarios, proporcionando una visión clara de las interacciones entre personas, y en algunos casos, la identificación de patrones de comunicación frecuente con ciertos números. En particular, se observaron ciertos picos de actividad en horarios específicos, lo que puede ser indicativo de eventos importantes o contactos frecuentes en momentos determinados.

En la mayoría de los dispositivos se detectaron tanto llamadas nacionales como internacionales, así como también se identificaron llamadas de larga duración, lo que podría indicar interacciones importantes.

4.1.4. Mensajes (SMS/MMS)

La recuperación de mensajes SMS y MMS fue un hallazgo clave para la investigación, debido a que se extrajeron tanto mensajes enviados como recibidos, proporcionando información de:

Contenidos de los mensajes, tanto de texto como de los archivos multimedia adjuntos (fotos, videos, audios).

Identidad de los contactos, es decir, los números telefónicos o nombres asociados a cada mensaje, que habían sido eliminados en algunos dispositivos permitiendo así una correlación directa con los registros de llamadas.

Fechas y horas de envío y recepción de los mensajes, lo que resultó útil para reconstruir conversaciones clave durante el periodo de investigación.

La recuperación de mensajes eliminados solo fue posible en algunos dispositivos, permitiendo acceder a comunicaciones previamente borradas, pero aún presentes en la memoria del dispositivo en las cuales los involucrados intentan ocultar o eliminar pruebas de interacciones pasadas e información.

En varios dispositivos se recuperaron conversaciones a través de aplicaciones de mensajería instantánea como WhatsApp, Facebook Messenger, y Telegram, que fueron fundamentales para la reconstrucción de interacciones entre usuarios.

Archivos Multimedia

La **recuperación de archivos multimedia** permitió acceder a una variedad de archivos que proporcionaron información valiosa de la actividad de los usuarios a través de los dispositivos. Entre los tipos de archivos recuperados se incluyen:

Fotos: Se recuperaron imágenes de forma parcial y total que fueron capturadas por la cámara del dispositivo o descargadas de aplicaciones de mensajería o redes sociales. Algunas de

estas fotos fueron de particular relevancia, ya que mostraban lugares, personas o eventos relacionados con la investigación.

Videos: Se extrajeron videos, que se consideraron relevantes por contener grabaciones de eventos, reuniones, e interacciones personales que fueron documentadas en video y forman parte clave para esclarecer las investigaciones.

Audios: Se recuperaron archivos de audio que, en algunos casos, contenían conversaciones o sonidos que podían proporcionar información adicional sobre los contextos de las interacciones.

El **análisis de los archivos multimedia** mediate los metadatos se identificaron momentos y ubicaciones clave, en fotos capturadas se identificaron coordenadas geográficas de referencia, los videos grabados permitieron determinar lugares específicos además que ayudaron a confirmar o refutar coartadas, y en algunos casos, a identificar interacciones que de otra manera no habrían sido documentadas en otro tipo de información.

En algunos dispositivos se recuperaron **fotos y videos eliminados**, los cuales proporcionaron evidencia visual crítica relacionada con la investigación y grabaciones de conversaciones que, resultaron ser relevantes para corroborar testimonios o establecer una cronología de eventos.

4.1.5. Aplicaciones Instaladas

Se identificaron aplicaciones presentes en los dispositivos, las cuales proporcionaron información relevante sobre las actividades y preferencias de los usuarios. Entre las cuales se incluyen:

Aplicaciones de mensajería instantánea: como WhatsApp, Telegram, Facebook Messenger, y Signal, las conversaciones de tipo chat incluían texto y archivos multimedia, mensajes que fueron fundamentales para la reconstrucción de las comunicaciones mantenida por los usuarios.

Redes sociales: Se identificaron aplicaciones de redes sociales como Instagram, Facebook, Twitter y Snapchat, que contenían mensajes directos, fotos, videos y publicaciones que podían estar directamente relacionadas con el caso.

Aplicaciones de geolocalización: se logró recuperar ubicaciones de las aplicaciones Google Maps y Uber, que proporcionaron información valiosa sobre los traslados que tuvo el propietario o usuario del dispositivo durante el periodo de interés.

El análisis de las aplicaciones instaladas permitió detectar patrones de uso, como la frecuencia con la que se accedía a ciertas aplicaciones, las horas en las que el usuario interactuaba más intensamente con las plataformas y usuarios de estas. En algunos casos, se encontraron aplicaciones ocultas en carpetas de difícil acceso o que se encontraban protegidas por contraseñas, mostrando así intentos de ocultar información.

Adicionalmente se encontraron aplicaciones relacionadas con la gestión de contraseñas, bancos y rastreo de ubicación, lo que sugiere que los usuarios estaban inmersos en actividades que requerían seguridades o supervisión en tiempo real. La presencia de aplicaciones de rastreo y software espía en algunos dispositivos podría ser un indicativo de actividades no autorizadas.

4.2. Análisis especifico de la información extraída y seleccionada en cada dispositivo.

4.2.1. ELEMENTO E1

Luego de realizar la extracción de información mediante la utilización de técnicas, herramientas y software forense se obtuvo la siguiente información:

Tabla 16

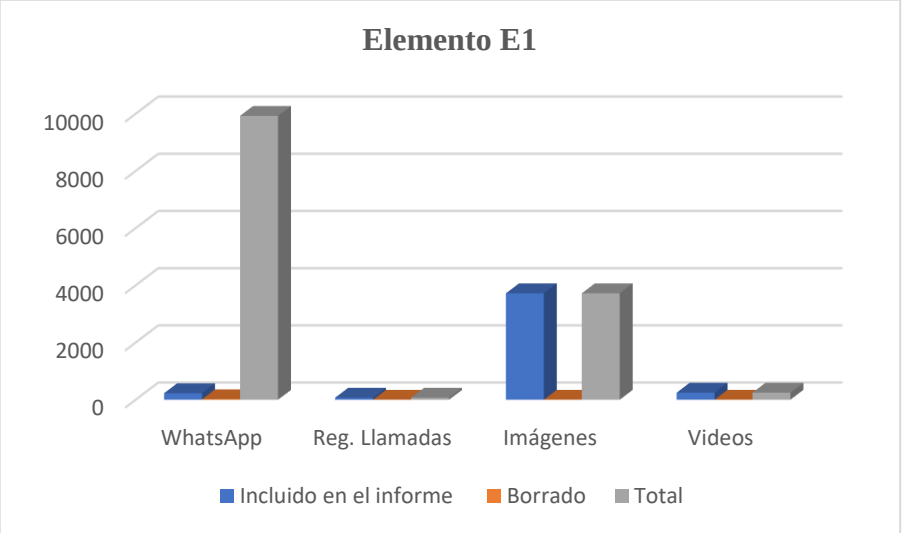
Análisis del ELEMENTO E1

Elemento E1			
Tipo	**Incluido en el informe**	**Borrado**	**Total**
WhatsApp	229	18	9928
Reg. Llamadas	70	0	70
Imágenes	3724	0	3724
Videos	247	0	247

Nota. La Tabla 16 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E1, del cual se obtuvieron un total de 9928 mensajes de la aplicación de mensajería WhatsApp, 70 registros de llamadas, 3724 imágenes y 247 videos, de lo cual se seleccionaron 229 mensajes de la aplicación de mensajería WhatsApp, 70 registros de llamadas, 3724 imágenes y 247 videos, de igual manera se constataron 18 registros borrados correspondientes a mensajes de la aplicación de mensajería WhatsApp.

Figura 14

Análisis del ELEMENTO E1



Nota. La Figura 14 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E1 de manera gráfica.

4.2.2. ELEMENTO E2

Luego de realizar la extracción de información mediante la utilización de técnicas, herramientas y software forense se obtiene la siguiente información:

Tabla 17

Análisis del ELEMENTO E2

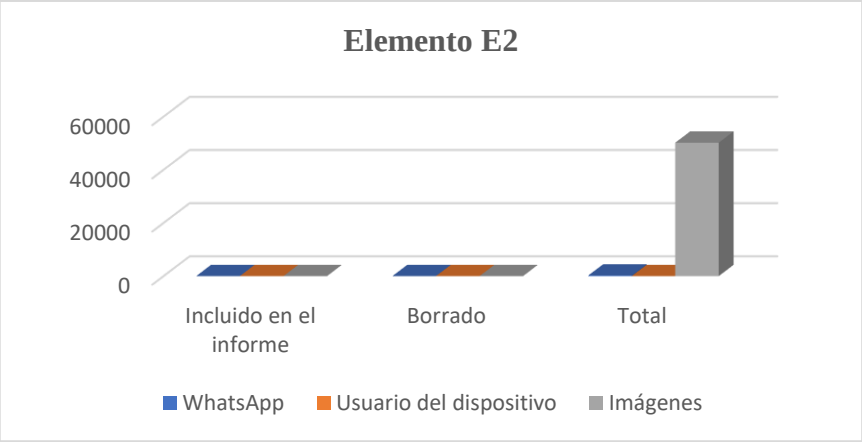
Elemento E2			
Tipo	**Incluido en el informe**	**Borrado**	**Total**
WhatsApp	2	5	210
Usuario del dispositivo	1	0	1
Imágenes	3	0	50196

La Tabla 17 muestra el contenido extraído del dispositivo que fue etiquetado como ELEMENTO E2, del cual se obtuvieron un total de 210 mensajes de la aplicación de mensajería

WhatsApp, 1 usuario del dispositivo, 50196 imágenes, de lo cual se seleccionó 210 mensajes de la aplicación de mensajería WhatsApp, 70 reg. Llamadas, 3 imágenes, de igual manera se verifica 5 registros borrados correspondientes a mensajes de la aplicación de mensajería WhatsApp.

