REVISIÓN DE EFECTIVIDAD DE HERRAMIENTAS FORENSES EN LA EXTRACCIÓN Y RECUPERACIÓN DE DATOS EN DISPOSITIVOS DE ALMACENAMIENTO MASIVO DE EQUIPOS PERSONALES

YUBIAN GUILLERMO DALLOS SANTOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2024

REVISIÓN DE EFECTIVIDAD DE HERRAMIENTAS FORENSES EN LA EXTRACCIÓN Y RECUPERACIÓN DE DATOS EN DISPOSITIVOS DE ALMACENAMIENTO MASIVO DE EQUIPOS PERSONALES

YUBIAN GUILLERMO DALLOS SANTOS

Proyecto de Grado – Monografía presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMATICA

Asesor: EDUARD ANTONIO MANTILLA TORRES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2024

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá, mayo de 2024

DEDICATORIA

Con profundo amor dedico este trabajo a mi esposa e hijos, que con su amor y comprensión me han acompañado en mi trasegar, colaborándome de manera directa e indirecta y alentándome permanentemente para culminar este y tantos otros proyectos.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar paralelamente, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

CONTENIDO

Pág.

INTRODUCCIÓN 17
1. DEFINICIÓN DEL PROBLEMA 18
1.1 ANTECEDENTES DEL PROBLEMA 18
1.2 FORMULACIÓN DEL PROBLEMA 19
2 JUSTIFICACIÓN 20
3 OBJETIVOS 21
3.1 OBJETIVOS GENERAL 21
3.2 OBJETIVOS ESPECÍFICOS 21
4 MARCO REFERENCIAL 22
4.1 MARCO TEÓRICO 22
4.1.1 INFORMATICA FORENSE 22
4.1.2 EXTRACCIÓN DE INFORMACIÓN 23
4.1.3 DISPOSITIVOS DE ALMACENAMIENTO MASIVO 24
4.1.4 CRIPTOGRAFÍA 24
4.1.5 ELIMINACIÓN DE DATOS 24
4.1.6 COMPRESIÓN 25
4.1.7 CONSIDERACIONES ETICAS Y LEGALES 25
4.2 MARCO CONCEPTUAL 26
4.2.1 AUTENTICIDAD 26
4.2.2 INTEGRIDAD 26
4.2.3 ADMISIBILIDAD 27
4.2.4 EXTRACCIÓN FORENSE DE DATOS 27
4.2.5 RECUPERACIÓN FORENSE DE DATOS 27
4.2.6 INTEGRIDAD DE LOS DATOS 27
4.2.7 CADENA DE CUSTODIA 27
4.2.8 HERRAMIENTAS FORENSES 27
4.3 MARCO HISTÓRICO 28
4.4 ANTECDENTES O ESTADO ACTUAL 30
4.5 MARCO CIENTÍFICO O TECNOLÓGICO 32
4.5.1 SISTEMA DE ARCHIVOS 32
4.5.2 SOFTWARE DE RECUPERACIÓN DE DATOS 33
4.5.3 TÉCNICAS FORENSES 33
4.5.4 IMÁGENES DE DISCO 33
4.5.5 ALGORITMOS DE RECUPERACIÓN DE DATOS 33

4.5.6 HERRAMIENTAS FORENSES 33
4.6 MARCO LEGAL 39
4.7 MARCO REGLAMENTARIO 39
5 SELECCIÓN DE LAS HERRAMIENTAS FORENSES 41
5.1 HERRAMIENTA FORENSE AXIOM 41
5.2 HERRAMIENTA FORENSE WONDERSHARE RECOVERIT 43
5.2.1 CARACTERÍSTICAS Y FUNCIONALIDADES 44
5.2.2 CAPACIDAD PARA RECUPERAR DATOS PERDIDOS O ELIMINADOS 45
5.2.3 MODOS DE RECUPERACIÓN DE WONDERSHARE RECOVERIT 46
5.2.4 PROCESO DE RECUPERACIÓN SENCILLO EN WONDERSHARE RECOVERIT 48
5.3 HERRAMIENTA FORENSE FTK 50
5.4 HERRAMIENTA FORENSE AUTOPSY 52
6 PLANIFICACIÓN PARA LA REALIZACIÓN DE PRUEBAS 55
6.1 REALIZACIÓN DE LA IMAGEN FORENSE 55
6.2 SOFTWARE PARA LA GENERACIÓN DE LA IMAGEN FORENSE 57
6.3 PRUEBAS 58
6.4 HERRAMIENTAS 60
6.5 RESULTADOS 61
7 REALIZACIÓN Y EJECUCIÓN DE PRUEBAS 63
7.1 DISCO DURO EXTERNO 63
7.2 DISCO DURO INTERNO 64
7.3 MEMORIA USB 65
7.4 MEMORIA MICRO SD 66
7.5 ANÁLISIS DE RESULTADOS 91
7.6 ANÁLISIS DE RESULTADOS EN MEMORIA USB 64 GB 91
7.7 ANÁLISIS DE RESULTADOS EN MICRO SD 32 GB 92
7.8 ANÁLISIS DE RESULTADOS EN DISCO DURO 2 TB 92
7.9 ANÁLISIS COMPARATIVO 93
8 CONCLUSIONES 97
9 RECOMENDACIONES 99
10 BIBLIOGRAFÍA 100

LISTA DE TABLAS

Pág.

Tabla 1 Comparativo de las herramientas forenses ……..….. 37
Tabla 2 Comparativo de las herramientas forenses en Memoria USB 64 GB….. 92
Tabla 3 Comparativo de las herramientas forenses en MICRO SD 32 GB…..... 92
Tabla 4 Comparativo de las herramientas forenses en Disco duro interno..……. 93

LISTA DE FIGURAS

Pág.

Figura 1 Interfaz gráfica de usuario Axiom 41
Figura 2 Interfaz gráfica de usuario de Wondershare Recoverit.....44
Figura 3 Interfaz gráfica de usuario de FTK.....51
Figura 4 Interfaz gráfica de usuario Autopsy 53
Figura 5 Interfaz gráfica de usuario FTK Imager versión 4.5.0.3 58
Figura 6 Disco duro interno de 2 TB marca Seagate. 63
Figura 7 Creación de la imagen forense con FTK Imager versión 4.5.0.3 64
Figura 8 Memoria USB de 64 GB marca Kingston.....64
Figura 9 Creación de la imagen forense con FTK Imager versión 4.5.0.3 65
Figura 10 Memoria Micro SD de 32 GB marca SanDisk Ultra 65
Figura 11 Creación de la imagen forense con FTK Imager versión 4.5.0.3 66
Figura 12 Procesamiento de la imagen forense de la MEMORIA USB en la herramienta AXIOM 67
Figura 13 Archivos existentes y recuperados del dispositivo MEMORIA USB en la herramienta AXIOM 68
Figura 14 Procesamiento de la imagen forense de la MEMORIA USB en la herramienta AUTOPSY.....69
Figura 15 Archivos existentes y recuperados del dispositivo MEMORIA USB en la herramienta AUTOPSY.....70
Figura 16 Procesamiento de la imagen forense de la MEMORIA USB en la herramienta WONDERSHARE RECOVERIT 71
Figura 17 Archivos existentes y recuperados del dispositivo MEMORIA USB en la herramienta WONDERSHARE RECOVERIT 72
Figura 18 Procesamiento de la imagen forense de la MEMORIA USB en la herramienta FTK.....73
Figura 19 Archivos existentes y recuperados del dispositivo MEMORIA USB en la herramienta FTK.....74
Figura 20 Procesamiento de la imagen forense de la MICRO SD en la herramienta AXIOM 75
Figura 21 Archivos existentes y recuperados del dispositivo MICRO SD en la herramienta AXIOM 76
Figura 22 Procesamiento de la imagen forense de la MICRO SD en la herramienta AUTOPSY.....77
Figura 23 Archivos existentes y recuperados del dispositivo MICRO SD en la herramienta AUTOPSY.....78
Figura 24 Procesamiento de la imagen forense de la MICRO SD en la herramienta WONDERSHARE RECOVERIT 79
Figura 25 Archivos existentes y recuperados del dispositivo MICRO SD en la herramienta WONDERSHARE RECOVERIT. 80
Figura 26 Procesamiento de la imagen forense de la MICRO SD en la herramienta FTK. 81

Figura 27 Archivos existentes y recuperados del dispositivo MICRO SD en la herramienta FTK 82
Figura 28 Procesamiento de la imagen forense de la DISCO DURO INTERNO en la herramienta AXIOM 83
Figura 29 Archivos existentes y recuperados del dispositivo DISCO DURO INTERNO en la herramienta AXIOM. 84
Figura 30 Procesamiento de la imagen forense de la DISCO DURO INTERNO en la herramienta AUTOPSY 85
Figura 31 Archivos existentes y recuperados del dispositivo DISCO DURO INTERNO en la herramienta AUTOPSY 86
Figura 32 Procesamiento de la imagen forense de la DISCO DURO INTERNO en la herramienta WONDERSHARE RECOVERIT 87
Figura 33 Archivos existentes y recuperados del dispositivo DISCO DURO INTERNO en la herramienta WONDERSHARE RECOVERIT 88
Figura 34 Procesamiento de la imagen forense de la DISCO DURO INTERNO en la herramienta FTK 89
Figura 35 Archivos existentes y recuperados del dispositivo DISCO DURO INTERNO en la herramienta FTK 90

LISTA DE CUADROS

Pág.

Cuadro 1 Comparativo de herramientas forenses utilizadas en dispositivos de almacenamiento masivo…….94

LISTA DE ANEXOS

Pág.

Anexo A Titulo de anexo.....

(Se indican de dos formas: Si son menos de 27 anexos, se listan con las letras del alfabeto, si son mayores de 27 anexos, se listan con números. Al igual que las anteriores listas, también llevan el título completo en mayúscula inicial y esta tabla debe ser automática)

GLOSARIO

CADENA DE CUSTODIA: Proceso documentado y controlado que se aplica a la evidencia física o digital desde el momento de su recolección inicial hasta su presentación en un tribunal u otro contexto legal. Es un procedimiento fundamental para garantizar la integridad, autenticidad y confiabilidad de la evidencia a lo largo de todo el proceso, evitando su alteración, contaminación o manipulación.

CONFIDENCIALIDAD: Propiedad o característica de la información o los datos que asegura que solo las personas autorizadas tengan acceso y conocimiento de ellos. Implica mantener la privacidad y evitar la divulgación no autorizada o el acceso no permitido a la información sensible.

CRIPTOGRAFIA: Campo de estudio y práctica que se enfoca en técnicas y métodos para proteger y asegurar la información mediante el uso de algoritmos y claves de cifrado. Consiste en transformar datos legibles en un formato ininteligible llamado texto cifrado, con el objetivo de proteger la confidencialidad, la integridad y la autenticidad de la información.

DATOS: Se refieren a representaciones simbólicas de hechos, información o conocimiento. Son valores numéricos, textos, imágenes, sonidos u otro tipo de información que se almacenan, procesan y transmiten en formato digital.

DISPONIBILIDAD: Propiedad o característica de la información, los sistemas o los recursos tecnológicos de estar accesibles y funcionales cuando se necesitan. Implica que la información o los servicios estén disponibles y utilizable en el momento requerido, sin interrupciones o fallos significativos.

DISPOSITIVOS DE ALMACENAMIENTO MASIVO: Dispositivos electrónicos diseñados para almacenar grandes cantidades de datos de manera permanente o temporal. Estos dispositivos proporcionan capacidad de almacenamiento adicional y permiten a los usuarios guardar y acceder a archivos, documentos, medios digitales y otro tipo de información.

EVIDENCIA DIGITAL: Cualquier tipo de información o datos electrónicos que pueden ser utilizados como prueba en investigaciones legales, judiciales o forenses. Incluye documentos electrónicos, correos electrónicos, registros de llamadas, archivos de audio o video, metadatos, registros de actividad en línea y cualquier otro dato digital que pueda ser relevante para demostrar o refutar un hecho en un proceso legal. La evidencia digital se obtiene a través de técnicas especializadas de recopilación, preservación y análisis forense de datos digitales.

EXTRACCIÓN DE DATOS: Proceso de obtener información específica o completa de una fuente de datos, como bases de datos, archivos, dispositivos de almacenamiento u otros medios digitales. Consiste en recopilar selectivamente los datos requeridos según criterios establecidos, utilizando técnicas y herramientas especializadas. La extracción de datos puede involucrar la selección y extracción de ciertos campos, registros o elementos de datos de una fuente más grande. El objetivo de la extracción de datos es obtener la información deseada de manera

precisa y eficiente para su posterior análisis, procesamiento o uso en diferentes contextos.

HERRAMIENTAS FORENSES: Son aplicaciones o programas informáticos diseñados específicamente para realizar análisis forenses en dispositivos y sistemas digitales. Estas herramientas permiten a los investigadores y profesionales forenses recopilar, preservar, examinar y analizar evidencia digital de manera efectiva y eficiente.

INFORMÁTICA FORENSE: Disciplina especializada que se ocupa de recolectar, analizar y preservar evidencia digital en investigaciones legales o incidentes de seguridad. Combina técnicas de informática, ciencias forenses y derecho para identificar, recuperar y examinar datos electrónicos con el objetivo de presentar pruebas válidas en un contexto legal.

INTEGRIDAD: Propiedad o característica de la información, los datos o los sistemas de mantenerse completos, precisos y sin alteraciones no autorizadas. Implica garantizar que la información no haya sido modificada, manipulada o corrompida de manera no intencionada o maliciosa durante su creación, almacenamiento, transmisión o procesamiento.

METADATOS: Son datos descriptivos que proporcionan información sobre otros datos. Son información adicional que acompaña a un conjunto de datos y brindan detalles sobre su origen, formato, estructura, contexto y características. Los metadatos pueden incluir información como la fecha y hora de creación, el autor, la ubicación geográfica, el tamaño del archivo, la versión, los permisos de acceso, entre otros.

