UNIVERSIDAD ESTATAL PENÍNSULA

DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TITULO DEL TRABAJO DE TITULACIÓN

APLICACIÓN DE TÉCNICAS DE FILE CARVING PARA LA RECUPERACIÓN DE DATOS EN DISPOSITIVOS MÓVILES

AUTOR

ALEJANDRO SOLÓRZANO DAVID RUBÉN

EXAMEN COMPLEXIVO

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

TUTOR

Ing. Walter Armando Orozco Iguasnia. Mgt.

La Libertad, Ecuador

2024

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez Aquino MSc.
DIRECTOR DE LA CARRERA

Ing. Walter Orozco Iguasnia Mgt.
TUTOR

Ing. Carlos Sánchez León Mgt.
DOCENTE ESPECIALISTA

Ing. Marjorie Coronel Suárez Mgt.
DOCENTE GUÍA UIC

UNIVERSIDAD ESTATAL PENÍNSULA

DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

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

La Libertad, a los 3 días del mes de diciembre del año 2024

TUTOR

WALTER ARMANDO OROZCO IGUASNIA
Firmado digitalmente por WALTER ARMANDO OROZCO IGUASNIA
Fecha: 2024.12.03 16:12:35 -05'00'

Ing. Walter Orozco Iguasnia. Mgt.

UNIVERSIDAD ESTATAL PENÍNSULA

DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Alejandro Solórzano David Rubén**

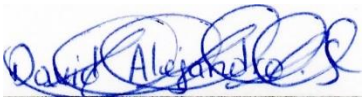
DECLARO QUE:

El trabajo de Titulación, **"APLICACIÓN DE TÉCNICAS DE FILE CARVING PARA LA RECUPERACIÓN DE DATOS EN DISPOSITIVOS MÓVILES"** previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

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

La Libertad, a los 3 días del mes de diciembre del año 2024

EL AUTOR



Alejandro Solórzano David Rubén

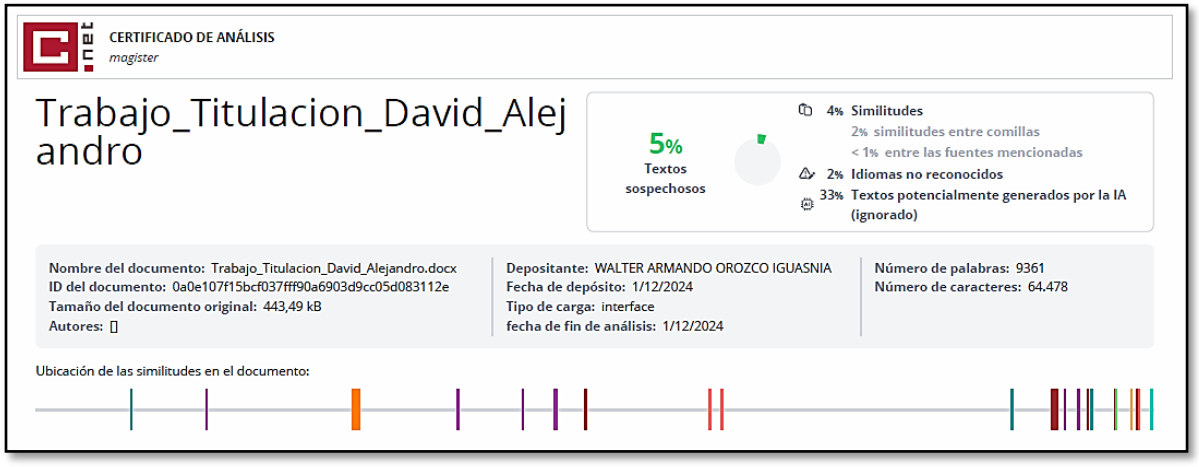
UNIVERSIDAD ESTATAL PENÍNSULA

DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **"APLICACIÓN DE TÉCNICAS DE FILE CARVING PARA LA RECUPERACIÓN DE DATOS EN DISPOSITIVOS MÓVILES"**, presentado por el estudiante, **ALEJANDRO SOLÓRZANO DAVID RUBÉN** fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 5%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



TUTOR

WALTER ARMANDO OROZCO IGUASNIA
Firmado digitalmente por WALTER ARMANDO OROZCO IGUASNIA
Fecha: 2024.12.03 16:12:35 -05'00'

Ing. Walter Orozco Iguasnia. Mgt.

UNIVERSIDAD ESTATAL PENÍNSULA

DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **ALEJANDRO SOLÓRZANO DAVID RUBÉN**

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

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

Santa Elena, a los 3 días del mes de diciembre del año 2024

EL AUTOR

Alejandro Solórzano David Rubén

AGRADECIMIENTO

A Dios por brindarme salud y vida, por darme fuerzas en culminar mi etapa universitaria.

A mis padres, por darme el estudio y haberme inculcado valores y principios, les agradezco por todo el apoyo y confianza que me brindan.

A mis hermanos y a toda mi familia que me acompañaron durante el camino, estoy eternamente agradecido con todos.

Agradezco a mi novia Suly Ortiz, por darme el apoyo necesario y ser mi fortaleza en tiempos difíciles.

Por último, expreso mi agradecimiento a mis docentes, Ingeniera Marjorie Coronel e Ingeniero Walter Orozco, por compartir sus conocimientos y lograr terminar mi trabajo de titulación.

David Rubén Alejandro Solórzano

DEDICATORIA

Este trabajo va dedicado a mis padres por su esfuerzo y perseverancia, a mi familia en general por estar presentes en mi formación profesional. A mi novia por brindarme su amor y dedicación, este logro es gracias a sus consejos y apoyo esencial.

David Rubén Alejandro Solórzano

ÍNDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

INDICE DE IMÁGENES

RESUMEN

Hoy en día, a medida que las personas utilizan cada vez más dispositivos móviles y almacenan información digital en ellos, la recuperación de datos se ha vuelto más desafiante, aumentando particularmente para aquellos casos en que el sistema de archivos está destruido o los datos están eliminados. Por lo tanto, el file carving se destaca con técnicas utilizadas para recuperar información valiosa.

Estas técnicas, como el carving basado en cabeceras y pies o el carving estructural, permiten extraer información de forma eficiente al identificar patrones característicos en los datos almacenados. La metodología utilizada incluye un enfoque exploratorio y práctico, evaluando herramientas especializadas como HxD Editor Hexadecimal y Foremost para identificar fortalezas y limitaciones en distintos sistemas de archivos, como NTFS y ext4. Los resultados obtenidos confirman que el file carving es una técnica eficaz en contextos de recuperación de datos críticos, especialmente en la informática forense.

Palabras clave: file carving, recuperación de datos, dispositivos móviles.

ABSTRACT

Nowadays, as people use more and more mobile devices and store digital information on them, data recovery has become more challenging, particularly increasing for those cases where the file system is destroyed or the data is deleted. Therefore, file carving stands out with techniques used to retrieve valuable information.

These techniques, such as header and footer based carving or structural carving, allow to extract information efficiently by identifying characteristic patterns in the stored data. The methodology used includes an exploratory and practical approach, evaluating specialized tools such as HxD Hexadecimal Editor and Foremost to identify strengths and limitations in different file systems, such as NTFS and ext4. The results obtained confirm that file carving is an effective technique in critical data recovery contexts, especially in computer forensics.

Keywords: file carving, data recovery, mobile devices.

INTRODUCCIÓN

La recuperación de información en los dispositivos móviles ha adquirido bastante relevancia. El file carving se emplea con mayor frecuencia, siendo un método que facilita la extracción de archivos o datos a partir de una serie de patrones específicos, lo cual puede realizarse sin requerir la estructura lógica del sistema de archivos. Este enfoque resulta especialmente ventajoso en circunstancias en las que los datos están fragmentados o el sistema de archivos ha experimentado daños. La presente investigación analiza diversas técnicas de file carving, subrayando su efectividad en la recuperación de datos almacenados en dispositivos móviles, abordando tanto aspectos prácticos como teóricos.

Capítulo I: En el presente capítulo a mencionar se desarrolla la exploración de todas las necesidades que embarca la recuperación de datos en dispositivos Android a través de técnicas forense, tales como las técnicas de File Carving, se destaca las debilidades y fortalezas del beneficio donde se hace uso de las técnicas forense al realizar este estudio y conocer más a detalle las cada una al momento de emplear estás técnicas. Por lo tanto, se abarcan todas las falencias y así poder lograr establecer mejoras con el estudio en desarrollo.

Capítulo II: Esta sección comprende el marco teórico, la metodología del proyecto, al comienzo del capítulo se destacan temas relevantes sobre la naturaleza de los dispositivos Android, las técnicas forenses de File Carving, los tipos de archivos en cuestión de almacenamiento en Android y Windows, también ejercer el análisis correspondiente del modelado de las técnicas, conocer las herramientas ideales para el estudio, como también presentar las fases precisas para el desarrollo en el siguiente capítulo.

CAPITULO III: En esta sección se ofrece la propuesta detallada sobre el proceso de recuperación de datos, incluyendo las fases correspondientes del tema, el análisis de las técnicas, las herramientas a utilizar, el desarrollo de los escenarios de prueba, la tabla de resultados y así mismo emplear el manual de buenas prácticas sobre el estudio propuesto.

CAPÍTULO I

1 FUNDAMENTACIÓN

1.1 ANTECEDENTES

El creciente interés en la informática forense en los últimos años muestra la importancia de encontrar nuevas formas de satisfacer las necesidades de este campo. La recuperación de datos desde dispositivos móviles se ha convertido en una gran demanda en la investigación científica y la recuperación de datos, especialmente porque estos dispositivos se utilizan en la vida diaria y la información que almacenan es grande [1].

Por esta razón, recuperar datos en el nuevo entorno digital se considera importante y puede causar daños graves, como pérdida de datos, pérdida importante de confianza de los consumidores, interrupciones comerciales e incluso cierres de empresas. Los datos son activos informativos valiosos; en consecuencia, su uso inapropiado o su perdida podría provocar eventos trágicos y un considerable desorden en ausencia de un plan de emergencia [2].

La recuperación de información debe asegurar la protección de la información de los usuarios en dispositivos móviles, es fundamental tener en cuenta las características inherentes a dichos dispositivos. Los dispositivos móviles están diseñados para utilizar tecnologías como la memoria flash NAND para optimizar la energía y el almacenamiento. Además, la recuperación de datos de dispositivos móviles es difícil porque los datos a menudo están fragmentados y dispersos en diferentes partes del dispositivo. Esto se debe a que los datos utilizados están optimizados para maximizar el uso de recursos como la energía y el almacenamiento [3].

Para la presente investigación se dará énfasis temas relacionados, artículos, tesis que estén asociados al tema que abordar en la aplicación de técnicas de File Carving para la recuperación de datos en dispositivos móviles, el objetivo es conocer el contexto que ejerce un backup eficiente para desarrollar una seguridad y privacidad de la información de los usuarios. Por lo tanto, se da mención a tres estudios referenciales como el internacional, nacional y local que abarque una pauta a la indagación.

El **título "Herramienta forenses de análisis digital para la obtención de información aplicado a ordenadores y dispositivos móviles"** de Quetzal Tenango, indica como la información o los activos de información cumplen un papel crucial sobre todo en el mundo de los negocios u organizaciones debido que mantienen el uso de sistemas informáticos especializados para almacenar, gestionar y crear datos importante, que si no es protegido pueden ser víctimas de escenarios como delitos informáticos, perdida de información, entre otros. La investigación aborda el objetivo de reunir una serie de herramientas forenses utilizadas en el entorno digital para recabar datos superficiales para ser usadas en casos judiciales como es el caso de identificar, manejar, resguardar evidencias digitales y respaldos para ser posterior analizados acorde a su contexto de caso [4].

Por otra parte, la tesis que tiene como título **"Creación de una guía de recuperación de datos utilizando forense file carving para ordenadores Windows"**, proporcionada por la Universidad Nacional de Chimborazo del Ecuador menciona como la sociedad se ha acostumbrado a uso eminente de medios como ordenadores para la creación, procesamiento y almacenamiento de datos informático que requiere de mecanismos de protección o una guía clara que indique al usuario la metodología correcta para la recuperación de archivos perdidos. Debido que existen métodos como técnicas forense cruciales para aquella tarea y una de ellas es File Carving que abarca en todo el contexto de recuperación de fragmentos de archivos [5].

Además, el tema de tesis **"Análisis forense de evidencias digitales en entornos iCloud"**, proporcionada por la Universidad Estatal Península de Santa Elena, hace mención a como los entornos tecnológicos a lo largo de los años van evolucionado; surgen servicios de almacenamiento en la nube, como es el caso de ICloud. Su servicio permite el almacenamiento para guardar videos, fotos, entre otros; utilizando diferentes formatos en función de la necesidad del usuario y asociado a una cuenta para acceso al servicio. El trabajo cumple con el factor de implementar un ambiente controlado con la finalidad de ejercer el análisis forense de evidencias digitales a través de amenazas cibernéticas y así emplear el marco legislativo como el respetivo informare que describe los resultados de la investigación con sus requerimientos [6].

En síntesis y en concordancia con los trabajos citados, el tema de recuperación de información tiene su base en planes de recuperación de datos a través de enfoques tecnológicos del área de computación forense, como el uso de herramientas de OpenSource y técnicas como el file carving. Por lo tanto, el objetivo es garantizar la seguridad y privacidad de los datos del usuario implementando mejoras apropiadas y creando estrategias para reducir los riesgos de efectos aleatorios como el desgaste de la memoria, la corrupción de datos y la recuperación de datos.

1.2 DESCRIPCIÓN DEL PROYECTO

La recopilación inadecuada de protección y recuperación de datos demuestra la importancia de la seguridad informática para los datos personales y sensibles. La recuperación de datos requiere acceso al almacenamiento de su teléfono; por lo tanto, es importante garantizar que el proceso no comprometa la seguridad o confidencialidad de los datos.

La recuperación de datos consiste en sistemas informáticos especializados diseñados para utilizar tecnología para acceder y restaurar fácilmente datos almacenados digitalmente, incluso si están dañados, defectuosos o con información incorrecta. Este proceso implica el uso de herramientas y técnicas precisas para recuperar datos de dispositivos relevantes y garantizar la integridad de los datos. Nuevamente, estas técnicas deben usarse con precaución para evitar daños mayores al sistema o al estado de los datos, garantizando así que los datos sean recuperables.

En cuestión el tema se guiará a la metodología UNE 71506/2013 como enfoque para llevar a cabo pruebas experimentales, seguido de RFC 3227 la cual es una guía para recolectar y archivar evidencia.

Fase 1: Adquisición

- Investigar las técnicas de file carving para la recuperación de datos en dispositivos móviles.
- Identificar y registrar todos los datos de los dispositivos móviles y medios de almacenamiento relevantes.

Fase 2: Preparación

- Identificar las herramientas de File Carving más adecuadas para el análisis, considerando el tipo de dispositivo y el sistema de archivos.
- Desarrollar escenarios con texto habituales para la recuperación de datos en dispositivos móviles Android.

Fase 3: Análisis

- Utilizar las herramientas seleccionadas que permitan recuperación de datos eliminados basándose en firmas de ficheros y estructuras conocidas, centrándose en los tipos de archivos relevantes.
- Elaborar un cuadro descriptivo que detalle los procedimientos realizados durante la aplicación de la técnica de file carving para recuperar los diferentes tipos de archivos.

Fase 4: Documentación

Este documento tiene como objetivo proporcionar una guía clara sobre el proceso de recuperación de datos sensibles, abordando técnicas de protección y evaluación de seguridad informática a los datos extraídos. Entre otros aspectos, incluye una introducción general al tema, los objetivos a cumplir, el alcance de las operaciones, las observaciones técnicas necesarias para garantizar la integridad de la información y una serie de recomendaciones para asegurar la privacidad y la seguridad de los datos recuperados.

1.3 OBJETIVOS DEL PROYECTO

1.3.1 OBJETIVO GENERAL

Identificar las técnicas de file carving mediante la evaluación de herramientas especializadas para extracción y análisis según el modelo de los dispositivos, para recuperar datos en dispositivos móviles.

1.3.2 OBJETIVOS ESPECÍFICOS

- Analizar las diferentes técnicas de file carving existentes y su aplicabilidad en sistemas operativos móviles como Android.
- Diseñar diversos escenarios de pérdida de datos en dispositivos móviles para ejercer la evaluación de las técnicas de File Carving en recuperación de datos.
- Desarrollar un manual que incluya las mejores prácticas, herramientas recomendadas y metodologías para la aplicación efectiva de técnicas de file carving en la recuperación de datos en dispositivos móviles.

1.4 JUSTFICACIÓN DEL PROYECTO

La adopción de técnicas de file carving para la recuperación de información en dispositivos móviles es fundamental en el contexto forense digital, dado el aumento de la relevancia de estos dispositivos en la vida cotidiana y en las investigaciones criminales. Esta técnica facilita la recuperación de archivos sin requerir información de metadatos, lo cual resulta esencial en situaciones donde los sistemas de archivos se encuentran comprometidos o los datos han sido eliminados de manera intencionada. A continuación, se presentan las ventajas y beneficios de la implementación de esta solución.

En las investigaciones criminales, la capacidad de recuperar datos de dispositivos móviles puede proporcionar pruebas importantes. Los dispositivos móviles suelen contener información personal importante, como mensajes, fotos, llamadas y datos de aplicaciones que pueden identificarse en un caso. Incluso si se eliminan los datos o se daña el dispositivo, los investigadores pueden recuperar estos datos utilizando técnicas de file carving [7].
Las técnicas de file carving son efectivas cuando el sistema de archivo está dañado o los datos no se eliminan correctamente. Esta técnica permite crear archivos fragmentados analizando bloques de datos independientemente del sistema de archivos. El tallado de datos puede recuperar datos fragmentados sin la necesidad de procesarlos, lo que aumenta el éxito de la recuperación de datos.

La adaptabilidad de las técnicas de file carving a diferentes sistemas de datos es otra ventaja importante. Los dispositivos móviles utilizan varios sistemas como ext4, F2FS, YAFFS2 en Android y APFS en iOS. La técnica de file carving se puede utilizar de forma eficaz para todos estos sistemas, proporcionando una forma unificada para recuperar datos de varios dispositivos. Al adaptar las técnicas a las diferencias en la gestión de datos entre diversos sistemas de archivos, lo que amplía su aplicabilidad [8].

En un entorno empresarial, las copias de seguridad de datos no pueden proteger datos importantes. Las empresas que utilizan dispositivos móviles para gestionar operaciones, almacenar información de clientes y realizar negocios pueden beneficiarse enormemente de la capacidad de recuperar datos perdidos o dañados. La implementación de técnicas de file carving pueden garantizar la continuidad del negocio y minimizar las interrupciones comerciales causadas por la pérdida de datos.

La investigación y desarrollo de técnicas avanzadas de file carving no solo benefician la recuperación de datos en dispositivos móviles, sino que también contribuyen al campo de la informática forense en general. Estas técnicas pueden ser adaptadas y mejoradas para su aplicación en otros tipos de dispositivos y sistemas de almacenamiento, fomentando el avance tecnológico y mejorando las capacidades de recuperación de datos en diversas situaciones.

1.5 ALCANCE DEL PROYECTO

El presente trabajo investigativo llevará a cabo un estudio de las técnicas de File Carving que son actualmente aplicables a sistemas de archivos y medios de almacenamientos; permitiendo analizar la viabilidad de las diversas técnicas y efectividad en el entorno de estudios a través de pruebas experimentales diseñadas para el efecto.

Fase 1: Adquisición

Durante esta etapa, se investigan y catalogan las técnicas de recuperación de datos, como el File Carving, mediante un cuadro comparativo que evalúa su eficacia en dispositivos móviles. Además, se identifican y registran todos los datos relevantes de los dispositivos y medios de almacenamiento, garantizando su preservación para el análisis forense posterior.

Fase 2: Preparación

Durante esta etapa, se identifican las herramientas de File Carving más adecuadas para el análisis, teniendo en cuenta el tipo de dispositivo y el sistema de archivos. También se configura un ambiente de trabajo seguro para realizar las pruebas, evitando el riesgo de pérdida de archivos recuperados y asegurando la integridad de los datos durante el proceso.

Fase 3: Análisis

Se utilizan las herramientas seleccionadas para recuperar datos eliminados, basándose en firmas de ficheros y estructuras conocidas, y se enfoca en los tipos de archivos relevantes. Además, se elabora un cuadro descriptivo que detalla los procedimientos realizados en la aplicación de la técnica para recuperar los distintos tipos de archivos.

Fase 4: Documentación

Se elabora un informe detallado que incluye una introducción al proceso, el objetivo y alcance del análisis, observaciones técnicas y recomendaciones basadas en los hallazgos. Esta documentación asegura que el proceso y los resultados sean claros y accesibles para futuros usos o revisiones.

Finalmente, el proyecto no incluirá el desarrollo de nuevas herramientas o la creación de técnicas para la recuperación de datos, se enfocará en la aplicación de las técnicas de File Carving.

CAPÍTULO II

2 MARCO TEÓRICO Y METODOLOGÍA DEL PROYECTO

2.1 MARCO CONCEPTUAL

2.1.1 INFORMÁTICA FORENSE

La informática forense, también conocida como forense digital, es un área que estudia cómo recopilar pruebas digitales para que sean válidas en un tribunal. También se conoce como forense informático, computación forense o ciber forense, y es una mezcla de ciencia forense jurídica e informática. Este campo se utiliza en investigaciones que van desde delitos informáticos como hackeos y fraudes hasta investigaciones corporativas para encontrar infracciones de seguridad. El objetivo principal es garantizar que las pruebas digitales sean recopiladas, preservadas y presentadas de manera que mantengan su integridad legal y sean útiles en un juicio [9].

2.1.1.1 IMPORTANCIA DE LA INFORMÁTICA FORENSE

Debido a la gran cantidad de formatos digitales conectados en todo el mundo, los objetivos principales de la informática forense son superficiales. La gestión de la evidencia digital es relevante para resolver delitos informáticos y recuperar datos importantes. El trabajo del investigador informático se abarca en recopilar, examinar y salvaguardar la evidencia digital [10].

- **Recopilación de evidencias**

  Comprende en la obtención de copias de la información sospechosa que este estrictamente vinculada con algún incidente, es relevante la modificación de cualquier dato que es utilizado, siempre se debe generar copias bit a bit con herramientas especializadas y dispositivos adecuado para la evidencia. Además, es muy imprescindible debido que adelante se desarrolle la recuperación de archivos borrados o particiones ocultas, logrando tener como resultado un activo de información correspondiente al disco estudiado en cuestión [11].

- **Preservación**

  La preservación de la evidencia digital es una fase importante debido que se deben de mantener intacta u originales aquellos activos de información para que no pierdan en ningún momento su valides y confiabilidad y se debe garantizar la reproductividad de los estudios afectados por cualquier entrono de análisis forense o laboratorio designado para su análisis [12].

- **Análisis**

  Evidencia digital para revelar patrones, determinar la secuencia de eventos, determinar la naturaleza y alcance de la actividad. Este proceso incluirá recuperación de archivos eliminados e información detallada sobre la situación [13].

- **Documentación**

  Durante este proceso, se debe registrar toda la información visual. Colabora en la reconstrucción e investigación de las escenas del crimen. Incluya información relevante sobre derechos de autor, incluidas fotografías, dibujos y mapas. Además, se utilizan técnicas efectivas de recuperación de datos, como escaneo de discos duros, redes y dispositivos móviles. Todas estas actividades se llevan a cabo según estrictos procedimientos para garantizar la autenticidad de las pruebas y evitar que sean manipuladas o destruidas [14].

- **Presentación**

  Finalmente, los resultados del análisis deben presentarse de manera clara, concisa y fácil de entender para personas que no son expertas. El informe debe incluir una descripción detallada del procedimiento utilizado y los resultados. El auditor forense puede ser requerido para testificar como experto en un tribunal y explicar cómo se recolectaron, preservaron, analizaron y presentaron las pruebas [15].

2.1.2 FILE CARVING

El File Carving ofrece diversas ventajas en el ámbito de la informática forense, destacándose especialmente en la recuperación y restauración de información. Esta técnica es particularmente útil para identificar y reconstruir archivos importantes que se hayan deteriorado o perdido. En su implementación actual, el proceso de File Carving crea réplicas de todos los archivos que logra recuperar. Sin embargo, esta metodología también tiene como consecuencia la generación de archivos irrelevantes o innecesarios durante su ejecución [16].

File carving se basa en la identificación y extracción de archivos a partir de sus patrones característicos presentes en los datos sin procesar del medio de almacenamiento. Esta técnica es independiente de la estructura del sistema de archivos, lo que la convierte en una herramienta invaluable en situaciones donde la información del sistema de archivos se ha visto comprometida.

2.1.2.1 ORIGEN Y EVOLUCIÓN

Cuando se elimina un archivo, el sistema realiza varias operaciones. Primero, reemplaza los indicadores que señalan los clústers del archivo (siendo un clúster la unidad mínima de almacenamiento en un sistema de archivos) con el valor hexadecimal "00". Este cambio indica que esos espacios de almacenamiento están ahora disponibles para ser utilizados. Sin embargo, es importante notar que la entrada del directorio correspondiente a ese archivo aún mantiene la referencia al primer clúster donde se almacenaba el archivo, incluso después de que se han reiniciado estos enlaces. Como paso final del proceso de eliminación, el sistema modifica el primer carácter del nombre del archivo, señalando así que se trata de un archivo que ha sido borrado.

Diferentes sistemas de archivos implementan diversas acciones al eliminar un archivo, pero comparten una característica común: en ningún caso sobrescriben el contenido del clúster, ya que esto afectaría negativamente el rendimiento debido al tiempo necesario para escribir en el dispositivo.

Los clústers que pertenecían a un archivo eliminado mantienen su contenido, pero se marcan como disponibles en la tabla de asignación o en la estructura correspondiente del sistema de archivos. Los datos contenidos en estos clústers solo se perderán cuando se reasignen y se utilicen para almacenar un nuevo archivo [17].

2.1.2.2 TECNICAS DE FILE CARVING

- **HEADER FOOTER CARVING**

  El header-footer carving es la técnica original y más simple de recuperación de archivos en análisis forense digital. Se basa en la búsqueda de encabezados (headers) y pies de página (footers) específicos que delimitan el inicio y el final de un archivo en el sistema de almacenamiento. Aunque permite recuperar archivos de manera efectiva, es muy susceptible a generar falsos positivos, ya que en ocasiones puede identificar incorrectamente áreas de datos no relacionadas como parte de un archivo válido [18].

- **FILE STRUCTURE BASED CARVING**

  La tecnología de recuperación de datos basada en modelos de datos se basa en la estructura interna y la estructura de los archivos. Este método define patrones específicos y organización de tipos de archivos para el análisis y la recuperación de datos. Estas técnicas son relevantes para el análisis ya que permiten evaluar la integridad y coherencia de los datos a analizar, reduciendo así la posibilidad de falsos positivos [18].

- **STATISTICAL CARVING**

  La talla estadística es una técnica de recuperación de archivos que utiliza medidas estadísticas para analizar los bloques de datos y los formatos de archivo que se pretenden reconstruir. La técnica utiliza patrones y distribuciones estadísticas para determinar el inicio, el final y los bloques intermedios de los archivos, lo que ayuda en la toma de decisiones durante la reconstrucción de los archivos. A diferencia de otras técnicas, la talla estadística se basa en la probabilidad estadística de que un bloque de datos pertenezca a un archivo específico en lugar de en firmas o estructuras fijas [18].

- **FRAGMENT RECOVERY CARVING**

  Los algoritmos basados en grupos utilizan un conjunto de símbolos para determinar si un bloque pertenece a un tipo particular. Utilizando técnicas para estructurar datos mediante grupos de fragmentos, agrupando datos que comparten propiedades o están relacionados con el formato deseado. Este enfoque permite la creación de más archivos, especialmente cuando el archivo se distribuye en diferentes partes del sistema de almacenamiento [18].

- **SEMANTIC CARVING**

  Para crear archivos coherentes y comprensibles, esta familia de sistemas utiliza el índice de contenido para conectar bloques de manera significativa. La capacidad de separar dos archivos de texto escritos en diferentes idiomas es siempre un ejemplo, pero este método se puede utilizar para aumentar la precisión en la creación de documentos con diferentes tipos de contenido [18].

- **GRAPH THEORETIC CARVING**

  Este sistema utiliza dispositivos de almacenamiento para buscar archivos fragmentados, similar a la destrucción inversa. Luego, los fragmentos se separan y se crea un grafo donde se utiliza un algoritmo de rutas múltiples con diferentes puntos de inicio y finalización para optimizar la recuperación del archivo. Smart Shaping es un ejemplo comercial de esta técnica. Aunque es un cálculo complejo y costoso de utilizar, se puede utilizar junto con otras técnicas para aumentar su efectividad. Las medidas de similitud utilizadas al asignar pesos a los vértices en el grafo de fragmentos son muy importantes para la calidad de los resultados [18].

2.1.3 ANÁLISIS FORENSE

La disciplina conocida como Análisis Forense Informático, que recibe diversos nombres como informática forense, computación forense, análisis forense digital, cómputo forense o examen forense digital, consiste en la implementación de metodologías científicas y técnicas analíticas avanzadas en el ámbito de los sistemas tecnológicos. Su objetivo principal es detectar, conservar, examinar y exponer información de manera que pueda ser considerada legítima y admisible en procedimientos judiciales. Esta rama especializada se enfoca en el manejo experto de evidencias digitales para respaldar procesos legales [19].

Después de una violación de la seguridad informática, como intrusiones o robo de información, se lleva a cabo un análisis forense en ciberseguridad, que es esencial para identificar qué sucedió, como sucedió y quién fue el responsable, permitiendo así denunciar al culpable y tomar medidas preventivas. Además de comprender qué es la ciberseguridad, es crucial comprender cómo actúan los piratas informáticos durante un ciberataque para identificar las debilidades del sistema y fortalecerlo adecuadamente [20].