Figura 15

Análisis del ELEMENTO E2



Nota. La Figura 15 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E2 de manera gráfica.

4.2.3. ELEMENTO E3

Luego de realizar la extracción de información mediante la utilización de técnicas, herramientas y software forense se obtiene la siguiente información:

Tabla 18

Análisis del ELEMENTO E3

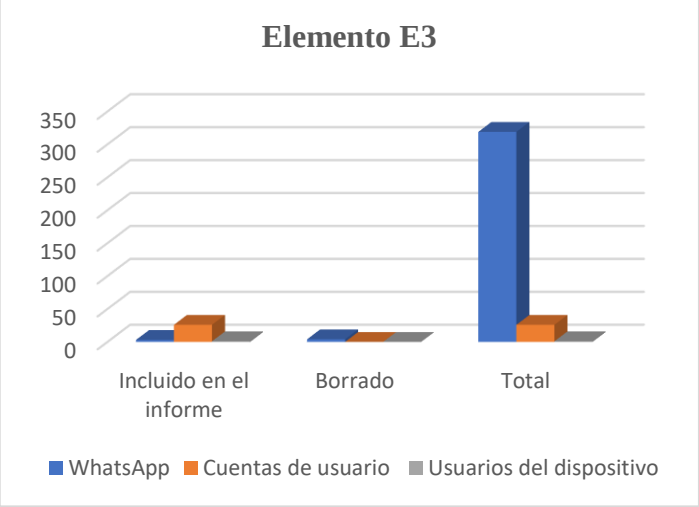
Elemento E3			
Tipo	**Incluido en el informe**	**Borrado**	**Total**

WhatsApp	3	4	319
Cuentas de usuario	26	0	26
Usuarios del dispositivo	1	0	1

Nota. La Tabla 18 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E3, del cual se obtuvieron un total de 399 mensajes de la aplicación de mensajería WhatsApp, 1 usuario del dispositivo, 26 cuentas de usuario, de lo cual se seleccionó 3 mensajes de la aplicación de mensajería WhatsApp, 1 usuario del dispositivo y 26 cuentas de usuario, de igual manera se verifica 4 registros borrados correspondientes a mensajes de la aplicación de mensajería WhatsApp.

Figura 16

Análisis del ELEMENTO E3



Nota. La

Nota. La Tabla 18 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E3, del cual se obtuvieron un total de 399 mensajes de la aplicación de mensajería WhatsApp, 1 usuario del dispositivo, 26 cuentas de usuario, de lo cual se seleccionó 3 mensajes de la aplicación de mensajería WhatsApp, 1 usuario del dispositivo y 26 cuentas de usuario, de igual manera se verifica 4 registros borrados correspondientes a mensajes de la aplicación de mensajería WhatsApp.

Figura 16 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E3 de manera gráfica.

4.2.4. ELEMENTO E4

Luego de realizar la extracción de información mediante la utilización de técnicas, herramientas y software forense se obtiene la siguiente información:

Tabla 19

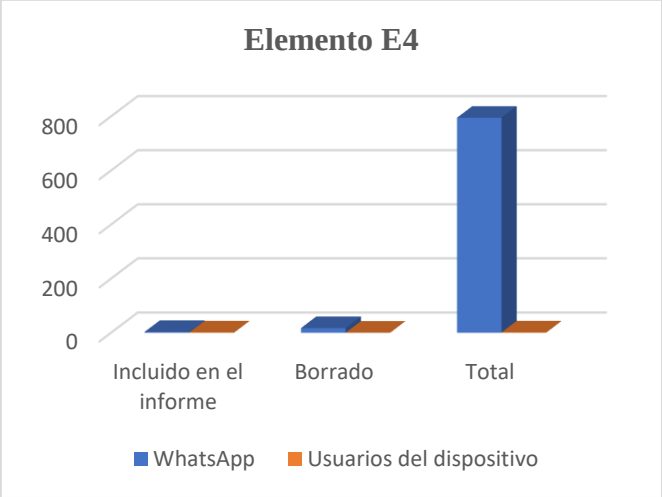
Análisis del ELEMENTO E4

	Elemento E4		
Tipo	**Incluido en el informe**	**Borrado**	**Total**
WhatsApp	3	17	795
Usuarios del dispositivo	1	0	1

Nota. La Tabla 19 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E4, del cual se obtuvieron un total de 795 mensajes de la aplicación de mensajería WhatsApp, 1 cuenta de usuario, de lo cual se seleccionó 2 mensajes de la aplicación de mensajería WhatsApp, 1 cuenta1 de usuario, de igual manera se verifica 17 registros borrados correspondientes a mensajes de la aplicación de mensajería WhatsApp.

Figura 17

Análisis del ELEMENTO E4



Nota. La Nota. La Tabla 19 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E4, del cual se obtuvieron un total de 795 mensajes de la aplicación de mensajería WhatsApp, 1 cuenta de usuario, de lo cual se seleccionó 2 mensajes de la aplicación de mensajería WhatsApp, 1 cuenta1 de usuario, de igual manera se verifica 17 registros borrados correspondientes a mensajes de la aplicación de mensajería WhatsApp.

Figura 17 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E4 de manera gráfica.

4.2.5. ELEMENTO E5

Luego de realizar la extracción de información mediante la utilización de técnicas, herramientas y software forense se obtiene la siguiente información:

Tabla 20

Análisis del ELEMENTO E5

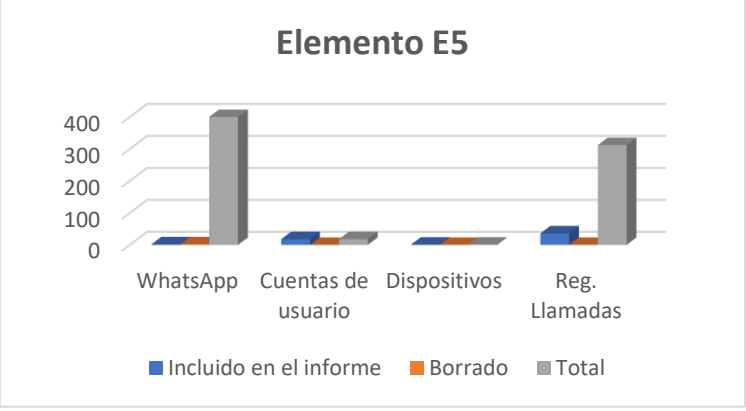
Elemento E5

Tipo	**Incluido en el informe**	**Borrado**	**Total**
WhatsApp	2	2	400
Cuentas de usuario	18	0	18
Dispositivos	1	0	1
Reg. Llamadas	36	0	312

Nota. La Tabla 20 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E5, del cual se obtuvieron un total de 400 mensajes de la aplicación de mensajería WhatsApp, 18 cuentas de usuario, 1 dispositivo, 312 reg. llamadas de lo cual se seleccionó 2 mensajes de la aplicación de mensajería WhatsApp, 18 cuentas de usuario, 1 dispositivo, 36 reg. llamadas, de igual manera se verifica 02 registros borrados correspondientes a mensajes de la aplicación de mensajería WhatsApp.

Figura 18

Análisis del ELEMENTO E5



Nota. La Figura 18 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E5 de manera gráfica.

4.2.6. ELEMENTO E6

Luego de realizar la extracción de información mediante la utilización de técnicas, herramientas y software forense se obtiene la siguiente información:

Tabla 21

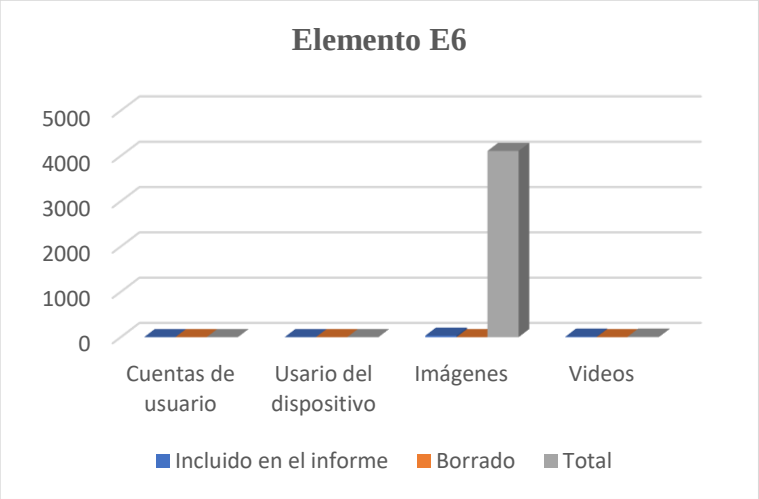
Análisis del ELEMENTO E6

Elemento E6			
Tipo	**Incluido en el informe**	**Borrado**	**Total**
Cuentas de usuario	1	0	1
Usario del dispositivo	1	0	1
Imágenes	31	0	4110
Videos	10	0	10

Nota. La Tabla 21 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E6, del cual se obtuvieron un total de 1 cuenta de usuario, 1 usuario del dispositivo, 4110 imágenes y 10 videos, de lo cual se seleccionó 1 cuenta de usuario, 1 usuario del dispositivo, 31 imágenes y 10 videos

Figura 19

Análisis del ELEMENTO E6



Nota. La Figura 19 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E6 de manera gráfica.