RECUPERACIÓN DE DATOS: Proceso de restaurar información perdida, dañada o inaccesible desde dispositivos de almacenamiento, como discos duros, unidades USB, tarjetas de memoria u otros medios digitales. Consiste en utilizar técnicas y herramientas especializadas para recuperar los archivos y datos que han sido eliminados accidentalmente, formateados, corrompidos o afectados por fallos del sistema. El objetivo principal de la recuperación de datos es restaurar la integridad y accesibilidad de la información para que pueda ser nuevamente utilizada por los usuarios.

RESUMEN

El objetivo principal de esta investigación es evaluar la efectividad de las herramientas forenses en la extracción y recuperación de datos en dispositivos de almacenamiento masivo de equipos personales. Para lograrlo, se llevará a cabo un estudio que comprenderá cuatro herramientas forenses utilizadas en dichos procesos, a través de la planificación y ejecución de pruebas simuladas y reales en un entorno controlado. El propósito de estas pruebas es obtener y evaluar la efectividad de las herramientas forenses seleccionadas, así como proponer recomendaciones pertinentes para los procedimientos de extracción y recuperación de datos.

Asimismo, se busca desarrollar un marco conceptual y teórico que abarque las metodologías, regulaciones y herramientas forenses empleadas en los procesos de extracción y recuperación de datos en dispositivos de almacenamiento masivo. Además, se llevará a cabo un análisis exhaustivo del tratamiento y manejo de la información obtenida por estas herramientas forenses, con el fin de garantizar la confidencialidad, disponibilidad e integridad de los datos almacenados en los dispositivos personales de almacenamiento masivo.

Mediante este estudio, se busca mejorar la comprensión de las herramientas forenses y su efectividad en la extracción y recuperación de datos en dispositivos de almacenamiento masivo de equipos personales. También se pretende analizar el manejo adecuado y seguro de la información extraída, con el objetivo de salvaguardar la privacidad y la integridad de los datos.

ABSTRACT

The main objective of this research is to determine the effectiveness of forensic tools in extracting and recovering data from personal storage devices. To achieve this, a study will be conducted that will encompass four forensic tools used in these processes, through the planning and execution of simulated and real tests in a controlled environment. The purpose of these tests is to obtain and evaluate the effectiveness of the selected forensic tools, as well as to propose relevant recommendations for data extraction and recovery procedures.

Furthermore, the aim is to develop a conceptual and theoretical framework that encompasses the methodologies, regulations, and forensic tools used in the extraction and recovery of data from mass storage devices. Additionally, a comprehensive analysis of the treatment and handling of the information obtained by these forensic tools will be carried out to ensure the confidentiality, availability, and integrity of the data stored in personal mass storage devices.

Through this study, the goal is to enhance the understanding of forensic tools and their effectiveness in extracting and recovering data from personal storage devices. It also intends to analyze the appropriate and secure handling of the extracted information in order to safeguard the privacy and integrity of the data.

INTRODUCCIÓN

La informática forense es un campo especializado que se encarga de la investigación y el análisis de evidencia digital en investigaciones criminales y procesos legales. En la era digital actual, donde la mayoría de las actividades se llevan a cabo a través de dispositivos electrónicos, la extracción y recuperación de datos se ha vuelto esencial para obtener pruebas digitales que puedan respaldar o esclarecer casos legales.

La informática forense aborda la recolección, el análisis y la interpretación de datos almacenados en dispositivos electrónicos como computadoras, teléfonos móviles, discos duros, dispositivos de almacenamiento externo y otros dispositivos tecnológicos. Estos dispositivos almacenan una gran cantidad de información, incluyendo comunicaciones, archivos, registros de actividad y metadatos, que pueden ser cruciales para la resolución de casos criminales y legales.

La cadena de custodia es uno de los pilares fundamentales de la informática forense. Se refiere al proceso de documentar y preservar la integridad y el control de la evidencia digital desde el momento de su descubrimiento hasta su presentación en el tribunal. La cadena de custodia asegura que la evidencia se mantenga intacta y no sea alterada o contaminada durante su recolección, análisis y almacenamiento. Esto es vital para garantizar su autenticidad y su aceptación como prueba en un proceso legal.

La preservación de evidencia es otro concepto clave en la informática forense. Dado que la evidencia digital puede ser fácilmente modificada o eliminada, es esencial tomar medidas para protegerla y preservarla en su forma original. Esto implica utilizar técnicas y herramientas forenses especializadas que permitan la extracción de datos sin alterar ni comprometer la integridad de la información recolectada.

La necesidad de herramientas forenses confiables es fundamental en la informática forense. Estas herramientas son software y técnicas especializadas diseñadas para adquirir, analizar y recuperar datos digitales de manera forense. Deben ser confiables, precisas y capaces de manejar diferentes tipos de dispositivos y sistemas operativos. Además, deben cumplir con estándares y prácticas reconocidas para garantizar la validez y la integridad de los resultados obtenidos.

La extracción y recuperación de datos en investigaciones criminales y procesos legales desempeñan un papel crucial en la búsqueda de la verdad y la justicia. Los datos digitales pueden proporcionar pruebas valiosas para identificar a los perpetradores de delitos, establecer motivos, corroborar coartadas, rastrear comunicaciones y establecer conexiones entre personas y eventos.

En casos de delitos cibernéticos, fraudes financieros, abusos y explotación infantil, terrorismo y otros delitos graves, la evidencia digital puede ser la clave para el esclarecimiento de los hechos y la condena de los responsables. Además, en casos civiles, como disputas legales o violaciones de derechos de autor, los datos digitales pueden ser fundamentales para respaldar las reclamaciones y tomar decisiones informadas.

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Los dispositivos de almacenamiento masivo se han convertido en una parte integral de la vida moderna, ya que son ampliamente utilizados para almacenar y transferir datos en una variedad de contextos, desde el almacenamiento de archivos personales hasta la transferencia de información confidencial en empresas y organizaciones gubernamentales. Sin embargo, a medida que la cantidad de datos almacenados en estos dispositivos ha aumentado, también lo ha hecho la necesidad de poder extraer información de ellos en el contexto de investigaciones forenses y legales.

En la actualidad, existen diferentes herramientas forenses utilizadas para la extracción de información de dispositivos de almacenamiento masivo, como discos duros, unidades flash USB, tarjetas de memoria y otros medios de almacenamiento. Cada una de estas herramientas tiene sus ventajas y desventajas, y se hace necesario evaluar la efectividad de cada una de éstas en un ambiente controlado de pruebas.

El problema que se aborda en este estudio es evaluar la efectividad de diferentes herramientas forenses de pago y open source en la extracción de información de dispositivos de almacenamiento masivo de equipos personales. En particular, se busca comprender cómo diferentes herramientas pueden afectar la calidad y la cantidad de la información extraída, y si algunas herramientas son más efectivas que otras para ciertos tipos de dispositivos o información.

Entre las herramientas forenses que se analizarán en este estudio se encuentran las herramientas de recuperación de datos, las herramientas de imagen de disco y las herramientas de análisis forense. Cada una de estas herramientas utiliza diferentes enfoques para la extracción de información y puede ser más efectiva para diferentes tipos de dispositivos o información.

Para abordar este problema, se llevará a cabo un estudio empírico utilizando diferentes dispositivos de almacenamiento masivo y herramientas forenses para extraer y recuperar datos. Se evaluará la calidad y la cantidad de la información extraída y se comparará la efectividad de diferentes herramientas en diferentes dispositivos y tipos de información. Además, se llevará a cabo un análisis del tratamiento y manejo de la información extraída por parte de estas herramientas forenses para garantizar la confidencialidad, disponibilidad e integridad de los datos en los dispositivos de almacenamiento masivo.

Se espera que los resultados de este estudio ayuden a los investigadores forenses y legales a comprender mejor las herramientas disponibles para la extracción de información de dispositivos de almacenamiento masivo y a tomar decisiones informadas sobre qué herramientas utilizar en diferentes situaciones. Además,

también puede ayudar a desarrolladores de herramientas forenses a mejorar la efectividad de sus herramientas y a adaptarlas mejor a diferentes tipos de dispositivos y situaciones.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo la evaluación de herramientas forenses en dispositivos de almacenamiento masivo puede determinar la efectividad en extracción y recuperación de datos en equipos personales?

2 JUSTIFICACIÓN

En la actualidad, realizar este análisis es esencial debido a la importancia de los dispositivos de almacenamiento masivo en nuestra sociedad y la necesidad de extraer información de ellos en el contexto de investigaciones forenses y legales, particularmente en Colombia. A medida que se almacena cada vez más información en estos dispositivos, se han vuelto más frecuentes en las investigaciones judiciales, y se ha vuelto necesario comprender qué herramientas son más efectivas para la extracción de información.

El análisis de la efectividad de diferentes herramientas forenses es importante por varias razones. En primer lugar, las herramientas forenses son necesarias para extraer información de dispositivos de almacenamiento masivo en el contexto de investigaciones forenses y legales. Si las herramientas utilizadas son ineficaces, esto puede afectar negativamente la calidad y la cantidad de información que se extrae, lo que puede ser perjudicial para el resultado de la investigación.

En segundo lugar, una comprensión clara de qué herramientas son más efectivas en diferentes situaciones puede ayudar a los investigadores a tomar decisiones informadas sobre qué herramientas utilizar en diferentes casos. Esto puede ser especialmente importante en casos de alta complejidad o alta sensibilidad, donde se necesitan las herramientas más efectivas para garantizar que se extraiga toda la información relevante y se realice una investigación completa.

En tercer lugar, el análisis de la efectividad de diferentes herramientas puede ayudar a los desarrolladores de herramientas forenses a mejorar la efectividad de sus herramientas y adaptarlas mejor a diferentes tipos de dispositivos y situaciones. Los resultados de este estudio pueden ser valiosos para los desarrolladores de herramientas, ya que pueden proporcionar información sobre qué características y enfoques son más efectivos para la extracción de información de dispositivos de almacenamiento masivo en diferentes situaciones.

En cuarto lugar, el análisis de la efectividad de diferentes herramientas puede contribuir a un mayor desarrollo y mejora de la práctica forense. Al proporcionar información sobre qué herramientas son más efectivas para diferentes tipos de dispositivos y situaciones, este estudio puede contribuir a un mayor entendimiento de las mejores prácticas para la extracción de información de dispositivos de almacenamiento masivo en el contexto de investigaciones forenses y legales.

En este contexto, la efectividad de diferentes herramientas forenses en la extracción de información de dispositivos de almacenamiento masivo es importante para el éxito de las investigaciones forenses y legales. Además, los resultados de este estudio pueden ayudar a los investigadores a tomar decisiones informadas sobre qué herramientas utilizar, a los desarrolladores de herramientas forenses a mejorar la efectividad de sus herramientas y a contribuir al desarrollo y mejora de la práctica forense en general.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Evaluar la efectividad en extracción y recuperación de datos de cuatro herramientas forenses, mediante un ambiente controlado de pruebas, para dispositivos de almacenamiento masivo en equipos personales.

3.2 OBJETIVOS ESPECÍFICOS

1. Establecer el marco conceptual y teórico de metodologías, normatividad y herramientas forenses en extracción y recuperación de datos en dispositivos de almacenamiento masivo.
2. Seleccionar las herramientas forenses para la extracción y recuperación de datos en dispositivos de almacenamiento masivo en equipos personales.
3. Planificar la realización de pruebas simuladas y reales para la evaluación de la efectividad de las herramientas forenses seleccionadas.
4. Desarrollar las pruebas para la obtención de la efectividad de las herramientas forenses seleccionadas, proponiendo las recomendaciones pertinentes a los procesos de extracción y recuperación de datos.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

En la actualidad, los dispositivos de almacenamiento masivo, como discos duros, unidades flash USB, tarjetas de memoria y discos ópticos, desempeñan un papel fundamental en nuestra vida cotidiana. Estos dispositivos almacenan una gran cantidad de información personal y profesional, convirtiéndose en un recurso valioso para las investigaciones forenses. La extracción y recuperación de información de estos dispositivos se ha vuelto crucial en casos legales y de seguridad; Por tanto, el análisis de la efectividad de diferentes herramientas forenses en la extracción de información en dispositivos de almacenamiento masivo requiere un marco conceptual y teórico que permita entender los elementos clave de la informática forense y la recuperación de datos. En este marco se incluyen conceptos sobre Informática forense, herramientas forenses, los dispositivos de almacenamiento masivo, la criptografía, la eliminación de datos y la compresión. El objetivo de este marco es proporcionar una base teórica sólida para el análisis de la efectividad de las herramientas forenses en la extracción de información.

4.1.1 **Informática Forense**

La informática forense, también conocida como ciencia forense digital o forense computacional, es una disciplina especializada que se ocupa de la investigación, recolección, preservación, análisis y presentación de evidencia digital con fines legales. Su objetivo principal es descubrir y documentar información electrónica que pueda ser utilizada en investigaciones criminales, litigios o cualquier otra actividad legal.
La informática forense se basa en la premisa de que cualquier acción realizada en el entorno digital deja rastros, ya sea en dispositivos electrónicos, redes, sistemas informáticos o medios de almacenamiento. Estos rastros digitales pueden ser recuperados y analizados para reconstruir eventos, identificar culpables, probar la comisión de delitos o presentar evidencia en un tribunal [1].

El proceso de informática forense involucra varias etapas bien definidas:

4.1.1.1 Adquisición de datos: Hace referencia a la recopilación de información digital relevante a través de métodos seguros y confiables. Esto puede incluir la copia bit a bit de discos duros, la extracción de datos de dispositivos móviles, la captura de paquetes de red o la recuperación de archivos eliminados.

[1] CANO, J. Introducción a la informática forense: Una disciplina técnico-legal. 2006. Revista Sistemas, Asociación Colombiana de Ingenieros de Sistemas (ACIS). Vol.96, pp. 64-73. [En línea] http://52.0.140.184/typo43/fileadmin/Rev ista_96/dos.pdf

4.1.1.2 Preservación de la evidencia: Es fundamental garantizar que la evidencia digital se mantenga intacta y sin modificaciones durante todo el proceso de investigación. Esto implica utilizar técnicas y herramientas especializadas para preservar la cadena de custodia y asegurar la integridad de los datos.