2.1.4 SISTEMA OPERATIVO ANDROID

Android es un sistema operativo móvil basado en Linux desarrollado por Google específicamente para dispositivos móviles como teléfonos inteligentes y tabletas. La plataforma es flexible y adaptable porque su arquitectura abierta permite a los usuarios y empresas personalizar la interfaz y la funcionalidad del sistema. Android destaca por su ecosistema de aplicaciones (disponibles en Google Play) y su capacidad de integrarse con multitud de servicios y dispositivos. Es uno de los sistemas operativos móviles más populares del mundo debido a su diversidad y accesibilidad [21].

Android está basado en el núcleo de Linux y utiliza una máquina virtual personalizada diseñada para optimizar el uso de recursos de memoria y hardware en dispositivos móviles. Al ser de código abierto, permite que sea modificado y extendido libremente para integrar nuevas tecnologías emergentes. La plataforma seguirá evolucionando gracias a la colaboración de la comunidad de desarrolladores, quienes contribuyen a crear aplicaciones móviles innovadoras a lo largo del tiempo [22].

Apoya la innovación tecnológica al permitir la personalización y modificación manteniendo un alto nivel de apertura en el ecosistema de Android. De esta forma, se asegura la relación entre productos y permite a las empresas crear soluciones únicas para que la competencia empresarial no se vea afectada por la empresa conjunta [23].

Android ha recibido muchas actualizaciones desde su lanzamiento inicial. La siguiente imagen muestra las distintas versiones de Android y sus nombres en clave con cambios a lo largo del tiempo. Cada versión mejora el rendimiento, la seguridad y la experiencia del usuario siguiendo las necesidades de la tecnología y el mercado móvil [24].

Este esquema de licenciamiento equilibra los valores del software libre con los objetivos comerciales de los fabricantes de dispositivos (Figura 1) [24].

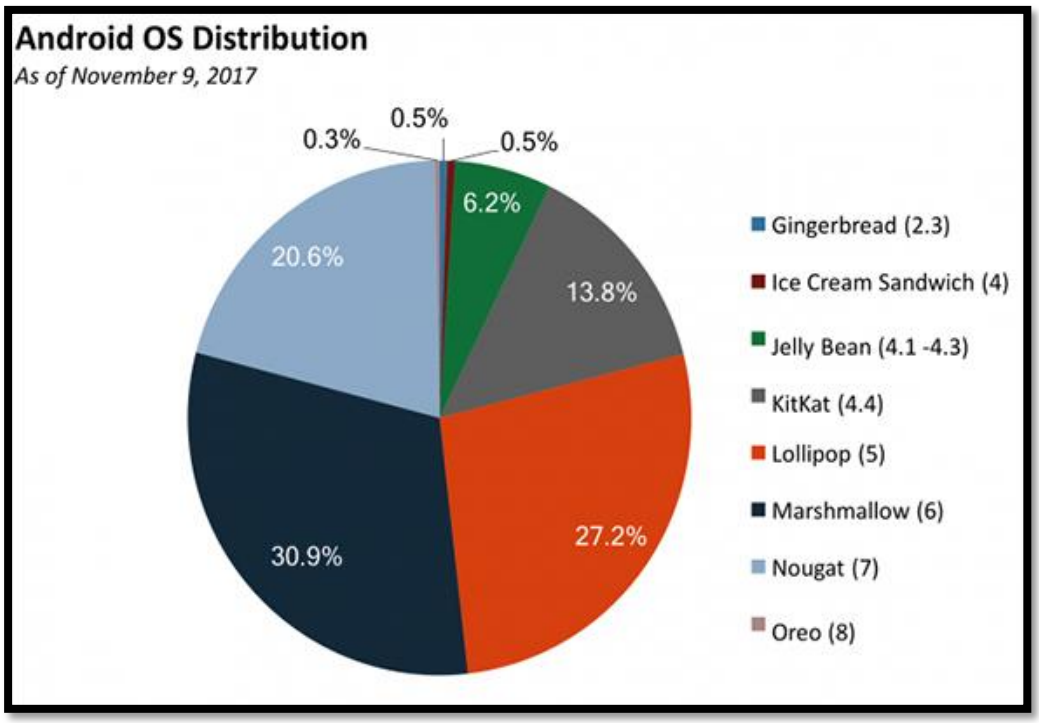


Figura 1. Distribución de versiones: [24].

2.1.5 RECUPERACIÓN DE DATOS

La falla de los dispositivos móviles es una causa común de pérdida de datos en todo el mundo. Según un estudio reciente, el 69% de los usuarios experimentó algún tipo de problema al usar su dispositivo, mientras que el 17% experimentó pérdida de datos. También se observó que

el 14% de los usuarios experimentaron fallas en sistemas de alto rendimiento como los sistemas RAID en el entorno de trabajo, lo que indica la vulnerabilidad de seguridad de los datos importantes. Estos problemas pueden deberse a fallas de hardware, daños en el software o errores humanos; por lo tanto, es fundamental utilizar soluciones de copia de seguridad y recuperación de datos para proteger la integridad de sus datos [23].

Esto demuestra que la pérdida de datos afecta no sólo a las personas sino también a los profesionales. La recuperación de datos desde dispositivos móviles incluye métodos y técnicas para mitigar las condiciones que conducen a la pérdida de datos. La principal causa de pérdida de datos en estos dispositivos son los daños en los componentes internos por impactos y caídas [25].

2.1.5.1 CAUSAS DE PERDIDA DE INFORMACIÓN

Principales causas que afectan la integridad de los datos en los sistemas de almacenamiento, junto con las consecuencias asociadas (Tabla 1) [26].

Causas	**Consecuencias**
Error de software	Sobreescritura de archivos, acceso indebido a la información
Malware	Daño en la integridad de la información.
Error humano	Eliminación de archivos, destrucción de información.
Falla eléctrica	Error en el cabezal de lectura, daño en la placa lógica
Desastres naturales	Destrucción física de la unidad de almacenamiento.

Tabla 1. Relación entre causas y consecuencias: [26].

2.1.6 SISTEMA DE ALMACENAMIENTO EN DISPOSITIVOS MÓVILES

Los smartphones incluyen una variedad de tipos de memoria con características particulares. La memoria de acceso aleatorio, también conocida como RAM, es una memoria volátil que el procesador utiliza para almacenar temporalmente datos mientras está en proceso, lo que mejora el rendimiento del dispositivo. Por el contrario, la memoria interna se ha desarrollado para gestionar, almacenar y respaldar el sistema operativo y los datos del usuario. Los dispositivos móviles utilizan memoria flash no volátil, que también se encuentra en medios de almacenamiento como memorias USB y tarjetas SD, a diferencia de los discos duros utilizados en computadoras [27].

2.1.6.1 TIPOS DE ALMACENAMIENTO

- **ALMACENAMIENTO FLASH**

  La tecnología de almacenamiento de memoria flash utiliza chips de memoria flash para escribir y almacenar datos medidos en operaciones de entrada/salida por segundo (IOPS). A diferencia de la RAM o la memoria a corto plazo, la memoria flash no es volátil, lo que significa que los datos se conservan incluso cuando se corta la energía. Este tipo de almacenamiento incluye de todo, desde unidades USB hasta soluciones empresariales, tiene un tiempo de respuesta rápido y una latencia de microsegundos, y utiliza menos energía y espacio físico que el hardware [28].

- **UFS**

  Universal Flash Storage (UFS), un estándar flash altamente confiable, se usa ampliamente en dispositivos electrónicos como tabletas, teléfonos inteligentes, cámaras digitales y otros dispositivos móviles. Tiene velocidades rápidas de lectura y escritura, alto rendimiento, escalabilidad y baja latencia para proporcionar un acceso rápido y confiable a datos y aplicaciones. Esta tecnología mejora la experiencia del usuario al permitir un uso eficiente de aplicaciones, multimedia y contenido avanzado. UFS revoluciona el almacenamiento de dispositivos móviles al ofrecer alto rendimiento y eficiencia [29].

- **EMMC**

  La tarjeta multimedia integrada es un sistema de almacenamiento no volátil que combina memoria flash y controlador en un solo componente, admite el diseño de interfaz y libera al procesador de la administración de memoria. Es una solución popular para dispositivos móviles y productos como teléfonos inteligentes y tabletas. El diseño compacto y el bajo consumo de energía de eMMC lo hacen ideal para áreas restringidas como Internet de las cosas y dispositivos portátiles. JEDEC supervisa la especificación eMMC para garantizar la compatibilidad estándar y futura [30].

2.2 MARCO TEÓRICO

2.2.1 El ESTADO ACTUAL DE LAS TÉCNICAS DE FILE CARVING Y LA NECESIDAD DE NUEVAS TECNOLOGÍAS QUE IMPLEMENTEN CARVING INTELIGENTE.

El file carving es una técnica compleja que permite la recuperación de datos sin depender de los metadatos de un sistema de archivos. A pesar de que se ha demostrado que es efectivo, todavía enfrenta desafíos que requieren optimización. El objetivo del proyecto Carving Inteligente Aplicado a Recuperación de Archivos (CIRA) es investigar y analizar varios algoritmos de cortado de archivos, consolidar y formalizar esta información y, en una etapa posterior, desarrollar una herramienta especializada en este trabajo. Este documento explica el concepto de CIRA y los avances hasta ahora [31].

2.2.2 GUÍA PRÁCTICA ABIERTA PARA EL ANÁLISIS FORENSE DIGITAL EN DISPOSITIVOS ANDROID.

Android es el sistema operativo móvil más utilizado y el favorito de los ciberdelincuentes. El análisis forense digital, que recopila y analiza datos que se pueden usar como prueba mediante métodos científicos, también se aplica a dispositivos móviles. Muchos modelos y pautas para el proceso forense creados por varias instituciones e investigadores son obsoletos, demasiado técnicos o demasiado

generales, y no consideran adecuadamente los dispositivos móviles. Se propone una guía práctica abierta para estudiantes, grupos de investigación y profesionales que deseen comenzar a aprender e investigar en esta área como respuesta [32].

2.2.3 RECUPERACIÓN DE DATOS EN DISPOSITIVOS DE ALMACENAMIENTO SSD UTILIZANDO FILE CARVING.

Este informe analiza el estado actual de recuperación de datos de los dispositivos SSD afectados por daños físicos como impactos o exposición a la humedad. Se explican escenarios comunes de pérdida de datos y se examinan varias técnicas de eliminación de datos según el tipo de pérdida de datos. Se ofrecen dos métodos de recuperación diferentes para detectar si el usuario tiene conocimiento de contenido falso. Finalmente, se analizan en detalle los avances actuales de la investigación y las perspectivas futuras sobre este tema [33]**.**

2.3 HERRAMIENTAS

Scalpel: Es una herramienta de recuperación de datos de código abierto que emplea patrones establecidos en un archivo de configuración para localizar y restaurar archivos que han sido eliminados. Resulta particularmente eficaz para la recuperación de información en sistemas de archivos que carecen de un esquema de recuperación de datos integrado. Su capacidad de definir patrones personalizados le confiere idoneidad para una diversidad de tipos de archivos y sistemas [33].

Foremost: Es otra herramienta de recuperación de archivos basada en cabeceras y pies de página. Su enfoque se centra en la recuperación de archivos utilizando firmas de datos, que son estructuras específicas que identifican el comienzo y el final de un archivo. Es útil para recuperar archivos de sistemas de archivos dañados o corruptos y puede trabajar en múltiples sistemas operativos [34].

DiskDigger: herramienta de recuperación de archivos capaz de recuperar datos borrados de diversos tipos de medios de almacenamiento, como discos duros, memorias USB, y tarjetas

de memoria Proporciona dos modalidades de escaneo: una rápida para la búsqueda de archivos eliminados recientemente y otra más exhaustiva destinada a la localización de archivos eliminados hace un periodo más prolongado o en sistemas de archivos que presentan daños [34].

PhotoRec: Es una herramienta concebida para la recuperación de fotografías y otros tipos de archivos multimedia; sin embargo, también tiene la capacidad de recuperar documentos y archivos comprimidos. Su metodología se fundamenta en la recuperación de archivos mediante el contenido en lugar de la estructura, lo que la convierte en una opción eficaz incluso en situaciones donde el sistema de archivos presenta daños o cuando los archivos han sido parcialmente sobrescritos [17].

Bulk Extractor: se trata de una herramienta avanzada que extrae información útil de discos y archivos de imagen, incluyendo correos electrónicos, URLs y otros datos contextuales. A diferencia de otras herramientas que se enfocan en la recuperación de archivos, Bulk Extractor está diseñada para realizar un análisis de datos a un nivel más profundo, con el fin de extraer información relevante que puede no estar organizadamente explicita en los archivos [19].

TSK (The Sleuth Kit): Se trata de un conjunto de herramientas y una biblioteca destinado al análisis de sistemas de archivos. Proporciona herramientas de línea de comandos para examinar y recuperar datos de sistemas de archivos, hacer análisis forenses y encontrar evidencias digitales. Es ampliamente utilizado en investigaciones forenses debido a su capacidad para manejar una variedad de sistemas de archivos y su extensibilidad [35].

Autopsy: Es una plataforma de análisis digital que utiliza The Sleuth Kit y otras herramientas para ofrecer un entorno integrado para el análisis de datos. Ofrece capacidades avanzadas de file carving, análisis de sistemas de archivos y recuperación de datos. Su interfaz gráfica facilita la visualización y el análisis de los datos recuperados, lo que lo convierte en una herramienta popular para investigadores forenses [36].

2.4 METODOLOGÍA DEL PROYECTO

2.4.1 METODOLOGÍA DE INVESTIGACIÓN

En la fase inicial del proyecto se fundamentará en una metodología descriptiva. Esta fase estará dirigida hacia el estudio y análisis minucioso de las técnicas de file carving que son aplicables a dispositivos móviles. Se llevará a cabo una revisión exhaustiva de la literatura existente, abarcando investigaciones anteriores, artículos científicos y estudios de caso que guardan relación con la recuperación de datos en dispositivos móviles [37].

El propósito de esta fase consiste en describir y documentar las técnicas más efectivas, así como sus principios operativos y las condiciones bajo las cuales funcionan de manera óptima. Esta descripción exhaustiva ofrecerá una base sólida para el desarrollo del protocolo de recuperación de datos específicos para dispositivos Android.

Una vez que se hayan identificado y descrito las técnicas de file carving más prometedoras, se avanzara a la fase experimental del proyecto. Esta fase comprenderá el desarrollo, implementación y prueba de un protocolo de recuperación de datos fundamentado en las técnicas estudiadas previamente. La metodología experimental implicara la realización de pruebas controladas en diversos dispositivos móviles, bajo diferentes escenarios de perdida de datos.

Estos escenarios abarcaran la eliminación involuntaria de archivos, la corrupción de sistemas de archivos y la fragmentación de datos. Cada experimento será elaborado con el propósito de evaluar la efectividad del protocolo en relación con la tasa de recuperación, la integridad de los datos recuperados y el tiempo requerido para la recuperación [38].

2.4.2 BENEFICIARIOS

El estudio que se realiza sobre la aplicación de técnicas de file carving para recuperar datos en dispositivos móviles, integra a grupos de estudiantes en educación media - básica o universitaria y a su vez, involucra especialistas en áreas como Seguridad Informática, Análisis Forense Digital y personal docente de la Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena.

2.4.3 VARIABLE

Lo que se plantea es reducir la pérdida de datos mediante la aplicación adecuada de técnicas de File Carving en teléfonos móviles Android, el análisis será clave para determinar la eficacia de las metodologías empleadas en la recuperación de datos, lo cual medirá la efectividad de las técnicas evaluando la cantidad de información recuperada en distintos escenarios.

2.4.4 TECNICAS DE RECOLECCION DE INFORMACIÓN

TÉCNICAS

- **Estado del arte, fuentes bibliográficas**

INSTRUMENTO

Con el fin de asegurar la calidad y pertinencia de los datos obtenidos, se realizarán entrevistas con el personal docente de la Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena. Dichas entrevistas serán fundamentales para adquirir un entendimiento profundo del panorama actual respecto al tema de investigación, garantizando de este modo que la investigación se fundamente en un conocimiento sólido y actualizado de las prácticas y perspectivas en el uso de tecnologías relevantes.

2.4.5 METODOLOGÍA DE DESARROLLO DEL PROYECTO

Se empleará la siguiente metodología UNE 71506/2013 como enfoque para llevar a cabo las pruebas experimentales, por la cual es una guía para recolectar y archivar evidencia.

UNE 71506:2013 que será base esencial para la realización de las pruebas experimentales para el análisis forense de evidencias digitales. Este marco referencial proporciona un marco estructurado para llevar a cabo investigaciones forenses sobre dispositivos digitales, computadores, teléfonos móviles, tables, dispositivos de almacenamiento USB, entre otros [39].

El estándar RFC (Request For Comments) 3227 es un documento que establece las directrices fundamentales para la recopilación y conservación de pruebas digitales, convirtiéndose en un estándar ampliamente reconocido para dichos procedimientos. Este documento detalla un

procedimiento para la recolección de evidencias que asiste al perito informático en la adquisición y catalogación de las pruebas digitales [40].

FASE I: PRESERVACIÓN - En esta fase, se garantiza la conservación de todas las evidencias, tanto digitales como físicas, evitando cualquier tipo de perdida. Se procede a la verificación de los dispositivos o elementos sometidos a análisis y se asegura la validez legal de las pruebas recolectadas. Se implementan medidas para prevenir la alteración, daño o manipulación de la información, ya sea por acciones humanas o por eventos naturales, en caso de ser necesario.

Fase II: ADQUISICIÓN - Durante esta etapa, se llevará a cabo la recopilacion de las evidencias, tanto físicas como digitales, verificando la autenticidad de los dispositivos que están sujetos a análisis. Se adquirirán las herramientas necesarias, tanto de hardware como de software, para la recolección de datos. Asimismo, se llevará a cabo una copia de seguridad de la evidencia encontrada para preservar la integridad de la evidencia original.

Fase III: ANÁLISIS - Durante esta fase, se utilizan herramientas especializadas para llevar a cabo el análisis forense. Se selecciona el método de investigación más adecuado para el caso en cuestión. Se implementan medidas para asegurar que la integridad de la información extraída de las pruebas no se vea comprometida en ningún momento del proceso.

Fase IV: DOCUMENTACIÓN - Dentro de esta fase, se procede a la elaboración de la documentación a través de un informe pericial que describe detalladamente el proceso de obtención a pruebas. Se registran los datos obtenidos mediante fotografías o capturas de pantalla. Asimismo, se confecciona un informe técnico que sintetiza las conclusiones derivadas del proceso llevado a cabo.

FASE V: PRESENTACIÓN - Durante esta fase, se exponen los resultados obtenidos del análisis forense. Se realiza una presentación clara y convincente, donde se detallan las herramientas y metodologías empleadas durante todo el proceso. Se explican con detalle las conclusiones previamente expuestas en la fase de documentación, garantizando que sean comprendidas de manera accesible para el público objetivo.

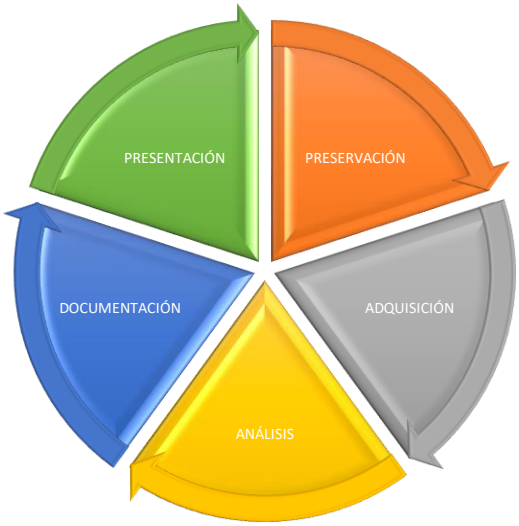


Figura 2. Metodología de desarrollo: Autor.

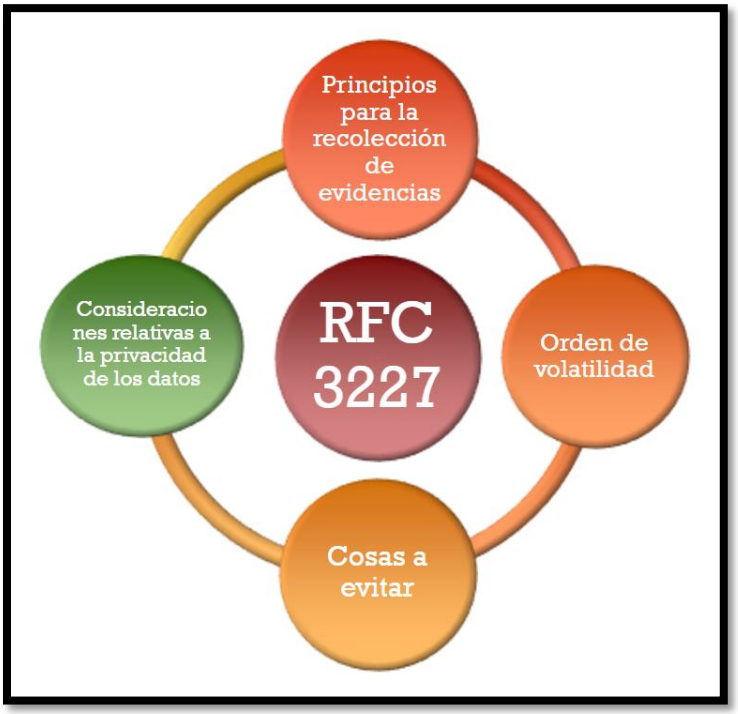


Figura 3. Estándar RFC 3227: [41] .

CAPÍTULO III

3 PROPUESTA

3.1 DESARROLLO

3.1.1 FASE I: ADQUISICIÓN

En esta fase se desarrolla la investigación de las técnicas de File Carving reconocidas para la clasificación a través de parámetros de descripción óptimos para la correcta información y que sea necesaria para desembocar las técnicas en el estudio de la parte práctica. Se da con detalle el siguiente cuadro con la información más relevante de las técnicas correspondiente a File Carving en la recuperación de datos.

CUADRO COMPARATIVO DE TECNICAS DE FILE CARVING DE INFORMATICA FORENSE

Técnica de File Carving	**Precisión de Recuperación**	**Velocidad del Proceso**	**Compatibilidad de Formatos**	**Integridad de los Datos**	**Uso de Recursos del Sistema**	**Facilidad de Implementación**	**Eficiencia en Archivos Corruptos**
Carving Basado en Cabeceras y Pies	Alta, ya que usa delimitadores específicos para identificar archivos completos.	Relativamente rápido, ya que busca delimitadores específicos.	Compatible con formatos que tienen cabeceras y pies definidos (e.g., JPEG).	Mantiene la integridad si el archivo no está fragmentado.	Bajo consumo de recursos, ya que no requiere análisis profundo.	Fácil de implementar con herramientas simples y automatizadas.	Baja, los archivos corruptos o incompletos pueden ser difíciles de recuperar.

Carving Basado en la Estructura del Sistema de Archivos	Muy alta, recupera archivos respetando la estructura del sistema de archivos.	Moderada, depende del tamaño y complejidad del sistema de archivos.	Alta compatibilidad con muchos tipos de archivos soportados por el sistema.	Alta integridad, preserva el contenido exacto del archivo si no está dañado.	Consumo moderado de recursos, requiere más procesamiento que otras técnicas.	Moderada, depende de la familiaridad con el sistema de archivos específico.	Alta, puede identificar y recuperar archivos parcialmente dañados.
Carving Basado en Firmas	Alta, busca patrones únicos de bytes en los archivos.	Moderada, puede tardar si busca muchas firmas diferentes.	Amplia compatibilidad, basado en patrones de muchos tipos de archivos.	La integridad puede verse afectada si se encuentran archivos fragmentados.	Requiere más recursos, especialmente en sistemas con muchos archivos.	Relativamente fácil si se dispone de las firmas correctas para los archivos.	Moderada, depende de si las firmas pueden ser identificadas en archivos corruptos.
Carving Fragmentado	Baja precisión si el archivo está muy fragmentado.	Lento, requiere reconstrucción de fragmentos de archivos.	Compatible con cualquier archivo fragmentado.	Puede comprometer la integridad, ya que reconstruir fragmentos es complicado.	Alto consumo de recursos debido a la reconstrucción fragmentaria.	Difícil de implementar, requiere conocimientos avanzados en reconstrucción.	Alta en teoría, pero en la práctica puede ser poco fiable con archivos gravemente fragmentados o corruptos.
Carving Basado en Hash	Muy alta, verifica la exactitud usando hashes de los archivos.	Moderada, depende de la cantidad de archivos y de su tamaño.	Alta compatibilidad con cualquier archivo que tenga un hash conocido.	Alta integridad al verificar archivos con hashes preexistentes.	Requiere recursos considerables para comparar los hashes y archivos.	Requiere herramientas específicas y bases de datos de hashes predefinidos.	Alta, siempre que el hash de referencia sea exacto.

Tabla 2. Comparación de técnicas de File Carving

3.1.2 FASE II: PREPARACIÓN

En esta fase de la investigación sobre las técnicas del tallado de información, se profundiza en lo esencial que son para la recuperación de datos en sistemas de archivos como NTFS y ext4, entre otros. El objetivo es crear un cuadro descriptivo de cada técnica de file carving, analizando su aplicación en la recuperación de datos en diversos sistemas de archivos.

Adicionalmente, se abordan los pasos de preparación necesarios para el proceso de root (parchado) en dispositivos móviles, lo cual facilitará el acceso total al sistema y permitirá aplicar técnicas avanzadas de recuperación y análisis de datos.

Información general del dispositivo de estudio

- **Galaxy A10**
- **Modelo SM-A105M**
- **Número de serie: R58MXXXXXXX**
- **Versión de Android: 11**
- **Versión de One UI: 3.1**
- **Tarjeta SD 8 GB**
- **Almacenamiento Interno 32 GB**

El proceso de root en un dispositivo móvil consiste en otorgar acceso de administrador para habilitar permisos exclusivos que permitan el análisis de las particiones y carpetas del sistema, cabe destacar que este procedimiento varía según el modelo y la marca del dispositivo, en el caso de dispositivos Android, especialmente la marca Samsung Galaxy, es recomendable debido a la disponibilidad de herramientas de código abierto que son accesibles y relativamente fáciles de usar, sin embargo, se debe proceder con precaución, ya que el root puede invalidar la garantía y exponer el dispositivo a riesgos de seguridad (Preparación Proceso ROOT).

CUADRO DESCRIPTIVO DE HERRAMIENTAS PARA ANÁLISIS DE PRUEBAS

HERRAMIENTA	TIPO DE DISPOSITIVO	COMPATIBILIDAD DE SISTEMAS DE ARCHIVOS	TIPO DE ARCHIVOS SOPORTADOS	FACILIDAD DE USO	REQUERIMIENTOS DEL SISTEMA
SCALPEL	Discos duros, sistemas de archivos variados	Funciona bien en sistemas de archivos sin recuperación integrada.	Archivos definidos por patrones personalizados.	Moderada, requiere configuración de patrones.	Requerimientos mínimos, funciona en sistemas ligeros.
FOREMOST	Discos duros, USB, tarjetas de memoria	Compatible con múltiples sistemas de archivos.	Archivos de diversos tipos, basado en firmas.	Fácil de usar con configuraciones predeterminadas.	Bajo, pero puede requerir más para escaneos profundos.
HxD Editor Hexadecimal	Dispositivos de almacenamiento, archivos individuales	Compatible con cualquier sistema de archivos; permite edición directa de sectores.	Cualquier tipo de archivo; soporte de análisis hexadecimal.	Moderada, requiere conocimientos básicos de edición hexadecimal.	Requerimientos mínimos; ideal para sistemas ligeros.
PHOTOREC	Discos duros, USB, tarjetas de memoria	Funciona en la mayoría de sistemas de archivos.	Principalmente archivos multimedia, pero también documentos.	Moderada, interfaz de línea de comandos.	Requerimientos mínimos, ideal para sistemas de bajo rendimiento.
DR. FONE	Dispositivos móviles (Android, iOS)	Compatible con sistemas de archivos móviles (Android, iOS).	Fotos, videos, contactos, mensajes, y otros datos móviles.	Muy fácil, interfaz gráfica intuitiva.	Requerimientos moderados, ideal para sistemas de gama media y alta.
AUTOPSY	Discos duros, servidores	Compatible con diversos sistemas de archivos.	Amplia variedad de tipos de archivos.	Muy fácil, interfaz gráfica intuitiva.	Moderados, pero más eficaces en sistemas con más recursos.

Tabla 3. Descripción de herramientas Forenses

3.1.3 FASE III: ANÁLISIS

En esta fase, se utilizarán técnicas de file carving en cuatro escenarios simulados de pérdida de datos en un dispositivo Android. Las herramientas **HxD Editor Hexadecimal**, **PhotoRec**, **Autopsy**, **Scalpel** y **Foremost** se emplearán junto a técnicas de carving según estructura del sistema, firmas y fragmentación, con el objetivo de recuperar archivos específicos como imágenes JPG, documentos PDF y videos MOV en cada caso de prueba.