4.2.7. ELEMENTO E7

Luego de realizar la extracción de información mediante la utilización de técnicas, herramientas y software forense se obtiene la siguiente información:

Tabla 22

Análisis del ELEMENTO E7

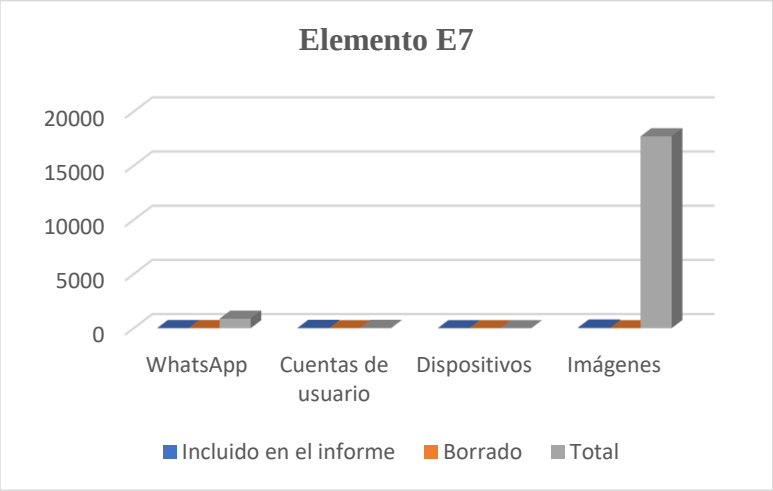
Elemento E7

Tipo	**Incluido en el informe**	**Borrado**	**Total**
WhatsApp	4	4	874
Cuentas de usuario	27	0	27
Dispositivos	2	0	2
Imágenes	62	1	17709

Nota. La Tabla 22 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E7, del cual se obtuvieron un total de 874 mensajes de la aplicación de mensajería WhatsApp, 27 cuentas de usuario, 2 dispositivos y 17709 imágenes de lo cual se seleccionó 4 mensajes de la aplicación de mensajería WhatsApp, 27 cuentas de usuario, 2 dispositivos y 62 imágenes de igual manera se verifica 04 registros borrados correspondientes a mensajes de la aplicación de mensajería WhatsApp y 1 de imágenes.

Figura 20

Análisis del ELEMENTO E7



Nota. La

Nota. La Tabla 22 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E7, del cual se obtuvieron un total de 874 mensajes de la aplicación de mensajería WhatsApp, 27 cuentas de usuario, 2 dispositivos y 17709 imágenes de lo cual se seleccionó 4 mensajes de la aplicación de mensajería WhatsApp, 27 cuentas de usuario, 2 dispositivos y 62 imágenes de igual manera se verifica 04 registros borrados correspondientes a mensajes de la aplicación de mensajería WhatsApp y 1 de imágenes.

Figura 20 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E7 de manera gráfica.

4.2.8. ELEMENTO E8

Luego de realizar la extracción de información mediante la utilización de técnicas, herramientas y software forense se obtiene la siguiente información:

Tabla 23

Análisis del ELEMENTO E8

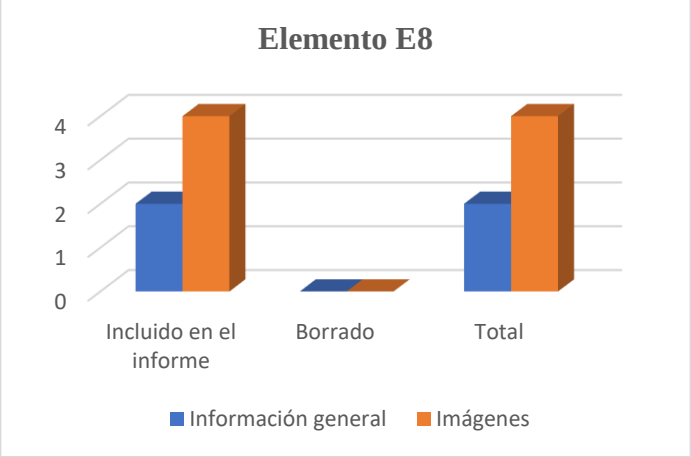
Elemento E8

Tipo	**Incluido en el informe**	**Borrado**	**Total**
Información general	2	0	2
Imágenes	4	0	4

Nota. La Tabla 23 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E8, del cual se obtuvieron un total de 2 información general y 2 imágenes, de lo cual se seleccionó 2 información general y 2 imágenes.

Figura 21

Análisis del ELEMENTO E8



Nota. La Figura 21 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E8 de manera gráfica.

4.2.9. ELEMENTO E9

Luego de realizar la extracción de información mediante la utilización de técnicas, herramientas y software forense se obtiene la siguiente información:

Tabla 24

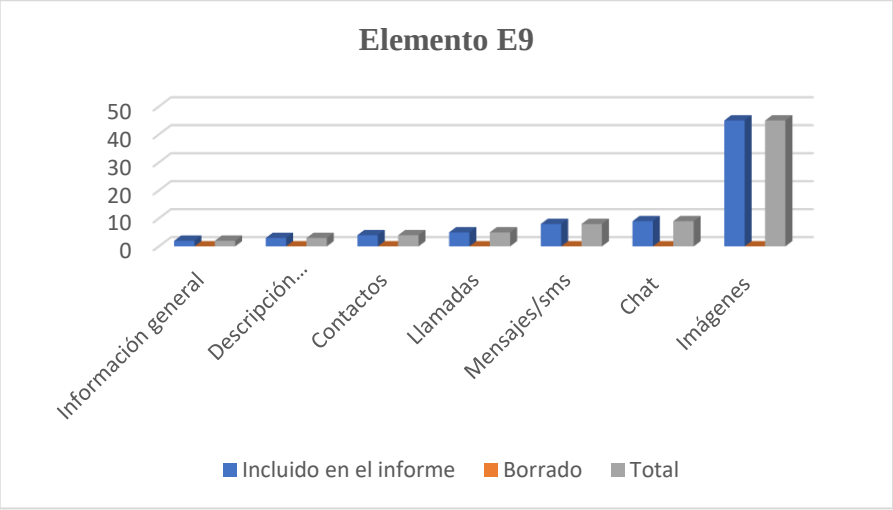
Análisis del ELEMENTO E9

Elemento E9			
Tipo	**Incluido en el informe**	**Borrado**	**Total**
Información general	2	0	2
Descripción genera del dispositivo	3	0	3
Contactos	4	0	4
Llamadas	5	0	5
Mensajes/sms	8	0	8
Chat	9	0	9
Imágenes	45	0	45

Nota. La Tabla 24 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E9, del cual se obtuvieron un total de 2 información general, 3 descripción del dispositivo, 4 contactos, 5 llamadas, 8 mensajes/sms, 9 chat y 45 imágenes, de lo cual se seleccionó 2 información general, 3 descripción del dispositivo, 4 contactos, 5 llamadas, 8 mensajes/sms, 9 chat y 45 imágenes.

Figura 22

Análisis del ELEMENTO E9



Nota. La Figura 22 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E9 de manera gráfica.

4.2.10. ELEMENTO E10

Luego de realizar la extracción de información mediante la utilización de técnicas, herramientas y software forense se obtiene la siguiente información:

Tabla 25

Análisis del ELEMENTO E10

Elemento E10

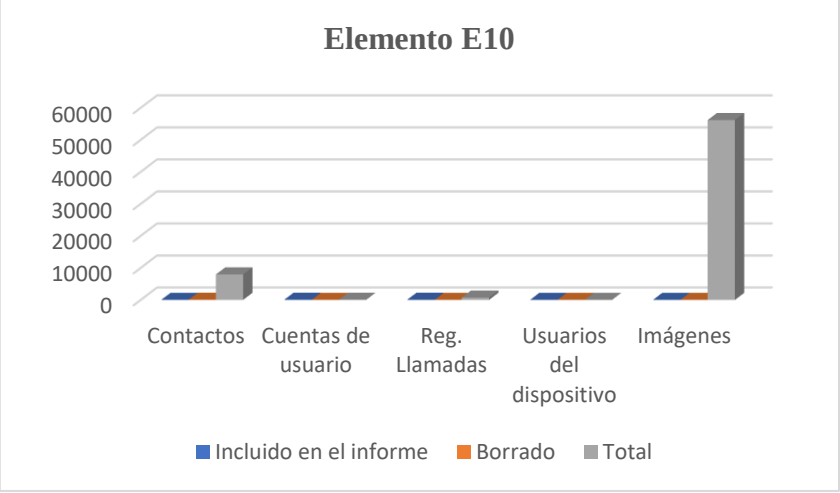
Tipo	**Incluido en el informe**	**Borrado**	**Total**
Contactos	3	27	7953
Cuentas de usuario	36	0	36

Reg. Llamadas	20	5	726
Usuarios del dispositivo	1	0	1
Imágenes	5	0	56180

Nota. La Tabla 25 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E10, del cual se obtuvieron un total de 3 contactos, 36 cuentas de usuario, 726 reg. llamadas, 1 usuario del dispositivo, 56180 imágenes, de lo cual se seleccionó 3 contactos, 36 cuentas de usuario, 20 reg. llamadas, 1 usuario del dispositivo y 5 imágenes, de igual manera se verifica 27 registros borrados correspondientes a contactos y 5 registros de llamadas.