4.1.1.3 Análisis de datos: En esta etapa, los investigadores forenses examinan y procesan la evidencia digital recolectada. Utilizan diversas técnicas y herramientas para identificar y extraer información relevante, como archivos, correos electrónicos, registros de actividad, metadatos, mensajes de chat, imágenes, videos, entre otros. Interpretación de los resultados: Los datos obtenidos durante el análisis se interpretan y se les da contexto para comprender su relevancia en el contexto de la investigación. Esto implica correlacionar diferentes fuentes de información, reconstruir eventos, identificar patrones o establecer relaciones entre personas, dispositivos o actividades.

4.1.1.4 Presentación de resultados: Los hallazgos y resultados del análisis se documentan y presentan de manera clara y precisa. Esto incluye la elaboración de informes forenses detallados que describen los métodos utilizados, los hallazgos obtenidos y las conclusiones derivadas de la evidencia digital analizada. Estos informes pueden ser presentados como pruebas en un tribunal o en otros procedimientos legales.

La informática forense se aplica en una amplia gama de casos, incluyendo delitos informáticos, fraude electrónico, espionaje corporativo, violaciones de datos, acoso en línea, entre otros. Los investigadores forenses deben tener un profundo conocimiento técnico de sistemas informáticos, redes, software, criptografía, así como también comprender los aspectos legales y éticos de su trabajo.

4.1.2 **Extracción de Información:**

La extracción de información es el proceso de obtener datos almacenados en dispositivos de almacenamiento masivo. Para llevar a cabo esta tarea, se utilizan diversas herramientas forenses, entre las cuales se destacan:

a) Herramientas de Adquisición: Estas herramientas permiten hacer copias bit a bit de los dispositivos de almacenamiento sin alterar la información original. Ejemplos de herramientas comunes incluyen Forensic Toolkit (FTK), AccessData, y X-Ways Forensics [2].

[2] Romero M., La informática Forense desde un enfoque práctico. 2020. [En línea]. [Fecha de consulta abril de 2023] Manabí, Ecuador. Disponible en: https://gc.scalahed.com/recursos/files/r161r/w26124w/LA_INFORMATICA_FORENSE_DESDE_UN_ENFOQUE_PRACTICO_compressed.pdf

b) Herramientas de Recuperación de Datos: Estas herramientas se centran en recuperar datos borrados o dañados en los dispositivos de almacenamiento. Utilizan técnicas de recuperación avanzadas para reconstruir la información eliminada o dañada. Ejemplos notables son EnCase, R-Studio y GetDataBack [3].

4.1.3 **Dispositivos de almacenamiento masivo**

Los dispositivos de almacenamiento masivo son dispositivos electrónicos diseñados para almacenar grandes cantidades de datos, como documentos, imágenes, videos, música, entre otros. Estos dispositivos se utilizan en una variedad de dispositivos, incluyendo computadoras, teléfonos móviles, cámaras, entre otros.
Entre los dispositivos de almacenamiento masivo más comunes se incluyen los discos duros, las unidades flash USB, las tarjetas de memoria, los discos ópticos y las unidades de almacenamiento externas. Cada uno de estos dispositivos tiene sus propias características y requerimientos para la recuperación de datos, lo que hace que sea importante seleccionar la herramienta forense adecuada para cada dispositivo [4].

4.1.4 **Criptografía**

La criptografía es la técnica de codificar y decodificar información para proteger su privacidad. La criptografía se utiliza en muchos dispositivos de almacenamiento masivo para proteger la información almacenada. La información cifrada sólo puede ser descifrada por la persona que tiene la clave de descifrado.
Las herramientas forenses tienen la capacidad de descifrar datos cifrados, pero esta tarea puede ser complicada y requiere de un enfoque específico para cada tipo de cifrado. La capacidad de una herramienta forense para descifrar datos cifrados puede ser una consideración importante en el análisis de su efectividad en la extracción de información en dispositivos de almacenamiento masivo.

4.1.5 **Eliminación de datos**

La eliminación de datos es el proceso de borrar la información almacenada en un dispositivo de almacenamiento masivo. Existen varios métodos para eliminar datos, que van desde la eliminación de archivos individuales hasta el formateo completo del dispositivo. La eliminación de datos también puede implicar la eliminación de

[3] Romero M., La informática Forense desde un enfoque práctico. 2020. [En línea]. [Fecha de consulta abril de 2023] Manabí, Ecuador. Disponible en: https://gc.scalahed.com/recursos/files/r161r/w26124w/LA_INFORMATICA_FORENSE_DESDE_UN_ENFOQUE_PRACTICO_compressed.pdf

[4] INFO-LAB. Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense. 2016. Universidad FASTA, Ministerio Público Fiscal de la Provincia de Buenos Aires y la Municipalidad de General Pueyrredon. Buenos Aires. Argentina.

metadatos y otros rastros que puedan indicar la existencia de información en el dispositivo.
Las herramientas forenses tienen la capacidad de recuperar información eliminada, aunque el grado de éxito puede variar dependiendo del método utilizado para eliminar los datos. Algunas herramientas forenses también pueden proporcionar información sobre los métodos de eliminación utilizados en el dispositivo, lo que puede ser importante para la evaluación de la integridad de los datos recuperados.

4.1.6 **Compresión**

La compresión es la técnica de reducir el tamaño de los archivos de datos para facilitar su almacenamiento y transmisión. La compresión se utiliza comúnmente en dispositivos de almacenamiento masivo para maximizar su capacidad de almacenamiento.
Sin embargo, la compresión puede dificultar la recuperación de datos, ya que los datos comprimidos deben ser descomprimidos antes de que puedan ser analizados por una herramienta forense. Algunas herramientas forenses tienen la capacidad de descomprimir datos comprimidos automáticamente, mientras que otras requieren que el usuario realice esta tarea manualmente [5].

4.1.7 **Consideraciones Éticas y Legales**

Es importante tener en cuenta que el uso de herramientas forenses en la extracción y recuperación de información en dispositivos de almacenamiento masivo debe llevarse a cabo dentro de un marco ético y legal. Esto implica respetar la privacidad de las personas y cumplir con las leyes y regulaciones aplicables en cada jurisdicción.
a) Privacidad y Consentimiento: Es fundamental obtener el consentimiento legal para acceder y analizar la información almacenada en los dispositivos de almacenamiento. En algunos casos, puede requerirse una orden judicial para llevar a cabo estas acciones.
b) Cadena de Custodia: La cadena de custodia es el registro detallado de todos los cambios y manipulaciones realizadas en la evidencia digital desde su adquisición hasta su presentación en un tribunal. Es esencial mantener una cadena de custodia adecuada para garantizar la integridad y validez de la evidencia.
c) Marco Legal: Es importante tener conocimiento y comprensión de las leyes y regulaciones relacionadas con la informática forense en la jurisdicción donde se lleva a cabo la investigación. Esto incluye leyes de protección de datos, leyes de propiedad intelectual y leyes de procedimiento penal.

[5] LÁZARO, F. Introducción a la informática forense. 2014. [En línea]. [Fecha de consulta abril de 2023]. Paracuellos de Jarama, Madrid, RAMA Editorial. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ ereader/unad/106250?page=246

El análisis de la efectividad de diferentes herramientas forenses en la extracción de información en dispositivos de almacenamiento masivo requiere una comprensión sólida de los conceptos clave relacionados con la informática forense y la recuperación de datos.

4.2 MARCO CONCEPTUAL

La informática forense y la evidencia digital están estrechamente relacionadas y se complementan entre sí en el ámbito de la investigación legal.
La informática forense se centra en la aplicación de técnicas y metodologías especializadas para recopilar, preservar y analizar la evidencia digital. En este sentido, la evidencia digital es el objeto principal de estudio de la informática forense. Los profesionales forenses utilizan herramientas y técnicas específicas para extraer, examinar y analizar la información almacenada en dispositivos electrónicos con el objetivo de descubrir y documentar pruebas que puedan ser utilizadas en investigaciones o procesos legales.

La evidencia digital se refiere a cualquier información o datos que son almacenados o generados en formato digital y que pueden ser utilizados como prueba en un proceso legal. Esta evidencia puede ser encontrada en una amplia variedad de dispositivos y sistemas, como computadoras, teléfonos móviles, tabletas, dispositivos de almacenamiento, servidores y sistemas en la nube.
La evidencia digital desempeña un papel crucial en los casos legales modernos, ya que la mayoría de las actividades y comunicaciones humanas se realizan a través de medios digitales. Esta evidencia puede incluir archivos de documentos, correos electrónicos, mensajes de texto, registros de llamadas, registros de actividad de dispositivos, imágenes, videos, datos de geolocalización, registros de transacciones financieras y cualquier otro tipo de información almacenada o transmitida digitalmente [6].
Al igual que con la evidencia física, la evidencia digital debe cumplir con ciertos requisitos para ser considerada válida y admisible en un tribunal de justicia. Estos requisitos incluyen:

4.2.1 Autenticidad: La evidencia digital debe ser auténtica, lo que significa que se debe poder demostrar que los datos recopilados provienen de la fuente que se pretende representar. Se utilizan técnicas como la verificación de firmas digitales, hash de archivos y registros de auditoría para garantizar la autenticidad de la evidencia.

4.2.2 Integridad: La integridad de la evidencia digital se refiere a su estado original y a la ausencia de alteraciones o modificaciones no autorizadas. Se utilizan técnicas

[6] Maras, M. H. Forense Digital: Delitos Informáticos, Leyes y Evidencias. 2012. Jones & Bartlett Publishers.

de cifrado, firmas digitales y control de acceso para preservar la integridad de la evidencia durante su recolección, almacenamiento y análisis.

4.2.3 Admisibilidad: La evidencia digital debe cumplir con los requisitos legales para ser considerada admisible en un tribunal. Esto puede incluir la aplicación de leyes de privacidad y protección de datos, la obtención de órdenes judiciales adecuadas para la recopilación de la evidencia y el cumplimiento de estándares y procedimientos forenses reconocidos.

4.2.4 Extracción forense de datos: La extracción forense de datos se refiere al proceso de copiar y recolectar de manera forense los datos almacenados en dispositivos de almacenamiento masivo. Esta extracción debe realizarse de manera cuidadosa y precisa para garantizar la integridad y autenticidad de la evidencia digital recopilada. Se utilizan herramientas y técnicas especializadas para adquirir una copia exacta del contenido del dispositivo sin alterar los datos originales.

4.2.5 Recuperación forense de datos: La recuperación forense de datos se centra en la búsqueda, identificación y reconstrucción de datos eliminados o dañados en dispositivos de almacenamiento masivo. Se utilizan técnicas avanzadas de análisis y recuperación para recuperar información oculta, archivos borrados o fragmentados, registros de actividad y otros datos relevantes para la investigación. Esto puede incluir el uso de algoritmos de recuperación, análisis de metadatos y técnicas de carvado de archivos.

4.2.6 Integridad de los datos: La integridad de los datos es un concepto fundamental en la extracción y recuperación forense. Se refiere a la garantía de que los datos recopilados y recuperados se mantienen sin cambios y sin alteraciones durante todo el proceso de análisis y presentación como evidencia. Se deben aplicar métodos y técnicas para verificar y documentar la integridad de los datos, asegurando su confiabilidad y admisibilidad legal.

4.2.7 Cadena de custodia: La cadena de custodia se refiere al registro documentado y el control de todos los pasos y personas que han tenido acceso a la evidencia digital durante el proceso de extracción y recuperación. Es esencial para garantizar la integridad y autenticidad de la evidencia y su aceptación en un tribunal de justicia. La cadena de custodia debe seguir procedimientos rigurosos y garantizar que no se haya alterado, modificado o contaminado la evidencia durante su manipulación [7].

4.2.8 Herramientas forenses: Las herramientas forenses son software especializados utilizados en la extracción y recuperación de datos en dispositivos de almacenamiento masivo. Estas herramientas incluyen software comercial y

[7] Marcella, A. J., & Greenfield, L. Forense Cibernética: Manual de Campo para la Recolección, Examen y Preservación de Evidencias de Delitos Informáticos. 2004. CRC Press.

proporcionan funcionalidades para adquirir, analizar, interpretar y presentar la evidencia digital recopilada de manera forense.

Para recopilar y presentar la evidencia digital de manera efectiva, se utilizan técnicas y herramientas especializadas de informática forense. Estas técnicas pueden incluir la adquisición forense de datos, el análisis de metadatos, la recuperación de archivos borrados, el análisis de redes y la interpretación de registros de actividad, entre otros. Las herramientas forenses, tanto comerciales como de código abierto, están diseñadas para facilitar la extracción, el análisis y la presentación de la evidencia digital de manera forense y legalmente válida.

4.3 MARCO HISTÓRICO

El campo de la informática forense comenzó a surgir a finales de los años 70, poco después de que las computadoras personales se volvieran una opción viable para los consumidores. En 1978, el estado de Florida reconoció los delitos relacionados con sistemas informáticos en el Computer Crimes Act, que abarcaba casos de sabotaje, infracción de derechos de autor, alteración de datos y ataques similares.

En 1981, Central Point Software lanzó Copy II PC, también conocido como copy2pc, que permitía realizar copias exactas de disquetes, los cuales generalmente estaban protegidos para evitar copias ilegales. Este producto fue posteriormente incorporado a Pc Tools. La compañía tuvo un gran éxito y fue adquirida por Symantec en 1994. Posteriormente, en 1982, Peter Norton publicó UnErase: Norton Utilities 1.0, la primera versión de la suite Norton Utilities, que incluía destacadas herramientas como UnErase, una aplicación para recuperar archivos borrados accidentalmente. Otras aplicaciones como FileFix o TimeMark también resultaron útiles desde el punto de vista forense. Debido al éxito de esta suite de aplicaciones, Norton publicó varios libros técnicos, entre ellos Inside the I.B.M. Personal Computer: Access to Advanced Features and Programming, cuya octava edición se publicó en 1999, 11 años después de la primera edición. En 1984, el FBI creó el Programa de Medios Magnéticos, que más tarde se convirtió en el Computer Analysis and Response Team (CART) en 1991[8].

En 1986, Clifford Stoll colaboró en la detección del hacker Markus Hess y en 1988 publicó el documento Stalking the Wily Hacker, donde relató lo sucedido. Este documento se convirtió en un libro en 1989, anticipando una metodología forense. En 1987 se fundó la compañía AccessData, pionera en el desarrollo de productos orientados a la recuperación de contraseñas y el análisis forense, como la actual Forensic Toolkit (FTK). En 1988 se estableció la International Association of Computer Investigative Specialists (IACIS), que otorga la certificación Certified

[8] Roatta S., M.E. Casco, M. Fogliato. El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012. 2020. Facultad Tecnología Informática / Universidad Abierta Interamericana. Argentina.