ESCENARIOS DE RECUPERACIÓN DE DATOS MEDIANTE TECNICAS FILE CARVING EN DISPOSITIVO ANDROID

#	ESCENARIO	TECNICA	HERRAMIENTA	OBJETIVO	RESULTADOS OBTENIDOS	DETALLE
1	**Tarjeta SD formateada accidentalmente – Recuperar Imágenes formato JPG**	**Carving basado en la estructura del Sistema de Archivos**	**HxD Editor Hexadecimal**	**Recuperar imágenes en formato JPG de la tarjeta SD después de un formateo accidental.**	**Recuperación de 4 imágenes JPG completas según el nivel de fragmentación.**	ESCENARIOS DE PRUEBA - 1
2	**Tarjeta SD formateada accidentalmente – Recuperar en su totalidad los archivos existentes**	**Carving Basado en Firmas**	**PHOTOREC**	**Recuperar los archivos que existieron en el SD imágenes, doc, entre otros.**	**Se ha recuperado un total de 10500 archivos incluyendo fotos, videos, pdf, entre otros. Clasificado los archivos en 20 carpetas cada una tiene aproximadamente 520 archivos**	ESCENARIOS DE PRUEBA - 2

3	**Recuperar documentos PDF de la carpeta WhatsApp Documentos**	**Carving Fragmentado** **Carving Basado en Cabeceras y Pies**	**AUTOPSY**	**Recuperar los archivos pdf de la carpeta documentos de WhatsApp**	**Se ha recuperado un total de 3 archivos pdf en donde se ha clasificado por tipo de archivo como también conocer las imágenes e información que cuenta el documento – 16 imágenes – 1 correo electrónico, entre otros datos personales**	ESCENARIOS DE PRUEBA - 3
4	**Recuperar archivos de videos de la carpeta DCIM**	**Carving Basado por firmas**	**SCALPEL** **FOREMOST**	**Recuperar archivos de videos.mov de la carpeta media DCIM**	**Se ha recuperado un total de 6 videos de la copia de seguridad de DCIM y como resultado un reporte del análisis**	ESCENARIOS DE PRUEBA - 4

Tabla 4. Escenarios de pruebas para la recuperación de datos

3.1.4 FASE IV: DOCUMENTACIÓN

La fase de documentación del proceso en este manual tiene como objetivo proporcionar un marco claro y detallado sobre la aplicación de técnicas de file carving para la recuperación de datos en dispositivos móviles Android.

En este contexto, el manual incluye muchas cosas importantes que deben aplicarse para una análisis efectivo y ético. Se divide en varias secciones como introducción, que explica el contexto del estudio; el alcance y objetivo, que definen los límites, metas de la recuperación de datos y el análisis de escenarios, detalla ejemplos prácticos y la evaluación de técnicas. También incluye secciones sobre herramientas recomendadas, mejores prácticas durante la recuperación y la importancia de la recuperación de datos. Además, se considera el cumplimiento ético y legal, el uso de herramientas validadas, y la gestión adecuada de evidencias (Ver anexo 4: Documentación).

Por lo tanto, este manual documenta todo el proceso de recuperación de datos desde la selección de herramientas hasta la verificación y manejo ético de la evidencia, asegurando que cada paso se ejecute de manera rigurosa y conforme a las mejores prácticas en el campo.

CONCLUSIONES

La recopilación de datos es esencial en el proceso de recuperación de información, ya que ofrece el contexto requerido para elegir las herramientas, el entorno de trabajo y las técnicas más adecuadas, permite tener un enfoque claro y eficiencia al tiempo que reduce el riesgo de perder otros datos durante el proceso.

El proceso de investigación, permitió acceder en su totalidad al sistema operativo en situaciones específicas. Este procedimiento habilitó la ejecución de operaciones avanzadas, porque estaban restringidas por las limitaciones del sistema.

Acceder a las particiones protegidas que almacenan datos de aplicaciones y archivos del sistema, resultó esencial para alcanzar los objetivos planteados en la recuperación de información.

El uso de técnicas avanzadas resulta importante ya que ayuda a extraer y reconstruir datos eliminados o dañados sin depender de la estructura original del sistema de archivos. Esto resulta especialmente crucial en escenarios donde los metadatos o las particiones del dispositivo han sido modificados o eliminados. A pesar de sus limitaciones, el file carving se confirma como una técnica sólida que al combinarse con herramientas especializadas y buenas prácticas, puede ofrecer resultados significativos tanto en investigaciones forenses como en la recuperación de información crítica.

RECOMENDACIONES

Tomar precauciones relacionadas con la realización de root, ya que puede atentar contra la seguridad del dispositivo cuando se administra de manera inapropiada, otra desventaja es que, en numerosas ocasiones, la realización de root implica la perdida de la garantía ofrecida por el fabricante.

Desarrollar continuamente algoritmos más eficaces y confiables para aumentar su precisión y adaptarse al comportamiento en entornos cada vez más complejos. Permitiendo mejorar los procesos de recuperación de datos y garantizar una efectividad mayor ante los retos de las nuevas tecnologías y formas de almacenamiento.

Ampliar el análisis sobre el impacto de la fragmentación de archivos y los sistemas de gestión de memoria de los dispositivos móviles en la efectividad de las técnicas de file carving. Este enfoque optimizará el proceso de recuperación identificando áreas de mejora y creando soluciones a las limitaciones existentes.

BIBLIOGRAFÍAS

[1] Marco Espinoza M., «Informática forense: una revisión sistemática de la literatura,» Universidad Ecotec, Guayaquil - Ecotec, 2019.

[2] IBM, «IBM,» ¿Qué es la recuperación de datos?, [En línea]. Available: https://www.ibm.com/mx-es/topics/data-recovery. [Último acceso: 02 Septiembre 2024].

[3] Morishita K. , Suzuki K. & Sato H. , «Fragmentation impact on file carving in mobile device,» Journal of digital forensics, security and law, 2021.

[4] Carlos Maldonado E. , «Herramientas forenses de análisis digital para la obtención de información aplicado a ordenadores y dispositivos móviles,» Universidad Rafael Landívar, QUETZALTENANGO - Guatemala, 2020.

[5] Luis Borja B. , «Creación de una guía de recuperación de datos utillizando la técnica forense file carving para ordenadores Windows,» Universidad Nacional de Chimborazo, Riobamba - Ecuador, 2021.

[6] Carlos Pita V., «Análisis Forense de evidencias digitales en entornos Icloud,» Universidad Estatal Península de Santa Elena, Santa Elena - Ecuador , 2024.

[7] Jorge M. , Karina S. , Pablo H., «Estudi y Análisis de Evidencia Digitales en Teléfonos Celulares con Tecnologia GSM para procesos Judiciales,» Facultad de Ingeniería Eléctrica y Electrónica, Escuela Pólitécnica Nacional, 2012.

[8] IBM, «Sistemas de archivos,» [En línea]. Available: https://www.ibm.com/docs/es/aix/7.2?topic=management-file-systems. [Último acceso: 09 Septiembre 2024].

[9] IBM, «¿Qué es la informática forense?,» [En línea]. Available: https://www.ibm.com/es-es/topics/computer-forensics. [Último acceso: 25 Septiembre 2024].

[10] Coursera Staff, «¿Qué es la informática forense? Tipos, técnicas y carreras,» 22 Abril 2024. [En línea]. Available: https://www.coursera.org/mx/articles/computer-forensics. [Último acceso: 25 Septiembre 2024].

[11] Lucas Paus & Mario Micucci, «5 fases fundamentales del análisis forense digital,» 01 Diciembre 2023. [En línea]. Available: https://www.welivesecurity.com/es/recursos-herramientas/5-fases-fundamentales-del-analisis-forense-digital/. [Último acceso: 25 Septiembre 2024].

[12] López Delgado M., «Análisis Forense Digital - Segunda Edición,» Hackers & Seguridad , 2007.

[13] Muñoz Bermudez A., «Informática forense: seis aspectos para investigar y resolver delitos cibernéticos,» 07 Febrero 2024. [En línea]. Available: https://es.linkedin.com/pulse/inform%C3%A1tica-forense-seis-aspectos-para-investigar-y-mu%C3%B1oz-bermudez-32iee. [Último acceso: 25 Septiembre 2024].

[14] Miguel J., «Análisis Forense Digital,» 21 Marzo 2020. [En línea]. Available: https://es.linkedin.com/pulse/an%C3%A1lisis-forense-digital-miguel-jimenez. [Último acceso: 25 Septiembre 2024].

[15] CertJoin, «¡Tu puerta de entrada al mundo de la informática forense!,» 06 Marzo 2024. [En línea]. Available: https://es.linkedin.com/pulse/tu-puerta-de-entrada-al-mundo-la-inform%C3%A1tica-forense-certjoin-5fp9f. [Último acceso: 25 Septiembre 2024].

[16] L. F. B. Brito, «CREACIÓN DE UNA GUÍA DE RECUPERACIÓN DE DATOS UTILIZANDO LA TÉCNICA FORENSE FILE CARVING PARA ORDENADORES WINDOWS,» FACULTAD DE INGENIERÍA CARRERA DE SISTEMAS Y COMPUTACIÓN, Riobamba, 2021.

[17] J. W. Bruno Constanzo, «El Estado Actual de las Técnicas de File Carving y la Necesidad de Nuevas Tecnologías que Implementen Carving Inteligente,» COPITEC/FUNDETEC, 2012.

[18] Ana H. , Martín C. , Bruno C. , Hugo C. , Julián W. , Sabrina B. , María F. , Pablo C. , Ariel P. , Juan I. , Fernando G. , Juan A. , Gonzalo M. , Santigo T. , Luciano N., «El Rastro Digital del Delito - Aspectos Técnicos, Legales y Estrategicos de la Informática Forense,» Universidad FASTA - Facultad de Ingeniería, Mar de plata - Argentina , 2017.

[19] D. Pereyra y J. Eterovic, «Desarrollo de una Guía de Asistencia para el Análisis Forense Informático en un Ambiente Piloto,» Facultad de Informática, Ciencias de la Comunicación y Técnicas Especiales, Morón, 2013.

[20] UNIR - La Universidad en Internet, «¿Qué es un análisis forense digital y cómo se realiza?,» [En línea]. Available: https://colombia.unir.net/actualidad-unir/analisis-forense-digital/. [Último acceso: 14 Octubre 2024].

[21] Alberto Cruz, «Android: El sistema operativo móvil de Google,» 25 Abril 2023. [En línea]. Available: AfmBOop8O7n6oxN9DLKa4DK2qhfu4Av2wof5na3yuqsTzg3UGwswg6F1. [Último acceso: 14 Octubre 2024].

[22] Open Handset Alliance, «Android,» [En línea]. Available: https://www.openhandsetalliance.com/android_overview.html. [Último acceso: 14 Octubre 2024].

[23] Alejandro Chávez, «¿Qué es un Sistema RAID y por qué es una Solución Viable para la Gestión de Datos?,» 01 Octubre 2024. [En línea]. Available: https://fixdata.com.mx/que-es-un-sistema-raid-y-por-que-es-una-solucion-viable-para-la-gestion-de-datos/. [Último acceso: 14 Octubre 2024].

[24] Anand Mahajan, «Android Vs. iOS : Which One to Consider First?,» 03 Marzo 2020. [En línea]. Available: https://customerthink.com/android-vs-ios-which-one-to-consider-first/. [Último acceso: 14 Octubre 2024].

[25] G. P. C. S. G. G. T. D. J. &. P. D. Ninahualpa, Restoring data in solid state devices damaged by crushing and falling, using file carving technique, Riobamba: UNIVERSIDAD NACIONAL DE CHIMBORAZO , 2018.

[26] B. B. L. F. Molina Granja Fernando Tiverio, « Creación de una guía de recuperación de datos utillizando la técnica forense file carving para ordenadores Windows,» Riobamba, Universidad Nacional de Chimborazo, Riobamba, 2021.

[27] Evision Systems, «Tipos de memoria en los smartphones,» [En línea]. Available: https://evision-webshop.es/blog/tecnologias-de-almacenamiento-en-smartphones#:~:text=A%20diferencia%20de%20los%20ordenadores,con%20memoria%20ampliable%20(SD).. [Último acceso: 14 Octubre 2024].

[28] IBM, «¿Qué es el almacenamiento flash?,» [En línea]. Available: https://www.ibm.com/mx-es/topics/flash-storage. [Último acceso: 14 Octubre 2024].

[29] Sebastián Romero, «¿Qué es UFS o Almacenamiento Flash Universal?,» 20 Enero 2022. [En línea]. Available: El estándar avanzado de almacenamiento flash Universal Flash Storage (UFS) se encuentra en dispositivos electrónicos como tablets, smartphones, cámaras digitales y otros dispositivos móviles. Se distingue por ofrecer una alta velocidad de lectura y escrit. [Último acceso: 14 Octubre 2024].

[30] Kingston, «Componente de eMMC - Tarjeta multimedia integrada para fabricantes de dispositivos,» [En línea]. Available: https://www.kingston.com/es/embedded/emmc-embedded-flash#:~:text=La%20eMMC%20es%20un%20componente,numerosas%20aplicaciones%20industriales%20e%20integradas.. [Último acceso: 14 Octubre 2024].

[31] Julian Bruno C., «El Estado Actual de las Técnicas de File Carving y la Necesidad de Nuevas Tecnologías que implemente Carving Inteligente,» Universudad FASTA , 2020.

[32] Johan R. , Dewar R. , Cesar D. , «Guía Práctica abierta para el análisis forense digital en dispositivos android,» RISTI , 2018.

[33] Geovanni Ninahualpa Quiña, , Sang Guun Yoo, , Teresa Guarda, «Recuperación de Datos en Dispositivos de Almacenamiento SSD Utilizando File Carving,» Revista Ibérica de Sistemas e Tecnologias, 2016.

[34] Ana Haydée Di Iorio, Martín Castellote, Ariel Podestá, Fernando Greco, Bruno Constanzo, Julián Waimann, «EL FRAMEWORK CIRA, UN APORTE A LAS TÉCNICAS DE FILE CARVING,» Universidad Fasta, Mar de Plata, 2013.

[35] K. Morishita, K. Suzuki, y H. Sato, «Fragmentation impact on file carving in mobile device,» Journal of Digital Forensics, Security and Law, 2021.

[36] Ana Haydée Di Iorio, Martín Castellote, Ariel Podestá, Fernando Greco¸ Bruno Constanzo, Julián Waimann, «Un framework de file Carving como solución a una necesidad detectada en la generación de un PURI,» Journal CADI, 2013.

[37] Salvador, José Antonio Pérez, «ELABORACIÓN DE UNA METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES BASADOS EN ANDROID,» Barcelona, 2017.

[38] Brito, Luis Felipe Borja, «CREACIÓN DE UNA GUÍA DE RECUPERACIÓN DE DATOS UTILIZANDO LA TÉCNICA FORENSE FILE CARVING PARA ORDENADORES WINDOWS,» FACULTAD DE INGENIERÍA CARRERA DE SISTEMAS Y COMPUTACIÓN, Riobamba, 2021.

[39] G. Lab, «peritos informaticos,» [En línea]. Available: https://peritosinformaticos.es/iso-71506-2013-perito-informatico/#:~:text=La%20norma%20UNE%2071506%2F2013,de%20la%20norma%20UNE%2071505.. [Último acceso: 2 Octubre 2023].

[40] MOLINA, ANTHONY ALEXANDER GUZMÁN, «IMPLEMENTACIÓN DE HERRAMIENTAS PARA LA EXTRACCIÓN DE EVIDENCIA DIGITAL,» Escuela Politécnica Nacional, Quito, 2023.

[41] R. M. Arnao, «Análisis Forense,» SlidePLayer, 2016. [En línea]. Available: https://slideplayer.es/slide/1069548/. [Último acceso: 25 10 2024].

[42] J. A. P. Salvador, «ELABORACIÓN DE UNA METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES BASADOS EN ANDROID,» Barcelona, 2017.

[43] R. H. Carlos Agualimpia, «Análisis forense en dispositivos móviles con Symbian OS,» Documento de maestría, Bogotá, 2009.

ANEXOS

ANEXO #1
FASE: PREPARACIÓN

Proceso ROOT

Preparación: Celular Acceso (ROOT)

1. Activar las opciones del programador de nuestro dispositivo, verificamos si esta activado, luego ingresamos activamos las siguientes opciones: Desbloqueo de OEM – Depuración por USB.

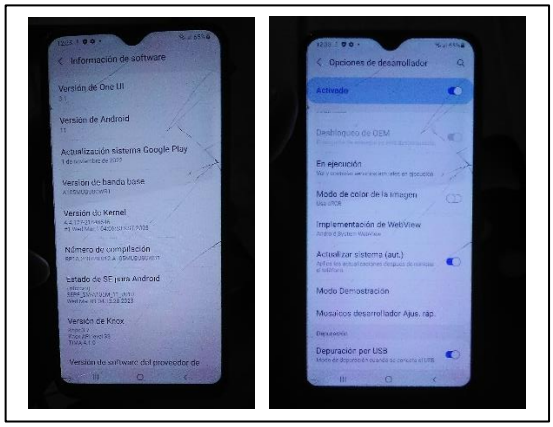


Imagen 1. Activar Opciones del desarrollador - Habilitar las opciones

2. Verificar que este actualizado el Software de nuestro dispositivo Movil.

Imagen 2. Software actualizado - Dispositivo Reiniciando.

3. Desbloquear el bootloader del dispositivo, presionando la tecla de subir volumen y bajar volumen, a su vez conectarlo mediante el cable USB, ya sea cargando o conectado a una PC, no omitir este paso, caso contrario no se podrá acceder al modo descarga del dispositivo.

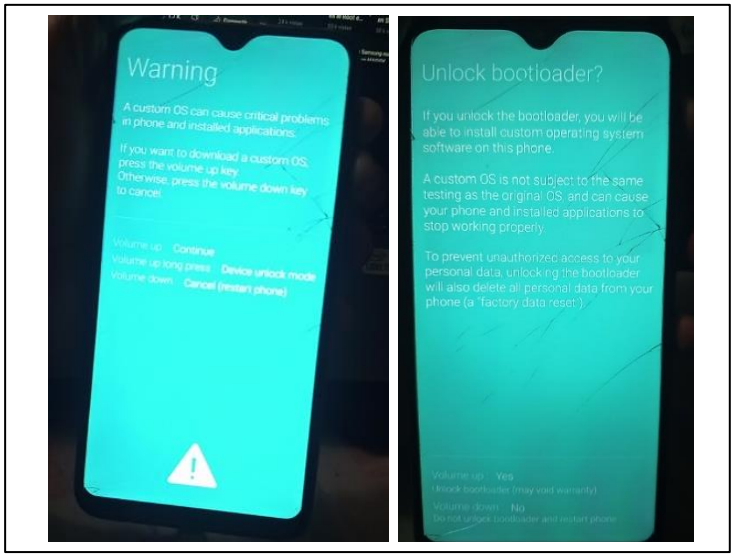


Imagen 3. Modo Descarga - Desbloquear Bootloader.

4. Aquí se muestra que en nuestro dispositivo a sido desbloqueado el bootloader, el cual permitira que tengamos acceso a las particiones del dispositivo.

Imagen 4. Dispositivo Reiniciando - Sistema Cargando.

5. Descargar el Firmware del dispositivo, cabe recalcar que dependerá el modelo del dispositivo, en este caso se usó un **SAMSUNG GALAXY A10**, luego pasamos el archivo al almacenamiento del dispositivo, conectando el cable de datos a la computadora.

Nombre	Tipo	Tamaño comprimido	Protegido ...	Tamaño	Relación	Fecha de modificación
_FirmwareInfo_Samfw.com	Documento de texto	1 KB	No	1 KB	62%	9/9/2021 0:21
AP_A105MUBU8CWB1_CL2184854...	Archivo MD5	3.284.980 KB	No	3.851.321 KB	15%	7/3/2023 0:31
BL_A105MUBU8CWB1_CL21848546...	Archivo MD5	2.136 KB	No	2.401 KB	12%	7/3/2023 0:31
CP_A105MUBU8CWB1_CP2379209...	Archivo MD5	20.391 KB	No	24.671 KB	18%	7/3/2023 0:35
CSC_OMC_OWA_A105MOWA8CWB...	Archivo MD5	148.634 KB	No	163.581 KB	10%	7/3/2023 0:35
HOME_CSC_OMC_OWA_A105MOW...	Archivo MD5	148.620 KB	No	163.561 KB	10%	7/3/2023 0:35

Imagen 5. Firmware Descargado.

6. Se instala la app **Magisk**, luego saldrá que debemos seleccionar un método de instalación, presionamos, nos dirigirá a la búsqueda de un archivo, aquí escogeremos el archivo **AP**, le damos a instalar.

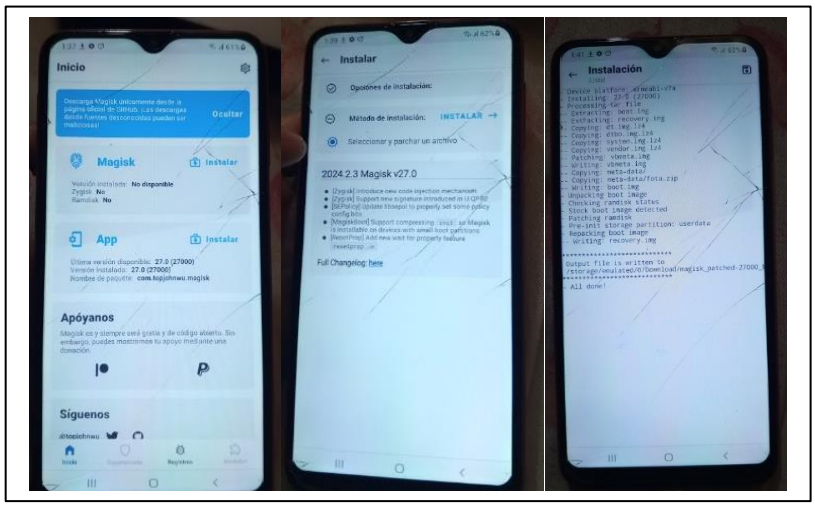


Imagen 6. Parchar nuestro dispositivo móvil con Magisk.

7. Descargar la aplicación Odin desde el siguiente link: https://odin-samsung.com/es/odin-3-14-4-odin-descarga-todas-las-versiones-para-samsung-flash.html

La ejecutamos como administrador para trabajar en la transición de archivos al dispositivo móvil.

8. Seleccionamos y verificamos en Options que tengan marcado lo siguiente: Auto Reboot – F.Reset Time

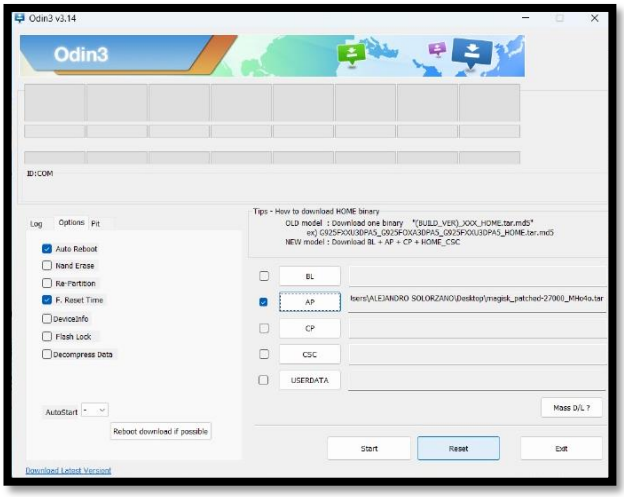


Imagen 7. Verificar las opciones marcadas.

9. Para hacer la transición del archivo debemos acceder en el dispositivo al modo descarga, presionando volumen abajo y volumen arriba, a su vez conectarlo a la PC, damos click en Start.

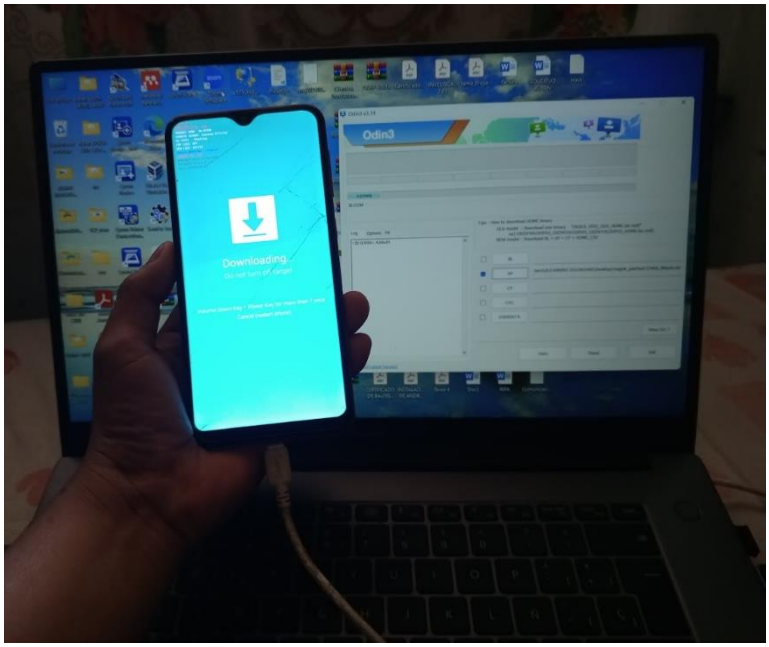


Imagen 8. Transferencia del archivo al dispositivo móvil.

10. Luego se Reiniciara el dispositivo procedemos abrir la aplicación de **Magisk**, si no le aparece la vuelve a descargar, verificamos que nos salga instalada, ademas descargar de la Play Store la app **Root Checker Basic**, verificamos el acceso root dentro de nuestro dispositivo.

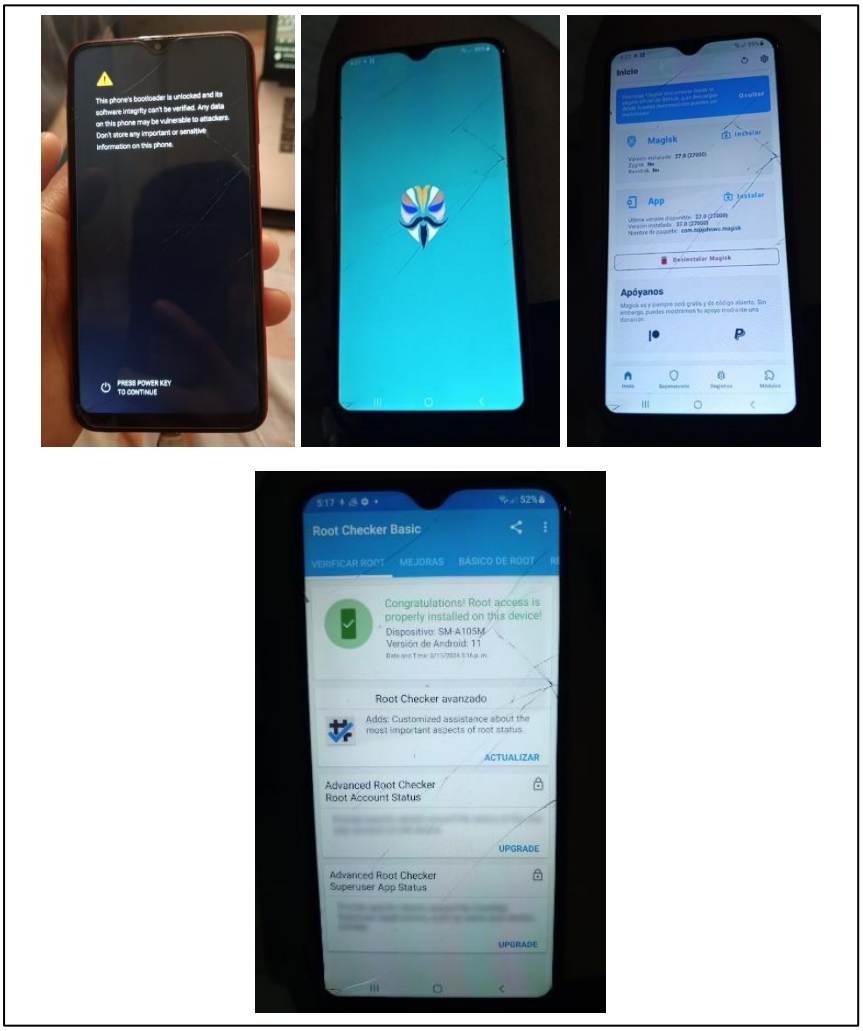


Imagen 9. Proceso ROOT terminado

Con este proceso obtenemos acceso root en nuestro dispositivo movil, para poder acceder a las particiones del dispostivo, posrteriormente crear una imagen de disco a las carpetas y poder realizar un analisis mediante las herramientas donde se aplicaran las tecnicas mas efectivas para la recuperacion de archivos en el celular.