Figura 23

Análisis del ELEMENTO E10



Nota. La

Nota. La Tabla 25 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E10, del cual se obtuvieron un total de 3 contactos, 36 cuentas de usuario, 726 reg. llamadas, 1 usuario del dispositivo, 56180 imágenes, de lo cual se seleccionó 3 contactos, 36 cuentas de usuario, 20 reg. llamadas, 1 usuario del dispositivo y 5 imágenes, de igual manera se verifica 27 registros borrados correspondientes a contactos y 5 registros de llamadas.

Figura 23 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E10 de manera gráfica.

4.2.11. ELEMENTO E11

Luego de realizar la extracción de información mediante la utilización de técnicas, herramientas y software forense se obtiene la siguiente información:

Tabla 26

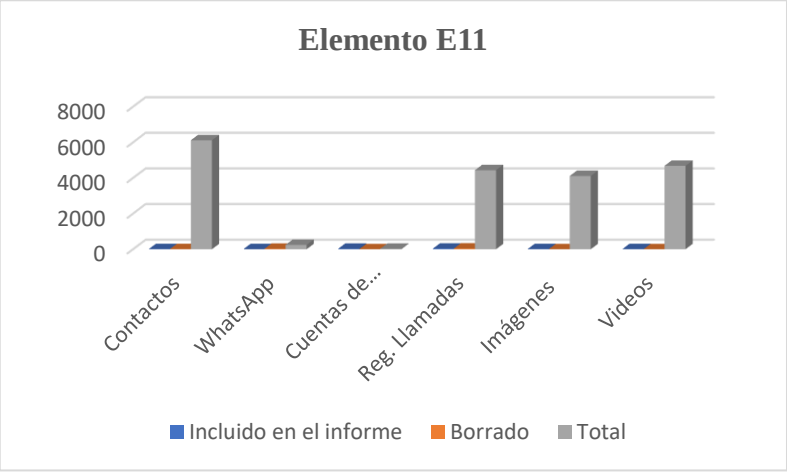
Análisis del ELEMENTO E11

Elemento E11

Tipo	**Incluido en el informe**	**Borrado**	**Total**
Contactos	7	7	6117
WhatsApp	4	25	242
Cuentas de usuario	25	1	25
Reg. Llamadas	35	38	4438
Imágenes	8	0	4114
Videos	6	0	4681

Figura 24

Análisis del ELEMENTO E11



Nota. La Figura 24 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E11 de manera gráfica.

Nota. La Tabla 26 muestra el contenido extraído del dispositivo etiquetado como ELEMENTO E11, del cual se obtuvieron un total de 6117 contactos, 242 conversaciones en WhatsApp, 25 cuentas de usuario, 4438 reg. llamadas, 4114 imágenes y 4681 videos, de lo cual se seleccionó 7 contactos, 4 conversaciones en WhatsApp, 25 cuentas de usuario, 35 reg. llamadas, 8 imágenes y 6 videos de igual manera se verifica 7 registros borrados correspondientes a contactos y 25 mensajes de WhatsApp, 1 cuenta de usuario y 38 registros de llamadas.

5. CONCLUSIONES

Una vez ejecutado el presente trabajo de titulación se llega a las siguientes conclusiones:

El proyecto de investigación aporta significativamente, al sistema de justicia, debido a que, mediante la extracción y análisis de información, a través de la utilización de software forense especializado, se garantiza la autenticidad e integridad de los datos e información plasmados dentro del informe técnico pericial. Este enfoque tecnológico asegura que los datos recuperados sean precisos, completos, auténticos e íntegros, cumpliendo con los estándares más rigurosos los cuales serán presentados como prueba favoreciendo la justicia y la transparencia en el proceso judicial.

La presente investigación no solo proporcionan acceso a los datos almacenados en los dispositivos móviles, sino que también brindan un análisis detallado de los mismos, permitiendo a los operadores de justicia identificar patrones y conexiones entre los datos recuperados. Esto facilita la toma de decisiones informadas sobre el curso de la investigación, ayudando a los fiscales a reconstruir eventos clave, establecer líneas de tiempo precisas y, en muchos casos, descubrir elementos probatorios cruciales que pueden no haber sido evidentes a simple vista.

El uso de software especializado para la extracción de información de dispositivos móviles es indispensable en el contexto de las investigaciones judiciales, ya que optimiza el proceso de recolección de evidencia, asegurando que se mantenga la cadena de custodia y que la información presentada sea fiable, legalmente válida y admisible, lo que fortalecerá la argumentación del caso ante el tribunal contribuyendo al esclarecimiento de los hechos, favoreciendo la justicia y la transparencia en el proceso judicial.

Las herramientas forenses utilizadas, tienen una capacidad única para adaptarse a las tecnologías móviles en constante evolución, ya sea en términos de nuevos modelos de teléfonos, actualizaciones del sistema operativo o métodos de cifrado avanzado. Esto asegura que los

investigadores puedan acceder a la información crítica incluso cuando los dispositivos estén protegidos con las últimas medidas de seguridad. De este modo, las herramientas forenses permiten mantener la actualización constante en cuanto a la compatibilidad con las tecnologías emergentes, brindando a los operadores de justicia un recurso confiable y siempre accesible.

El uso de programas de extracción forense es esencial para la recuperación de evidencia digital crítica, que de otro modo podría haber sido inaccesible o irrecuperable, especialmente en dispositivos que contienen datos cifrados o eliminados por el usuario. Herramientas como UFED, XRY y GRAKEY, son capaces de desbloquear teléfonos móviles y extraer información oculta en áreas del sistema operativo o almacenamiento interno del dispositivo que no están accesibles por medios convencionales. Esta capacidad de acceder a información crítica es vital en la investigación de delitos complejos, donde los dispositivos móviles son a menudo una fuente primaria de evidencia.

6. RECOMENDACIONES

Para garantizar la admisibilidad y validez de la evidencia extraída en un proceso judicial, es indispensable seguir estrictos protocolos de cadena de custodia. Se recomienda reforzar la documentación de cada paso realizado durante la extracción de datos, desde la intervención inicial hasta la presentación de los resultados en la audiencia judicial. Esto incluye el registro detallado de la fecha y hora de cada acción, los dispositivos utilizados, y la autenticación del personal involucrados en el proceso.

Aunque el presente estudio se ha centrado en el sistema operativo Android, muchos de los principios y métodos de análisis pueden ser aplicados a otros sistemas operativos móviles como

iOS. Se recomienda incorporar herramientas forenses multiplataforma que permitan un análisis integral de dispositivos con diferentes sistemas operativos, de modo que se pueda realizar un estudio más amplio en investigaciones que involucren dispositivos móviles de distintas marcas y sistemas operativos.

Durante el proceso de extracción de datos de dispositivos móviles, la seguridad de la información debe ser una prioridad. Se recomienda implementar protocolos adicionales de seguridad para la protección de los datos recuperados durante todo el proceso forense, especialmente en aquellos casos que involucren información sensible o confidencial. Esto incluye medidas como el cifrado de los archivos de evidencia, el uso de almacenamiento seguro y la protección del acceso a los dispositivos.

En muchos casos, los dispositivos móviles se encuentran protegidos por sistemas de cifrado avanzados o métodos de bloqueo de acceso que dificultan la recuperación de datos. Se recomienda realizar más investigaciones y desarrollo de herramientas forenses que puedan mejorar la capacidad para acceder a dispositivos con protección por contraseña, huella dactilar u otros métodos de seguridad. Asimismo, es fundamental investigar la recuperación de datos en dispositivos dañados o aquellos que han sufrido un formateo completo.

7. REFRENCIAS

7.1. Referencia

Cellebrite. (2024, 14 mayo). Cellebrite UFED | Access and Collect Mobile Device Data

Magnet Forensics. (2024b, octubre 10). Magnet Graykey | Mobile forensic access tool.

International Organization for Standardization. (2012). ISO/IEC 27037:2012: Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.

7.2. Referencia

International Organization for Standardization. (2015). ISO/IEC 27043:2015: Information technology — Security techniques — Incident investigation principles.

Cellebrite. (2024a, mayo 14). Cellebrite Physical Analyzer | Forensic Examination of Digital Evidence.