Forensic Computer Examiner (CFCE), una de las más prestigiosas en el campo forense, a profesionales de agencias gubernamentales. En el mismo año, se implementó el programa Seized Computer Evidence Recovery Specialists (SCERS) con el objetivo de formar a profesionales en informática forense. En 1992, el libro A forensic methodology for countering computer crime de P. A. Collier y B. J. Spaul acuñó el término "informática forense". Otros libros posteriores, como High-Technology Crime: Investigating Cases Involving Computers de Kenneth S. Rosenblatt, continuaron desarrollando el término y la metodología [9].

En 1995 se estableció la International Organization on Computer Evidence (IOCE) como un punto de encuentro para especialistas en evidencia electrónica e intercambio de información. A partir de 1996, Interpol ha organizado el Simposio Internacional de Ciencias Forenses, un foro para discutir avances en el campo forense y compartir conocimientos. En agosto de 2001 se creó el Digital Forensic Research Workshop (DFRWS), un nuevo grupo internacional de debate y discusión para compartir información [10].

Hasta el año 2012, dos instituciones eran consideradas fundamentales en el análisis forense: el National Institute of Standart and Technology (NIST) y el Federal Bureau of Investigation (FBI). Actualmente, la norma ISO/IEC 27037:2012 es la referencia global en este campo.

La norma ISO/IEC 27037:2012 establece directrices y lineamientos para la evidencia digital en el contexto de la informática forense. Esta norma proporciona un marco de trabajo para la recolección, el análisis y la presentación de pruebas digitales en investigaciones criminales y litigios legales.
Entre los aspectos principales que aborda la norma se encuentran:

4.3.1 Proceso de recolección de evidencia: Establece los procedimientos y técnicas adecuadas para la recolección y preservación de la evidencia digital, garantizando la integridad y la autenticidad de los datos.
4.3.2 Análisis forense: Define los pasos y las prácticas recomendadas para llevar a cabo un análisis exhaustivo de la evidencia digital, incluyendo la identificación, extracción, interpretación y documentación de los hallazgos.
4.3.3 Presentación de pruebas: Ofrece directrices sobre cómo presentar la evidencia digital de manera clara, precisa y comprensible, asegurando su validez y fiabilidad en un entorno legal.
4.3.4 Consideraciones éticas y legales: Se enfoca en los aspectos éticos y legales que los profesionales de la informática forense deben tener en cuenta

[9] Roatta S., M.E. Casco, M. Fogliato. El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012. 2020. Facultad Tecnología Informática / Universidad Abierta Interamericana. Argentina.
[10] Roatta S., M.E. Casco, M. Fogliato. El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012. 2020. Facultad Tecnología Informática / Universidad Abierta Interamericana. Argentina.

durante todo el proceso, incluyendo la privacidad, la confidencialidad y el cumplimiento de las leyes y regulaciones aplicables.
La norma ISO/IEC 27037:2012 se ha convertido en un punto de referencia internacional en el ámbito de la informática forense, proporcionando una guía sólida y confiable para las organizaciones y profesionales que se dedican a la recolección y análisis de pruebas digitales en investigaciones y litigios[11].

4.4 ANTECEDENTES O ESTADO ACTUAL

A continuación, se presentan algunos trabajos y/o documentos relacionados con la extracción y recuperación de datos mediante herramientas forenses en diferentes dispositivos de almacenamiento:

El “Manual Básico de Cateo y Aseguramiento de Evidencia Digital", escrito por Gabriel Andrés Campoli en México en 2006, busca servir como una guía para llevar a cabo el cateo o aseguramiento de equipos electrónicos encontrados en la escena de un crimen que puedan contener evidencia digital. El manual proporciona acciones y mecanismos mínimos para estos procesos[12].

El estudio titulado "Recuperación de información en discos duros" de Mario Rodríguez Argueta en México en 2007 tiene como objetivo proporcionar una metodología que sirva de referencia para peritos y especialistas en seguridad informática. Esta metodología busca obtener o recuperar la información de un disco duro mediante el uso de herramientas forenses de software libre[13].

En 2009, en México, el estudio realizado por Catañeda Vilchis Francisco Javier, Rojas Barrera Victos Israel y Villanueva Pallares Norma Zarahy tiene como objetivo evaluar el rendimiento, fiabilidad e integridad de las diferentes herramientas disponibles en el mercado para el análisis forense de discos duros[14].

En un proyecto de investigación denominado PURI "Proceso Unificado de Recuperación de la Información", Sansevero, Rita, Castellote, Martin, Podestá, Ariel, Greco, Fernando, Constanzo, Bruno, Waimann, Julian, Di Iorio, Ana y el Laboratorio Info-Lab presentan avances obtenidos hasta el momento en la formalización de un proceso marco que abarque las fases, tareas, herramientas y

[11] Roatta S., M.E. Casco, M. Fogliato. El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012. 2020. Facultad Tecnología Informática / Universidad Abierta Interamericana. Argentina
[12] Campoli, G. Manual Básico de Cateo y Aseguramiento de Evidencia Digital. 2006. México.
[13] Rodríguez M. Recuperación de información en discos duros. 2007. México.
[14] Castañeda F., Rojas V., Villanueva N., Evaluación de herramientas para análisis forense orientado a discos duros. 2009. México.

actividades aplicables a diversos entornos y dispositivos en el campo de la recuperación de información y la informática forense[15].

El trabajo presentado por el Ingeniero José Bernardo Cortés de la Rosa en Pasto en 2014, titulado "Manejo de evidencia digital en dispositivos de almacenamiento pendrive usb" sustentado en la norma ISO/IEC 27037:2012, tiene como objetivo aplicar la norma mencionada en el manejo de evidencia digital en dispositivos de almacenamiento pendrive USB. Propone procedimientos aplicables a dicha norma para el manejo de evidencia digital en estos dispositivos[16].

En La Paz en 2014, Remy Vladimir Huanca Quispe desarrolla una metodología de análisis forense digital especialmente diseñada para dispositivos móviles con sistema operativo Android. Esta metodología busca mejorar la extracción de datos almacenados en dichos dispositivos, incluso cuando presenten restricciones de seguridad y métodos de autenticación[17].

En el artículo titulado "Un enfoque para la validación de las funciones de recuperación de archivos en herramientas de software forense digital"[18] en 2014, se demuestra la recuperación de archivos mediante el uso de herramientas tanto comerciales como gratuitas, como Recuva, FTK, Encase, Recover My Files y Blade. Como resultado de las pruebas realizadas, la herramienta que mostró el mejor rendimiento en el análisis fue Blade, mientras que "Recover My Files" fue la que tuvo peor desempeño.

En un estudio realizado en Mumbai en 2016, India, se llevó a cabo un análisis comparativo de diversas herramientas forenses enfocadas en dispositivos móviles. Las herramientas comerciales consideradas en este estudio fueron MOBIL-edit Forense y UFED Physical Analyzer, mientras que las herramientas de código abierto examinadas fueron The Sleuth Kit y SANS SIFT. Se creó una matriz de comparación y se realizó un análisis de los resultados obtenidos. Este estudio proporciona una observación importante: no se puede definir una solución universal para la selección de herramientas forenses, ya que depende de factores específicos y es probable que se requiera la interoperabilidad de un conjunto de herramientas[19].

---

[15] Sansevero, R. & Castellote, M. & Podestá, A. & Greco, F. & Constanzo, B. & Waimann, J. & Di Iorio, A. & Laboratory, Info-Lab. La recuperación de la información y la informática forense: Una propuesta de proceso unificado. 2012. Buenos Aires, Argentina.

[16] Cortés de la Rosa B., Manejo de evidencia digital en dispositivos de almacenamiento pendrive usb aplicando la norma ISO/IEC 27037:2012. 2014. Pasto, Colombia.

[17] Huanca V., Metodología de análisis forense digital para la extracción de datos almacenados en dispositivos móviles basados en sistema operativo android. 2014. La Paz, Bolivia.

[18] Salem N., Iqbal F. y Alfandi O., «An Approach for the Validation of File Recovery Functions in Digital Forensics' Software Tools,» IEEE. 2014.

[19] Padmanabhan R., K. Lobo, M. Ghelani, D. Sujan y M. Shirole, «Comparative Analysis of Commercial and Open Source Mobile Device Forensic Tools,» IEEE. 2016.

El Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, a través de la estrategia de Gobierno en Línea, elabora un documento en marzo de 2016 titulado "Evidencia Digital: Seguridad y privacidad de la información". El propósito de este documento es proporcionar pautas a las entidades estatales sobre cómo llevar a cabo la identificación, recolección, análisis y manipulación de datos en casos de eventos o incidentes de seguridad que requieran evidencias digitales para su investigación[20]".

El trabajo realizado por S. Roatta, M.E. Casco y M. Fogliato en Argentina en 2020, titulado "El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012", presenta pautas para el manejo de la evidencia digital, incluyendo la identificación, adquisición, análisis y preservación de la misma. El objetivo es mantener la integridad de la evidencia y diseñar un proceso que cumpla con las normas ISO/IEC 27037:2012 para contribuir a su admisibilidad en procesos legales[21].

En su trabajo desarrollado en la Universidad Santo Tomás en Tunja, Colombia, (2015) Karen Daniela Cuervo Cely realiza una comparación de diferentes herramientas utilizadas para el análisis forense en dispositivos de almacenamiento extraíble. El objetivo es destacar las particularidades de cada herramienta y determinar cuál brinda un mejor análisis de la información[22].

El libro "Análisis Forense Informático" de Mario Guerra Soto en Madrid en 2021 proporciona una guía completa sobre el análisis forense de evidencias digitales en el ámbito de la informática. El autor aborda aspectos fundamentales como la recolección, preservación y análisis de pruebas digitales, así como las técnicas y herramientas utilizadas en el proceso de investigación forense[23].

4.5 MARCO CIENTÍFICO O TECNOLÓGICO

En la extracción y recuperación de datos en dispositivos de almacenamiento masivo, se utilizan varias tecnologías y herramientas. A continuación, se mencionan algunas de las tecnologías comunes utilizadas en este proceso:

4.5.1 **Sistemas de archivos**

[20] Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Evidencia Digital: Seguridad y privacidad de la información. 2016. Colombia.
[21] Roatta S., M.E. Casco, M. Fogliato.El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012. 2020. Facultad Tecnología Informática / Universidad Abierta Interamericana. Argentina.
[22] Cuervo K., Comparación de diferentes herramientas para el análisis forense en dispositivos extraíbles de tipo flash drive. 2015. Universidad Santo Tomás, Tunja- Colombia.
[23] Guerra M., Análisis Forense Informático. 2021. Editorial RA-MA. Madrid.

Los sistemas de archivos son la base para la organización y almacenamiento de datos en los dispositivos de almacenamiento masivo. Los sistemas de archivos más utilizados son NTFS (New Technology File System) en Windows, HFS+ (Hierarchical File System Plus) en macOS y ext4 (Fourth Extended File System) en sistemas basados en Linux[24].

4.5.2 **Software de recuperación de datos**

Existe variedad de software de recuperación de datos disponibles en el mercado. Estas herramientas utilizan algoritmos y técnicas especializadas para analizar los dispositivos de almacenamiento y recuperar los datos perdidos o eliminados. Ejemplos populares incluyen EaseUS Data Recovery Wizard, Recuva y TestDisk.

4.5.3 **Técnicas forenses**

En casos en los que se requiera recuperar datos para fines legales o de investigación, se aplican técnicas forenses. Estas técnicas implican la creación de una copia bit a bit del dispositivo original para preservar su integridad y garantizar que los datos recuperados sean admisibles como evidencia en un tribunal. Herramientas como EnCase Forensic y AccessData FTK (Forensic Toolkit) son ampliamente utilizadas en la recuperación forense de datos.

4.5.4 **Imágenes de disco**

Las imágenes de disco son copias exactas de todo el contenido de un dispositivo de almacenamiento, incluyendo el sistema de archivos y los datos almacenados. Las imágenes de disco se crean utilizando herramientas especializadas y se pueden examinar y analizar sin tener acceso directo al dispositivo original. Esto permite realizar investigaciones y recuperar datos sin correr el riesgo de modificar o dañar los datos originales.

4.5.5 **Algoritmos de reconstrucción de datos**

En algunos casos, los datos pueden estar parcialmente dañados o fragmentados en el dispositivo de almacenamiento. Los algoritmos de reconstrucción de datos se utilizan para ensamblar y recuperar los datos fragmentados, ya sea utilizando metadatos disponibles o analizando el contenido de los fragmentos. Estos algoritmos pueden ser específicos del sistema de archivos utilizado y del tipo de datos que se intenta recuperar.

4.5.6 **Herramientas forenses**

[24] Cortés de la Rosa B., Manejo de evidencia digital en dispositivos de almacenamiento pendrive usb aplicando la norma ISO/IEC 27037:2012. 2014. Pasto, Colombia.

Las herramientas forenses son equipos y/o programas informáticos diseñados para recopilar y analizar datos de los sistemas informáticos con fines forenses. Estas herramientas se utilizan para extraer información de dispositivos de almacenamiento masivo, como discos duros, unidades flash USB, tarjetas de memoria, entre otros. Las herramientas forenses son esenciales en el contexto de las investigaciones forenses y legales, ya que permiten a los investigadores analizar la información almacenada en los dispositivos y determinar su relevancia para la investigación.
En el campo de la informática forense, existen diversas herramientas especializadas utilizadas para la extracción y recuperación de información de manera forense. Estas herramientas permiten a los investigadores forenses adquirir, analizar y recuperar datos relevantes de dispositivos y sistemas digitales. A continuación, se presenta un resumen amplio de algunas de las herramientas forenses más utilizadas en este ámbito:

4.5.6.1 FTK (Forensic Toolkit): FTK, desarrollado por AccessData, es una herramienta forense ampliamente utilizada que ofrece una amplia gama de capacidades para la extracción y análisis forense de datos. Permite la adquisición forense de datos de discos duros, dispositivos móviles y medios en la nube. FTK utiliza un enfoque basado en índices para agilizar el proceso de búsqueda y análisis de grandes cantidades de datos. Además, ofrece herramientas para la recuperación de archivos borrados, análisis de metadatos, recuperación de contraseñas, visualización de registros y análisis de imágenes forenses[25].