ANEXO #2
MANUAL DE INSTALACIÓN HERRAMIENTAS

Instalación de PhotoRec

1. Descargar desde el siguiente link: https://www.tenorshare.net/ads/ultdata-windows-mac-a.html?gad_source=1&gclid=Cj0KCQiAire5BhCNARIsAM53K1hLwXH9pptnzKTX7XH5sjXd2A98dA66rz6XRdPgTITJaOwOFXXTgvMaAi3SEALw_wcB

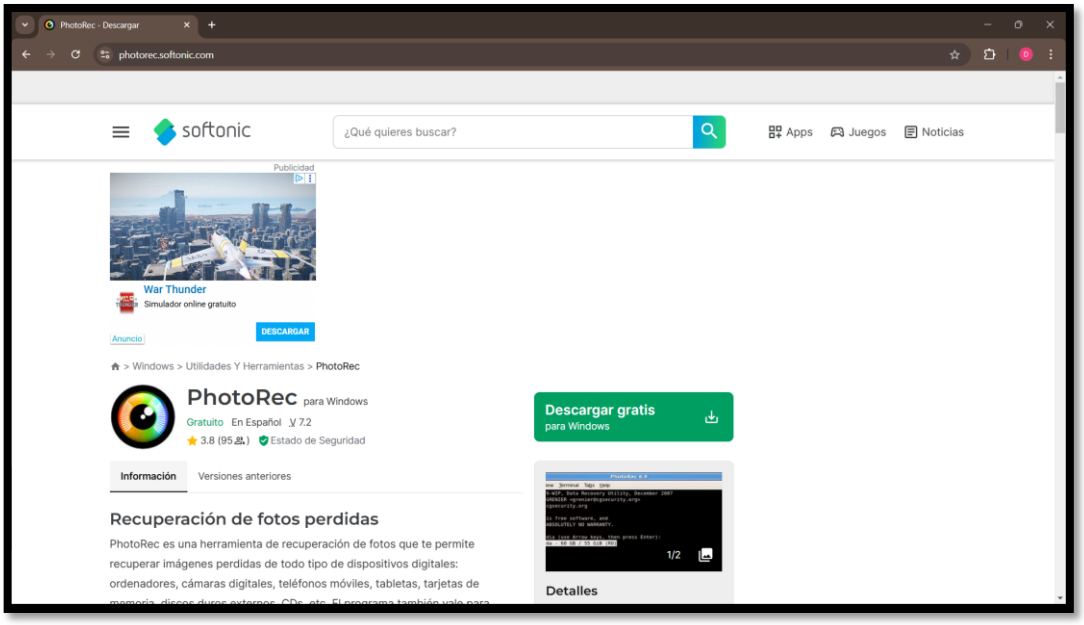


Imagen 10. Sitio PhotoRec

2. Abrir el archivo y ejecutar photorec_win.

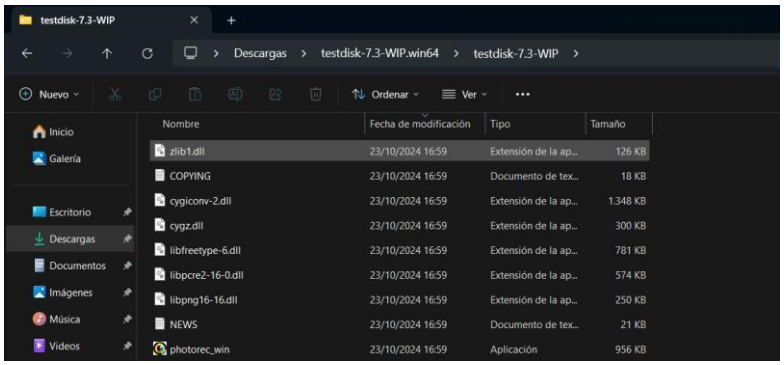


Imagen 11. Abrir PhotoRec

3. Interfaz de la Herramienta, para analizar y poder recuperar los archivos borrados.

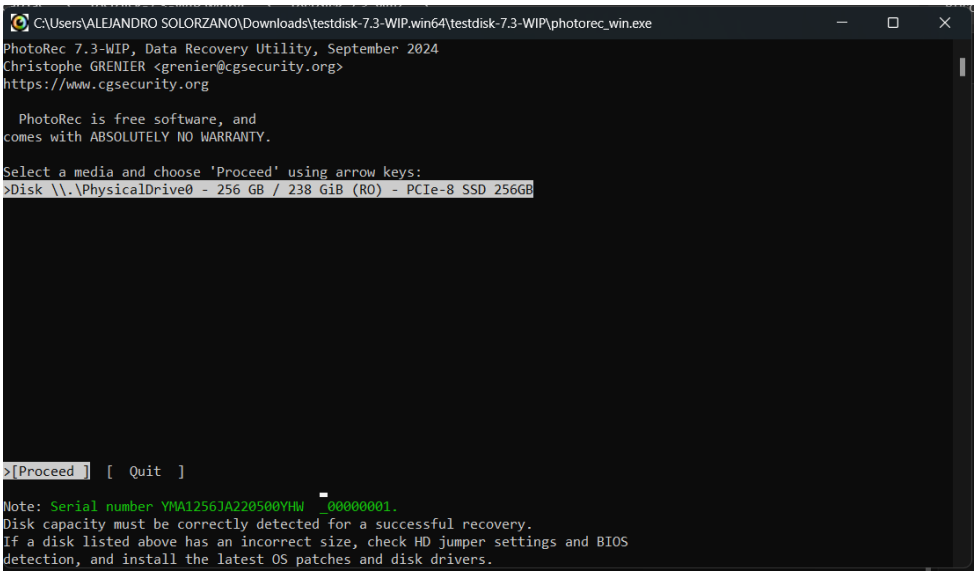


Imagen 12. Herramienta PhotoRec

Instalación de Editor Hexadecimal (HxD)

1. Descargar desde el siguiente link: https://hxd.es.download.it/

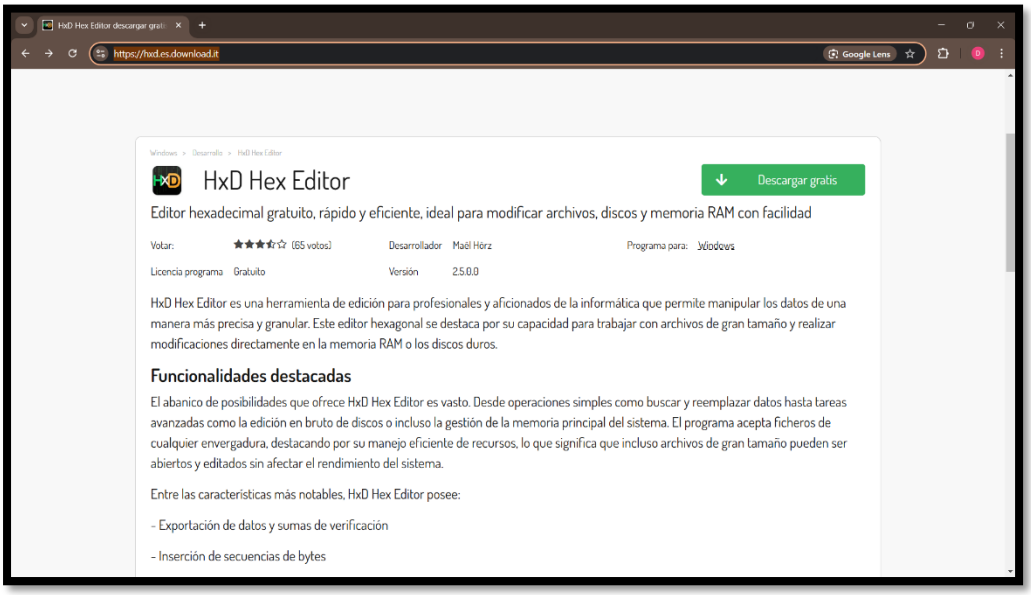


Imagen 13. Sitio de descarga HxD

2. Damos clic derecho y ejecutamos como administrador, seleccionamos el idioma.

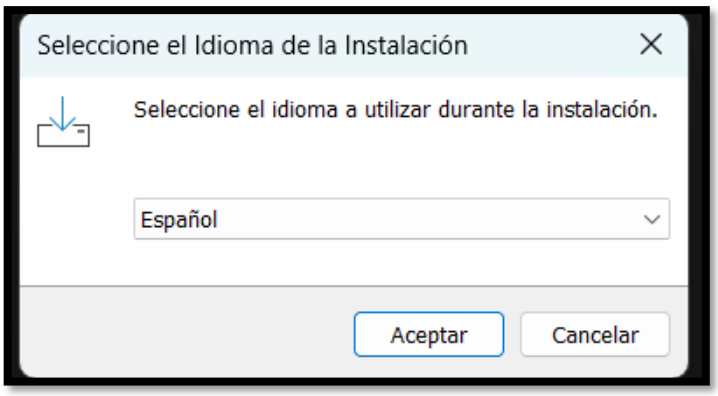


Imagen 14. Configurar Idioma

3. Le damos en ejecutar y abrirá el Editor Hexadecimal.

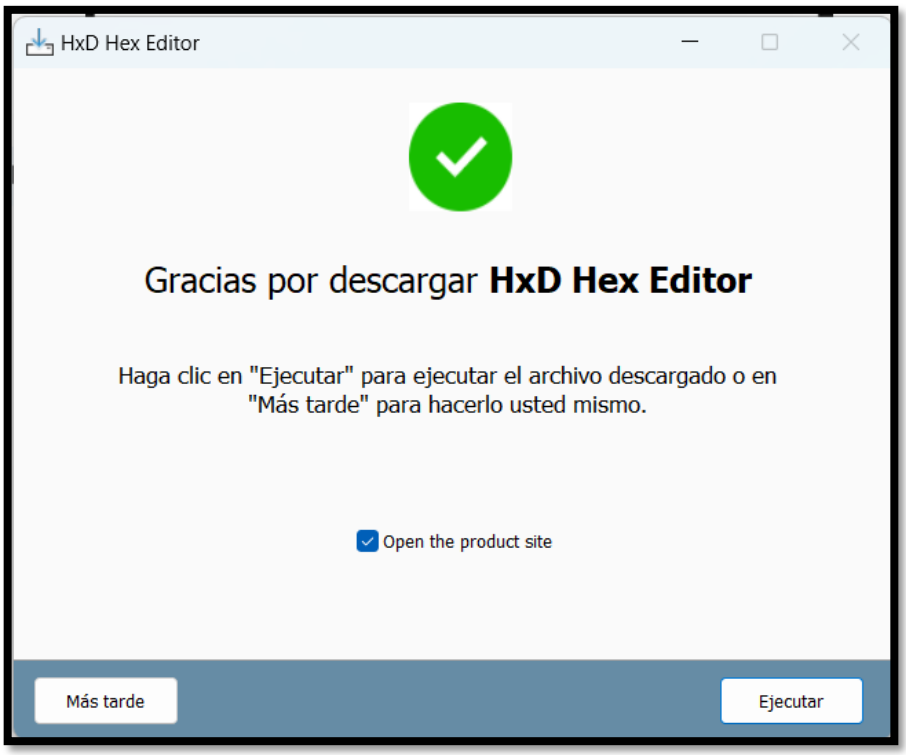


Imagen 15. Instalación terminada

4. Interfaz de la Herramienta instalada.

Imagen 16. Interfaz HxD

Instalación de Autopsy

1. Descargar desde el siguiente link: https://www.autopsy.com/download/

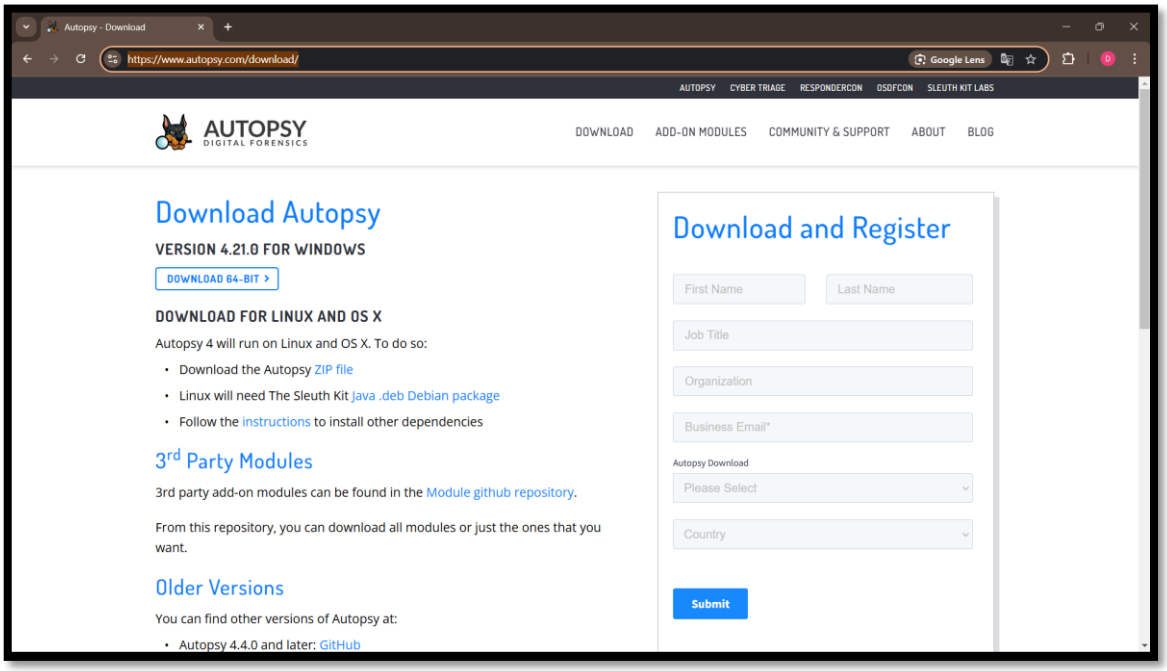


Imagen 17. Sitio de descarga Autopsy

2. Damos clic derecho y ejecutamos como administrador.

Imagen 18. Empezar la Instalación del Software

3. Procedemos a Instalar.

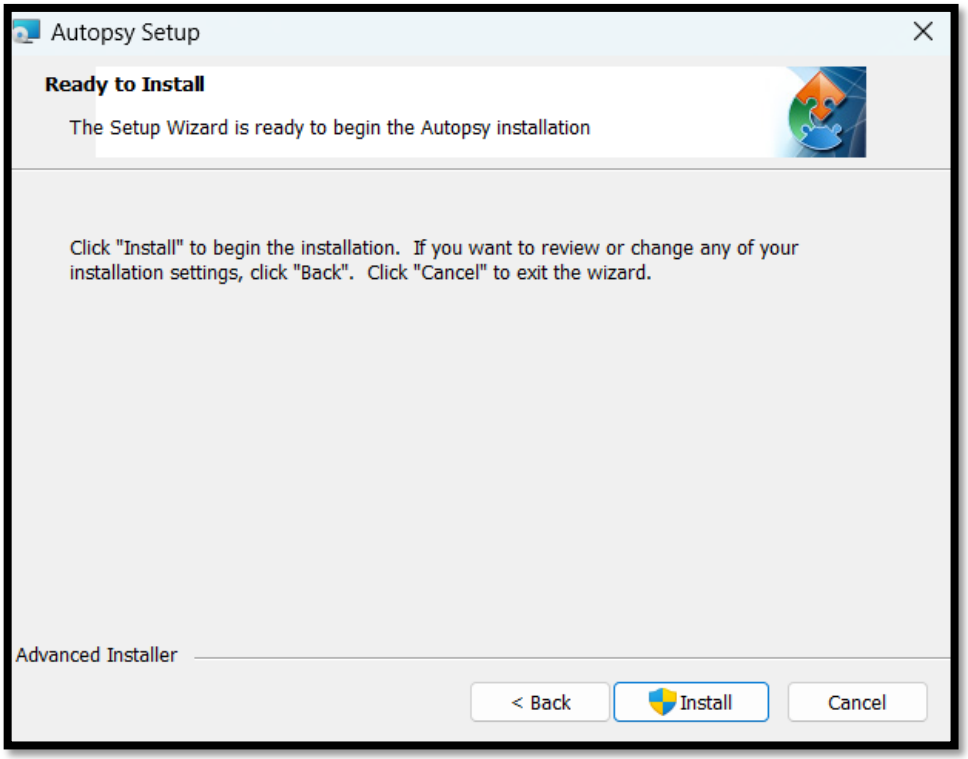


Imagen 19. Instalar Autopsy

4. Instalación terminada con éxito.

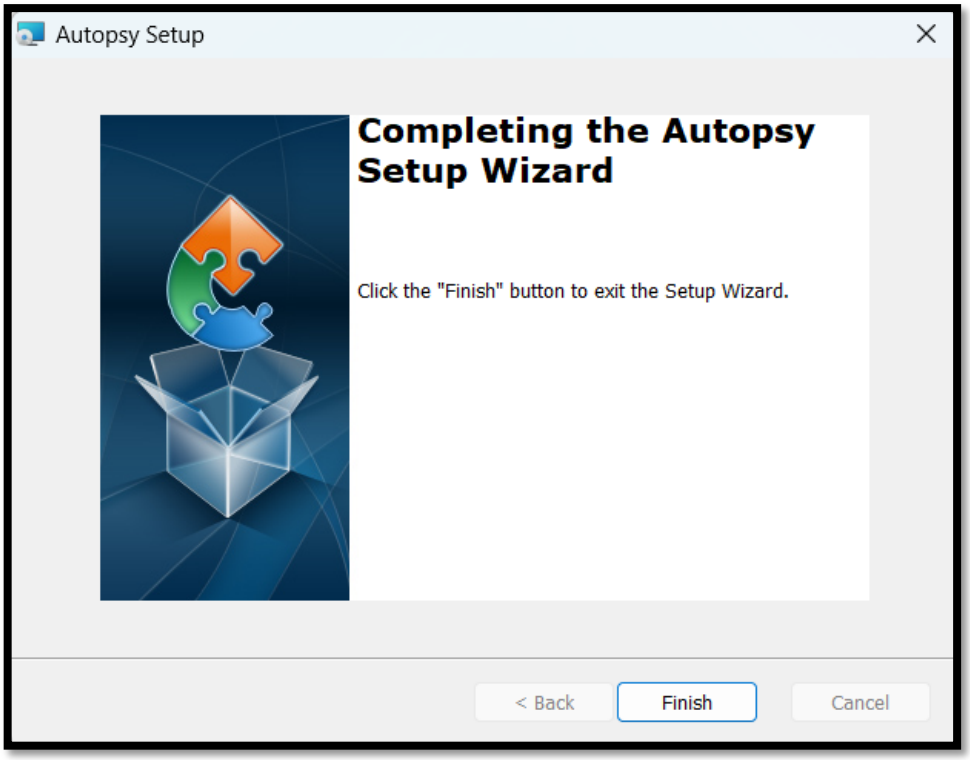


Imagen 20. Instalación completa

5. Interfaz de la Herramienta Autopsy.

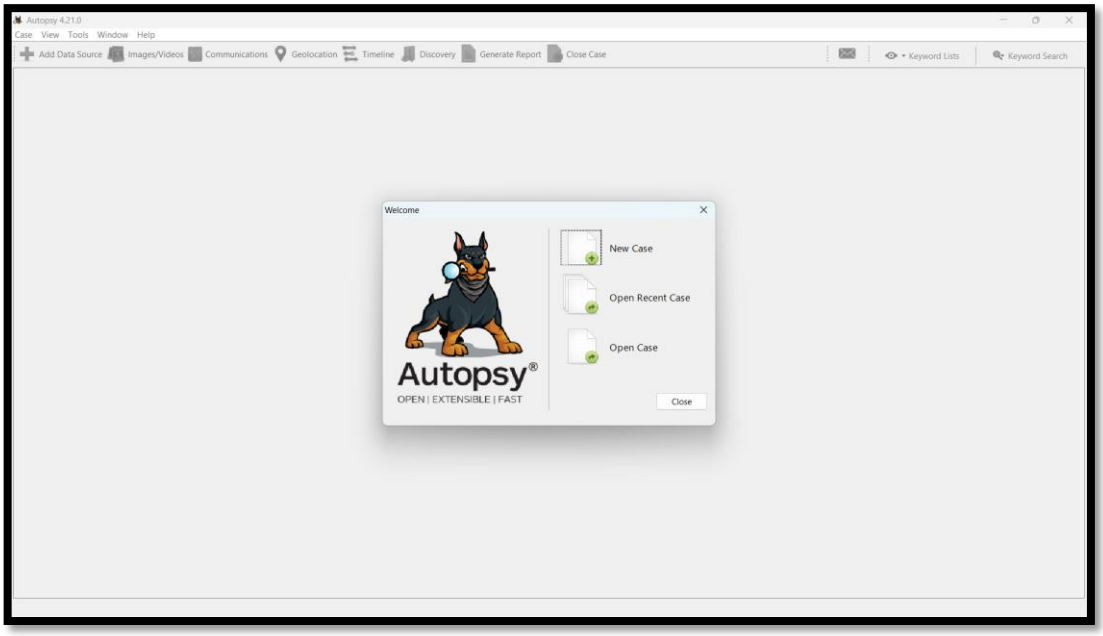


Imagen 21. Interfaz del software Autopsy

ANEXO #3
FASE: ANÁLISIS

ESCENARIOS DE PRUEBAS

Escenario_1: Tarjeta SD formateada accidentalmente – Recuperar Imágenes formato JPG

Herramienta: HXD Editor

Tiempo: 30 minutos

Técnica: Carving basado en la estructura del Sistema de Archivos

Objetivo: Recuperar imágenes en formato JPG de la tarjeta SD por un formateo accidental

1. Abrir la herramienta HXD editor, útil para investigación forense que permite abrir y editar archivos, discos y memoria.

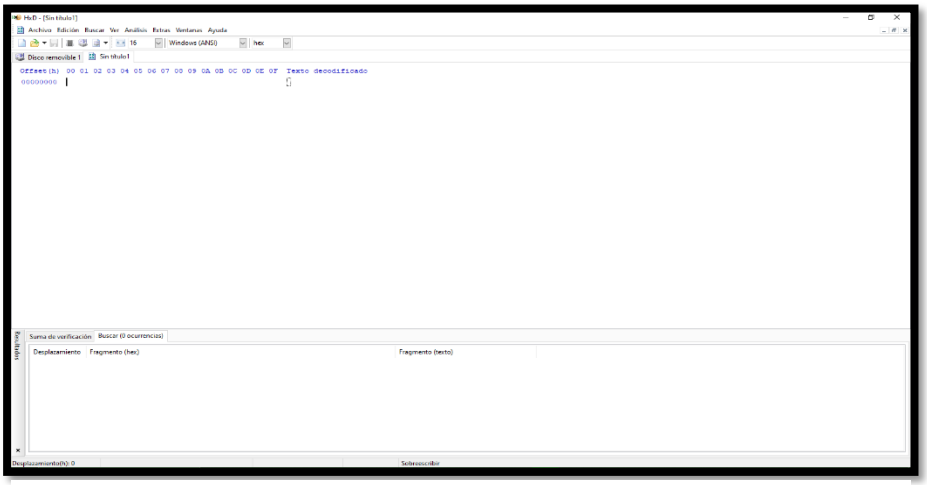


Imagen 22. Herramienta HXD editor

2. Seleccionar el archivo analizar sea disco o imagen, sea en formato .img .bin que contenta la información a indagar y recuperar. Dar clic en extras y seleccionar la unidad.

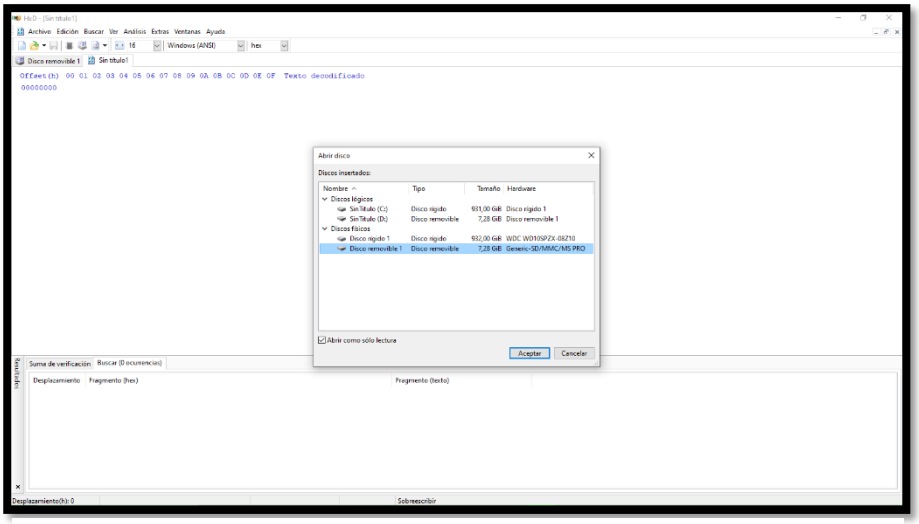


Imagen 23. Selección del archivo analizar

3. Ahora se muestra el formato hexadecimal de la unidad removible a estudiar correspondiente para la recuperación de imágenes.

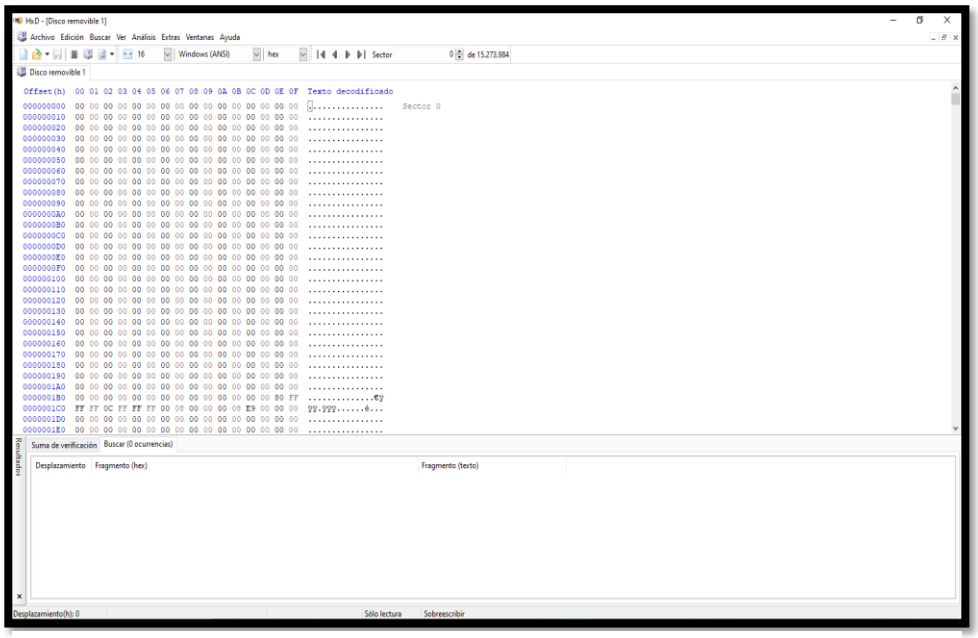


Imagen 24. Formato hexadecimal

4. Ahora para ejercer la búsqueda de los formatos de imágenes existe una estructura de archivo correspondiente a JPG que es FF D8 FF E0 como cabecera y pie FF D9, para ejercer la búsqueda dar clic en buscar y clic en buscar y seleccionar la opción valores hexadecimales y marcar todo, para luego clic en “buscar todo”.

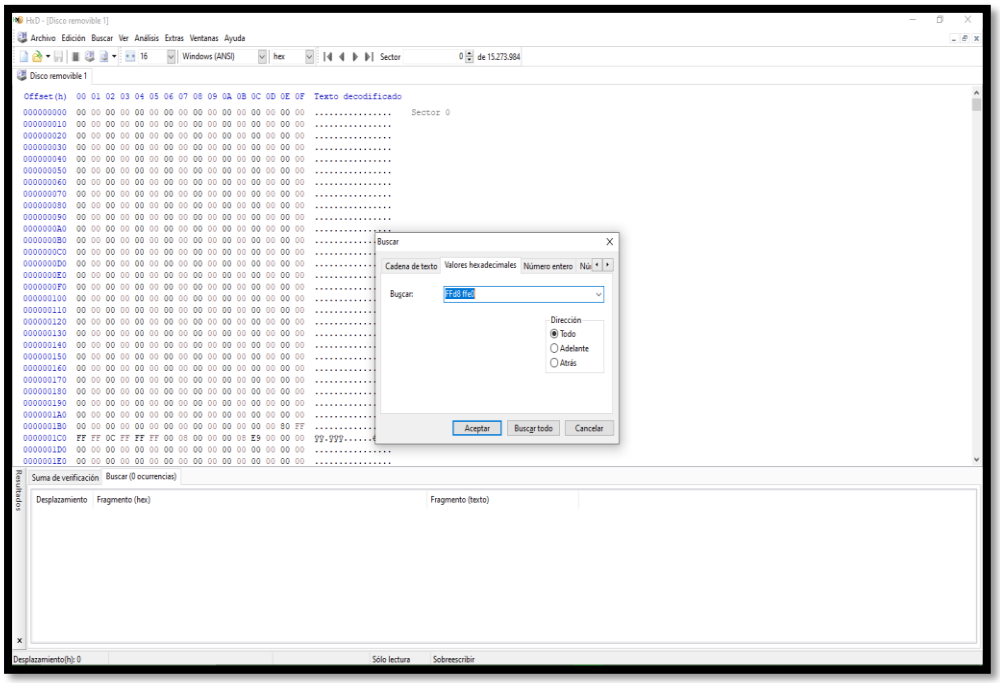


Imagen 25. Búsqueda por estructura de archivo – valor hexadecimal

5. Como resultado se evidencia un total de ocurrencia de la estructura de un archivo JPG.

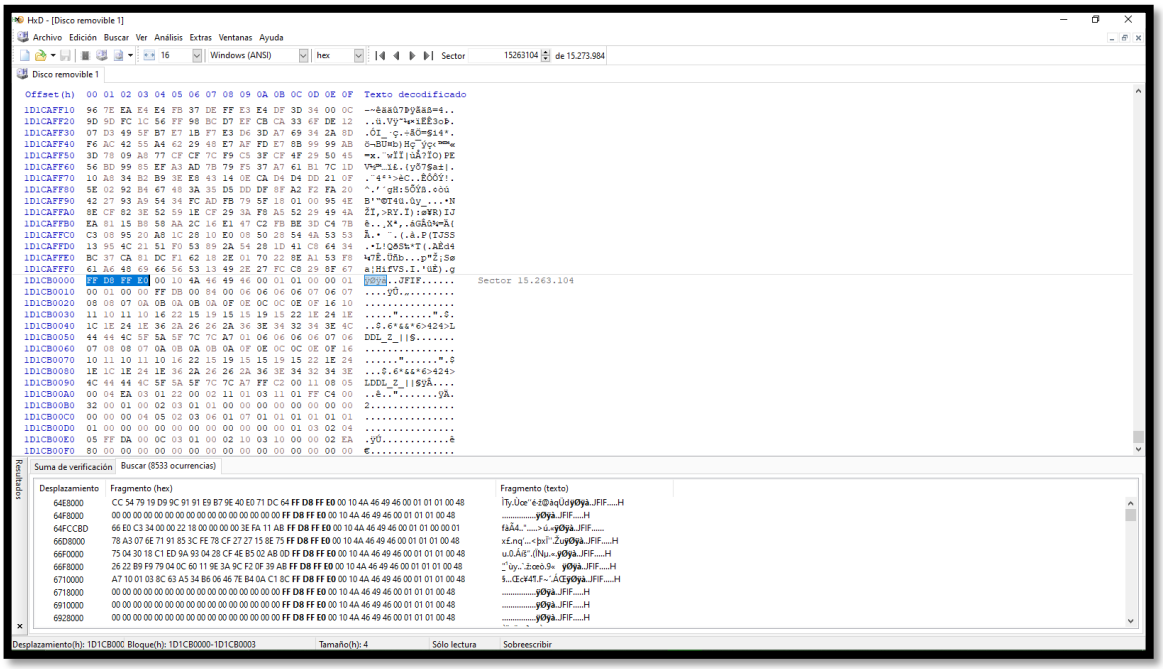


Imagen 26. Resultado de la búsqueda

6. En la parte de edición dar clic en seleccionar bloque para insertar los bloques de inicio y fin del archivo en selección para recuperar.