Google. (2023). Android Developers. Johnson, T. (2023). Trends in Android Development. Journal of Mobile Technology, 12(3), 45-58.

Smith, A. (2023). Security Challenges in Android Systems. Cybersecurity Review, 10(2), 20-34.

Statista. (2023). Mobile Operating System Market Share Worldwide.

Machado, NT, Ramírez, LJ, Basile, FRM (2019) Forense computacional como estratégia para investigacąõ em crime cibernéticos

10. Congresso de Inovacąõ, Ciência e Tecnologia do IFSP, Sorocaba, Brasil.

Basile, F. R., Ramírez, L. J., & Amate, F. C. (2019). Método para realizar copias de seguridad de imágenes médicas basado en tareas automatizadas. JINT. Journal of Industrial Neo-Technologies, 6(1), 26-33.

National Institute of Standards and Technology (NIST). (2020). Computer Forensics Tools & Techniques Catalog. https://toolcatalog.nist.gov.

Ponemon Institute. (2019). The cost of cybercrime. Ninth annual cost of cybercrime study. Accenture. https://accntu.re/38XZWug.

Scientific Working Group on Digital Evidence (SWGDE). (2020). SWGDE best practices for mobile device evidence collection & preservation, handling, and acquisition (version 1.2). https://bit.ly/3b5taK7.

Jennings, L.; Sorell, M.; Espinosa, H.G. Interpreting the location data extracted from the Apple Health database. Forensic Sci. Int. Digit. Investig. 2023, 44, 301504.

Referencia

Goh, C.M.J.L.; Wang, N.X.; Müller, A.M.; Yap, R.; Edney, S.; Müller-Riemenschneider, F. Validation of Smartphones and Different Low-Cost Activity Trackers for Step Counting Under Free-Living Conditions. J. Meas. Phys. Behav. 2023, 6, 79–87.

Goh, C.M.J.L.; Wang, N.X.; Müller, A.M.; Yap, R.; Edney, S.; Müller-Riemenschneider, F. Validation of Smartphones and Different Low-Cost Activity Trackers for Step Counting Under Free-Living Conditions. J. Meas. Phys. Behav. 2023, 6, 79–87.

Fukami, A.; Stoykova, R.; Geradts, Z. A new model for forensic data extraction from encrypted mobile devices. Forensic Sci. Int. Digit. Investig. 2021, 38, 301169.

Business Research Insights. Running Apps Market Size, Trend, Growth and Overview 2023 to 2030. 2023. Available online: https://www.businessresearchinsights.com/market-reports/running-apps-market-103263 (accessed on 8 August 2024).

Kent, K.; Chevalier, S.; Grance, T.; Dang, H. Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response Recommendations of the National Institute of Standards and Technology 2006. Available online: https://csrc.nist.gov/ pubs/sp/800/86/final (accessed on 8 August 2024).

Developers, A. Android 8.0 Behavior Changes—Android Developers. 2023. Available online: https://developer.android.com/ about/versions/oreo/android-8.0-changes#security-all (accessed on 8 August 2024).

Muraina, I.; Alobaedy, M.; Ibrahim, H. A Framework for Preserving Data Integrity during Mobile Device Forensic in Open Source Software Environment. In Proceedings of the Free and Open Source Software Conference (FOSSC), Muscat, Oman, 14–15 February 2017.

Kumar, A.; Sondarva, K.; Gohil, B.N.; Patel, S.J.; Shah, R.; Rajvansh, S.; Sanghvi, H. Forensics Analysis of TOR Browser. In Proceedings of the International Conference on Information Security, Privacy and Digital Forensics, Goa, India, 2–3 December 2022; Springer: Berlin/Heidelberg, Germany, 2022. 776–778.

Ghafarian, A.; Seno, S.A.H. Analysis of privacy of private browsing mode through memory forensics. Int. J. Comput. Appl. 2015,

132, 27–34. [CrossRef]

27. Kauser, S.; Malik, T.S.; Hasan, M.H.; Akhir, E.A.P.; Kazmi, S.M.H. Windows 10's Browser Forensic Analysis for Tracing P2P

Networks' Anonymous Attacks. Comput. Mater. Contin. 2022, 72, 1251–1273. [CrossRef]

28. Hejazi, S.M.; Talhi, C.; Debbabi, M. Extraction of forensically sensitive information from windows physical memory. Digit.

Investig. 2009, 6, S121–S131. [CrossRef]

8. APENDICE

INFORME TÉCNICO PERICIAL

CÓDIGO:	**INFORME PERICIAL DE INFORMÁTICA FORENSE No.** [Teléfono de la compañía]
Edición No. 01	

[Categoría]
D.M. de Quito, [Asunto]

INFORME TÉCNICO PERICIAL DE INFORMÁTICA FORENSE No. [Teléfono de la compañía]**.**

Referencia: [Dirección de la compañía]

Señora Doctora.
MERCEDES CUESTA VIVAR
SECRETARIA.
UNIDAD JUDICIAL ESPECIALIZADA

En su despacho. -

De nuestra consideración:

Los suscritos legalmente designados como peritos acreditados ante el Consejo de la Judicatura, presentan el siguiente informe Técnico Pericial de Informática Forense.

1. OBJETO DE PERICIA

Textualmente dice: "...Realizar la APERTURA, EXHIBICIÓN, EXAEN, EXTRACCIÓN, ANÁLISIS Y MATERIALIZACIÓN de la información de los dispositivos móviles ingresados en cadena de custodia Nro. 2024-0001…"

2. CONCEPTOS TÉCNICOS.

Extracción de datos móviles: la extracción de información forense se la realiza a través de

un hardware y software desarrollado para el análisis forense de dispositivos móviles, capaz de realizar la extracción de información de teléfonos celulares y sus componentes.

La extracción depende de las características del sistema operativo del dispositivo. Este proceso permite la adquisición de la mayor parte de los datos del dispositivo, dependiendo del equipo se puede extraer información de datos no visibles, generando informes claros y concisos en formato PDF, EXCEL, HTML y/u otros, para consultas en procesos judiciales. En la mayoría de los casos, no es posible realizar extracción de dispositivos bloqueados.

Extracción lógica: Extracción de datos usando el sistema operativo del dispositivo a través de una serie de comandos conocidos en tiempo real del dispositivo (Información Activa).

Extracción física: Implica el copiado bit a bit de la memoria del dispositivo móvil, este método de extracción permite la adquisición de datos intactos, datos ocultos y eliminados.

Extracción manual: Se utiliza cuando no se cuenta con instrumental compatible para la extracción de la información. Esta técnica manual permita adquirir y analizar los datos.

Tratamiento de evidencia digital: Comprende varias etapas por las que pasa la evidencia digital, surge luego de la adquisición de una imagen forense, o de la preservación de información, pasando por una etapa de procesamiento y análisis, finalizando con un reporte de las actividades realizadas.

Integridad: En informática se refiere al que el archivo digital no ha sido modificado ni alterado para cambiar su estructura inicial, garantizando que la información se encuentre completa, que sea la información original, para esta tarea se usan algoritmos matemáticos tales como: MD5, SHA1 y SHA256.

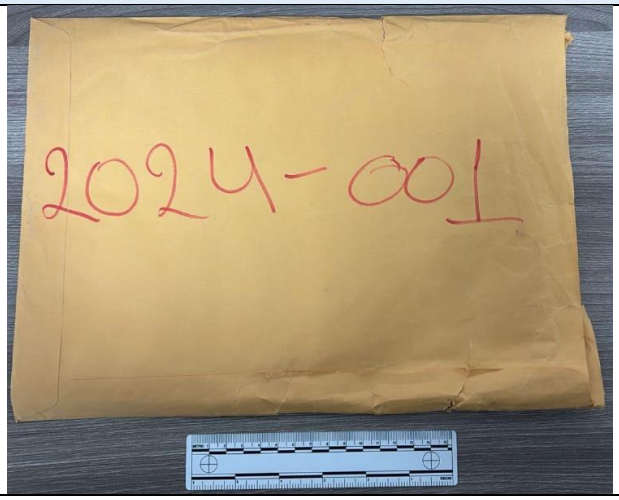
3. METODOLOGÍA PARA LA IDENTIFICACIÓN, RECOLECCIÓN, ADQUISICIÓN Y PRESERVACIÓN DE CONTENIDO DIGITAL

Para el desarrollo de esta actividad pericial requerida por Fiscalía, se ha considerado la metodología de normalización establecida por la ISO / IEC 27037:2012, bajo este precepto técnico se establece las siguientes etapas de trabajo forense para el tratamiento de evidencia digital:

a) Identificación.
b) Adquisición.
c) Preservación.
d) Análisis
e) Presentación (materialización) del contenido digital.