4.5.6.2 EnCase Forensic: EnCase Forensic, desarrollado por Guidance Software, es una herramienta líder en el campo de la informática forense. Ofrece capacidades completas para la adquisición y análisis forense de datos de diversas fuentes, como discos duros, dispositivos móviles, dispositivos USB, imágenes de disco y otros medios de almacenamiento al igual que redes y servicios en la nube de manera forensemente sólida, garantizando la integridad de la evidencia. EnCase Forensic permite la recuperación de datos borrados, análisis de metadatos, examen de registros de eventos, recuperación de contraseñas y examen de archivos y registros del sistema. Una vez que se ha adquirido la evidencia, EnCase proporciona una amplia gama de herramientas para el análisis de datos. Esto incluye la recuperación de archivos eliminados, la extracción de metadatos, la identificación de actividad sospechosa, el análisis de registros de eventos y mucho más. EnCase ofrece capacidades avanzadas de visualización que permiten a los investigadores examinar los datos de manera efectiva. Puede explorar relaciones entre archivos, visualizar actividades de usuario, seguir rutas de acceso y crear diagramas interactivos para comprender mejor los datos.
La herramienta cuenta con capacidades de "file carving" que permiten la recuperación de archivos fragmentados o eliminados, lo que es crucial para

[25] FTK (Forensic Toolkit). 2023. [En línea] [Fecha de consulta: 05 de junio de 2023] Disponible en: https://www.forensiccomputers.com/accessdata-ftk-7.

reconstruir evidencia que podría haber sido intencionalmente ocultada o eliminada por parte del usuario. EnCase cumple con estándares y prácticas forenses reconocidas a nivel internacional, lo que garantiza que la evidencia adquirida y analizada sea válida y aceptable en procedimientos legales y judiciales.
La herramienta permite la creación de informes forenses detallados y personalizables. Estos informes incluyen hallazgos, análisis, conclusiones y metadatos relevantes que respaldan investigaciones legales y procesos judiciales.
EnCase se integra con otras herramientas forenses y sistemas de gestión de casos para facilitar la colaboración entre equipos de investigación. También permite el etiquetado y la organización eficiente de la evidencia para un análisis y presentación efectivos.

La herramienta utiliza un enfoque forense riguroso para garantizar la integridad y la trazabilidad de la evidencia digital recopilada[26].

4.5.6.3 Cellebrite UFED: Cellebrite UFED (Universal Forensic Extraction Device) es una herramienta especializada en la extracción y análisis de datos de dispositivos móviles. UFED permite a los investigadores adquirir datos de teléfonos inteligentes, tabletas y dispositivos GPS, incluso si están bloqueados o protegidos por contraseña. La herramienta es capaz de extraer una amplia variedad de datos, como mensajes de texto, registros de llamadas, correos electrónicos, archivos multimedia, datos de aplicaciones y ubicaciones GPS. Cellebrite UFED es reconocida por su amplio soporte para dispositivos móviles y su capacidad para recuperar datos eliminados[27].

4.5.6.4 Oxygen Forensic Suite: Oxygen Forensic Suite es una herramienta forense especializada en la extracción y análisis de datos de dispositivos móviles. Ofrece capacidades avanzadas para adquirir datos de teléfonos inteligentes, tabletas, drones y otros dispositivos IoT. La herramienta es compatible con una amplia gama de dispositivos y sistemas operativos, lo que permite la extracción de datos de diferentes plataformas. Oxygen Forensic Suite puede recuperar mensajes de texto, chats en aplicaciones de mensajería, registros de llamadas, ubicaciones GPS, datos de redes sociales y otra información relevante para la investigación forense[28].

4.5.6.5 Autopsy: Autopsy es una plataforma forense digital de código abierto y gratuita que ofrece una amplia gama de herramientas para la extracción y análisis de información. Es utilizado por investigadores forenses para examinar sistemas de archivos, recuperar archivos borrados, analizar metadatos, realizar análisis de palabras clave, examinar registros de eventos y realizar un análisis avanzado de

[26] EnCase Forensic. [En línea] [Fecha de consulta: 05 de junio de 2023] Disponible en: https://tableau.guidancesoftware.com/index.php.
[27] Cellebrite UFED. [En línea] [Fecha de consulta: 06 de junio de 2023] Disponible en: https://enterprise.cellebrite.com/cellebrite-ufed/
[28] Oxygen Forensic Suite. 2023. [En línea] [Fecha de consulta: 07 de junio de 2023] Disponible en: https://oxygenforensics.com/en/.

imágenes. Autopsy ofrece una interfaz gráfica intuitiva que facilita la navegación y el análisis de datos, y permite una colaboración efectiva en equipos de trabajo forenses[29].

4.5.6.6 X-Ways Forensics: X-Ways Forensics es una herramienta forense de alto rendimiento utilizada para la extracción y análisis de datos digitales. Proporciona capacidades para la adquisición forense de discos duros y otros medios de almacenamiento, así como análisis de metadatos, recuperación de contraseñas, análisis de registros y filtrado de datos. X-Ways Forensics se destaca por su velocidad y eficiencia en el procesamiento de grandes volúmenes de datos. Además, ofrece una amplia gama de funciones avanzadas, como la recuperación y análisis de archivos ocultos, el análisis de archivos de sistema y la identificación de patrones en datos estructurados y no estructurados[30].

4.5.6.7 AXIOM: Axiom es una herramienta forense digital desarrollada por Magnet Forensics. Está diseñada específicamente para investigaciones forenses en dispositivos digitales, como computadoras y dispositivos móviles. Axiom ofrece una amplia gama de capacidades y características avanzadas para adquirir, analizar y visualizar datos de manera forense.

Una de las características destacadas de Axiom es su capacidad para adquirir y procesar grandes volúmenes de datos de manera eficiente. Puede realizar la adquisición forense de imágenes de discos duros, dispositivos móviles, archivos de imágenes y otros medios de almacenamiento, y analizarlos de manera rápida y exhaustiva. Axiom tiene la capacidad de decodificar y analizar una amplia gama de aplicaciones y formatos de archivo, lo que permite una investigación forense exhaustiva en diversas plataformas y sistemas operativos[31].

4.5.6.6 CAINE: Computer Aided INvestigative Environment, es una herramienta forense digital ampliamente utilizada por profesionales en el campo de la seguridad informática y la investigación forense. Está basado en Linux y está diseñado específicamente para tareas forenses. Esto significa que incluye una variedad de herramientas y utilidades preinstaladas que son útiles para la recolección y el análisis de datos digitales. Proporciona herramientas para la adquisición segura de datos, lo que implica hacer una copia forense de los dispositivos de almacenamiento como discos duros, dispositivos USB u otros medios digitales sin alterar la evidencia

---

[29] Autopsy. 2023. [En línea] [Fecha de consulta: 07 de junio de 2023] Disponible en: https://www.autopsy.com/

[30] X-Ways Forensics. 2023. [En línea] [Fecha de consulta: consultada el 07 de junio de 2023] Disponible en: https://www.x-ways.net/forensics/

[31] Magnet forensics. 2023. [En línea] [Fecha de consulta: 08 de junio de 2023] Disponible en: https://www.magnetforensics.com/?utm_source=Google&utm_medium=Search&utm_campaign=2023_homepage&gad=1&gclid=CjwKCAjw-IWkBhBTEiwA2exyO74FvM5MZjVO_mLo3d6nUXwFludzUHezDZDiwUXvk90O8p2PS0PPmRoC1PcQAvD_BwE.

original. Una vez que se ha adquirido la evidencia, CAINE ofrece una amplia gama de herramientas para el análisis de datos. Esto incluye herramientas para la recuperación de archivos eliminados, el análisis de registros de actividad, la búsqueda de metadatos, el examen de archivos de sistema y mucho más. Permite visualizar y presentar los datos de manera efectiva, lo que es crucial en la presentación de informes forenses. Puede generar informes detallados que incluyan hallazgos, análisis y conclusiones para respaldar investigaciones legales o procesos judiciales. La herramienta está diseñada para cumplir con estándares y prácticas forenses reconocidas internacionalmente, lo que garantiza la integridad y la confiabilidad de los datos recopilados y analizados. Aunque CAINE se basa en Linux, su interfaz gráfica de usuario (GUI) está diseñada para ser intuitiva y fácil de usar, lo que facilita su utilización por parte de investigadores forenses con diferentes niveles de experiencia técnica. CAINE se mantiene actualizado con las últimas herramientas y técnicas forenses, gracias a una comunidad activa de desarrolladores y usuarios que contribuyen al proyecto[32].

La siguiente tabla muestra una comparación de algunas de las herramientas forenses mas utilizadas y disponibles en el mercado, desde diferentes aspectos, tanto técnicos, comerciales como funcionales:

Tabla 1. Comparativo de las herramientas forenses.

Herramienta	Funcionalidades principales	Soporte	Alcance	Sistemas de archivos soportados	Costo
FTK	Adquisición de imágenes forenses, análisis de imágenes, búsqueda de archivos, extracción de datos, generación de informes	Windows, macOS, Linux	PC's, servidores, dispositivos móviles	FAT16, FAT32, exFAT, NTFS, HFS+, ext3/4, Btrfs, APFS, UFS, ReiserFS, XFS, ZFS, E01, entre otros.	Licencia comercial, Costo estimado desde 2.995 USD (abril de 2024)[25]
ENCASE	Adquisición de imágenes forenses, análisis de imágenes, búsqueda de archivos, extracción de datos, generación de informes, análisis de redes	Windows, macOS, Linux	PC's, servidores, dispositivos móviles	FAT16, FAT32, exFAT, NTFS, HFS+, ext3/4, Btrfs, APFS, UFS, ReiserFS, XFS, ZFS, E01, entre otros.	Licencia comercial, Costo estimado desde 3.157 USD (abril de 2024) [26]

[32] CAINE 8 Best Linux Distros for Forensics & Pentesting [En línea] [Fecha de consulta: 02 de abril de 2024] Disponible en: https://www.esecurityplanet.com/products/open-source-distros-for-pentesting-and-forensics/

UFED	Adquisición física y lógica de datos de dispositivos móviles, análisis de datos, extracción de datos, generación de informes	Android, iOS, Windows Phone, Blackberry, etc.	Dispositivos móviles	FAT, NTFS, exFAT, HFS+, ext3/4, Btrfs, APFS, UFDR, entre otros.	Licencia comercial, Costo estimado desde 9.000 USD (abril de 2024) [27]
OXYGEN FORENSIC	Adquisición de imágenes forenses, análisis de imágenes, búsqueda de archivos, extracción de datos, generación de informes, análisis de redes, análisis de malware	Windows, macOS, Linux	PC's, servidores, dispositivos móviles	FAT, NTFS, exFAT, HFS+, ext3/4, Btrfs, APFS, , entre otros.	Licencia comercial, Costo estimado desde 3.695 USD (abril de 2024) [28]
AUTOPSY	Adquisición de imágenes forenses, análisis de imágenes, búsqueda de archivos, extracción de datos, generación de informes	Windows, macOS, Linux	PC's, servidores, dispositivos móviles	FAT, NTFS, exFAT, HFS+, ext3/4, Btrfs, APFS, , entre otros.	Gratuito
X-Ways Forensics	Adquisición de imágenes forenses, análisis de imágenes, búsqueda de archivos, extracción de datos, generación de informes	Windows	PC's, servidores	FAT, NTFS, exFAT, HFS+, ext3/4, Btrfs, APFS, , entre otros.	Licencia comercial, Costo estimado desde 1.495 USD (abril de 2024) [30]
AXIOM	Análisis de imágenes forenses, búsqueda de archivos, extracción de datos, generación de informes	Windows	PC's, servidores	FAT16, FAT32, exFAT, NTFS, HFS+, ext3/4, Btrfs, APFS, UFS, ReiserFS, XFS, ZFS, E01, entre otros.	Licencia comercial, Costo estimado desde 3.245 USD (abril de 2024) [31]
CAINE	Adquisición de imágenes forenses, análisis de imágenes, búsqueda de archivos, extracción de datos, generación de informes, análisis de redes, análisis de malware	Linux	PC's, servidores	FAT, NTFS, exFAT, HFS+, ext3/4, Btrfs, APFS, , entre otros.	Gratuito

Fuente: Elaboración propia.

Estas herramientas forenses son solo algunas de las muchas disponibles en el campo de la informática forense. Cada una de ellas ofrece características y funcionalidades específicas que se adaptan a diferentes necesidades de

investigación y análisis forense. Es importante tener en cuenta que el uso de estas herramientas debe realizarse de acuerdo con las leyes y regulaciones aplicables, y en cumplimiento de los estándares éticos y técnicos de la investigación forense.