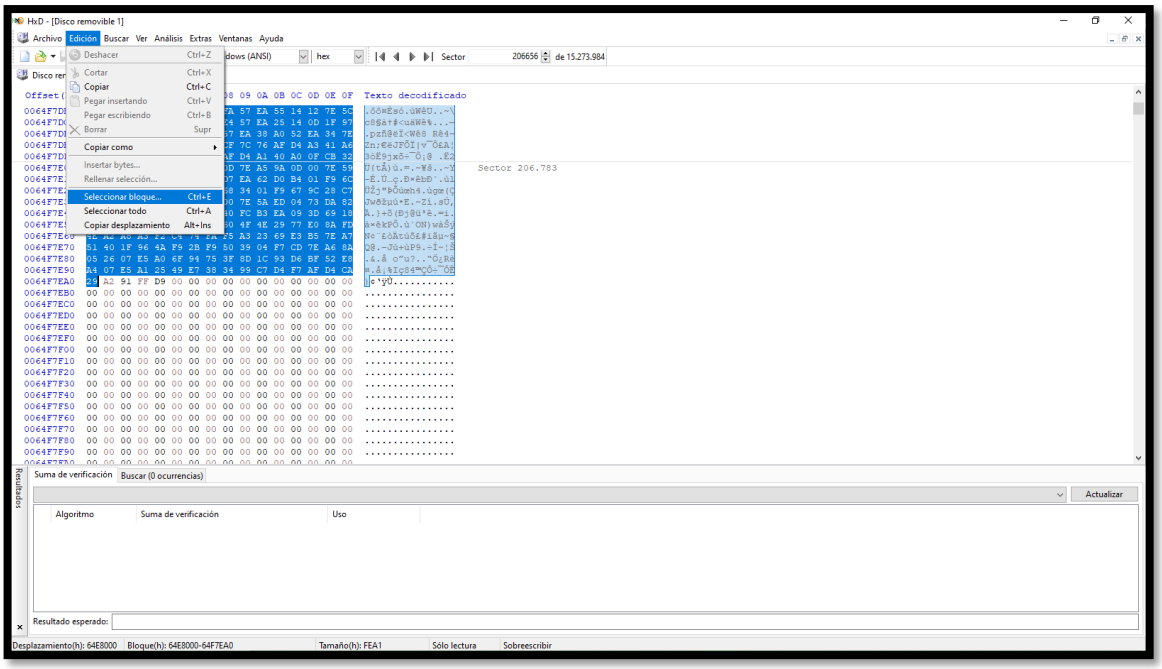


Imagen 27. Selección de bloques para recuperar archivos.

7. Una vez insertado los números correspondientes para seleccionar el fragmento por bloque dar clic en aceptar y se observa cómo se selecciona el apartado de la estructura de un archivo JPG.

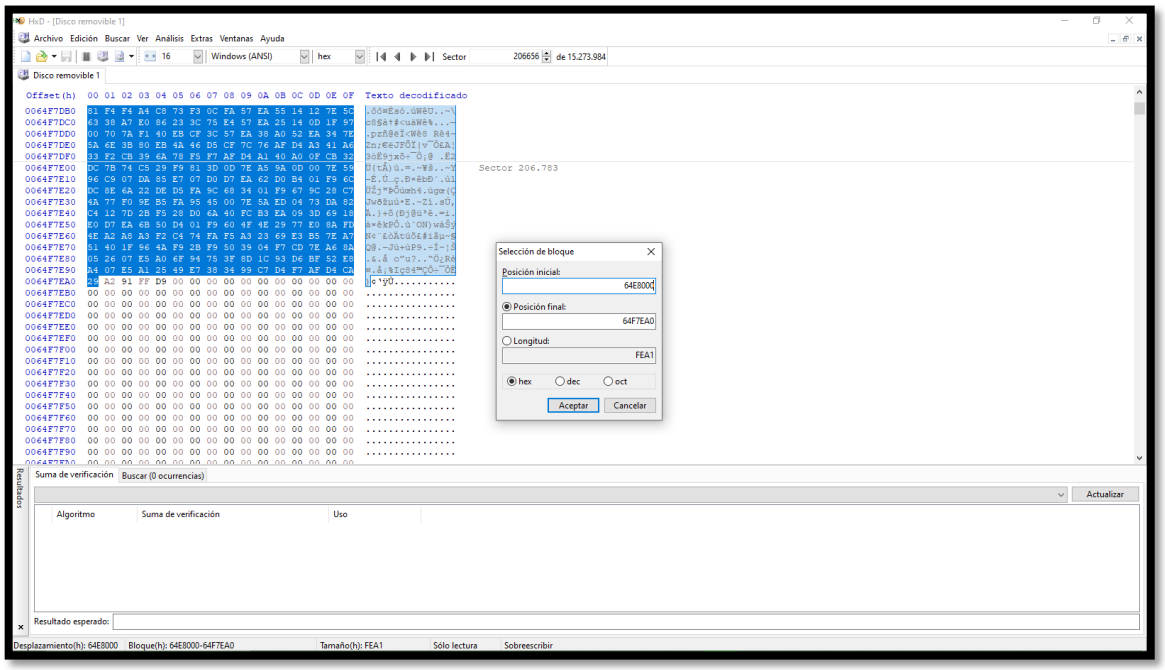


Imagen 28. Estructura inicio y fin del archivo a recuperar

8. En archivo dar clic en nuevo para pegar el fragmento seleccionado para así poder establecer el formato correspondiente JPG al realizar el “Guardar como”.

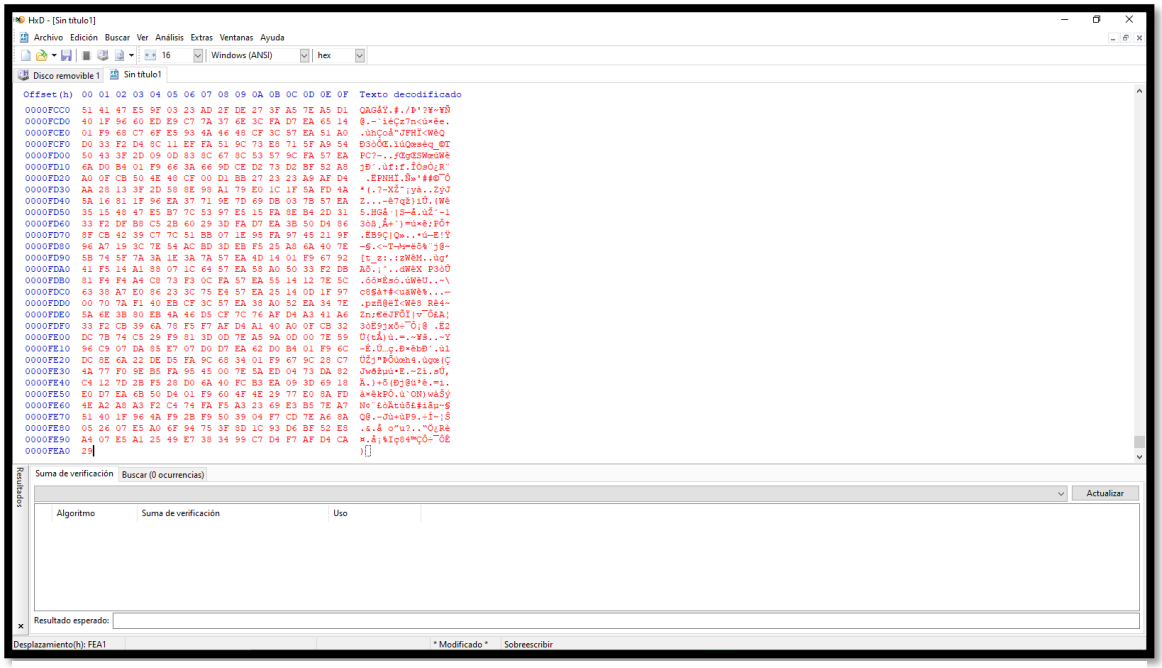


Imagen 29. Insertar un fragmento seleccionado y establecer el formato al guardar el archivo

9. Dar en “Guardar como” para establecer el recuperado del archivo JPG, guardar en una carpeta que permita el almacenamiento de los formatos a recuperar.

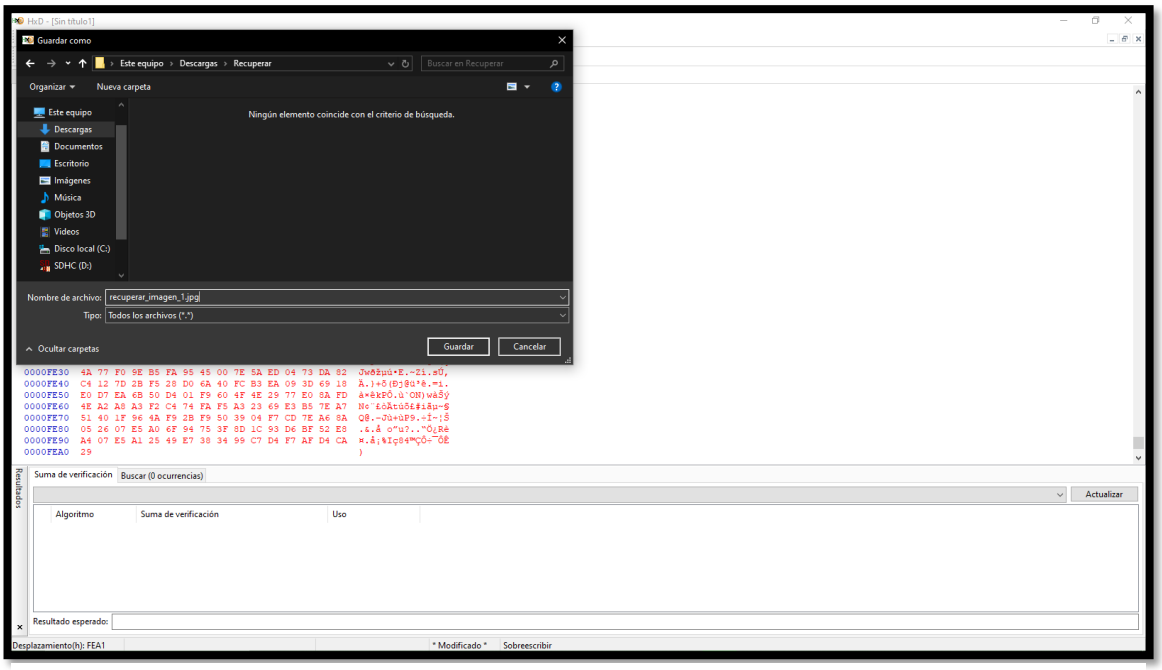


Imagen 30. Almacenar el archivo JPG recuperado en una carpeta específica

10. Archivo recuperado con éxito.

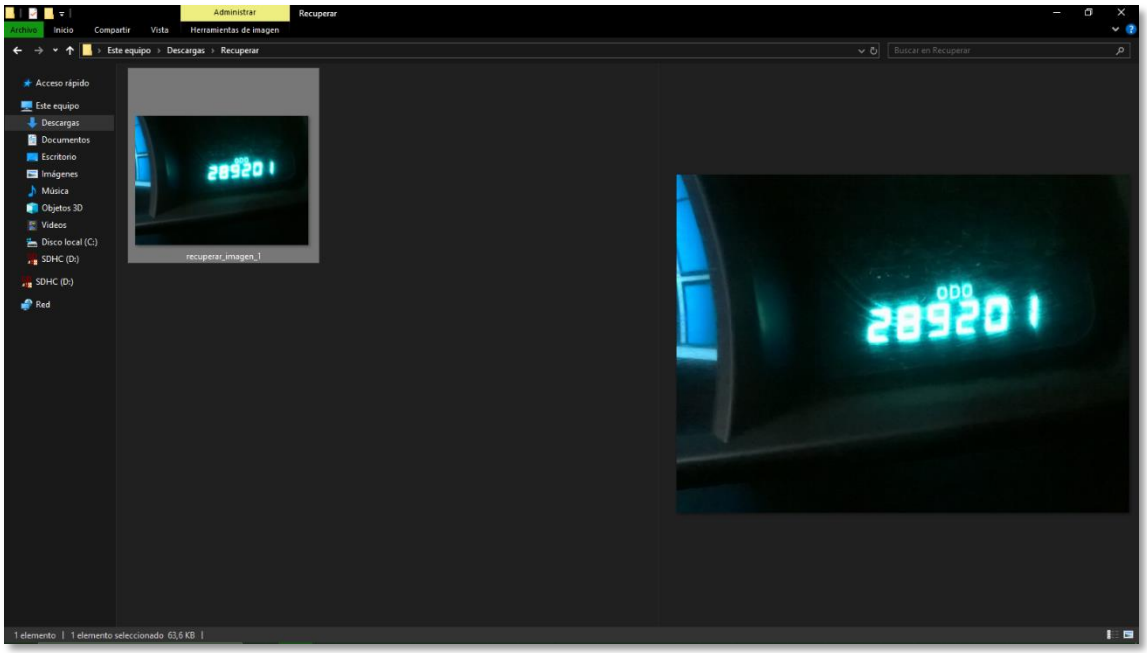


Imagen 31. Imagen recuperada con éxito

11. Presionar F3 para la búsqueda de la estructura del archivo JPG localizada en el sector 210.624, lista para su recuperación inmediata desde el fragmento inicial hasta el final.

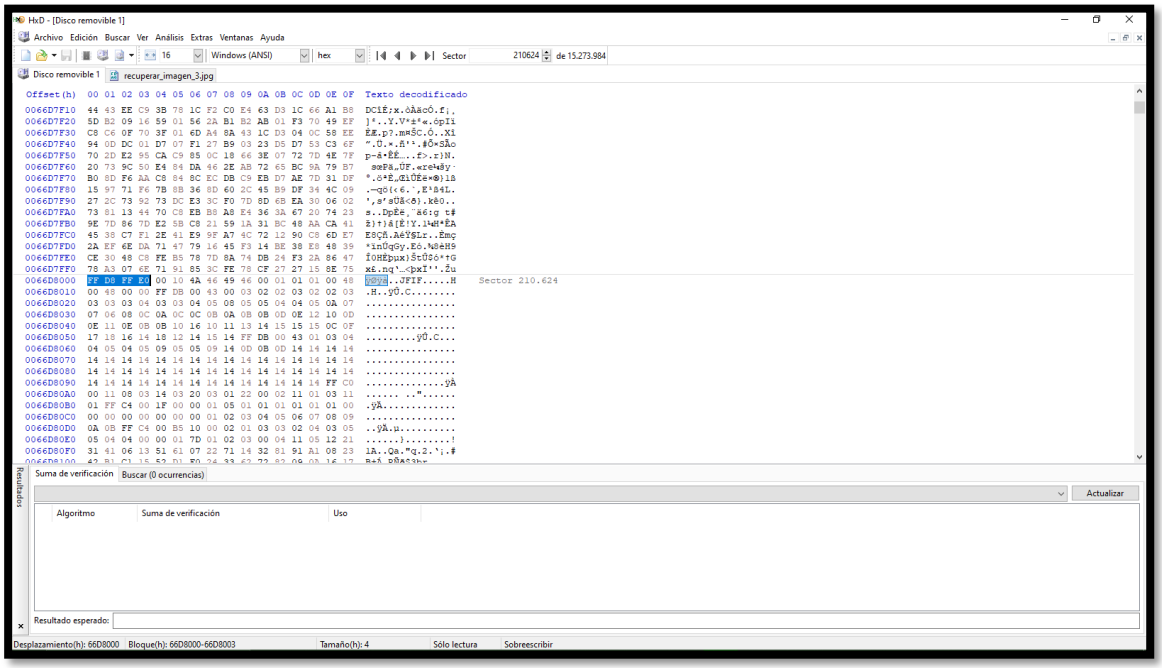


Imagen 32. Localización y recuperación de un archivo JPG en el sector 210.624

12. Se crea una nueva hoja de editor hexadecimal se pega la sección del fragmento para guardar en la carpeta destino incluyendo el nombre del archivo con la extensión .jpg.

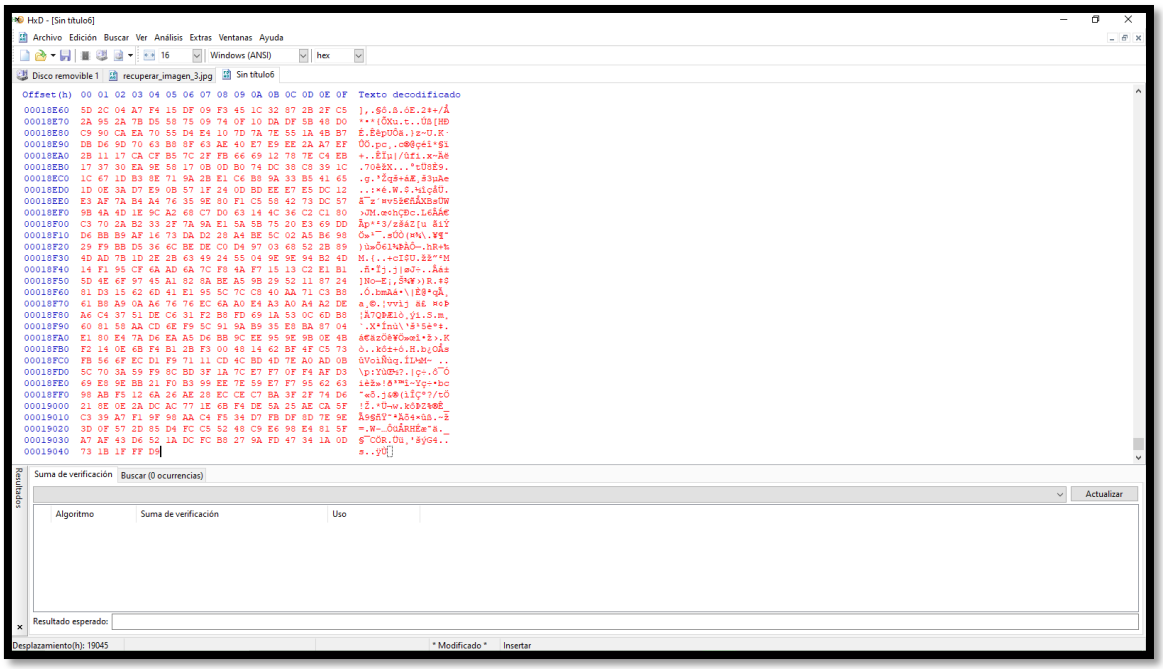


Imagen 33. Creación de archivo en editor hexadecimal

13. Imagen recuperada exitosamente, un proceso manual pero preciso en la recuperación de los archivos a restaurar del formateo accidental de la tarjeta SD del dispositivo Android.

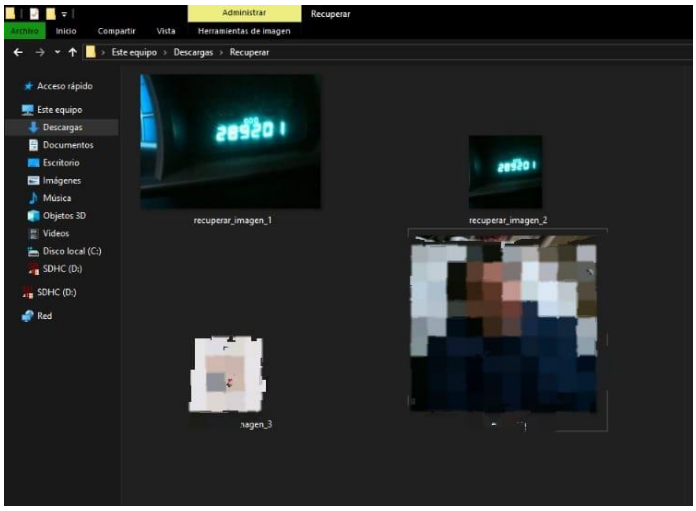


Imagen 34. Recuperación con éxito tras formateo accidental de tarjeta SD

Escenario_2: Tarjeta SD Formateada accidentalmente – Recuperar en su totalidad los archivos existentes

Herramienta: PHOTOREC

Tiempo: 9 minutos

Técnica: Carving basado en firmas

Objetivo: Recuperar los archivos que existieron en el SD como imágenes, doc, entre otros.

14. Abrir la herramienta Photorec y seleccionar la partición principal de la unidad a estudiar que este caso es el FAT32 LBA.

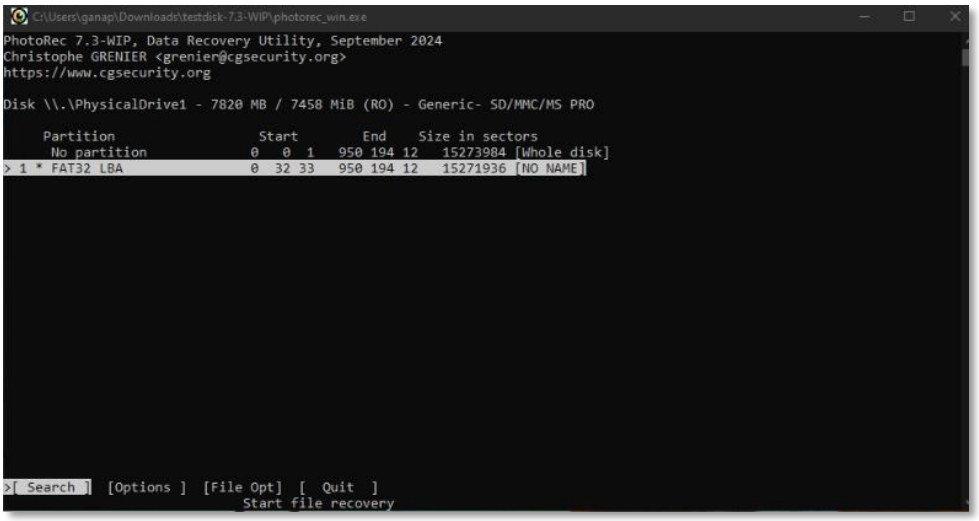


Imagen 35. Selección de partición FAT32 LBA para el análisis

15. Seleccionar el sistema de archivo que maneja la tarjeta, seleccionar Other para que ejerza el análisis en la mayoría de los sistemas de archivos existentes.

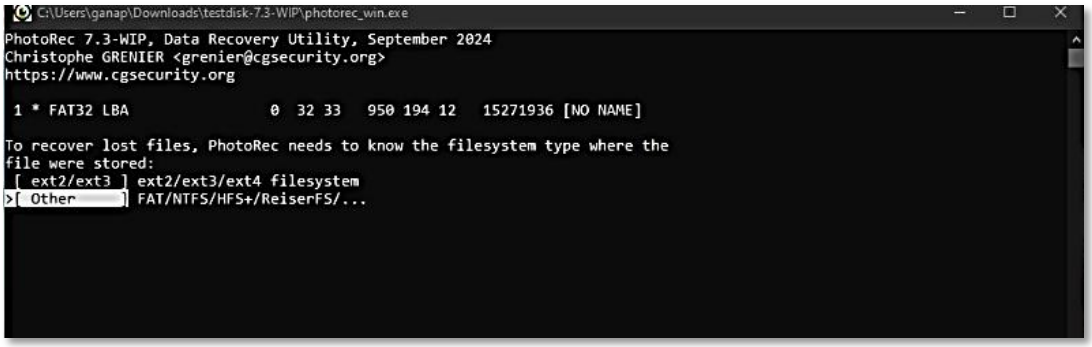


Imagen 36. Selección del sistema de archivos y análisis con 'Other'

16. Ya seleccionado la parte analizar, ubicar la ruta en donde se va almacenar los datos recuperados, guardar los datos reestablecido en la carpeta “Recuperar”.

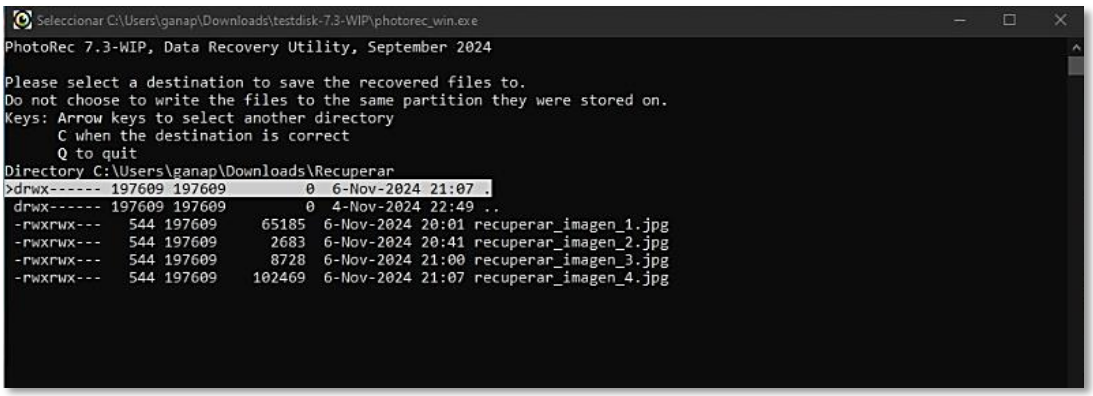


Imagen 37. Definición de ruta para guardar datos recuperados

17. Ya configurado todo, presionar la tecla C para empezar el proceso de análisis y recuperación de datos que la tarjeta SD contaba. Presenta un resultado aproximado de archivos como imágenes, documento, txt, entre otros.

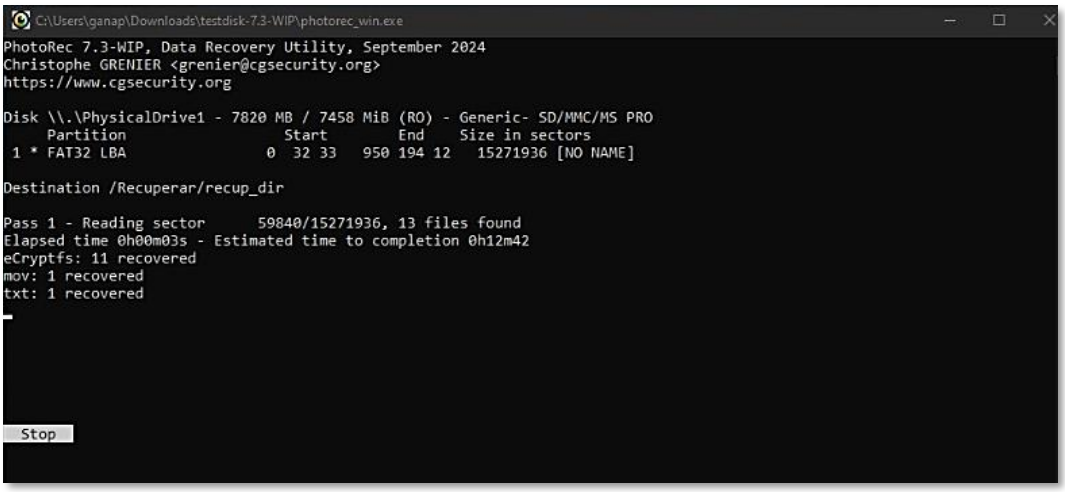


Imagen 38. Iniciar análisis y recuperación de datos con tecla C

18. Una vez finalizado presenta el mensaje recovery completed y ahora dirigirse a la carpeta destino para averiguar los archivos recuperados.

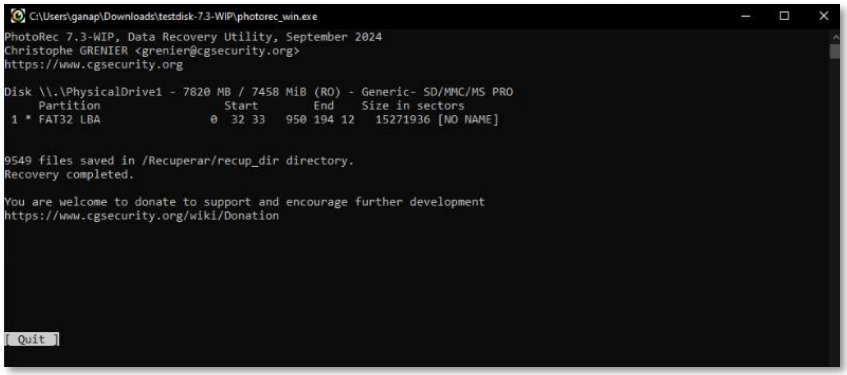


Imagen 39. Proceso completado, revisar archivos en carpeta destino

19. Se observa que ha generado un total de 20 carpetas en donde se ha visualizado un total de 520 elementos por carpetas. La unidad de estudio contaba con gran cantidad de espectro de información tras el formateo accidental.