4. ELEMENTOS RECIBIDOS

Para el desarrollo del presente informe técnico pericial y diligencia de audiencia privada, se recibió del centro de acopio dispositivos tecnológicos constantes bajo formulario de cadena de custodia No. 2024-001, elementos que se detallan en las siguientes tablas de especificaciones y características técnicas:

CADENA DE CUSTODIA No. 2024-001


4.1. Un dispositivo móvil de telefonía celular, cuyas identificaciones técnicas se describen en la siguiente tabla de datos:

ELEMENTO 1			
TELEFONO CELULAR		**TARJETA SIM (CHIPS)**	
MARCA:	XIAOMI	**COMPAÑÍA 1:**	CLARO
		SERIE:	895930100082915632
COLOR:	VERDE	**COMPAÑÍA 2:**	NO POSEE
MODELO:	23117RA68G	**SERIE:**	NO POSEE
IMEI:	863357065380362 863357065380370	**TARJETA DE MEMORIA**	
ESTUCHE:	NO POSEE	**MARCA:**	KINGSTON

MODO AVIÓN:	ACTIVADO	**CAPACIDAD:**	16 GB
BATERIA:	INTERNA	**ETIQUETADO**	NINGUNO
OBSERVACIONES: El teléfono celular se encuentra en regular estado de conservación y funcionamiento, el pin de desbloqueo fue proporcionado por el propietario			

Componente del dispositivo

Numeraciones físicas

4.2. Un dispositivo móvil de telefonía celular, cuyas identificaciones técnicas se describen en la siguiente tabla de datos:

ELEMENTO 2			
TELEFONO CELULAR		**TARJETA SIM (CHIPS)**	
MARCA:	TECNO	**COMPAÑÍA 1:**	CLARO
		SERIE:	895930100099792729
COLOR:	BLANCO	**COMPAÑÍA 2:**	TUENTI
MODELO:	TECNOKI7	**SERIE:**	8959300550511009938
IMEI LOGICO:	354531262931161 354531262931179	**TARJETA DE MEMORIA**	

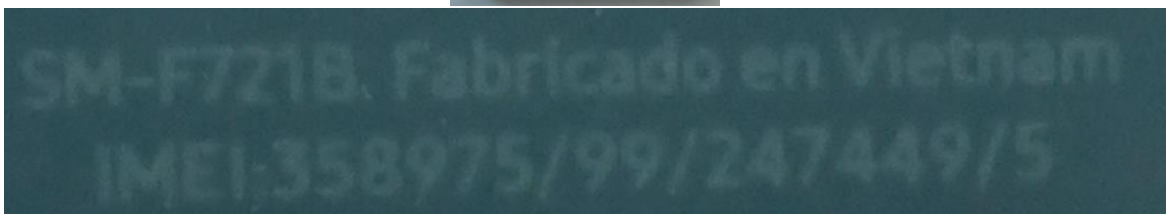
ESTUCHE:	SI POSEE	**MARCA:**	NO POSEE
MODO AVIÓN:	ACTIVADO	**CAPACIDAD:**	NO POSEE
BATERIA:	INTERNA	**ETIQUETADO**	NINGUNO
OBSERVACIONES: El teléfono celular se encuentra en regular estado de conservación y funcionamiento.			
			
Componente del dispositivo		Numeraciones físicas	

4.3. Un dispositivo móvil de telefonía celular, cuyas identificaciones técnicas se describen en la siguiente tabla de datos:

ELEMENTO 3			
TELEFONO CELULAR		**TARJETA SIM (CHIPS)**	
MARCA:	SAMSUNG	**COMPAÑÍA 1:**	CLARO
		SERIE:	895930100097455939
COLOR:	NEGRO	**COMPAÑÍA 2:**	NO POSEE
MODELO:	SM-F721B	**SERIE:**	NO POSEE
IMEI LOGICO:	358975992474495	**TARJETA DE MEMORIA**	

	359697852474493		
ESTUCHE:	NO POSEE	**MARCA:**	NO POSEE
MODO AVIÓN:	ACTIVADO	**CAPACIDAD:**	NO POSEE
BATERIA:	INTERNA	**ETIQUETADO**	NINGUNO

OBSERVACIONES: El teléfono celular se encuentra en regular estado de conservación y funcionamiento, posee trizada la tapa posterior



Componente del dispositivo	Numeraciones físicas

4.4. Un dispositivo móvil de telefonía celular, cuyas identificaciones técnicas se describen en la siguiente tabla de datos:

<table>
<tr><td colspan="4">ELEMENTO 4</td></tr>
<tr><td colspan="2">TELÉFONO CELULAR – ELEMENTO 1</td><td colspan="2">TARJETA SIM 1 (CHIP)</td></tr>
<tr><td>MARCA:</td><td>SAMSUNG</td><td>COMPAÑÍA:</td><td>MOVISTAR</td></tr>
<tr><td>COLOR:</td><td>NEGRO</td><td>SERIE:</td><td>8959300420558547408</td></tr>
<tr><td>MODELO:</td><td>SMA037M/DS</td><td>COLOR:</td><td>BLANCO</td></tr>
<tr><td>IMEI FISICO1:

IMEI FISICO2:</td><td>352550/42/999019/3

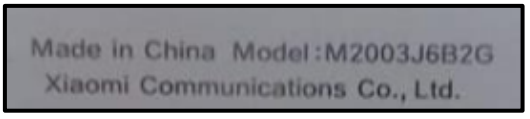
356627/90/999019/4</td><td colspan="2">TARJETA DE MEMORIA</td></tr>
<tr><td>IMEI LOGICO 1:

IMEI LOGICO 2:</td><td>352550429990193/01

356627909990194/01</td><td>MARCA:</td><td>NO APLICA</td></tr>
<tr><td>BATERIA:</td><td>INTERNA</td><td>CAPACIDAD:</td><td>NO APLICA</td></tr>
<tr><td>MODO AVIÓN:</td><td>ACTIVADO</td><td>ETIQUETADO:</td><td>NO APLICA</td></tr>
<tr><td colspan="4">OBSERVACIONES: NINGUNA</td></tr>
<tr><td colspan="2"> 
</td><td colspan="2"> 
</td></tr>
<tr><td colspan="2">Componente del dispositivo</td><td colspan="2">Numeraciones físicas</td></tr>
</table>

4.5. Un dispositivo móvil de telefonía celular, cuyas identificaciones técnicas se describen en la siguiente tabla de datos:

<table>
<tr><td colspan="6">ELEMENTO 5</td></tr>
<tr><td colspan="2">TELEFONO CELULAR</td><td colspan="4">TARJETA SIM (CHIPS)</td></tr>
<tr><td>MARCA:</td><td>XIAOMI</td><td colspan="2">COMPAÑÍA 1:</td><td colspan="2">NO POSEE</td></tr>
<tr><td></td><td></td><td colspan="2">SERIE:</td><td colspan="2">NO POSEE</td></tr>
<tr><td>COLOR:</td><td>BLANCO</td><td colspan="2">COMPAÑÍA 2:</td><td colspan="2">NO POSEE</td></tr>
<tr><td>MODELO:</td><td>M2003J6B2G</td><td colspan="2">SERIE:</td><td colspan="2">NO POSEE</td></tr>
<tr><td>IMEI LOGICO:</td><td>862532056140196
862532056140204</td><td colspan="4">TARJETA DE MEMORIA</td></tr>
<tr><td>ESTUCHE:</td><td>NO POSEE</td><td colspan="2">MARCA:</td><td colspan="2">NO POSEE</td></tr>
<tr><td>MODO AVIÓN:</td><td>ACTIVADO</td><td colspan="2">CAPACIDAD:</td><td colspan="2">NO POSEE</td></tr>
<tr><td>BATERIA:</td><td>INTERNA</td><td>ETIQUETADO</td><td colspan="3">NINGUNO</td></tr>
<tr><td colspan="6">OBSERVACIONES: El teléfono celular se encuentra en regular estado de conservación y funcionamiento.</td></tr>
<tr><td colspan="3">  </td><td colspan="3"> 


</td></tr>
</table>

Componente del dispositivo	Numeraciones físicas

4.6. Un dispositivo móvil de telefonía celular, cuyas identificaciones técnicas se describen en la siguiente tabla de datos:

<table>
<tr><td colspan="6">ELEMENTO 6</td></tr>
<tr><td colspan="2">TELEFONO CELULAR</td><td colspan="4">TARJETA SIM (CHIPS)</td></tr>
<tr><td rowspan="2">MARCA:</td><td rowspan="2">XIAOMI</td><td>COMPAÑÍA 1:</td><td colspan="3">NO POSEE</td></tr>
<tr><td>SERIE:</td><td colspan="3">NO POSEE</td></tr>
<tr><td>COLOR:</td><td>CELESTE</td><td>COMPAÑÍA 2:</td><td colspan="3">NO POSEE</td></tr>
<tr><td>MODELO:</td><td>22101317C</td><td>SERIE:</td><td colspan="3">NO POSEE</td></tr>
<tr><td>IMEI LOGICO:</td><td>867271067186725
867271067186733</td><td colspan="4">TARJETA DE MEMORIA</td></tr>
<tr><td>ESTUCHE:</td><td>NO POSEE</td><td colspan="2">MARCA:</td><td colspan="2">NO POSEE</td></tr>
<tr><td>MODO AVIÓN:</td><td>ACTIVADO</td><td colspan="2">CAPACIDAD:</td><td colspan="2">NO POSEE</td></tr>
<tr><td>BATERIA:</td><td>INTERNA</td><td>ETIQUETADO</td><td colspan="3">NINGUNO</td></tr>
<tr><td colspan="6">OBSERVACIONES: El teléfono celular se encuentra en regular estado de conservación y funcionamiento.</td></tr>
<tr><td colspan="3">  </td><td colspan="3"> 
</td></tr>
</table>