4.6 MARCO LEGAL

- Ley 527 de 1999 – Validez jurídica y probatoria de la información electrónica;
- Ley 594 de 2000 – Ley General de Archivos – Criterios de Seguridad;
- Ley 962 de 2005 – Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas;
- Ley 1150 de 2007 – Seguridad de la información electrónica en contratación en línea;
- Ley 1273 de 2009 – Delitos Informáticos y protección del bien jurídico tutelado que es la información;
- Ley 1341 de 2009 – Tecnologías de la Información y aplicación de seguridad;
- Ley 1437 de 2011 – Procedimiento Administrativo y aplicación de criterios de seguridad;
- Ley 1480 de 2011 – Protección al consumidor por medios electrónicos. Seguridad en transacciones electrónicas;
- CONPES 3701 DE 2011 –Lineamientos Ciberseguridad y Ciberdefensa
- Decreto Ley 019 de 2012 – Racionalización de trámites a través de medios electrónicos. Criterio de seguridad
- Ley 1621 de 2013 – Ley de Inteligencia – Criterios de seguridad art. 17, art. 28, 29
- LEY 1928 DE 2018 - Por medio de la cual se aprueba el “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest.
- COMPES 3854 DE 2016 - POLÍTICA NACIONAL DE SEGURIDAD DIGITAL

4.7 MARCO REGLAMENTARIO

- Decreto 2609 de 2012 – Expediente electrónico
- Decreto 2693 de 2012 – Gobierno electrónico
- Decreto 333 de 2014 – Entidades de certificación digital
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto N° 1.008 de 2018 - por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto número 1078 de 2015, Decreto

Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

- Resolución 0-2869. (29 de diciembre, 2003). Por medio de la cual se adopta el Manual de Procedimientos del Sistema de Cadena de Custodia.
- Resolución 0-6394. (22 de diciembre, 2004). Por medio de la cual se adopta el manual de procedimientos del Sistema de Cadena de Custodia para el Sistema Penal Acusatorio
- Resolución 2999 del 2008. Por el cual se adoptan las políticas de seguridad para el manejo de la información y se dictan otras normas para el uso y administración de los bienes y servicios informáticos del Ministerio TIC.
- Resolución 2034 de 2016. Por la cual se adoptó el Modelo de Responsabilidad Social Institucional en el Ministerio TIC.
- Resolución 2007 de 2018. Por la cual se actualiza la política de tratamiento de datos personales del Ministerio/Fondo TIC.
- Resolución 911 de 2018. Por la cual se actualiza el Modelo Integrado de Gestión del MinTIC.
- Resolución 512 de 2019. Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información

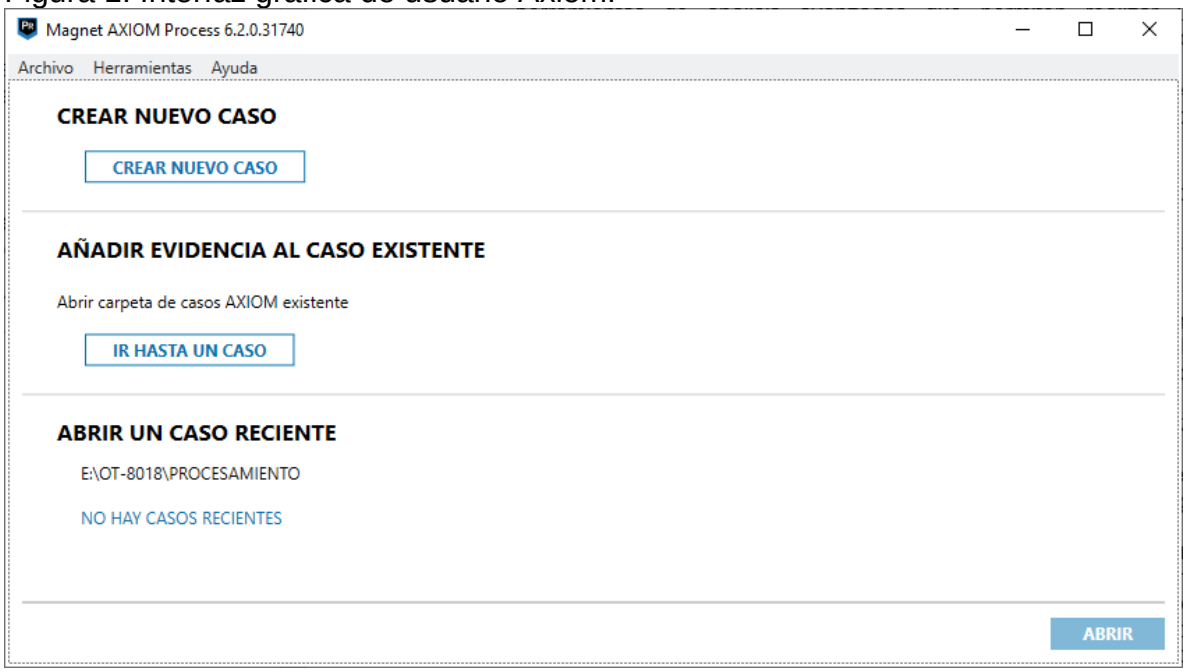
5 SELECCIÓN DE LAS HERRAMIENTAS FORENSES

Luego de realizar un detallado estudio de las herramientas forenses disponibles y ampliamente utilizadas en el análisis forense, se optó por seleccionar las siguientes cuatro herramientas forenses para la extracción y recuperación de datos en dispositivos de almacenamiento masivo en equipos personales, las cuales son muy conocidas por los diferentes profesionales y laboratorios en el análisis forense y corresponden tanto a herramientas de pago como a herramientas de uso libre y se describen a continuación:

5.1 HERRAMIENTA FORENSE AXIOM

Axiom es una herramienta forense de carácter pago muy conocida y utilizada en el campo de la investigación digital, desarrollada por Magnet Forensics, una reconocida empresa especializada en soluciones forenses digitales. Esta herramienta se utiliza para realizar análisis forenses exhaustivos en dispositivos y medios de almacenamiento digital, con el objetivo de descubrir y extraer información relevante para investigaciones criminales, incidentes de seguridad y otros casos legales.

Figura 1. Interfaz gráfica de usuario Axiom.



Fuente: Elaboración propia.

Una de las características destacadas de Axiom es su capacidad para recuperar y procesar datos de manera eficiente y efectiva. La herramienta utiliza técnicas avanzadas de adquisición forense para extraer datos de forma técnicamente sólida, preservando la integridad de la evidencia digital. Además, Axiom es compatible con

una amplia variedad de formatos de imagen forense, facilitando la importación y análisis de datos de diversas fuentes.
La interfaz de usuario de Axiom es intuitiva y fácil de usar, lo que permite realizar búsquedas complejas y análisis forenses de manera eficiente. La herramienta utiliza potentes algoritmos de búsqueda y filtrado para ayudar a encontrar rápidamente información relevante en grandes volúmenes de datos. Además, Axiom cuenta con herramientas de análisis avanzadas que permiten realizar un análisis en profundidad de los datos recuperados, identificar patrones, establecer relaciones y presentar los hallazgos de manera clara y concisa[33].
Axiom ofrece una amplia gama de capacidades y funcionalidades para abordar diferentes aspectos del análisis forense digital. Algunas de las características clave incluyen:

Recuperación y análisis de artefactos digitales: Axiom es capaz de analizar una amplia gama de artefactos digitales correos electrónicos, historial de navegación, archivos adjuntos, registros de actividad y metadatos. La herramienta puede recuperar datos incluso si han sido eliminados o están ocultos.
Análisis de redes sociales: Axiom proporciona funcionalidades para extraer y analizar datos de redes sociales populares, lo que permite obtener información valiosa de perfiles, mensajes, conexiones y actividades en línea. Esto es especialmente útil en casos que involucran delitos cibernéticos, acoso en línea o actividades sospechosas en plataformas sociales.
Análisis de imágenes y videos: Axiom tiene la capacidad de analizar imágenes y videos en busca de metadatos, información oculta, contenido inapropiado o cualquier otro aspecto relevante para una investigación. Esto puede ser de gran utilidad en casos que involucran pornografía infantil, distribución ilegal de contenido o manipulación de imágenes.
Análisis de datos de ubicación: Axiom puede analizar datos de ubicación, como registros de torres de telefonía celular y datos de GPS, para rastrear la ubicación de un dispositivo en un momento dado. Esto puede ser valioso en investigaciones de personas desaparecidas, seguimiento de delincuentes o reconstrucción de eventos.
Herramientas de visualización y generación de informes: Axiom ofrece herramientas de visualización avanzadas que permiten a los investigadores representar gráficamente los datos y las relaciones encontradas. Esto facilita la comprensión y presentación de los resultados de manera clara y convincente. Además, la herramienta permite generar informes detallados y personalizables con los hallazgos de la investigación, incluyendo tablas, gráficos, imágenes y otros elementos visuales[34].

---

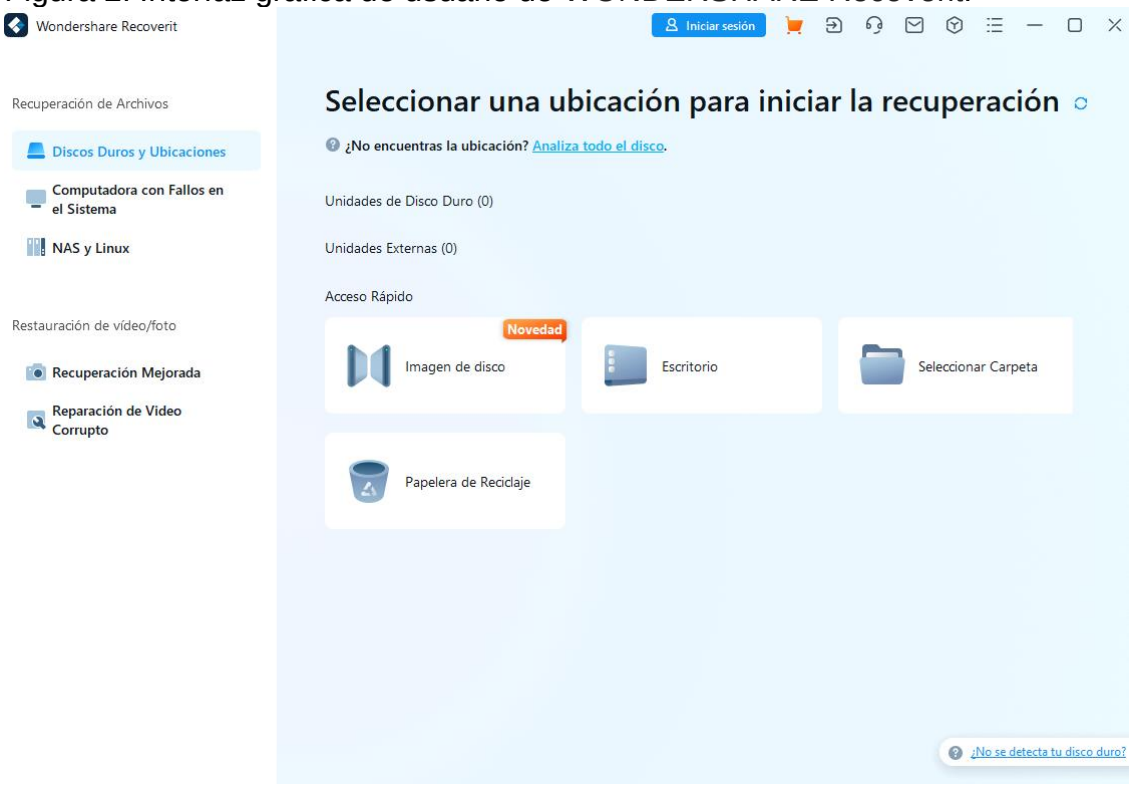
[33] Guerra M., *Análisis Forense Informático.* 2021. RA-MA Editorial. ISBN: 978-84-1897-124-2. Madrid.
[34] Magnet forensics. 2023. [En línea] [Fecha de consulta: 08 de junio de 2023] Disponible en: https://www.magnetforensics.com/?utm_source=Google&utm_medium=Search&utm_campaign=2023_homepage&gad=1&gclid=CjwKCAjw-IWkBhBTEiwA2exyO74FvM5MZjVO_mLo3d6nUXwFludzUHezDZDiwUXvk90O8p2PS0PPmRoC1PcQAvD_BwE.

Axiom es una herramienta forense completa y ampliamente utilizada que proporciona capacidades avanzadas para realizar análisis forenses digitales exhaustivos. Su amplia gama de funcionalidades, capacidad de recuperación de datos, análisis de artefactos digitales y generación de informes detallados hacen de Axiom una herramienta valiosa para los investigadores forenses y profesionales de la ciberseguridad.

5.2 HERRAMIENTA FORENSE WONDERSHARE RECOVERIT

Wondershare Recoverit es una herramienta forense con versiones tanto de pago como gratuita que se utiliza para recuperar datos perdidos o eliminados de dispositivos de almacenamiento, como discos duros, unidades flash, tarjetas de memoria, etc. La versión gratuita soporta los principales sistemas operativos, sin embargo, para acceder a las funciones premium es necesario contar con una suscripción de pago. La herramienta es compatible con una amplia gama de sistemas operativos, incluidos Windows, macOS y Linux.[35].

Figura 2. Interfaz gráfica de usuario de WONDERSHARE Recoverit.



Fuente: Elaboración propia.

[35] Wondershare Recoverit. 2023. [En línea] [Fecha de consulta: 08 de noviembre de 2023] Disponible en: https://recoverit.wondershare.es/

5.2.1 Características y funcionalidades

Wondershare Recoverit destaca por su capacidad para abordar una diversidad de dispositivos de almacenamiento, consolidándose como una herramienta forense versátil y completa. La amplitud de su compatibilidad incluye[36]:

Discos Duros Internos y Externos:

La herramienta es capaz de recuperar datos de discos duros internos, que son componentes fundamentales en computadoras de escritorio y portátiles. Además, su compatibilidad se extiende a discos duros externos, populares para realizar copias de seguridad o almacenar datos adicionales.

Unidades Flash USB:

Las unidades flash USB son comunes en la transferencia de datos entre dispositivos. Recoverit puede recuperar datos eliminados o perdidos de estas unidades, ya sean utilizadas para almacenar documentos importantes, archivos multimedia o información personal.

Tarjetas de Memoria:

Las tarjetas de memoria, presentes en cámaras digitales, teléfonos móviles y otros dispositivos, son propensas a la pérdida de datos. Recoverit ofrece soporte para estas tarjetas, permitiendo la recuperación de fotos, videos y otros archivos almacenados en ellas.

Discos Duros Virtuales:

Los discos duros virtuales, utilizados para almacenamiento en la nube o máquinas virtuales, son parte integral de la era digital. Wondershare Recoverit se adapta a estos entornos, lo que significa que los usuarios pueden recuperar datos directamente desde plataformas en la nube o máquinas virtuales.

Cámaras Digitales:

Las fotos y videos capturados con cámaras digitales pueden ser vitales para usuarios y profesionales. Recoverit permite la recuperación de archivos multimedia desde estas cámaras, incluso después de su eliminación accidental o formateo de la tarjeta de memoria.