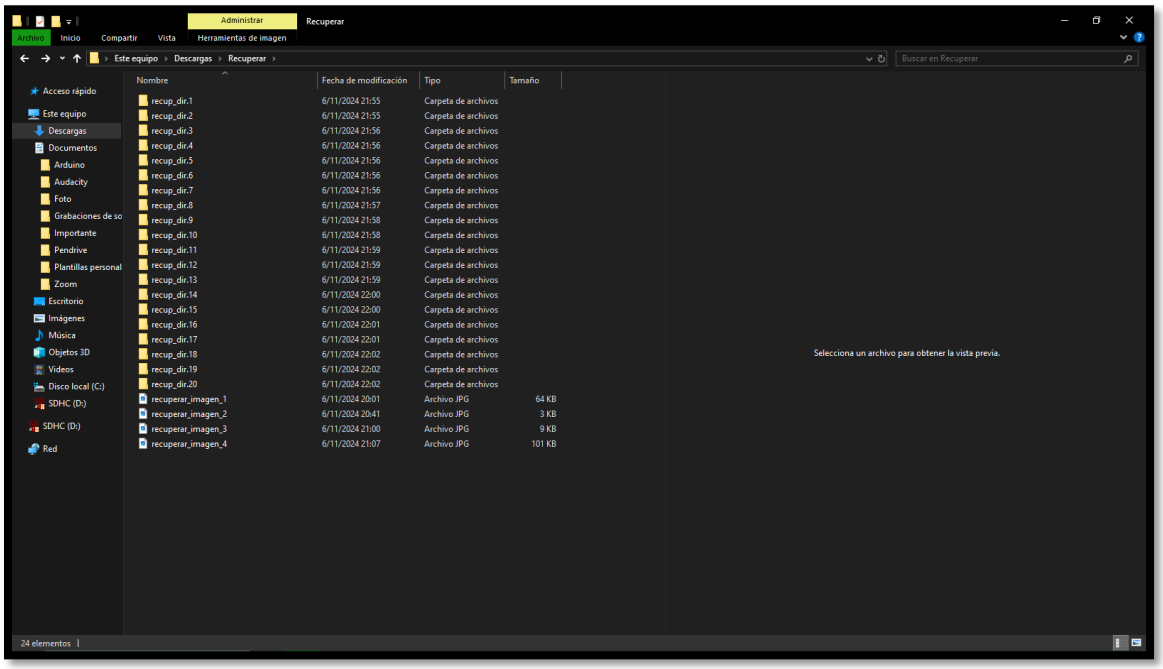


Imagen 40. Generación de carpetas con los elementos encontrados tras el análisis.

Escenarios_3: Recuperar documentos PDF de la carpeta WhatsApp Documentos

Herramienta: AUTOPSY

Tiempo: 20 minutos

Técnica: Carving basado en fragmento

Objetivo: Recuperar los archivos pdf de la carpeta documentos de WhatsApp

Extraer primero la copia de seguridad de la media del dispositivo – WhatsApp Documentos. Para ello, abrir la herramienta minimal ADB & fastboot como administrador.

20. Escribir el comando **"adb devices"** para listar los dispositivos Android conectados a la computadora a través de USB, el resultado que muestra es el número de serie del dispositivo y el estado del mismo, existen estados como **"device"** que significa listo para interactuar, **"unauthorized"**- necesita autorización en el dispositivo o **"offline"** – no está disponible.

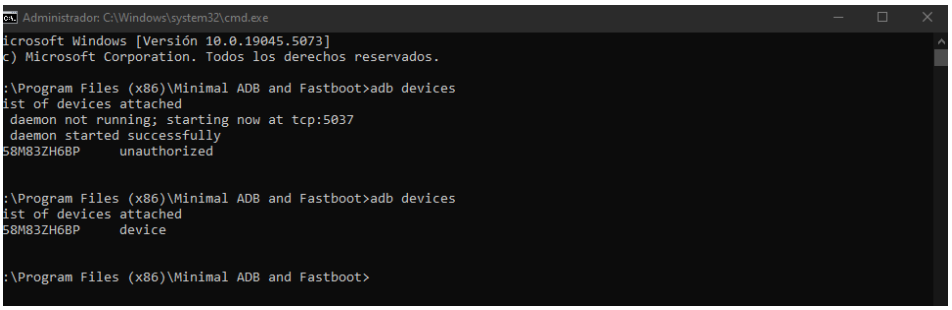


Imagen 41. Listar dispositivos conectados y verificar su estado

21. Insertar el comando **"adb root"** para reiniciar el servidor ADB en modo root, para a acceder a los privilegios de superusuario.

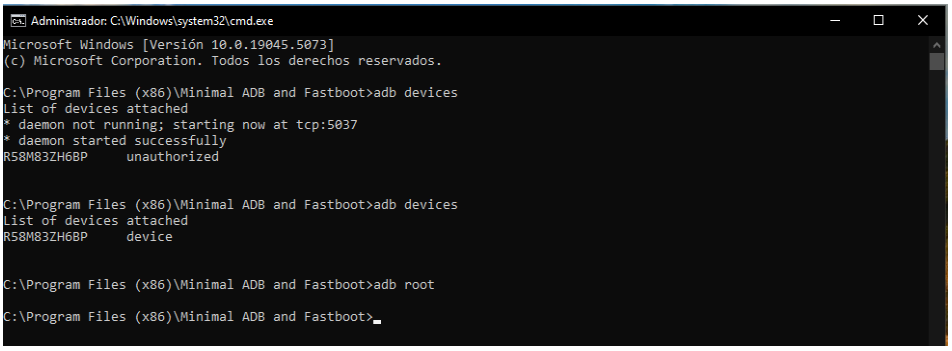


Imagen 42. Reiniciar ADB con privilegios de superusuario

22. Insertar el comando **“abd shell”** permite abrir una interfaz de línea de comandos Shell en el dispositivo Android en donde se ejecuten directamente en el Sistema Operativo como si fuera terminal Linux.

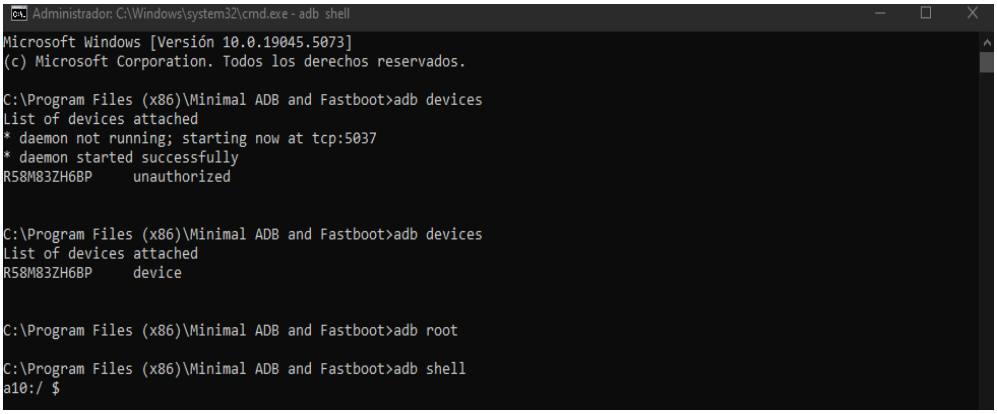


Imagen 43. Acceder a la línea de comandos del sistema Android

23. Insertar el comando **“su”** para interactuar como superusuario.

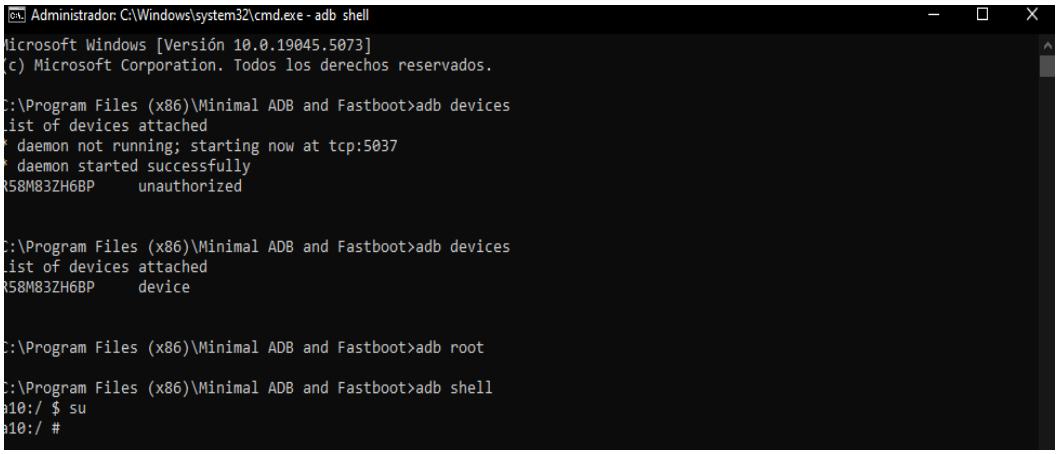


Imagen 44. Comando “su” - interactuar como superusuario

24. Insertar el comando **“dd if=/dev/zero of=/sdcard/WhatsApp_Documentos_backup.img bs=1M count=50”** permite crear un archivo de **50 M** en la memoria del dispositivo usando **/dev/zero** como entrada, el archivo tendrá valores hexadecimales de ceros, que significa que no contendrá ningún dato útil.

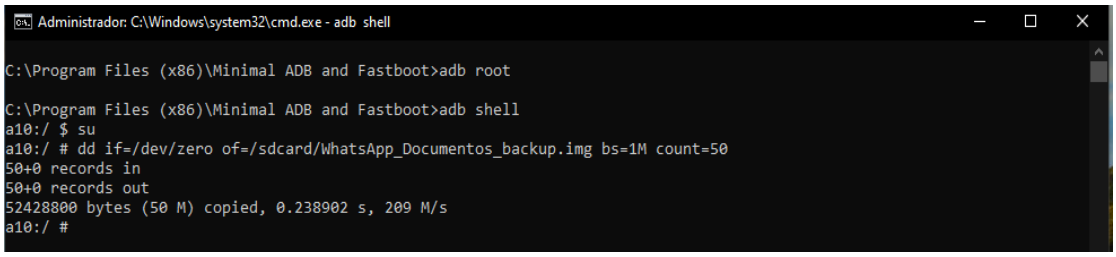


Imagen 45. Crear un archivo con valores hexadecimales en cero

25. Insertar el comando **mkfs.ext4 /sdcard/WhatsApp_Documentos_backup.img** para completar la acción de formatear la imagen y asignarle un sistema de archivos ext4, convirtiendo el archivo en un disco virtual que contiene la estructura de sistema de archivos ext4.

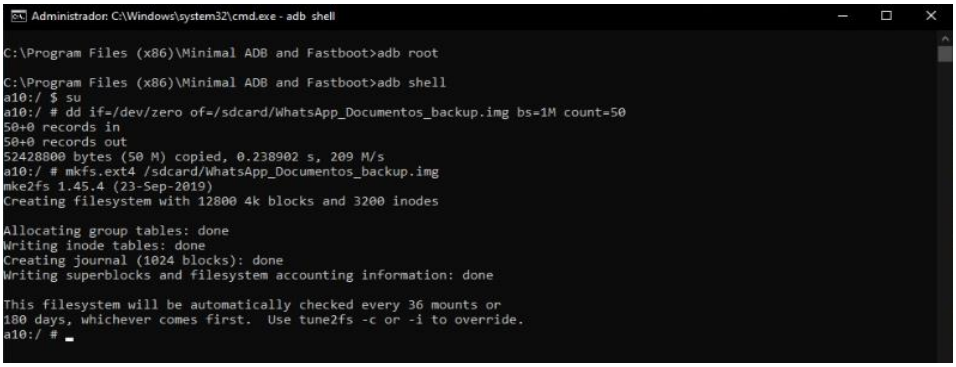


Imagen 46. Creación de un disco virtual con estructura del sistema de archivos ext4

26. Insertar el comando **"mkdir /sdcard/backup_mount"** permite crear un nuevo directorio llamado **"backup_mount en la ruta /sdcard"** del dispositivo Android.

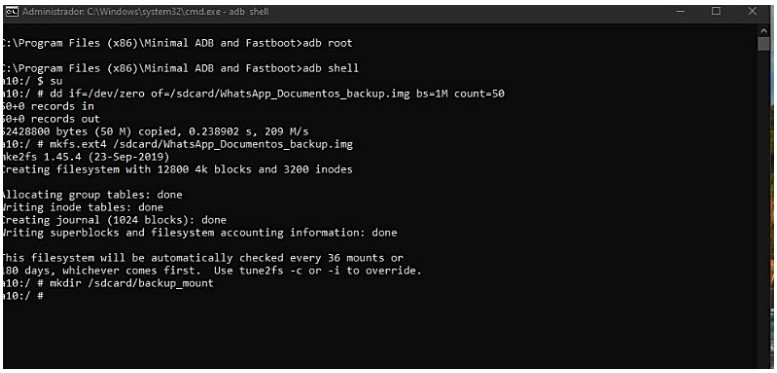


Imagen 47. Crear directorio donde se guardará el disco virtual

27. Insertar el comando "**mount -o loop /sdcard/WhatsApp_Documentos_backup.img /sdcard/backup_mount"**, permite montar un archivo imagen en el directorio de **/sdcard/backup_mount** para que sea accesible como si fuera una unidad de almacenamiento adicional.

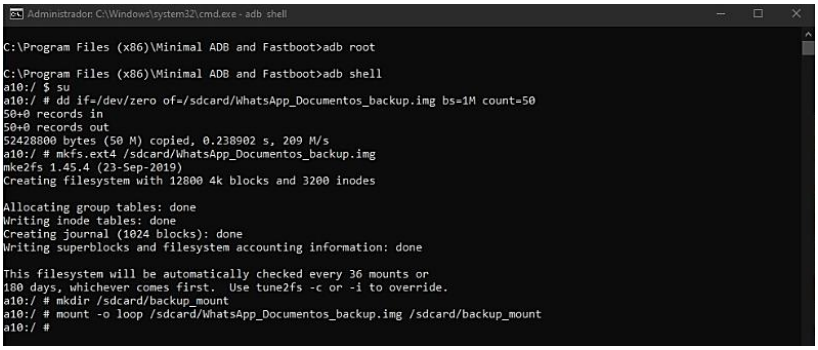


Imagen 48. Montar el archivo imagen permitiendo acceder al almacenamiento

28. Insertar el comando "**cp -r /data/media/0/Android/media/com.whatsapp/WhatsApp/Media/WhatsApp\ Documents/* /sdcard/backup_mount",** el comando permite copiar todos los archivos existentes o que existen en la carpeta y montar aquella información en la carpeta **backup_mount** en donde se encuentra montada la imagen.

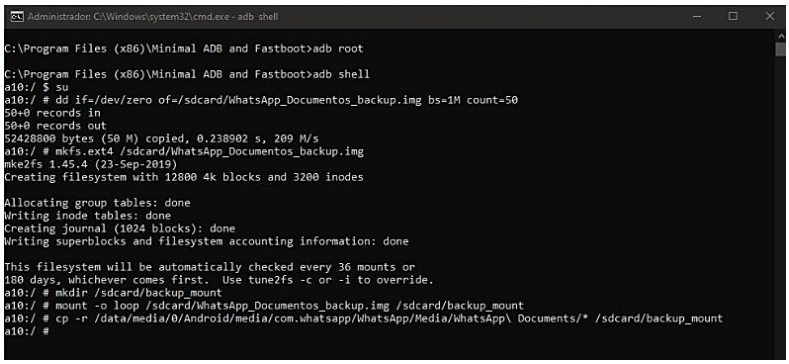


Imagen 49. Copiando archivos existentes y montarlo en el archivo img

29. Insertar el comando **"umount /sdcard/backup_mount"**, permite desmontar un Sistema de archivo o dispositivo antes de ser expulsado.

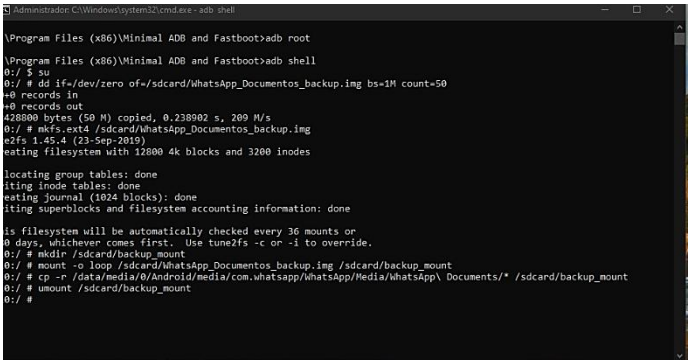


Imagen 50. Desmontar el sistema de archivo antes de expulsarlo

30. Insertar el comando **"exit"** para salir de la Shell desde el dispositivo Android y manejar la consola de la herramienta desde la terminal de Windows.

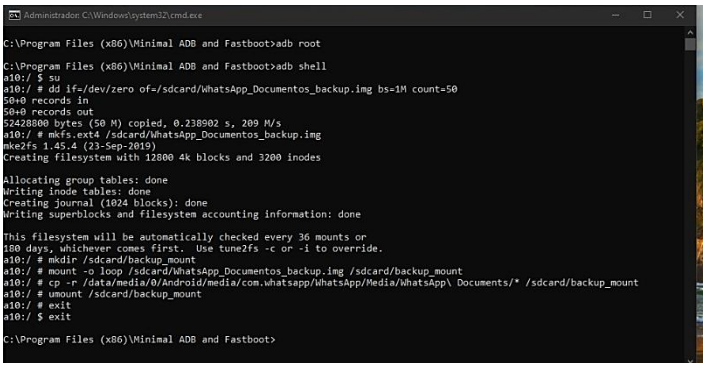


Imagen 51. Salida del Shell del dispositivo Android

31. Insertar el comando **“adb pull /sdcard/WhatsApp_Documentos_backup.img C:\Recuperacion”**, permite ejercer una copia de seguridad de la imagen localizada en el dispositivo y transferir hacia el computador.

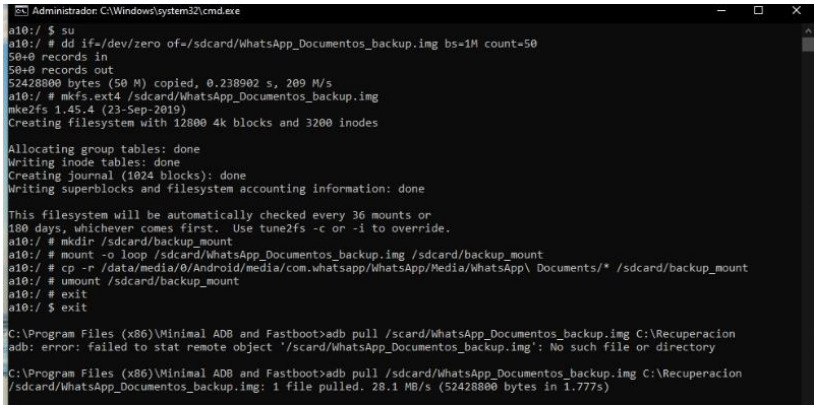


Imagen 52. Copia de Seguridad y trasferencia del archivo img al computador

32. Abrir la herramienta **Autopsy** para ejercer la técnica de File Carving basado en fragmentación, crear un nuevo caso establecer las configuraciones pertinentes como asignar el caso y detalles del mismo.

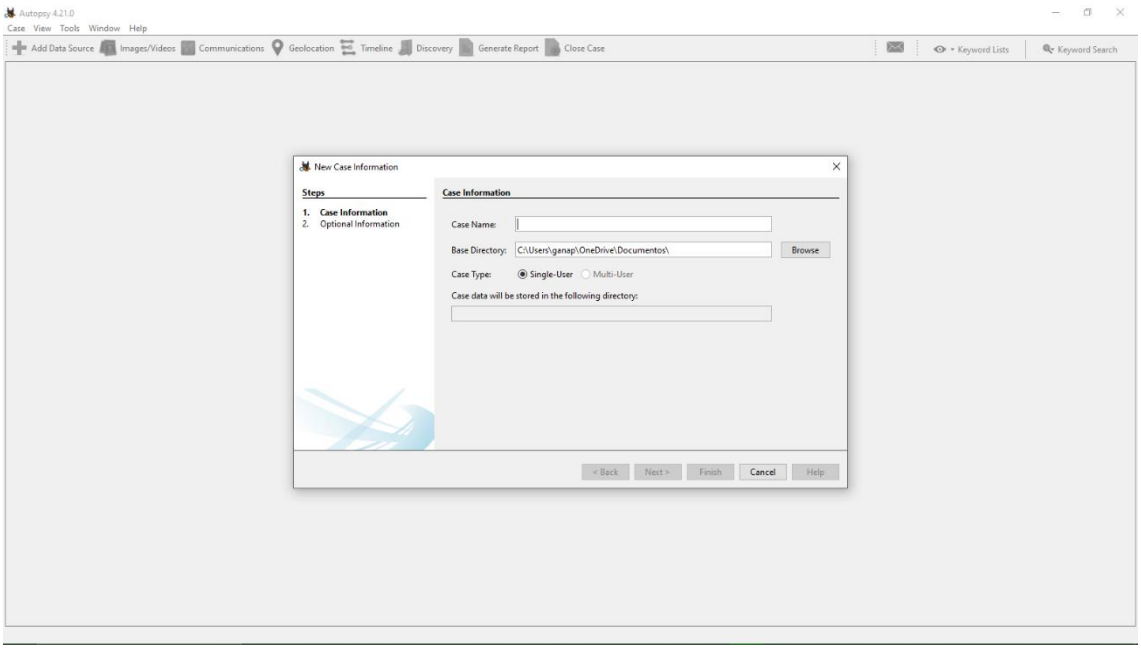


Imagen 53. Apertura de Autopsy para análisis con File Carving

33. Asignar detalles del caso como la información del dispositivo, numero de caso, email, entre otros, dar clic en finish para procesar el nuevo caso.

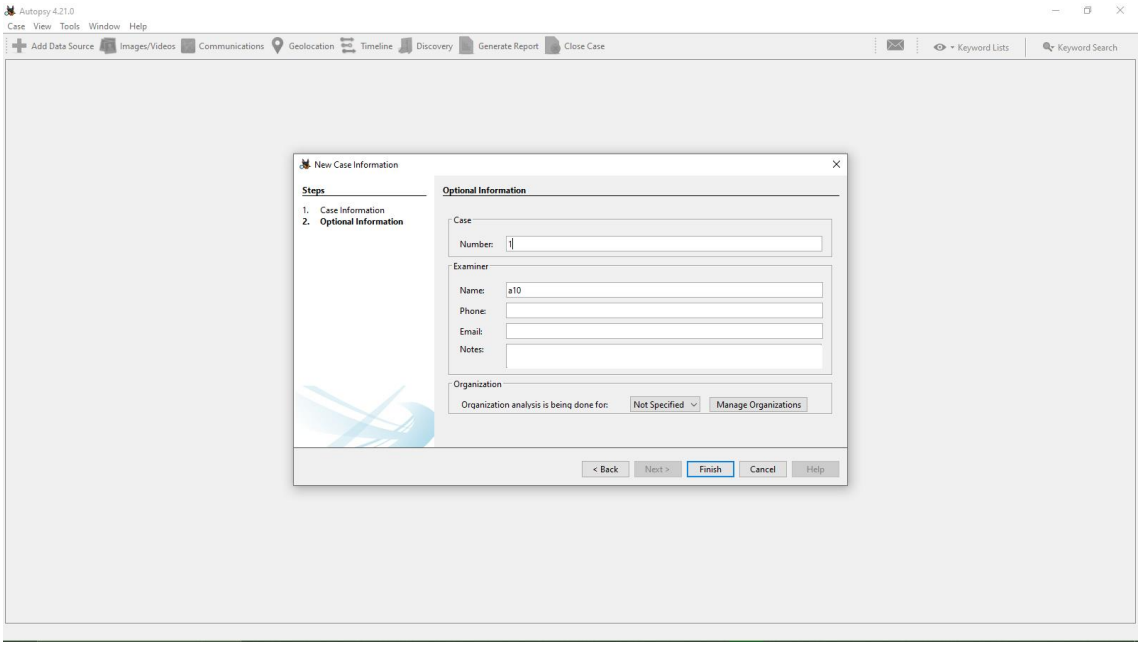


Imagen 54. Asignación de detalles del caso

34. Seleccionar el host donde estará generado la nueva fuente de datos.

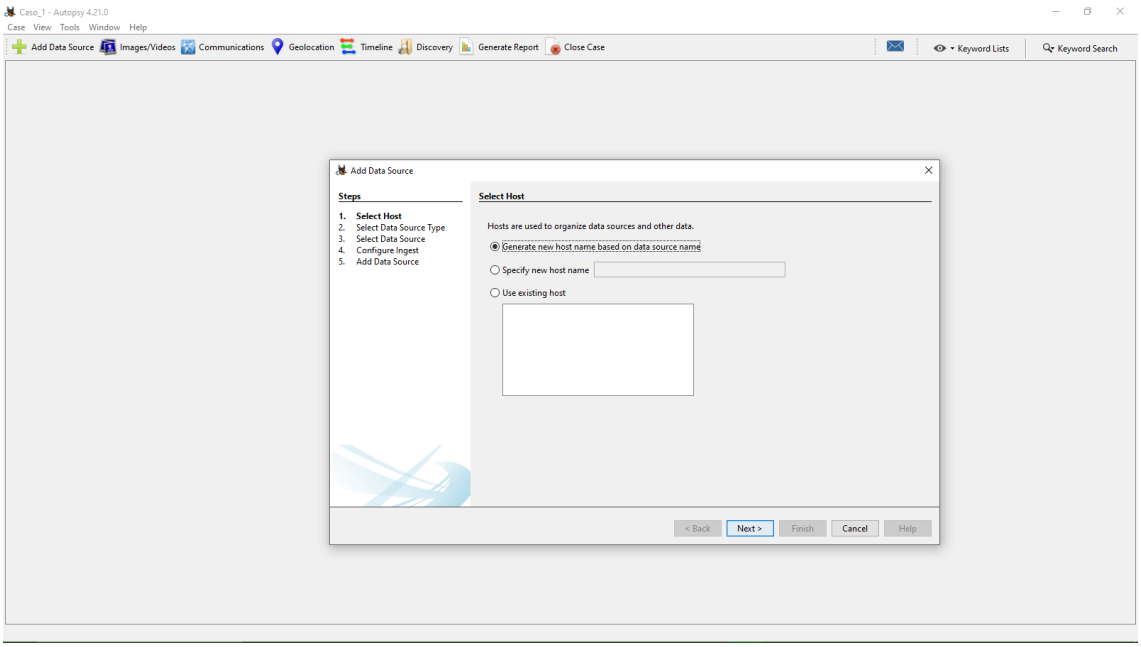


Imagen 55. Selección del host para la nueva fuente de datos.