Componente del dispositivo	Numeraciones físicas

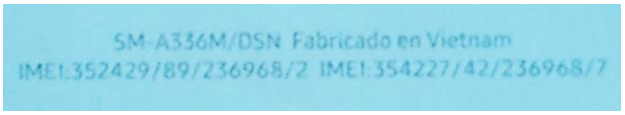
4.7. Un dispositivo móvil de telefonía celular, cuyas identificaciones técnicas se describen en la siguiente tabla de datos:

ELEMENTO 7					
TELEFONO CELULAR			**TARJETA SIM (CHIPS)**		
MARCA:	SAMSUNG		**COMPAÑÍA 1:**	MOVISTAR	
			SERIE:	8959300520555569329	
COLOR:	CELESTE		**COMPAÑÍA 2:**	NO POSEE	
MODELO:	SM-A715F/DS		**SERIE:**	NO POSEE	
IMEI LOGICO:	352635112087413 352636112087411		**TARJETA DE MEMORIA**		
ESTUCHE:	NO POSEE		**MARCA:**	NO POSEE	
MODO AVIÓN:	ACTIVADO		**CAPACIDAD:**	NO POSEE	
BATERIA:	INTERNA	**ETIQUETADO**	NINGUNO		
OBSERVACIONES: El teléfono celular se encuentra en regular estado de conservación y funcionamiento.					

	
	
Componente del dispositivo	Numeraciones físicas

4.8. Un dispositivo móvil de telefonía celular, cuyas identificaciones técnicas se describen en la siguiente tabla de datos:

ELEMENTO 8			
TELEFONO CELULAR		**TARJETA SIM (CHIP)**	
MARCA:	SAMSUNG	**COMPAÑÍA:**	CLARO
COLOR:	CELESTE	**SERIE:**	895930100104889801
MODELO:	SM-A336M/DSN	**COLOR:**	BLANCO - ROJO
IMEI FISICO 1: IMEI FISICO 2:	352429892369682 354227422369687	**TARJETA DE MEMORIA**	

IMEI LÓGICO1: IMEI LÓGICO2:	352429892369682 354227422369687	**MARCA:**	NO POSEE
BATERIA:	INTERNA	**CAPACIDAD:**	NO APLICA
MODO AVIÓN:	ACTIVADO	**ETIQUETADO:**	NO APLICA
OBSERVACIONES:	SIN NOVEDAD.		
		  	
Componente del dispositivo		Numeraciones Físicas	

4.9. Un dispositivo móvil de telefonía celular, cuyas identificaciones técnicas se describen en la siguiente tabla de datos:

ELEMENTO 9			
TELÉFONO CELULAR		**TARJETA SIM (CHIP)**	
MARCA:	INFINIX	**COMPAÑÍA:**	NO POSEE
COLOR:	AZUL	**SERIE:**	NO APLICA
MODELO:	X678B	**COLOR:**	NO APLICA
IMEI FISICO 1: IMEI FISICO 2:	353299481313485 353299481313493	**TARJETA DE MEMORIA**	
IMEI LÓGICO:	NO APLICA	**MARCA:**	NO POSEE
BATERIA:	INTERNA	**CAPACIDAD:**	NO APLICA
MODO AVIÓN:	ACTIVADO	**ETIQUETADO:**	NO APLICA
OBSERVACIONES:	SIN NOVEDAD.		

	
Componente del dispositivo	Numeraciones Físicas

4.10. Un dispositivo móvil de telefonía celular, cuyas identificaciones técnicas se describen en la siguiente tabla de datos:

ELEMENTO 10			
TELÉFONO CELULAR		**TARJETA SIM (CHIP)**	
MARCA:	SAMSUNG	**COMPAÑÍA:**	CLARO
		SERIE:	895930100105505757
MODELO:	SM-A217M	**COMPAÑÍA:**	NO APLICA
ESTUCHE	SI	**SERIE:**	NO APLICA
IMEI	354712/52/019148/9	**TARJETA DE MEMORIA**	
IMEI	NO APLICA	**MARCA:**	NO APLICA
CAPACIDAD	NO APLICA	**CAPACIDAD:**	NO APLICA
MODO AVIÓN	QUEDA ACTIVADO	**ETIQUETADO CELULAR**	NO APLICA
OBSERVACIONES: DISPOSITIVO BLOQUEADO.			

	
Componente del dispositivo	Observación

5. OPERACIONES REALIZADAS

- En primera instancia se realizó la descripción de las especificaciones técnicas de los elementos sometidos a estudio pericial, para posterior iniciar con la metodología de recolección, adquisición y preservación, finalizando con la presentación de diez (-10-) dispositivos individualizados como Elemento 01 al Elemento 10 los cuales se detallan en el acápite 4.

- Previa validación de las especificaciones técnicas físicas y lógicas de los dispositivos que fueron contrastadas con la delegación fiscal y orden judicial, se determinó la idoneidad de los dispositivos de telefonía celular.

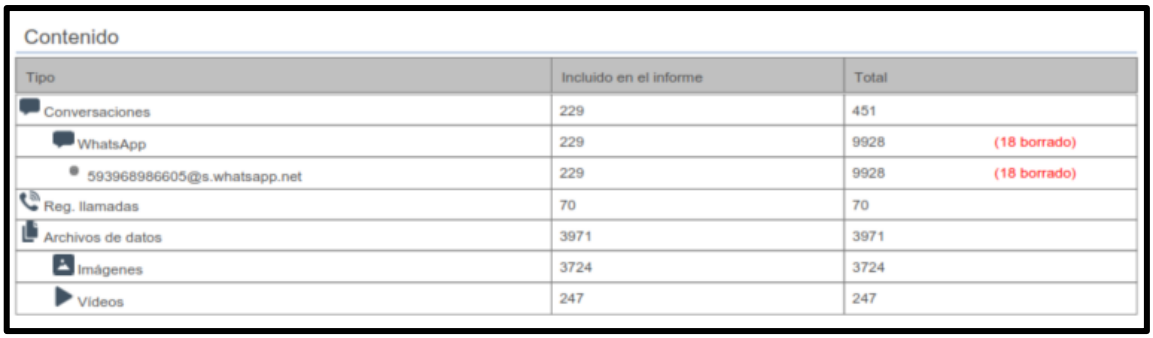
- Posteriormente siguiendo los parámetros de búsqueda proporcionados por la Unidad Judicial se procedió a realizar la extracción y selección de la información que guarda relación con la presente investigación la que se detalla a continuación

6. ADQUISICIÓN DEL CONTENIDO DIGITAL

ELEMENTO E1

Mediante el instrumental técnico forense UFED versión “7.68.0.809” se ha desarrollado la adquisición lógica avanzada de los datos almacenados en el dispositivo de telefonía celular de interés pericial, considerando, los criterios de búsqueda relacionados con el TRAFICO ILÍCITO DE SUSTANCIAS CATALOGADAS SUJETAS A FISCALIZACIÓN, se generó un reporte en

formato con extensión .pdf y html denominado “E1”, comprendido por mil cuatrocientas sesenta y tres (1463) páginas, contenido digital asociada a la presente investigación, datos que está relacionado con: mensajería instantánea tipo chat bajo el aplicativo WhatsApp, cuentas de usuario y registro de llamadas.



Contenido

Tipo	Incluido en el informe	Total	
Conversaciones	229	451	
WhatsApp	229	9928	(18 borrado)
593968986605@s.whatsapp.net	229	9928	(18 borrado)
Reg. llamadas	70	70	
Archivos de datos	3971	3971	
Imágenes	3724	3724	
Vídeos	247	247	

ELEMENTO E2

Mediante el instrumental técnico forense UFED versión “7.68.0.809” se ha desarrollado la adquisición lógica avanzada de los datos almacenados en el dispositivo de telefonía celular de interés pericial detallado en el acápite 3.2, considerando, los criterios de búsqueda relacionados con el presunto delito de ASESINATO, se generó un reporte en formato con extensión .pdf y html denominado “E2”, comprendido de cuarenta y siete (47) páginas, contenido digital asociada a la presente investigación, datos que está relacionado con contenido multimedia relacionado con imágenes y mensajería instantánea tipo chat bajo el aplicativo WhatsApp.