Teléfonos Móviles:

[36] Wondershare Recoverit. 2023. [En línea] [Fecha de consulta: 08 de noviembre de 2023] Disponible en: https://recoverit.wondershare.es/

La proliferación de datos en dispositivos móviles hace que la pérdida de información sea una preocupación frecuente. Wondershare Recoverit no solo es compatible con teléfonos móviles, sino que aborda distintos sistemas operativos como Android e iOS.
Tabletas:

Las tablets, utilizadas tanto para el trabajo como para el entretenimiento, pueden albergar datos importantes. Recoverit es capaz de recuperar información de estos dispositivos, proporcionando una solución integral para la pérdida de datos.

La versatilidad de Recoverit al abordar una amplia gama de dispositivos garantiza que los usuarios tengan una herramienta única para recuperar datos desde diversas fuentes de almacenamiento. Además, este enfoque integral aumenta la aplicabilidad de la herramienta en entornos forenses, donde la diversidad de dispositivos de almacenamiento utilizados exige una solución flexible y completa.

5.2.2 Capacidad para Recuperar Datos Perdidos o Eliminados:

Uno de los aspectos más destacados de Wondershare Recoverit es su capacidad robusta para abordar situaciones de pérdida de datos, ofreciendo una serie de características avanzadas que hacen posible la recuperación efectiva incluso en escenarios complejos. A continuación, se detallan aspectos específicos de la capacidad de la herramienta para recuperar datos perdidos o eliminados[37]:

Recuperación Después de Eliminación Accidental:

Wondershare Recoverit es eficaz en la recuperación de archivos que han sido eliminados accidentalmente. Este escenario común, donde un usuario borra por error archivos importantes, es abordado de manera efectiva por la herramienta, que puede restaurar estos datos a su estado original.
Recuperación Después de Formateo:

La capacidad de Recoverit para recuperar datos después de un formateo es crucial. Incluso cuando se realiza un formateo completo de un dispositivo de almacenamiento, la herramienta utiliza algoritmos avanzados para intentar recuperar los datos previos, minimizando la pérdida de información valiosa.
Recuperación de Datos Dañados:

En situaciones donde los archivos han sido dañados debido a errores en el sistema, sectores defectuosos o corrupción de datos, Recoverit se destaca al intentar

[37] Wondershare Recoverit. 2023. [En línea] [Fecha de consulta: 08 de noviembre de 2023] Disponible en: https://recoverit.wondershare.es/

recuperar y reconstruir estos archivos. La herramienta realiza un análisis exhaustivo para restaurar la integridad de los datos tanto como sea posible.

Algoritmos Avanzados de Recuperación:

Wondershare Recoverit emplea algoritmos avanzados de recuperación de datos, como el escaneo en profundidad y la búsqueda de firmas, para localizar y reconstruir archivos. Estos algoritmos permiten que la herramienta recupere datos incluso en condiciones donde otros métodos tradicionales podrían fallar.

Recuperación Después de Sobreescritura:

La capacidad de Recoverit para recuperar datos después de sobreescritura es crucial en escenarios donde se han creado nuevos archivos después de la pérdida de datos original. La herramienta realiza un análisis minucioso para identificar fragmentos de datos que aún son recuperables, incluso si han sido parcial o completamente sobreescritos.

Vista Previa Antes de la Recuperación:

Una característica importante es la capacidad de previsualización de archivos antes de la recuperación. Esto permite a los usuarios revisar y seleccionar los archivos específicos que desean recuperar, mejorando la eficiencia y evitando la recuperación innecesaria de datos.

Segmentación por Tipos de Archivos:

Recoverit tiene la capacidad de segmentar la búsqueda y recuperación según tipos de archivos específicos. Los usuarios pueden elegir recuperar solo ciertos tipos de archivos (imágenes, documentos, videos, etc.), lo que agiliza el proceso y permite una recuperación más selectiva.

Recuperación Selectiva:

Además de la vista previa, la herramienta permite a los usuarios realizar una recuperación selectiva. Esto significa que los usuarios pueden elegir recuperar solo ciertos archivos o carpetas, evitando la sobrecarga de almacenamiento innecesaria con datos no deseados.

La capacidad integral de Recoverit para abordar diversas circunstancias de pérdida de datos, combinada con su enfoque avanzado en algoritmos y opciones de recuperación selectiva, hace que la herramienta sea excepcionalmente poderosa en el ámbito forense y para usuarios en general que buscan recuperar datos críticos en diversas situaciones.

5.2.3 Modos de Recuperación de Wondershare Recoverit:

Wondershare Recoverit presenta dos modos de recuperación que se adaptan a diferentes escenarios y requisitos del usuario. Estos modos proporcionan flexibilidad

y opciones específicas para abordar diversas situaciones de pérdida de datos. Aquí se describen detalladamente ambos modos[38]:

5.2.3.1 Recuperación Rápida:

Escenario Ideal:

Este modo es adecuado para la recuperación de datos que han sido eliminados recientemente. Es particularmente útil en situaciones en las que los archivos fueron borrados accidentalmente o perdidos de manera reciente.
Características Clave:

Escaneo Rápido: La característica principal de este modo es la rapidez del escaneo. Se centra en buscar y recuperar archivos eliminados de manera eficiente, agilizando el proceso para usuarios que necesitan una solución rápida.
Eficiencia en la Recuperación Reciente:

Al enfocarse en la recuperación rápida, este modo es eficaz para recuperar archivos que aún no han sido sobrescritos por nuevas operaciones en el dispositivo de almacenamiento.

5.2.3.2 Recuperación Completa:

Escenario Ideal:

Este modo es más exhaustivo y se recomienda para situaciones en las que la pérdida de datos ocurrió hace más tiempo, o cuando se enfrenta a problemas más complejos como formateo de disco.
Características Clave:

Escaneo Profundo: La característica distintiva de este modo es el escaneo en profundidad. A diferencia del modo rápido, este proceso es más detallado y completo, explorando cada sector del dispositivo de almacenamiento en busca de datos perdidos.
Recuperación de Datos Antiguos:

La recuperación completa es más lenta pero tiene la capacidad de recuperar datos más antiguos o datos que podrían haber sido afectados por formateo o daños en el sistema de archivos.

Elección del Modo:
Flexibilidad del Usuario:

[38] Wondershare Recoverit. 2023. [En línea] [Fecha de consulta: 08 de noviembre de 2023] Disponible en: https://recoverit.wondershare.es/

Wondershare Recoverit ofrece a los usuarios la flexibilidad de elegir entre estos dos modos en función de la naturaleza de la pérdida de datos y la urgencia de la recuperación.
Recomendaciones del Usuario:

La recomendación general es comenzar con el modo de recuperación rápida para pérdidas de datos recientes. Si no se encuentran los archivos deseados o la pérdida de datos es más antigua o compleja, se puede optar por el modo de recuperación completa.

Previsualización de Resultados:

Ambos modos ofrecen la opción de previsualizar los resultados del escaneo antes de proceder con la recuperación. Esto permite a los usuarios revisar los archivos encontrados y seleccionar específicamente aquellos que desean recuperar.
Recuperación Selectiva:

Ambos modos permiten una recuperación selectiva, lo que significa que los usuarios pueden elegir recuperar solo ciertos tipos de archivos o carpetas, evitando la recuperación innecesaria de datos.
La presencia de estos dos modos en Wondershare Recoverit no solo proporciona una solución adaptada a diferentes circunstancias, sino que también coloca el control en manos del usuario. La flexibilidad y las opciones detalladas permiten una recuperación eficaz y personalizada de los datos perdidos o eliminados[39].

5.2.4 Proceso de Recuperación Sencillo en Wondershare Recoverit:

Wondershare Recoverit ha sido diseñado con una interfaz de usuario intuitiva que hace que el proceso de recuperación de datos sea accesible para usuarios de todos los niveles de experiencia. La simplicidad del proceso se manifiesta a través de los siguientes aspectos:

Inicio y Selección del Dispositivo:
El usuario inicia la aplicación y se encuentra con una interfaz clara y bien organizada. Desde aquí, selecciona el dispositivo de almacenamiento del cual desea recuperar datos. Esta etapa inicial establece la base para el resto del proceso.
Selección del Modo de Recuperación:
Wondershare Recoverit ofrece dos modos de recuperación: rápido y completo. El usuario elige el modo que mejor se adapte a sus necesidades, considerando la

[39] Wondershare Recoverit. 2023. [En línea] [Fecha de consulta: 08 de noviembre de 2023] Disponible en: https://recoverit.wondershare.es/

antigüedad de la pérdida de datos y la complejidad de la situación. Esta elección ofrece flexibilidad y adaptabilidad a diferentes escenarios.

Escaneo del Dispositivo:
Una vez seleccionado el modo de recuperación, el usuario inicia el escaneo del dispositivo de almacenamiento. Dependiendo del modo elegido, se lleva a cabo un escaneo rápido y eficiente o un escaneo en profundidad más detallado. El progreso del escaneo se muestra de manera clara para que el usuario pueda seguir el proceso.

Selección de Datos a Recuperar:
Después de completar el escaneo, Recoverit presenta los resultados de manera estructurada. Aquí, el usuario tiene la capacidad de previsualizar los archivos encontrados. Esta función permite una revisión minuciosa antes de proceder con la recuperación, lo que asegura que solo se recuperen los archivos deseados.

Recuperación de Datos Seleccionados:
Una vez que se han revisado los resultados y seleccionado los archivos que se desean recuperar, el usuario realiza el paso final: hacer clic en el botón de recuperación. Recoverit procede a restaurar los datos seleccionados en la ubicación deseada[40].

Características Facilitadoras:

Interfaz Intuitiva:
La interfaz de Wondershare Recoverit se presenta de manera clara y organizada, con secciones distintas que guían al usuario a través de cada fase del proceso. Esto reduce la curva de aprendizaje y hace que la herramienta sea accesible para usuarios no técnicos.

Vista Previa Antes de la Recuperación:
La capacidad de previsualizar archivos antes de la recuperación agrega un nivel adicional de control. Los usuarios pueden examinar los resultados del escaneo y asegurarse de que los archivos que desean recuperar estén presentes.

Recuperación Selectiva:
La opción de recuperación selectiva permite a los usuarios elegir específicamente los archivos o carpetas que desean restaurar. Esto evita la recuperación innecesaria de datos y garantiza una recuperación más eficiente.
Instrucciones Claras:

[40] Wondershare Recoverit. 2023. [En línea] [Fecha de consulta: 08 de noviembre de 2023] Disponible en: https://recoverit.wondershare.es/

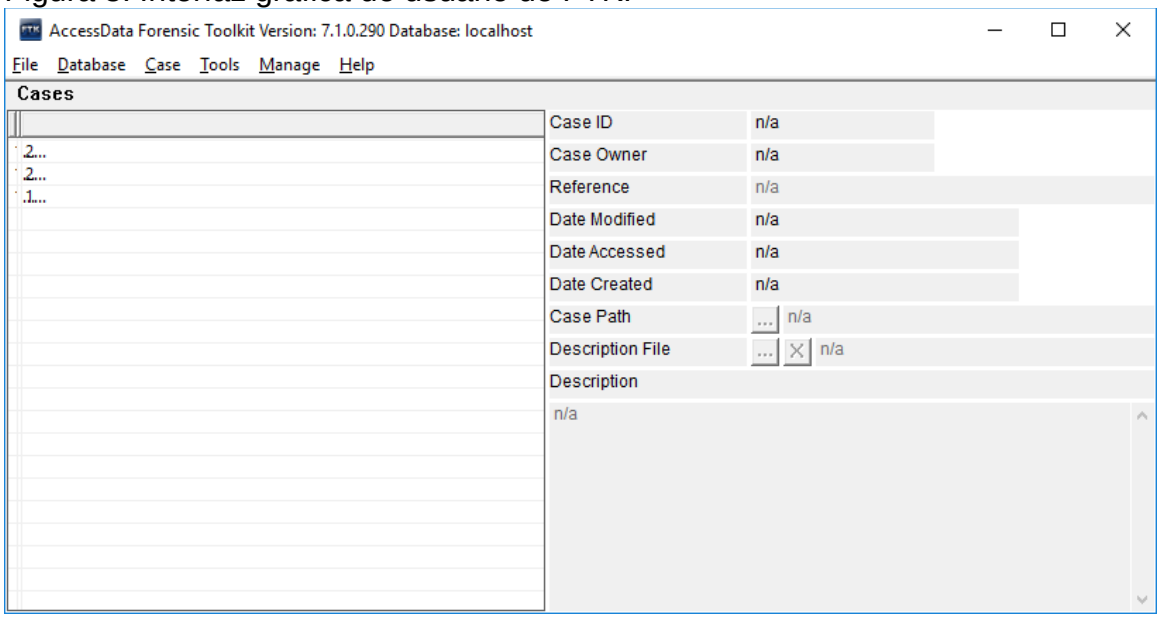
En cada etapa del proceso, Wondershare Recoverit proporciona instrucciones claras y mensajes informativos. Esto ayuda al usuario a entender el estado del proceso y a tomar decisiones informadas.

El proceso de recuperación sencillo en Wondershare Recoverit no solo se centra en la eficacia, sino también en la experiencia del usuario. Desde la selección del dispositivo hasta la recuperación final de datos, la herramienta ha sido diseñada para ser intuitiva y fácil de usar, permitiendo a los usuarios recuperar sus archivos de manera rápida y eficiente.

5.3 HERRAMIENTA FORENSE FTK

FTK (Forensic Toolkit) es una potente herramienta forense digital de uso comercial y carácter pago utilizada por profesionales de la seguridad y la aplicación de la ley para investigar y analizar evidencias digitales. Desarrollada por AccessData, FTK proporciona una amplia gama de funcionalidades diseñadas para adquirir, analizar y presentar evidencias digitales de manera eficiente y técnicamente sólida[41].

Figura 3. Interfaz gráfica de usuario de FTK.



Fuente: Elaboración propia.