35. Seleccionar el tipo de la fuente de datos, la imagen de disco que creamos.

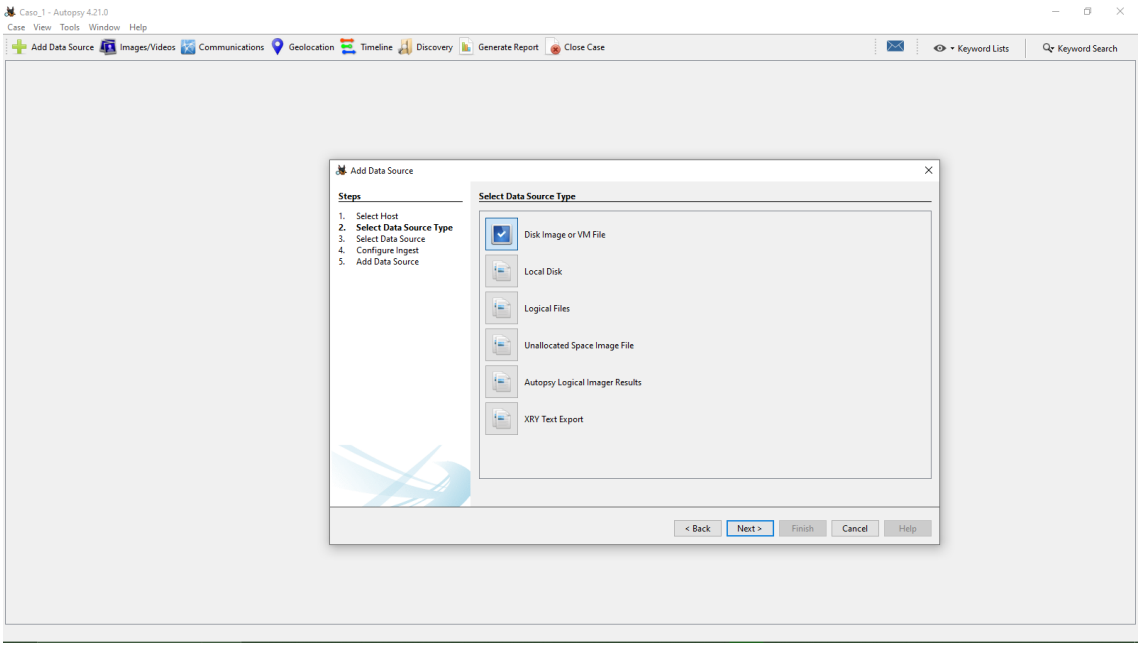


Imagen 56. Elección de la imagen de disco como fuente de datos

36. Buscamos la imagen de disco, para realizar el análisis.

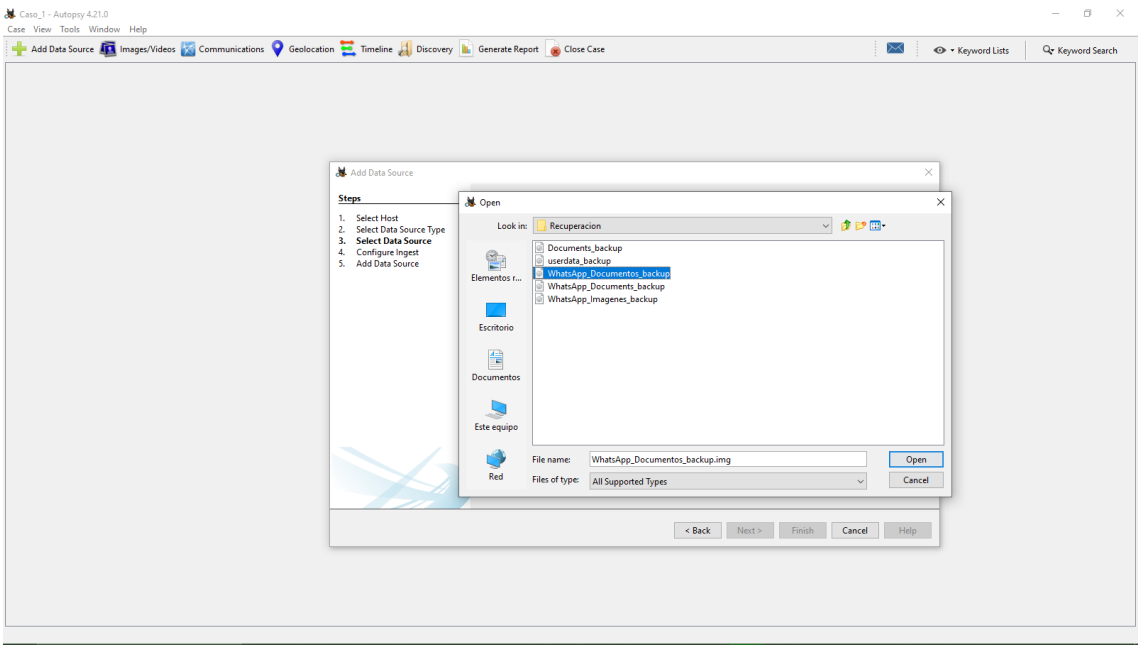


Imagen 57. Selección de la imagen de disco para análisis

37. Configuración de los módulos necesarios para el análisis correspondiente.

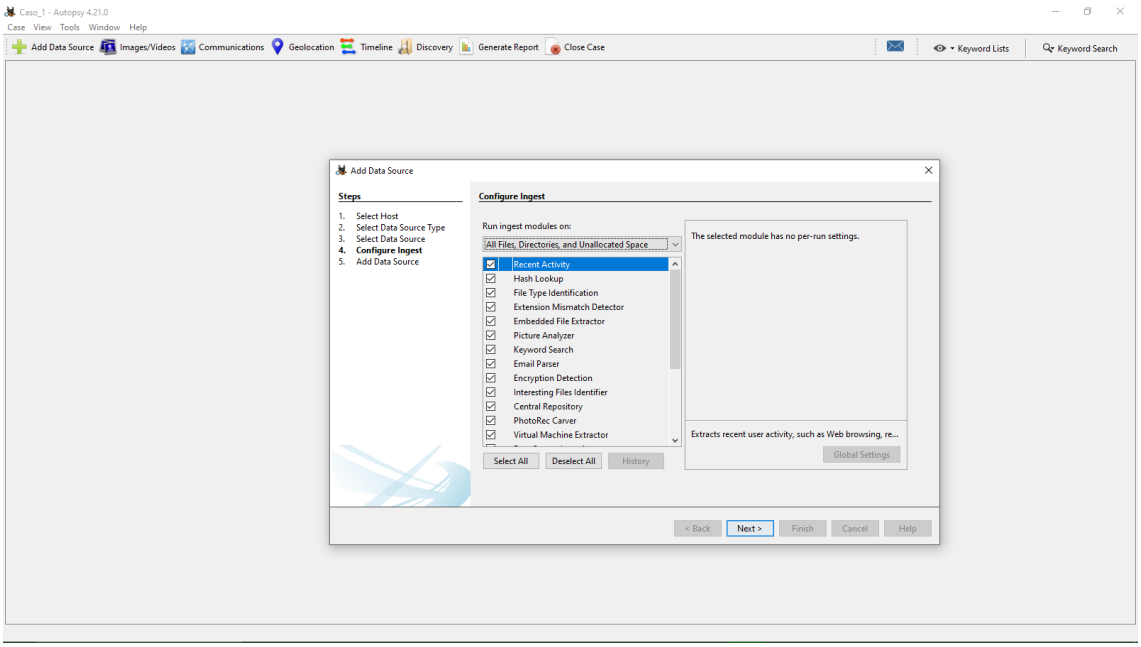


Imagen 58. Seleccionar los módulos para el análisis

38. Posteriormente se agrega nuestra fuente de datos y analizara lo antes seleccionado.

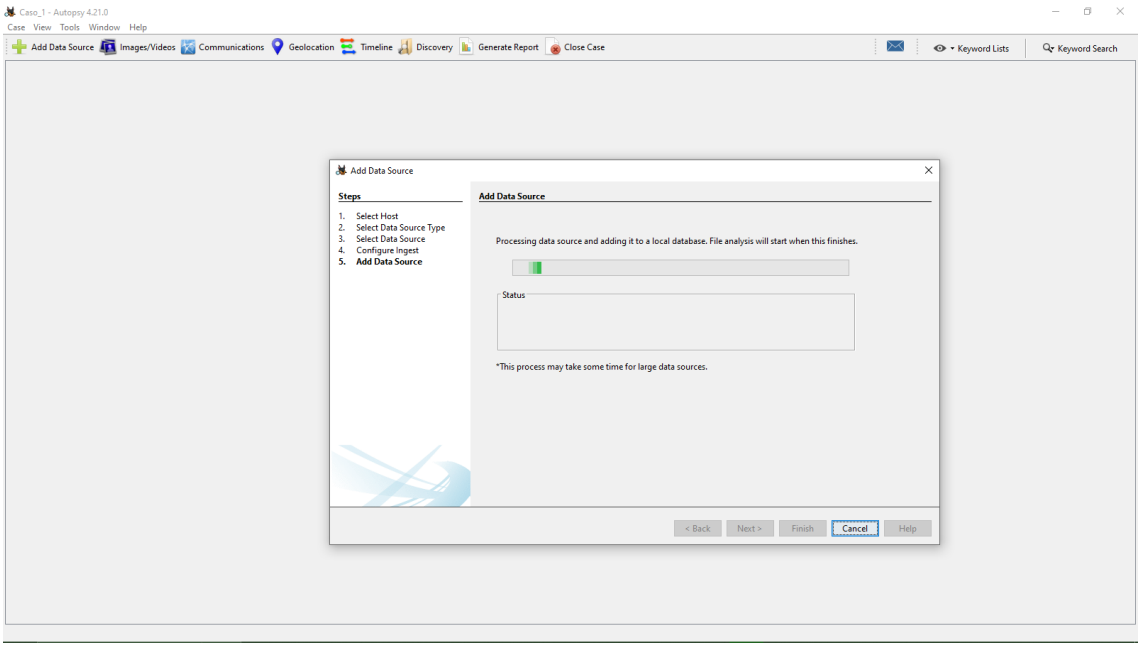


Imagen 59. Fuente de datos agregada para análisis

39. Tenemos el nombre del Host que ingresamos a la herramienta, al costado izquierdo tenemos los módulos seleccionados.

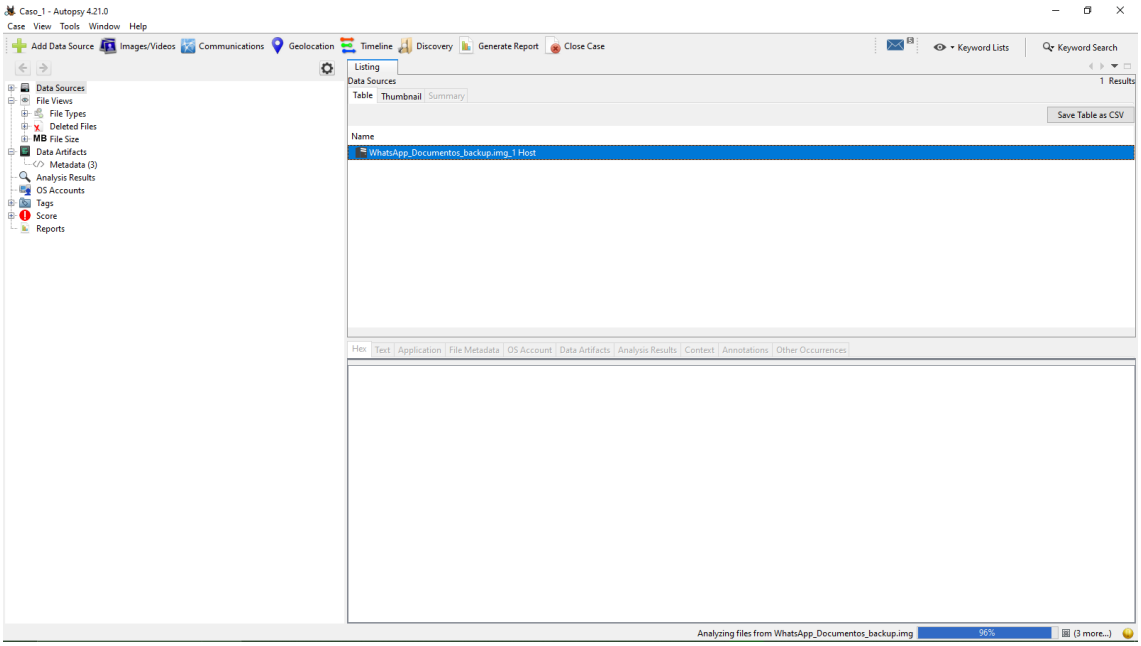


Imagen 60. Vista del host y módulos seleccionados en el panel izquierdo

40. En su proceso de recuperación la herramienta aplica la técnica de File Carving basado en fragmentación de un archivo especifico, pdf recuperados con éxito.

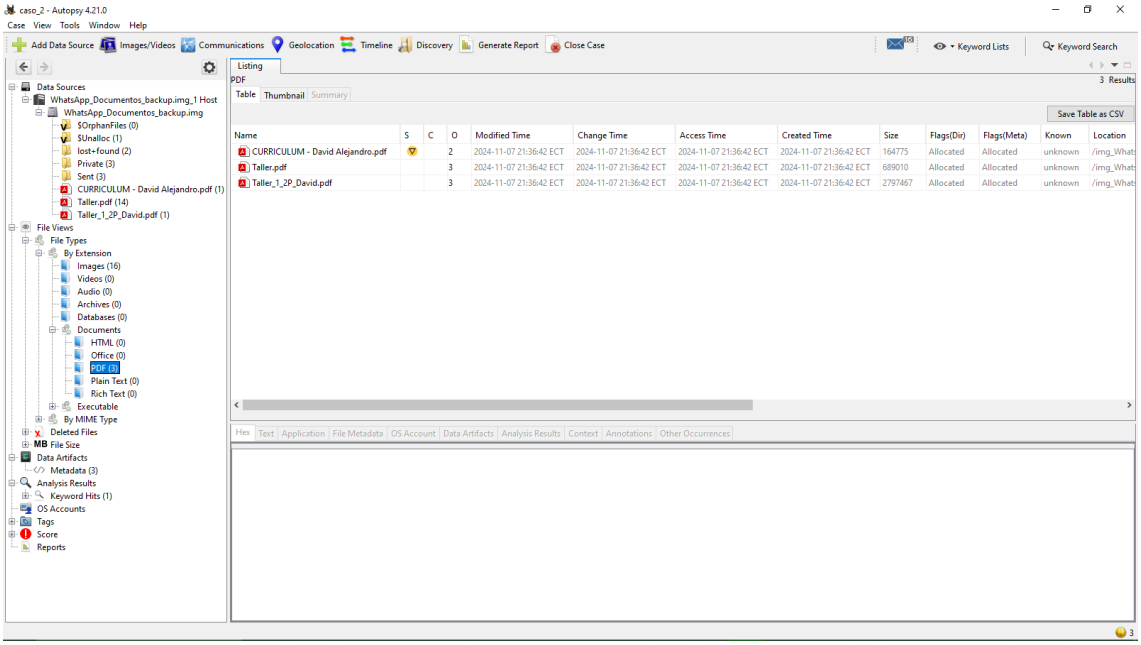


Imagen 61. Archivos PDF recuperados - File Carving basado en fragmentación

41. Dentro del análisis se recuperaron imágenes borradas dentro de la carpeta de WhatsApp.

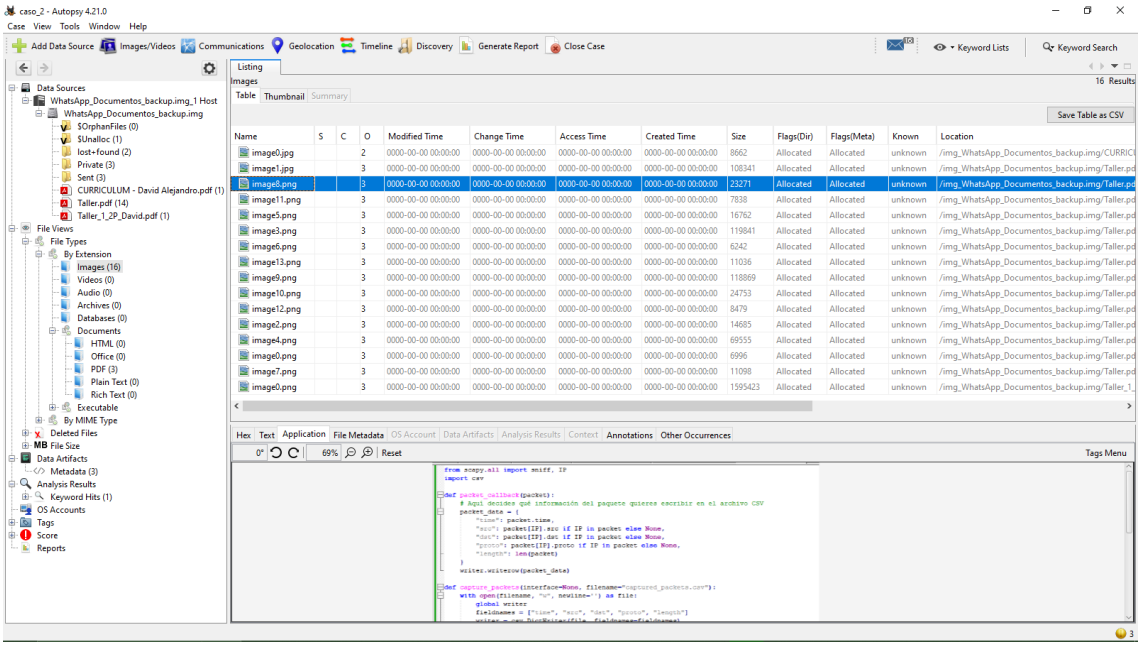


Imagen 62. Imágenes borradas de WhatsApp recuperadas durante el análisis

42. Al darle clic al archivo pdf, aparecen unas funciones que permiten visualizar el contenido hexadecimal, los metadatos y demás características sobre los archivos recuperados.

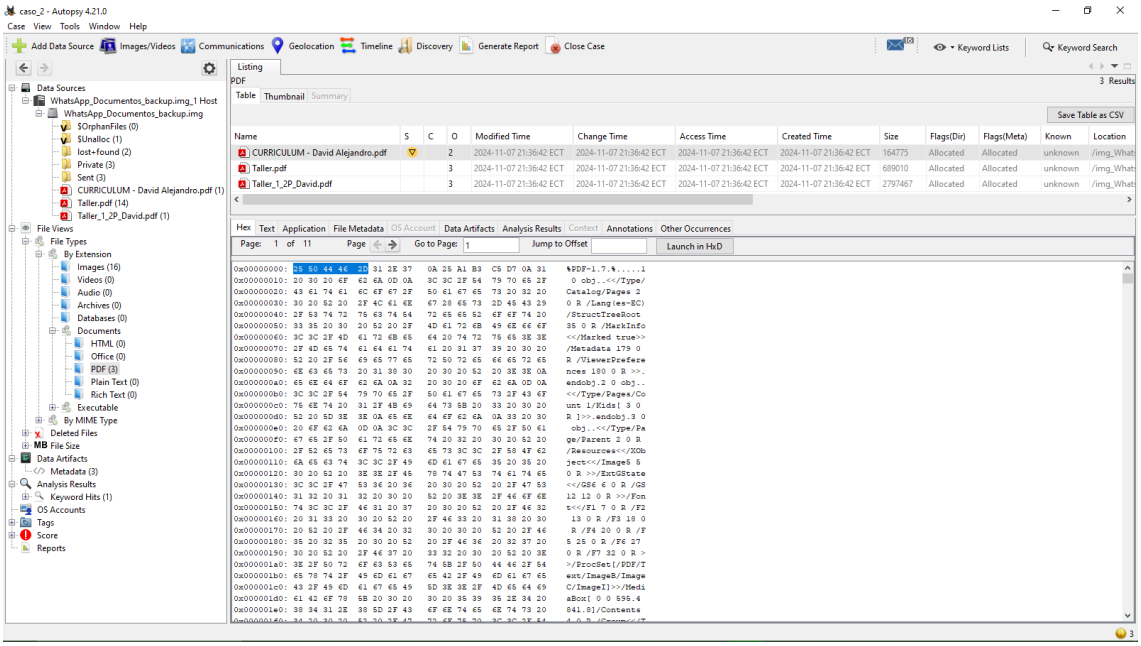


Imagen 63. Funciones para visualizar detalles de archivos PDF recuperados

Escenarios_4: Recuperar archivos de videos de la carpeta DCIM

Herramienta: SCALPEL

Tiempo: 5 minutos

Técnica: Carving basado por firmas

Objetivo: Recuperar archivos de videos extensión .mov de la carpeta media DCIM

43. Acceder al sistema de archivos del dispositivo Android con privilegios root,, específicamente hacia la carpeta **DCIM/media**, lo cual respalda el análisis y la recuperación de datos.

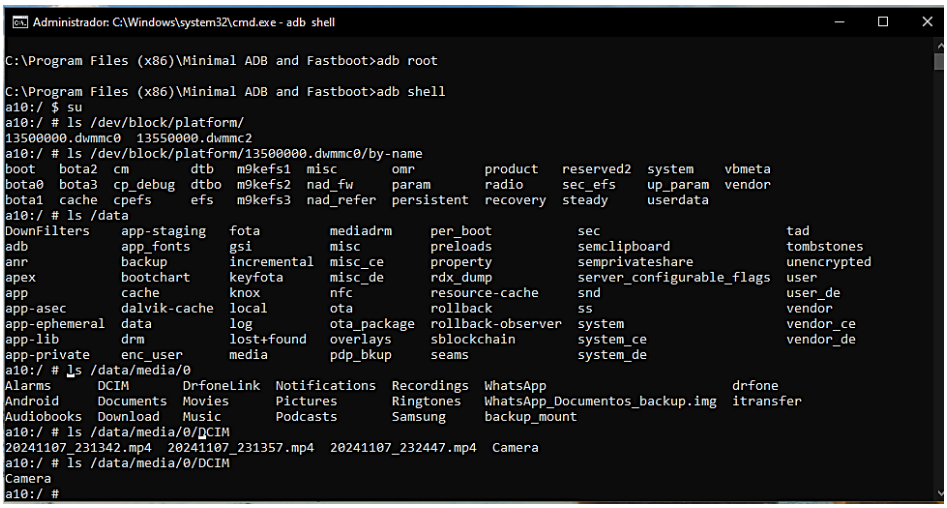


Imagen 64. Acceso a la carpeta con root, para crear una imagen de disco

44. Conectarse al dispositivo Android y realizar una copia de seguridad en formato de imagen del almacenamiento del dispositivo. Se crea y configura un archivo de sistema de respaldo utilizando comandos como **dd** y **mkfs.ext4**.

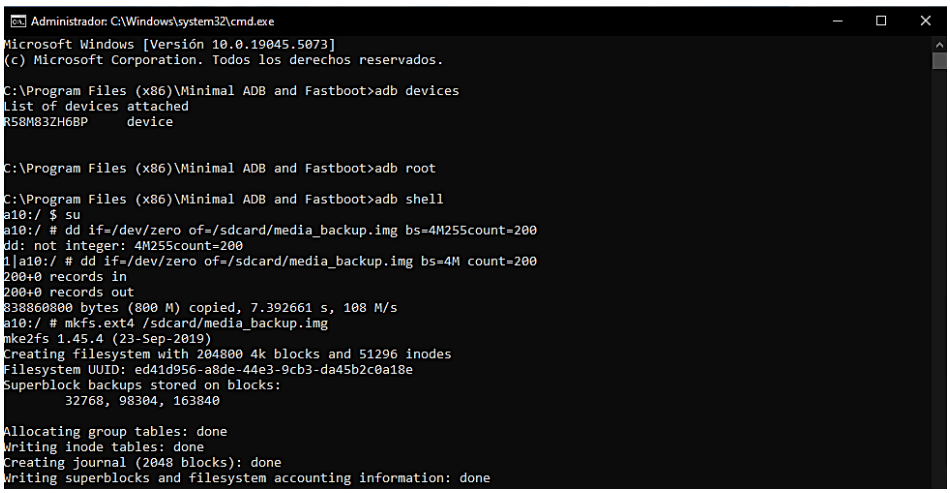


Imagen 65. Conexión ADB y respaldo del almacenamiento Android

45. Una vez finalizado la creación de imagen de la copia de seguridad de la carpeta media DCIM, abrir la herramienta scalpel.

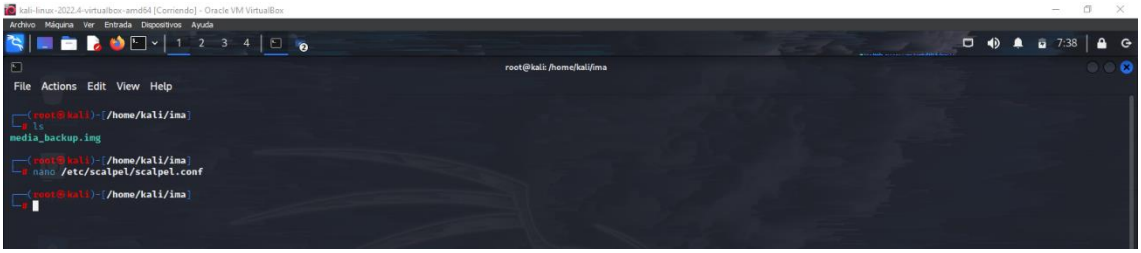


Imagen 66. Abrir Scalpel

46. Configuración **scalpel.conf** utilizando el editor de texto nano, activar los parámetros para recuperar archivos basados en firmas específicas, como formatos de video y .mov, este ajuste personaliza a la herramienta Scalpel.

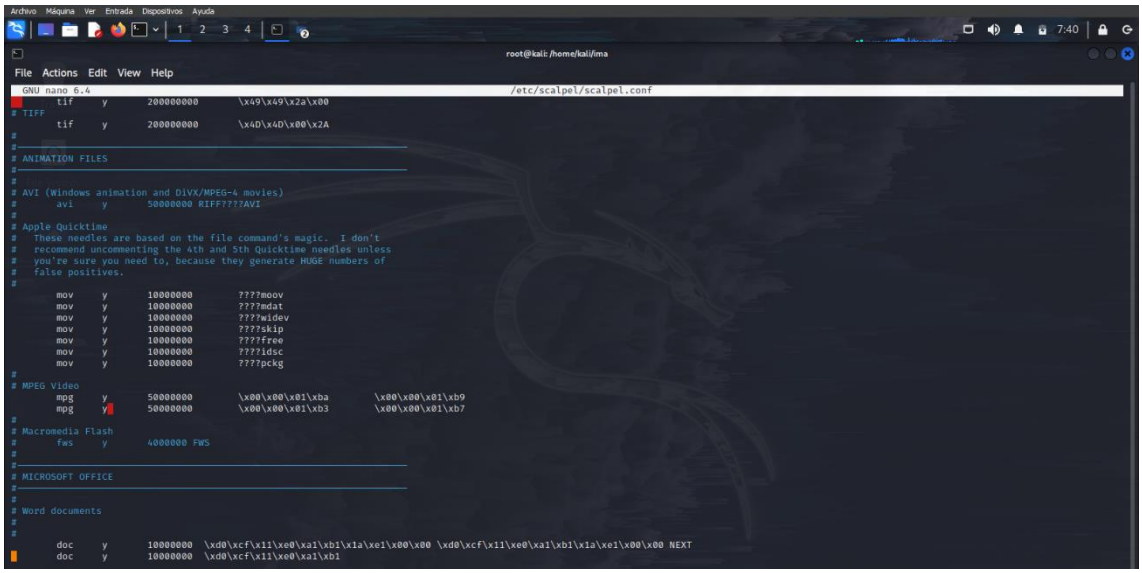


Imagen 67. Edición de scalpel.conf para configurar recuperación de archivos por firmas.

47. Buscar el archivo **media_backup.img**, la cual será la fuente de datos, crear la carpeta y especificar la ruta de destino **/home/kali/ima/recuperarvideo/**, ejecutamos scalpel con ruta correcta para almacenar los archivos recuperados.

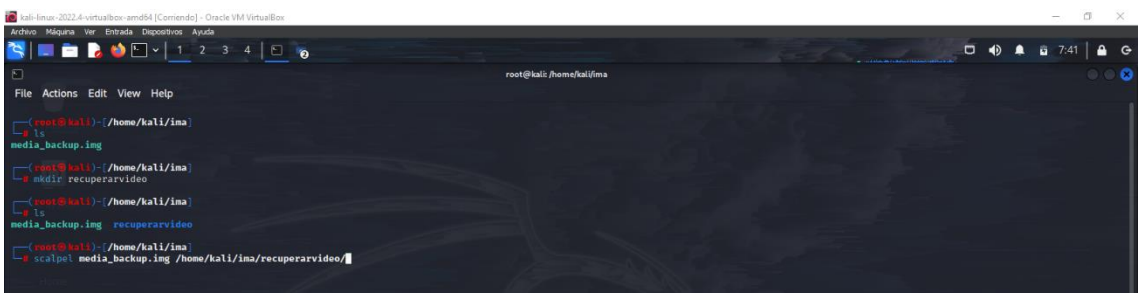


Imagen 68. Creación y verificación de directorios

48. Evidenciamos el progreso del análisis con un porcentaje (8.7%) y un tiempo estimado de finalización, para extraer archivos relevantes basados en las firmas configuradas.

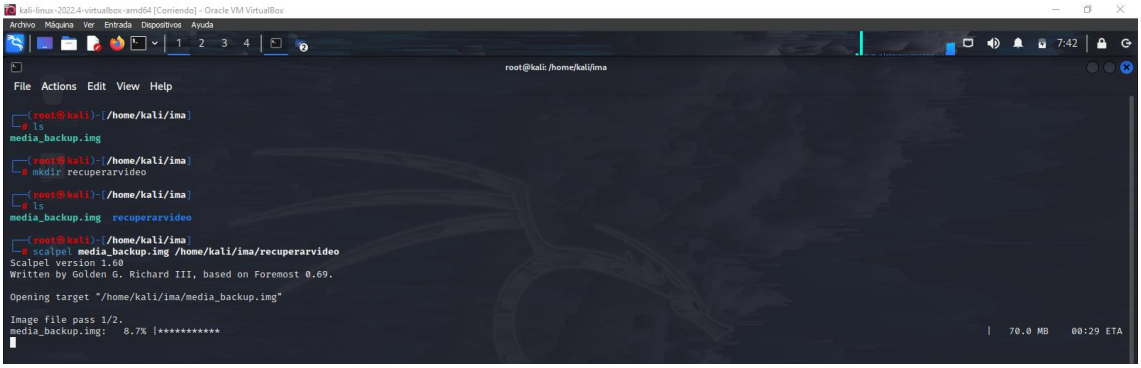


Imagen 69. Progreso del análisis y tiempo estimado, procesando datos

49. Buscando firmas headers y footers de diferentes tipos de archivos, como JPG, entre otros, reportando la cantidad que encuentra de cada tipo.

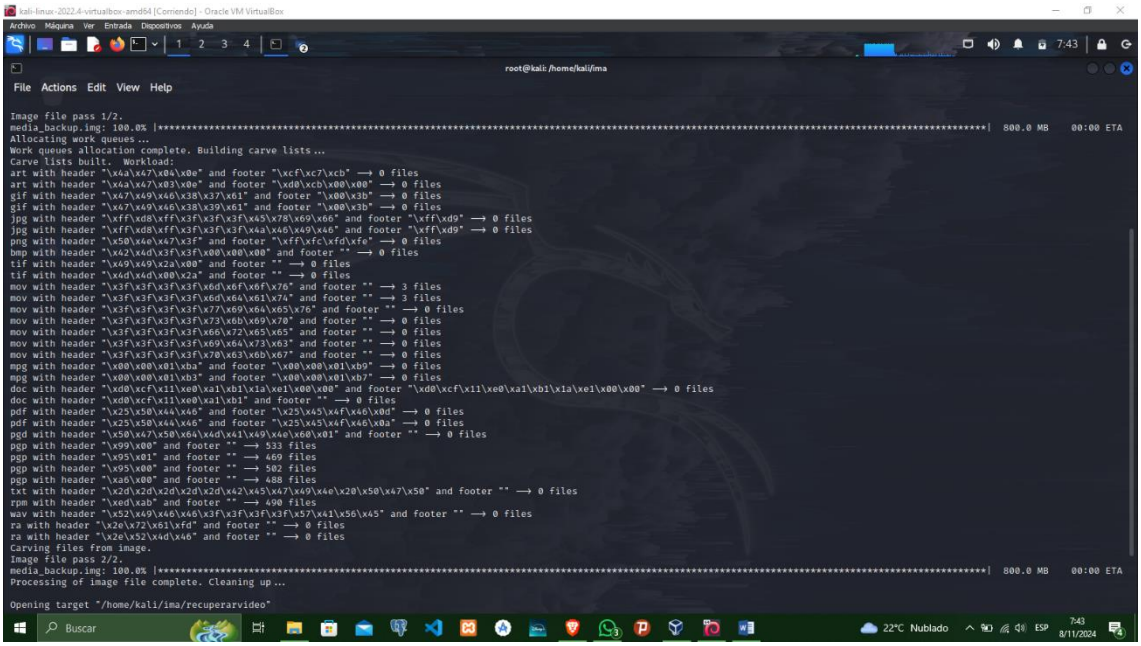


Imagen 70. Búsqueda de firmas de archivos como, cantidades encontradas por tipo

50. Listamos nuevamente, cambiamos el permiso del directorio con el siguiente comando "**chmod -R 777 scalpel-output"**, verificamos, accedemos al directorio **"cd scalpel-output"**.