Contenido

Tipo	Incluido en el informe	Total	
Conversaciones	2	249	(5 borrado)
WhatsApp	2	210	(5 borrado)
593987890115@s.whatsapp.net	2	210	(5 borrado)
Dispositivos	6	6	
Usuarios del dispositivo	1	1	
Archivos de datos	3	50196	
Imágenes	3	50196	

ELEMENTO E3

Mediante el instrumental técnico forense UFED versión “7.68.0.809” se ha desarrollado la adquisición lógica avanzada de los datos almacenados en el dispositivo de telefonía celular de interés pericial detallado en el acápite 3.3, considerando, los criterios de búsqueda relacionados con el presunto delito de ASESINATO, se generó un reporte en formato con extensión .pdf y html denominado “E3”, comprendido de treinta y cuatro (34) páginas, contenido digital asociada a la presente investigación, datos que está relacionado con mensajería instantánea tipo chat bajo el aplicativo WhatsApp y cuentas de usuario

Contenido

Tipo	Incluido en el informe	Total	
Conversaciones	3	399	(8 borrado)
WhatsApp	3	319	(4 borrado)
593991045440@s.whatsapp.net	3	319	(4 borrado)
Cuentas de usuario	26	26	
Usuarios del dispositivo	1	1	

ELEMENTO E4

Mediante el instrumental técnico forense UFED versión "7.68.0.809" se ha desarrollado la adquisición lógica avanzada de los datos almacenados en el dispositivo de telefonía celular de interés pericial detallado en el acápite 3.3, considerando, los criterios de búsqueda relacionados con el presunto delito de TRAFICO ILÍCITO DE SUSTANCIAS CATALOGADAS SUJETAS A FISCALIZACION, se generó un reporte en formato con extensión .pdf y html denominado "E5", comprendido de dieciséis (16) páginas, contenido digital asociada a la presente investigación, datos que está relacionado con mensajería instantánea tipo chat bajo el aplicativo WhatsApp y cuentas de usuario.

Contenido

Tipo	Incluido en el informe	Total	
Conversaciones	2	795	(17 borrado)
WhatsApp Business	2	795	(17 borrado)
593999986068@s.whatsapp.net	2	795	(17 borrado)
Cuentas de usuario	1	1	

ELEMENTO E5

Mediante el instrumental técnico forense UFED versión "7.68.0.809" se ha desarrollado la adquisición lógica avanzada de los datos almacenados en el dispositivo de telefonía celular de interés pericial, considerando, los criterios de búsqueda del delito de EXTORSIÓN, se generó un reporte en formato con extensión **.pdf** y **html** denominado **"E5"**, comprendido por cuarenta y cinco (45) páginas, contenido digital asociada a la presente investigación, datos que está relacionado con: mensajería instantánea tipo chat bajo el aplicativo WhatsApp, cuentas de usuario y registro de llamadas.

Contenido

Tipo	Incluido en el informe	Total	
Conversaciones	2	526	(3 borrado)
WhatsApp	2	400	(2 borrado)
593992741483@s.whatsapp.net	2	400	(2 borrado)
Cuentas de usuario	18	18	
Dispositivos	1	1	
Reg. llamadas	36	312	

ELEMENTO E6

Mediante el instrumental técnico forense UFED versión "7.68.0.809" se ha desarrollado la adquisición lógica avanzada de los datos almacenados en el dispositivo de telefonía celular de interés pericial, considerando, los criterios de búsqueda del delito de EXTORSIÓN, se generó un reporte en formato con extensión **.pdf** y **html** denominado **"E6"**, comprendido de ocho (08) páginas, contenido digital asociada a la presente investigación, datos que está relacionado con: mensajería instantánea tipo chat bajo el aplicativo WhatsApp, cuentas de usuario y registro de llamadas.

Contenido

Tipo	Incluido en el informe	Total
Cuentas de usuario	1	1
Usuarios del dispositivo	1	1
Archivos de datos	41	4110
Imágenes	31	4100
Vídeos	10	10

ELEMENTO E7

Mediante el instrumental técnico forense UFED versión "7.68.0.809" se ha desarrollado la adquisición lógica avanzada de los datos almacenados en el dispositivo de telefonía celular de interés pericial, considerando, los criterios de búsqueda del delito de EXTORSIÓN, se generó un reporte en formato con extensión **.pdf** y **html** denominado **"E7"**, comprendido por cuarenta y nueve (49) páginas, contenido digital asociada a la presente investigación, datos que está relacionado con: mensajería instantánea tipo chat bajo el aplicativo WhatsApp, cuentas de usuario y registro de llamadas.

Contenido

Tipo	Incluido en el informe	Total	
Conversaciones	4	882	(4 borrado)
WhatsApp Business	4	874	(4 borrado)
593991456292@s.whatsapp.net	4	874	(4 borrado)
Cuentas de usuario	27	27	
Dispositivos	2	2	
Archivos de datos	62	17709	(1 borrado)
Imágenes	62	17709	(1 borrado)

ELEMENTO E8

Se realiza la extracción “lógica” con la utilización del software forense XRY versión “10.7.1”, como resultado de los filtros de búsqueda relacionada al delito de TRÁFICO ILÍCITO DE SUSTANCIAS CATALOGADAS SUJETAS A FISCALIZACIÓN, se generó un reporte en formato con extensión .pdf denominado “E8”, conteniendo cuatro (04) páginas, con sus respectivos anexos multimedia.

21/5/2024

Contenido

ELEMENTO E9

Se realiza la extracción “lógica” con la utilización del software forense XRY versión “10.7.1”, como resultado de los filtros de búsqueda relacionada al delito de TRÁFICO ILÍCITO DE SUSTANCIAS CATALOGADAS SUJETAS A FISCALIZACIÓN, se generó dos reportes en formato con extensión .pdf denominado “E9”, conteniendo veintiocho (28) páginas y “E9_Informemessenger”, conteniendo trecientos cuarenta y cinco (345) páginas.

Contenido

ELEMENTO E10

Se realiza la extracción “lógica” con la utilización de diferentes técnicas forenses y Se realiza la extracción “lógica” con la utilización de diferentes técnicas forenses y mediante la utilización del software forense UFED, versión: 7.68, del dispositivo móvil, descrito en el acápite 2.4, como resultado de los filtros de relacionada con el delito DELINCUENCIA ORGANIZADA, se generó un reporte bajo la extensión .pdf denominado “E10”, conteniendo nueve (09) paginas, con sus respectivos anexos multimedia.

Contenido

Tipo	Incluido en el informe	Total	
Contactos	3	7953	(27 borrado)
Cuentas de usuario	36	36	
Reg. llamadas	20	726	(5 borrado)
Usuarios del dispositivo	1	1	
Archivos de datos	5	56180	
Imágenes	5	56180	

7. EXPORTACIÓN Y VERIFICACIÓN DEL CONTENIDO DIGITAL

El contenido digital obtenido, según lo detallado en el acápite 6, fue exportado a una unidad de almacenamiento óptico nuevo estéril tipo DVD-R; dispositivo que tiene las siguientes características técnicas y se adjunta al presente Informe Técnico Pericial como Anexo de Almacenamiento Óptico enviado únicamente a la Unidad Judicial.

MARCA	CAPACIDAD	NOMENCLATURA	SERIE DEL VOLUMEN
VERBATIM	4.7 GB	TESIS GRUPO 1	7072-D79D

```
:\>DIR
El volumen de la unidad E es 17571-2024-00478
El número de serie del volumen es: 7072-D79D

Directorio de E:\

0/09/2024  11:49    <DIR>          asus_ASUS_AI2201_C
0/09/2024  11:48            15.904 CODIGOS HASH INFORME 821.htm
               1 archivos         15.904 bytes
               1 dirs               0 bytes libres
```

8. CONCLUSIONES.

Finalizado la metodología de trabajo y procedimientos forenses enfocados a presentar los datos e información almacenados en los dispositivos de comunicación móvil de telefonía celular, se ha llegado a las siguientes conclusiones:

- En base a las normas de estandarización ISO / IEC 27037:2012 y los procesos metodológicos periciales, para el tratamiento de evidencia digital se desarrollaron las etapas de adquisición del contenido digital almacenados en los dispositivos de telefonía celular, mediante una extracción de datos, “lógica avanzada” de los elementos desde el **E1 hasta el E10;** considerando los criterios de búsqueda e intervalos de tiempo proporcionados se ha obtenido un reporte en formato con extensión .pdf y html por cada dispositivo descrito en el acápite 4, reportes que fueron exportados a un dispositivo de almacenamiento óptico y se adjunta como parte del presente Informe Técnico Pericial.

- A fin de mantener la integridad del contenido digital resultado de la aplicación de los parámetros de búsqueda proporcionados se procedió a generar los códigos hash con su código algorítmico MD5 Y SHA1 que se registran en un fichero asignado con el nombre “CÓDIGOS HASH” con extensión .HTML los cuales se adjuntan al presente Informe Técnico Pericial en el Anexo de almacenamiento externo.

Los reportes de los hallazgos generados por las herramientas forenses se adjuntan al informe pericial de manera digital como **Anexo de Almacenamiento Óptico.**

El presente informe técnico Pericial de Informática Forense está distribuido de la siguiente manera: diecisiete (17) **Folios** y un (01) **Anexo de almacenamiento óptico**

Los suscritos declaran bajo Juramento que el presente informe es independiente y corresponde a nuestra real convicción profesional, así como también, que toda la información que se ha proporcionado en este informe pericial es verdadera en honor a nuestro leal saber y entender, es nuestra opinión técnica. Conste. -

Atentamente,

Firma del graduando
Edgar Vinicio Tupiza Gualotuña

Firma del graduando
Guillermo Francisco Quiñonez Castro

Firma del graduando
Jonathan Alexis Cuasquer Garcia

Firma del graduando
Geovanna Belén Torres Bonilla