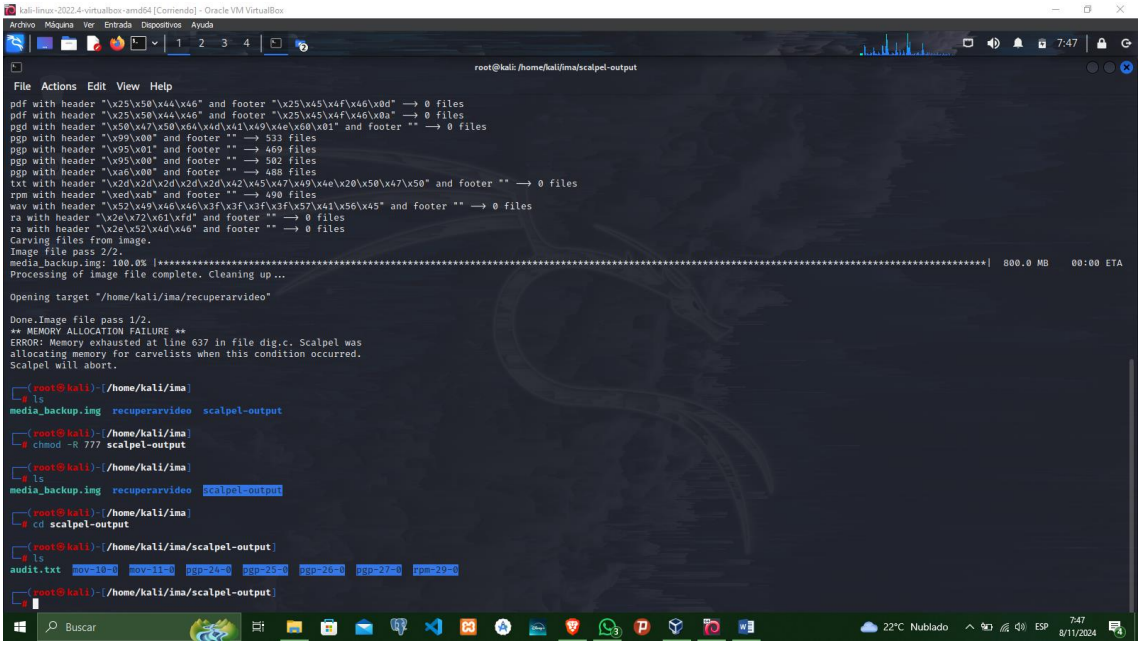


Imagen 71. Cambiar el permiso del directorio scalpel-output y acceder

51. Buscamos la carpeta donde se encuentran los elementos recuperados mediante el análisis.

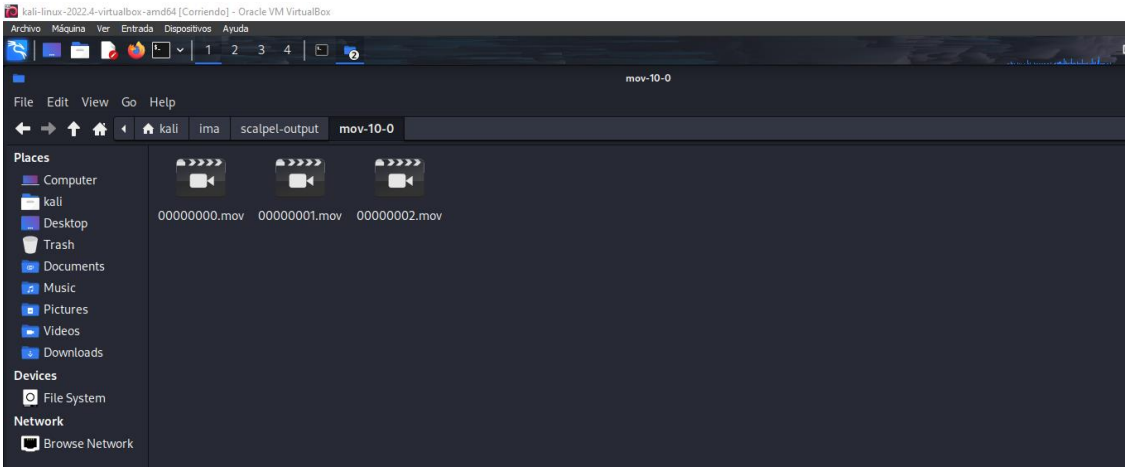


Imagen 72. Elementos recuperados

52. Elemento recuperado durante el análisis utilizando Carving basado en firmas.

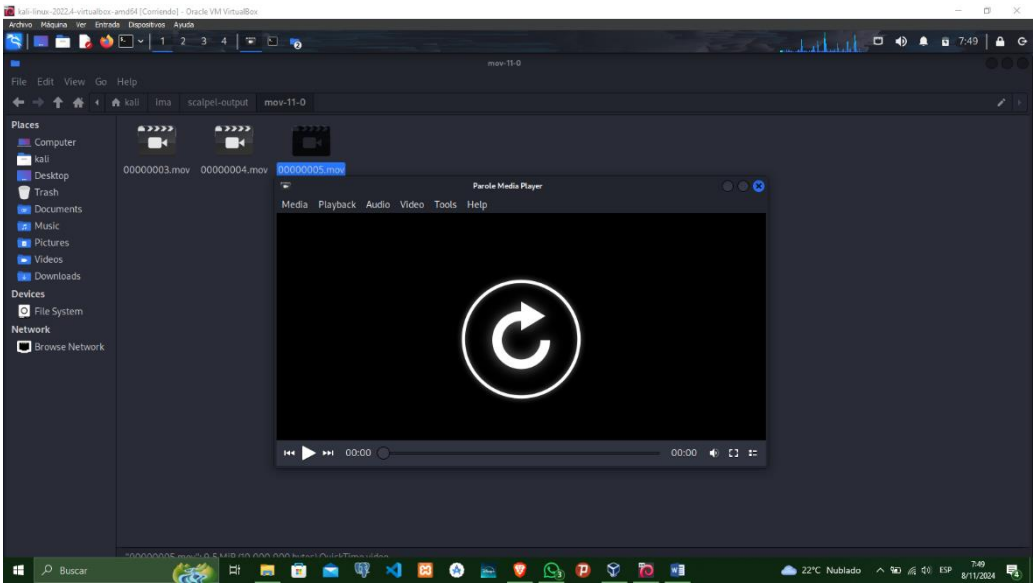


Imagen 73. Video recuperado usando Carving basado en firmas

Herramienta: FOREMOST

Tiempo: 5 minutos

Técnica: Carving basado por firmas

53. Editar la configuración de la herramienta Foremost, utilizando el editor de texto nano, el archivo abierto es **/etc/foremost.conf**.

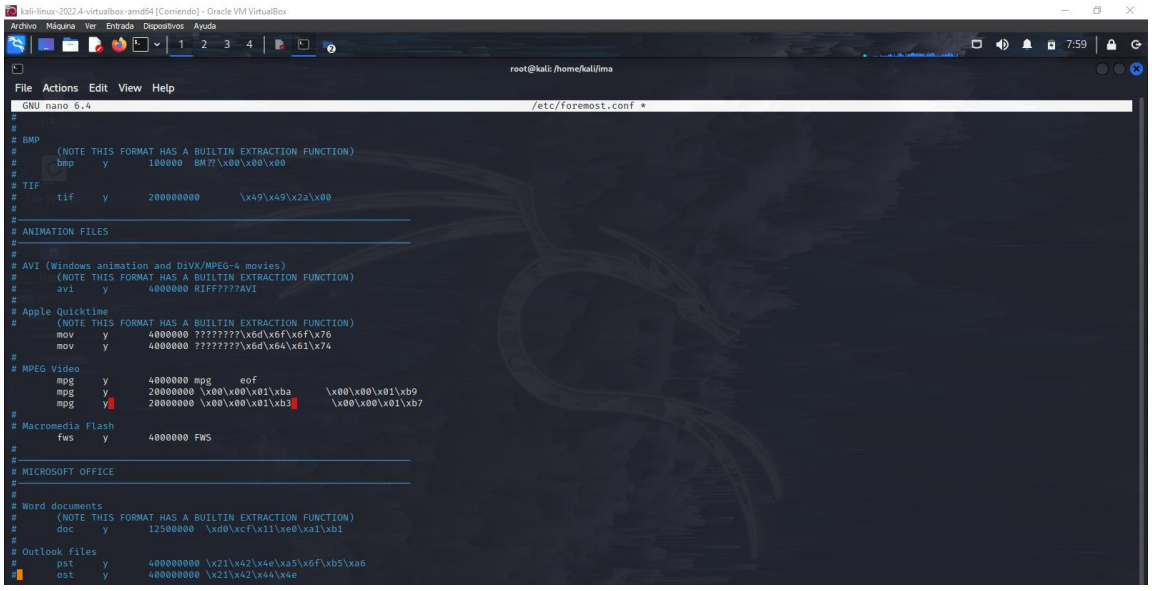


Imagen 74. Configuración de Foremost

54. Escribir el siguiente comando "**foremost -i media_backup.img -o /home/kali/ima/recuperarvideo**" donde "**-i**" especifica el archivo de entrada y "**-o**" indica donde serán almacenados los archivos recuperados.

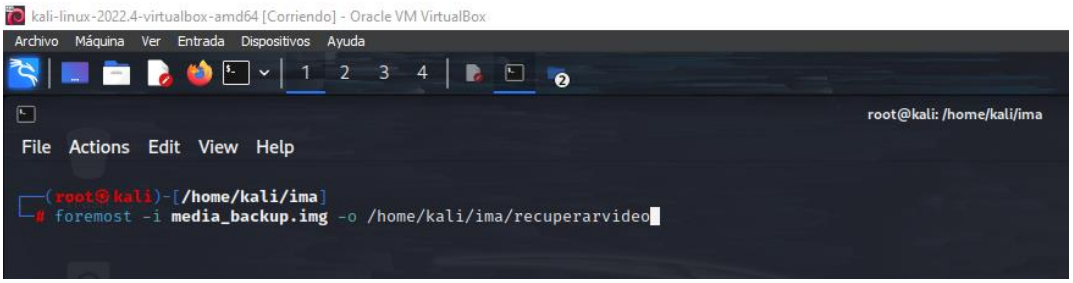


Imagen 75. Extracción de datos de la imagen de disco

55. Verificamos que podemos acceder a la carpeta creada "**recuperarvideo**", accedemos al directorio **"recuperarvideo"**, con "**ls**" listamos ingresamos a la carpeta "**mov**" y vemos los archivos .mov recuperados.

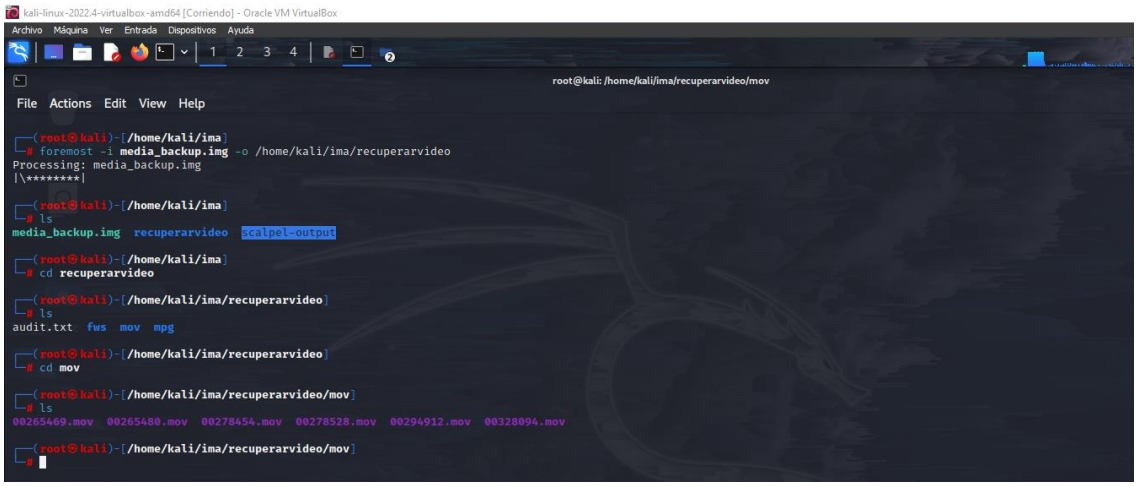


Imagen 76. Comandos para listar, acceder a las carpetas de los archivos recuperados

56. Cambiamos los permisos del directorio a todos los archivos y subdirectorios, para poder verlos dentro de la carpeta guardada.

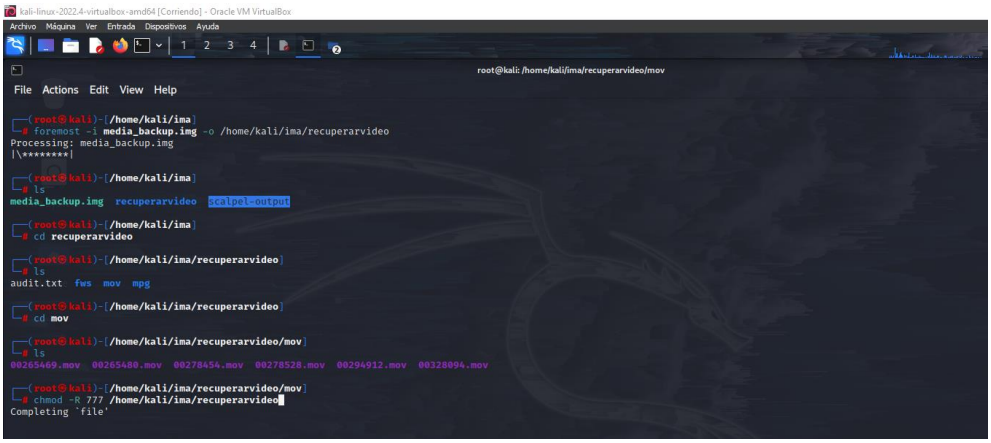


Imagen 77. Cambios de permisos a los directorio y archivos

57. Elementos recuperados durante el análisis utilizando Carving basado en firmas.

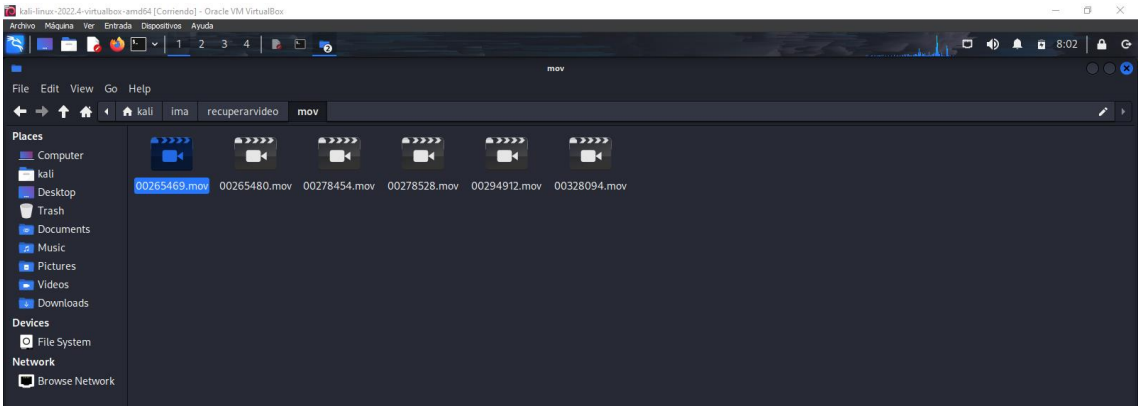


Imagen 78. Elementos recuperados

ANEXO #4
FASE: DOCUMENTACIÓN

MANUAL DE MEJORES PRÁCTICAS PARA LA APLICACIÓN DE TÉCNICAS DE FILE CARVING EN LA RECUPERACIÓN DE DATOS EN DISPOSITIVOS MÓVILES

INDÍCE

INTRODUCCIÓN

Es crucial en la informática forense la recuperación de datos en dispositivos móviles, particularmente cuando los archivos han sido borrados o los sistemas de archivos están dañados. El file carving es un método que posibilita la recuperación de archivos sin la necesidad de depender de la estructura del sistema de archivos, identificando patrones particulares en el contenido binario de la información.

Este manual está concebido para ofrecer una orientación práctica acerca de la implementación de file carving en aparatos móviles. En el documento, se tratarán las técnicas principales, las herramientas sugeridas y las mejores prácticas para recuperar información como imágenes, vídeos y documentos en plataformas como Android. Además, se proporcionarán ejemplos prácticos para simplificar su puesta en marcha.

ALCANCE

Este manual cubre el uso de técnicas de **file carving** para recuperar datos en dispositivos móviles, especialmente en Android. Se enfoca en la recuperación de archivos eliminados o inaccesibles debido a daños en el sistema de archivos o formateo, utilizando herramientas especializadas. No aborda la recuperación en dispositivos cifrados sin autorización ni la recuperación a nivel físico de discos dañados.

OBJETIVO

Proporcionar una guía práctica para recuperar datos en dispositivos móviles mediante técnicas de file carving, utilizando metodologías y herramientas especializadas de manera eficiente y ética.

ANALISIS DE ESCENARIOS

Escenario	Objetivo	Técnica Utilizada	Herramienta	Parámetros	Análisis	Resultado
1. Tarjeta SD formateada accidentalmente – Recuperar Imágenes JPG	Recuperar imágenes JPG tras formateo accidental	Carving basado en la estructura del Sistema de Archivos	HxD Editor Hexadecimal	Tipo de archivo: JPG Condición de la SD: Formateada, no sobrescrita Nivel de fragmentación: Alta Tamaño de archivo: 2-5 MB	La fragmentación alta afectó la recuperación, pero las cabeceras y pies permitieron identificar fragmentos de imágenes. La recuperación fue parcial debido a la fragmentación.	Recuperación de 4 imágenes JPG completas, con limitación por fragmentación.
2. Tarjeta SD formateada accidentalmente – Recuperar todos los archivos existentes	Recuperar todos los archivos (imágenes, documentos, videos)	Carving basado en Firmas	PhotoRec	Tipos de archivo: Imágenes, videos, documentos (PDF, DOCX) Condición de la SD: Formateada, no sobrescrita Tamaño de archivos: 100 KB a 10 GB Tasa de recuperación: Alta	La técnica de carving con firmas permitió recuperar una variedad de archivos. Sin embargo, la sobrescritura parcial hizo que algunos archivos no pudieran recuperarse completamente.	Recuperación de 10,500 archivos clasificados en 20 carpetas (~520 archivos por carpeta).

3. Recuperar documentos PDF de WhatsApp Documentos	Recuperar archivos PDF de WhatsApp	Carving Fragmentado & Carving basado en Cabeceras y Pies	Autopsy	Tipo de archivo: PDF Condición de la SD: Fragmentada Fragmentación de los archivos: Alta Metadatos recuperados: Imágenes, correos electrónicos	El carving fragmentado y la búsqueda de cabeceras/pies permitieron recuperar los documentos PDF. **Autopsy** ayudó a extraer metadatos adicionales como imágenes y correos asociados.	Recuperación de 3 PDFs, con 16 imágenes y 1 correo electrónico.
4. Recuperar archivos de video de DCIM	Recuperar videos MOV de la carpeta DCIM	Carving basado en Firmas	Scalpel	Tipo de archivo: MOV Condición de la SD: Sobrescrita parcialmente Tamaño de archivo: 10-100 MB Fragmentación: Baja	**Scalpel** identificó los videos MOV mediante firmas, pero la sobrescritura parcial afectó la recuperación de algunos archivos.	Recuperación de 6 videos con análisis de integridad.

HERRAMIENTAS RECOMENDADAS

Herramienta	Puntos Fuertes	Puntos Débiles	Soporte de Archivos
PhotoRec	- Recupera una amplia variedad de tipos de archivo (imágenes, videos, documentos) - Fácil de usar con pocos requerimientos de hardware - Soporta múltiples sistemas de archivos	- No recupera la estructura de carpetas original - Recuperación parcial en casos de sobrescritura de datos - Interfaz de usuario básica (línea de comandos)	- Imágenes: JPG, PNG, GIF, BMP, TIFF, etc. - Videos: AVI, MOV, MP4, MKV, etc. - Documentos: PDF, DOCX, XLSX, etc.
Scalpel	- Rápido y eficiente en la recuperación por firmas - Personalizable para diferentes tipos de archivos - Uso eficiente de recursos	- Solo trabaja con firmas predefinidas, limitando la flexibilidad - No maneja bien la fragmentación de archivos - Requiere conocimientos técnicos para configurar y personalizar las firmas	- Imágenes: JPG, PNG, GIF, BMP, TIFF - Archivos de texto: TXT, CSV - Videos: MOV, AVI, MP4
Autopsy	- Interfaz gráfica fácil de usar - Soporta una variedad de análisis forenses (metadatos, imágenes, correos, etc.) - Funciones avanzadas para visualización de datos recuperados	- Requiere más recursos de hardware y tiempo para grandes volúmenes de datos - Puede ser más lento que herramientas especializadas en carving	- Imágenes: JPG, PNG, GIF, BMP - Documentos: DOCX, PDF, TXT - Archivos de video: AVI, MOV, MP4, etc.
HxD Editor Hexadecimal	- Permite una visualización detallada y edición de los datos en bruto - Muy útil para recuperación manual y análisis de fragmentos	- Requiere un alto nivel de conocimiento técnico - No está específicamente diseñado para carving, lo que lo hace más lento para grandes volúmenes de datos	- Soporta todos los tipos de archivo, pero es necesario identificar manualmente las cabeceras y pies de cada archivo

Recuva	- Fácil de usar y tiene una interfaz amigable para usuarios no técnicos - Buen rendimiento en la recuperación de archivos eliminados accidentalmente - Soporta análisis de discos duros, tarjetas SD, y más	- No es tan efectivo en la recuperación de archivos tras formateos o sobrescrituras	- Imágenes: JPG, PNG, GIF, BMP - Videos: MP4, MOV, AVI - Archivos de documentos: PDF, DOCX, TXT
FTK Imager	- Excelente para la creación de imágenes forenses de discos - Ofrece una visualización de los archivos recuperados de forma organizada - Compatible con sistemas de archivos complejos	- Requiere hardware potente para el manejo de imágenes grandes - Licencia comercial necesaria para funciones avanzadas	- Imágenes: JPG, PNG, GIF, BMP - Videos: AVI, MOV, MP4, MKV - Documentos: DOCX, XLSX, PDF
TestDisk	- Recuperación de particiones y sectores de arranque - Potente para la recuperación de discos y particiones dañadas - Soporta múltiples sistemas de archivos	- Solo tiene interfaz de línea de comandos, lo que puede ser complicado para novatos - No es tan efectivo para recuperación de archivos individuales	- Soporta sistemas de archivos: FAT, NTFS, ext4, HFS, etc. - No se especializa en tipos de archivo específicos como las herramientas de carving

MEJORES PRÁCTICAS

CREACIÓN DE IMÁGENES:

- **Descripción:** Siempre trabajar con una copia bit a bit del dispositivo original, conocida como imagen forense, para evitar modificar la evidencia original.
- **Implementación adicional:**
    - Verificar la integridad de la imagen mediante el uso de hashes (MD5, SHA-1) para garantizar que la copia es exacta.
    - Crear las imágenes en un formato forense estándar, como. E01 o .dd, que incluya metadatos para asegurar la trazabilidad.

DOCUMENTACIÓN DEL PROCESO:

- **Descripción:** Mantener un registro detallado de cada paso en el proceso de recuperación, incluyendo las herramientas utilizadas, configuraciones específicas y los resultados obtenidos.
- **Implementación adicional:**
    - Registrar las fechas y horas exactas de cada acción realizada durante el análisis.
    - Incluir capturas de pantalla, logs y reportes generados por las herramientas utilizadas.
    - Utilizar un formato estandarizado para facilitar la revisión y auditoría del proceso, como un diario de trabajo o un informe técnico.

VERIFICACIÓN DE DATOS RECUPERADOS:

- **Descripción:** Es crucial validar que los archivos recuperados sean correctos y no estén dañados o corruptos.
- **Implementación adicional:**
    - Comparar los datos recuperados con las firmas de archivos conocidas, utilizando bases de datos de firmas o hashes de archivos de referencia.
    - Realizar una prueba de integridad de los archivos, como la apertura de archivos de imagen o vídeo para verificar que no están dañados.

CUMPLIMIENTO ÉTICO Y LEGAL:

- **Descripción:** Asegurar que todas las acciones realizadas cumplan con las leyes de privacidad y los estándares éticos correspondientes.
- **Implementación adicional:**
    - Obtener el consentimiento explícito del propietario del dispositivo, o de una persona autorizada, para proceder con el análisis y la recuperación de datos.
    - Asegurarse de que los datos sensibles y privados sean tratados con respeto, cumpliendo con las leyes de protección de datos (como el RGPD o la Ley de Privacidad de Información Personal en Internet).
    - Utilizar procedimientos audibles y transparentes que aseguren la trazabilidad y la legitimidad del análisis.

USO DE HERRAMIENTAS VALIDADAS:

- **Descripción:** Seleccionar herramientas que estén certificadas y validadas para la recuperación de datos en función de las necesidades específicas del análisis.
- **Implementación adicional:**
    - Utilizar herramientas que sean reconocidas en la comunidad forense por su fiabilidad y capacidad de recuperación de datos, como PhotoRec**,** FTK Imager, Autopsy**.**
    - Realizar pruebas de recuperación periódicas utilizando diferentes herramientas para comparar resultados y asegurar la mejor opción.

MINIMIZACIÓN DEL ACCESO AL DISPOSITIVO:

- **Descripción:** Para evitar la alteración de datos, es importante limitar al máximo el acceso al dispositivo original durante el análisis.
- **Implementación adicional:**
    - Utilizar un entorno de análisis aislado para evitar que el sistema operativo del dispositivo afecte la integridad de los datos.
    - Montar la imagen forense en modo solo lectura para evitar modificaciones accidentales.

- Desconectar el dispositivo de redes, evitando posibles sincronizaciones automáticas con servicios en la nube que puedan modificar los datos.

CONTROL DE CALIDAD DURANTE EL PROCESO:

- **Descripción:** Asegurar que el análisis y la recuperación se realicen con la máxima precisión y siguiendo procedimientos estandarizados.
- **Implementación adicional:**
  - Establecer un sistema de control de calidad en el que cada paso del proceso sea revisado y auditado por otro miembro del equipo.
  - Realizar pruebas de recuperación controlada para verificar que las herramientas de recuperación están funcionando correctamente antes de aplicar técnicas de file carving en el dispositivo original.

GESTIÓN ADECUADA DE EVIDENCIAS:

- **Descripción:** Las evidencias recuperadas deben ser manejadas con extrema cautela para evitar su alteración o pérdida.
- **Implementación adicional:**
  - Utilizar una cadena de custodia formalizada para registrar quién tiene acceso a las evidencias en todo momento.
  - Segregar las evidencias físicas y lógicas en ubicaciones seguras y protegidas.
  - Asegurarse de que los archivos recuperados sean copiados y almacenados en un medio independiente para evitar riesgos de alteración.

EVALUACIÓN DE LA VIABILIDAD DE LA RECUPERACIÓN:

- **Descripción:** Antes de iniciar la recuperación de datos, evaluar la probabilidad de éxito y la cantidad de datos que pueden ser recuperados, especialmente en casos de dispositivos dañados o formateados.
- **Implementación adicional:**
  - Realizar un análisis preliminar para estimar el nivel de fragmentación y la posibilidad de recuperación.

- Considerar la recuperación por partes, priorizando los archivos más importantes según el caso.

USO DE TÉCNICAS DE RECUPERACIÓN ESPECIALIZADAS:

- **Descripción:** Emplear técnicas de recuperación avanzadas en función del tipo de archivo y la estructura del sistema de archivos.
- **Implementación adicional:**
  - Para sistemas de archivos ext4 o NTFS, usar herramientas especializadas que entiendan la estructura del sistema y permitan la recuperación de archivos fragmentados.
  - Aplicar técnicas como carving basado en cabeceras y pies**,** carving basado en firmas o carving fragmentado según el tipo de datos y el nivel de daño.

PRUEBAS EN MÚLTIPLES ESCENARIOS:

- **Descripción:** Realizar el análisis en diferentes escenarios para garantizar que todos los posibles tipos de fragmentación o daños sean considerados.
- **Implementación adicional:**
  - Realizar pruebas en diferentes dispositivos o particiones para confirmar la efectividad de las herramientas y metodologías aplicadas.
  - Emplear muestras de control o imágenes de prueba para validar el enfoque de recuperación antes de analizar el dispositivo original.

OBSERVACIONES TÉCNICAS

- La fragmentación de archivos en tarjetas SD afecta la recuperación de datos.
- Las herramientas de carving tienen resultados variados dependiendo del nivel de daño en el sistema de archivos.
- El tiempo de recuperación está directamente relacionado con la cantidad de datos y la fragmentación.
- Los archivos parcialmente recuperados pueden perder calidad o integridad.
- La sincronización en la nube puede interferir en la recuperación de datos.

- El análisis forense de dispositivos Android requiere acceso root para mejores resultados.
- Las bases de datos de firmas de herramientas deben estar actualizadas para recuperar formatos recientes.
- Las tarjetas SD tienen mayor tasa de recuperación cuando no se sobrescriben datos tras el formateo.
- La calidad de los datos recuperados varía entre herramientas.
- Los archivos multimedia como videos y fotos tienen mayor probabilidad de recuperación completa.

RECOMENDACIONES

- Realizar el **rooteo** en dispositivos Android para acceso completo.
- Trabajar siempre con **imágenes forenses** del dispositivo para preservar la evidencia original.
- Desactivar la **sincronización en la nube** antes de iniciar el análisis.
- Utilizar herramientas de carving especializadas según el tipo de archivo a recuperar.
- Verificar la integridad de los datos recuperados mediante hashes.
- Realizar análisis en entornos aislados para evitar alteraciones de datos.
- Documentar cada paso del proceso de recuperación.
- Implementar controles de calidad durante el análisis para validar resultados.
- Repetir el proceso con distintas técnicas si el nivel de recuperación no es satisfactorio.
- Evaluar la fragmentación de los datos antes de decidir el enfoque de recuperación.