Adquisición de evidencias: FTK ofrece diversas opciones para la adquisición de evidencias digitales. Puede realizar adquisiciones forenses de discos duros, imágenes de dispositivos móviles, volcados de memoria y otros medios de

[41] Lázaro, F. Introducción a la informática forense. 2014. [En línea]. [Fecha de consulta abril de 2023]. Paracuellos de Jarama, Madrid, RAMA Editorial. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ ereader/unad/106250?page=246

almacenamiento. La herramienta permite realizar copias bit a bit, asegurando la integridad de los datos originales durante el proceso de adquisición.
Análisis forense: FTK cuenta con un potente motor de análisis que permite a los investigadores examinar y filtrar grandes volúmenes de datos en busca de información relevante. Los datos se organizan en una estructura jerárquica, lo que facilita la navegación y el análisis de archivos y directorios. Se pueden realizar búsquedas avanzadas, aplicar filtros y utilizar herramientas de visualización para identificar rápidamente evidencias clave[42].
Recuperación de contraseñas: FTK incluye funcionalidades para recuperar contraseñas de archivos y sistemas encriptados. Utiliza técnicas avanzadas de recuperación de contraseñas, como fuerza bruta, diccionarios y ataques basados en reglas para desbloquear archivos protegidos con contraseña. Esto permite a los investigadores acceder a datos críticos que podrían estar ocultos detrás de medidas de seguridad.
Análisis de registros de eventos: FTK es capaz de analizar y correlacionar registros de eventos de sistemas operativos y aplicaciones. Se pueden examinar registros de eventos de Windows, registros de bases de datos, registros de servidores web y otros registros relevantes para obtener información sobre actividades sospechosas, accesos no autorizados y otras pistas valiosas en una investigación forense.
Análisis de archivos de correo electrónico: FTK tiene la capacidad de analizar archivos de correo electrónico de diversas plataformas, como Microsoft Outlook, Lotus Notes y Thunderbird. Se pueden examinar metadatos de correos electrónicos, contenido de mensajes, archivos adjuntos y otra información relacionada para obtener pistas y evidencias importantes.
Análisis de navegadores web: La herramienta permite el análisis de datos relacionados con la actividad de navegación web. Puede extraer información de caché, cookies, historiales de navegación y contraseñas guardadas en varios navegadores web, como Internet Explorer, Mozilla Firefox, Google Chrome y otros. Esto puede ser crucial para reconstruir la actividad en línea de un sospechoso o víctima.
Análisis de archivos multimedia: FTK es capaz de analizar una amplia gama de archivos multimedia, como imágenes, videos y archivos de audio. Se puede examinar metadatos, realizar comparaciones de imágenes, extraer miniaturas y realizar análisis forenses específicos de archivos multimedia. Esto puede ser útil en casos donde los archivos de medios juegan un papel importante en la investigación[43].
Análisis de redes y tráfico: FTK cuenta con funcionalidades para analizar tráfico de red y realizar investigaciones relacionadas con redes informáticas. Puede examinar registros de tráfico, identificar patrones de comunicación, analizar protocolos de red

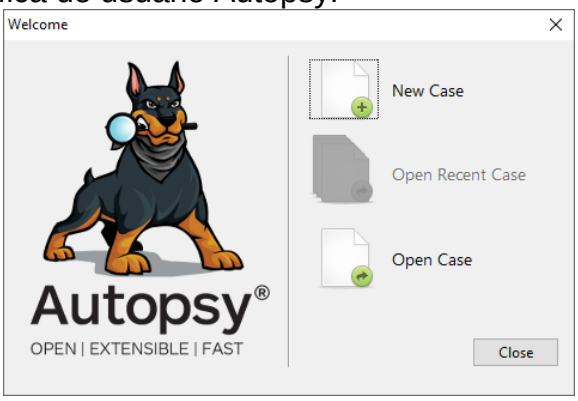
[42] Castañeda F., Rojas V., Villanueva N., *Evaluación de herramientas para análisis forense orientado a discos duros.* 2009. México.
[43] LMO Campos, E. Gomes y HP Martins, "Experiencia forense en dispositivos de almacenamiento USB Flash Drive: procedimientos y técnicas para evidencia", en *IEEE Latin America Transactions*, vol. 14, núm. 7, págs. 3427-3433. 2016. doi: 10.1109/TLA.2016.7587651.

y visualizar conexiones entre dispositivos. Esto es valioso en investigaciones de delitos cibernéticos y actividades maliciosas en línea.
Generación de informes: FTK permite generar informes detallados y profesionales que documentan los hallazgos y las evidencias recopiladas durante el proceso de análisis. Los informes pueden personalizarse según las necesidades del investigador y se pueden generar en formatos populares, como PDF, HTML y CSV. Esto facilita la presentación de resultados y la comunicación de las conclusiones de la investigación[44].
Integración con otras herramientas forenses: FTK se integra con otras herramientas y tecnologías forenses, lo que permite aprovechar un ecosistema más amplio de recursos y funcionalidades. Por ejemplo, se puede integrar con herramientas de análisis de imágenes forenses, herramientas de análisis de malware y bases de datos de hash para la comparación rápida de archivos conocidos.

5.4 HERRAMIENTA FORENSE AUTOPSY

Autopsy es una herramienta forense digital de código abierto y uso libre que proporciona una plataforma completa para la investigación y análisis forense de evidencias digitales. Es una herramienta ampliamente utilizada en el campo de la ciberseguridad y la aplicación de la ley debido a su interfaz intuitiva, capacidades de análisis avanzadas y su enfoque en la automatización[45].
Interfaz gráfica de usuario: Autopsy cuenta con una interfaz gráfica de usuario (GUI) que facilita el uso de la herramienta. La interfaz está diseñada de manera clara y organizada, lo que permite acceder a las funcionalidades y herramientas de análisis de manera eficiente. Proporciona paneles personalizables y vistas intuitivas para facilitar la navegación y el análisis de las evidencias digitales.

Figura 4. Interfaz gráfica de usuario Autopsy.



Fuente: Elaboración propia.

[44] FTK (Forensic Toolkit). 2023. [En línea] [Fecha de consulta: 05 de junio de 2023] Disponible en: https://www.forensiccomputers.com/accessdata-ftk-7.
[45] PADULA, E. J.; FOGLIATO, N.; CASCO, M. Análisis Digital Forense, Conceptos y Aplicaciones. 2016. Facultad de Ciencias Exactas, Ingeniería. Universidad Nacional de Rosario. Rosario, Santa Fe. Argentina.

Adquisición de evidencias: Una de las características principales de Autopsy es su capacidad para adquirir evidencias digitales de diferentes fuentes. Puede realizar adquisiciones forenses de discos duros, imágenes de dispositivos móviles, volcados de memoria y archivos de imágenes forenses (como DD y E01). La herramienta garantiza la integridad de los datos originales durante el proceso de adquisición y preserva la cadena de custodia.
Análisis de sistemas de archivos: Autopsy es compatible con una amplia gama de sistemas de archivos, como FAT, NTFS, HFS+, ext2/3/4 entre otras. Permite a los investigadores examinar la estructura del sistema de archivos, navegar por directorios y archivos, y recuperar información relevante para la investigación. Además, proporciona una visualización gráfica de la estructura del sistema de archivos para facilitar la comprensión y el análisis[46].
Análisis automatizado: Una de las fortalezas de Autopsy es su capacidad para realizar análisis automatizados de evidencias digitales. La herramienta ofrece una serie de módulos de análisis que automatizan tareas comunes, como la extracción de metadatos, la identificación de palabras clave, el análisis de archivos compartidos, la detección de pornografía infantil, entre otros. Esto permite ahorrar tiempo en el procesamiento y análisis de grandes volúmenes de datos.
Análisis de metadatos: Autopsy es capaz de extraer y analizar metadatos de archivos, como información de fecha y hora, ubicación geográfica, propiedades del dispositivo y más. Se puede utilizar esta información para establecer la cronología de eventos, identificar ubicaciones relevantes o reconstruir actividades en línea. Además, Autopsy proporciona herramientas de visualización de metadatos para una presentación clara y comprensible[47].
Análisis de comunicaciones: La herramienta permite el análisis de comunicaciones digitales, como registros de llamadas, mensajes de texto, correos electrónicos y registros de chat. Se puede examinar la información de los registros de comunicación, identificar patrones, analizar conexiones entre personas y reconstruir conversaciones relevantes. Además, Autopsy puede integrarse con herramientas de análisis forense de comunicaciones, como Volatility, para un análisis más profundo.
Análisis de navegadores web: Autopsy incluye funcionalidades para el análisis de la actividad de navegación web. Puede extraer información de caché, cookies, historiales de navegación y contraseñas almacenadas en diferentes navegadores web. Esto permite examinar la actividad en línea de un sospechoso o víctima, identificar sitios web visitados y recuperar información importante para la investigación.
Análisis de imágenes y videos: Autopsy ofrece capacidades de análisis de imágenes y videos. Se puede utilizar la herramienta para examinar metadatos de imágenes, realizar comparaciones visuales, extraer miniaturas y analizar contenido visual en

[46] Autopsy. 2023. [En línea] [Fecha de consulta: 07 de junio de 2023] Disponible en: https://www.autopsy.com/
[47] LÓPEZ DELGADO, Miguel. Análisis Forense Digital. 2007. [En Línea]. [Fecha de consulta: junio, 2023]. Disponible en: https://www.oas.org/juridico/spanish/cyb_ analisis_foren.pdf

busca de pistas y evidencias. Esto puede ser útil en casos donde las imágenes o videos son evidencia clave, como la identificación de personas o la detección de contenido ilícito.

Análisis de registros de eventos: Autopsy tiene la capacidad de analizar registros de eventos de sistemas operativos y aplicaciones. Se puede examinar registros de eventos de Windows, registros de bases de datos, registros de servidores web y otros registros relevantes para obtener información sobre actividades sospechosas, accesos no autorizados y otras pistas valiosas en una investigación forense.

Integración con herramientas externas: Autopsy se puede integrar con otras herramientas forenses y utilidades externas para ampliar su funcionalidad. Se puede aprovechar la integración con herramientas como Volatility para el análisis de memoria, RegRipper para el análisis de registro, y otras herramientas de código abierto y comerciales para complementar y mejorar el análisis forense.

Generación de informes: Autopsy facilita la generación de informes detallados y profesionales que documentan los hallazgos y las evidencias recopiladas durante el proceso de análisis forense. Los informes pueden personalizarse según las necesidades y se pueden generar en diferentes formatos, como PDF, HTML y CSV. Esto facilita la presentación de resultados y la comunicación de las conclusiones de la investigación.

Comunidad y soporte: Autopsy es una herramienta de código abierto respaldada por una comunidad activa de desarrolladores y usuarios. Esto proporciona acceso a una amplia base de conocimientos, recursos de aprendizaje y soporte de la comunidad. Los usuarios pueden colaborar, compartir experiencias y contribuir a la mejora continua de la herramienta[48].

[48] Autopsy. 2023. [En línea] [Fecha de consulta: 07 de junio de 2023] Disponible en: https://www.autopsy.com/

6 PLANIFICACIÓN PARA LA REALIZACIÓN DE PRUEBAS

Las pruebas se realizarán en un entorno controlado utilizando dispositivos de almacenamiento masivo que contengan archivos previamente guardados.

Se utilizarán los siguientes dispositivos de almacenamiento masivo:

- Disco duro externo de 2 TB
- Tarjeta MICRO SD de 32 GB
- Memoria USB de 64 GB

Los datos guardados corresponden a los siguientes tipos de archivos:

- Archivos de texto
- Archivos de imagen
- Archivos de video
- Archivos de audio
- Archivos de correo electrónico
- Archivos de bases de datos

6.1 Realización de la imagen forense:

La realización de una imagen forense en el análisis de discos duros es una práctica fundamental en el campo de la informática forense y la ciberseguridad. Se justifica por varias razones cruciales, que garantizan la integridad, la autenticidad y la preservación de la evidencia digital en investigaciones y procedimientos legales. La necesidad de realizar imágenes forenses en el análisis de discos duros se justifica por las siguientes razones:

6.1.1 Preservación de la Evidencia:

La principal razón para realizar una imagen forense es preservar la evidencia digital en su estado original y sin modificaciones. Una imagen forense es una copia exacta, bit a bit, del contenido del disco duro en un momento específico. Esto asegura que los datos no sean alterados o dañados durante el proceso de análisis.

6.1.2 Integridad de la Cadena de Custodia:

La creación de una imagen forense garantiza la integridad de la cadena de custodia, que es crucial en investigaciones legales. La cadena de custodia documenta quién tuvo acceso a la evidencia, cuándo y qué acciones se llevaron a cabo en cada etapa de la investigación. Esto es fundamental para demostrar que la evidencia se mantuvo segura y sin alteraciones desde su adquisición hasta su presentación en un tribunal.

6.1.3 Evitar Contaminación de la Evidencia:

Al trabajar con una imagen forense en lugar del disco duro original, se evita la contaminación de la evidencia. Cualquier intento de acceder o modificar los datos en el disco duro original podría invalidar la evidencia o hacer que no sea admisible en un tribunal.

6.1.4 Análisis Seguro:

La imagen forense permite a los investigadores realizar análisis de datos de manera segura, sin el riesgo de modificar o dañar accidentalmente los archivos. Esto es particularmente importante cuando se están investigando amenazas cibernéticas, delitos informáticos y casos de piratería.

6.1.5 Recuperación de Datos Eliminados:

En muchos casos, es necesario recuperar datos eliminados. Una imagen forense captura no solo los archivos activos, sino también los datos eliminados o sectores no utilizados del disco, lo que facilita la recuperación de información valiosa.

6.1.6 Múltiples Copias para Análisis:

Una vez que se ha creado una imagen forense, se pueden realizar múltiples copias para su análisis, sin afectar el disco original. Esto permite a varios investigadores trabajar en el caso sin temor a modificar los datos subyacentes.

6.1.7 Cumplimiento Legal y Admisibilidad en Tribunales:

Las imágenes forenses generalmente cumplen con los estándares legales y se consideran admisibles en los tribunales. Esto garantiza que la evidencia recopilada pueda ser utilizada en procedimientos legales y no sea cuestionada por su integridad.

6.1.8 Investigaciones Posteriores:

Una imagen forense también es útil para investigaciones posteriores o para futuros análisis. Permite a los investigadores volver a examinar la evidencia sin necesidad de acceder nuevamente al disco duro original.

6.1.9 Cumplimiento de Normativas de Privacidad:

Al utilizar imágenes forenses, se puede cumplir con regulaciones de privacidad y protección de datos. Estas regulaciones exigen que la información se maneje de manera segura y se eviten exposiciones no autorizadas.

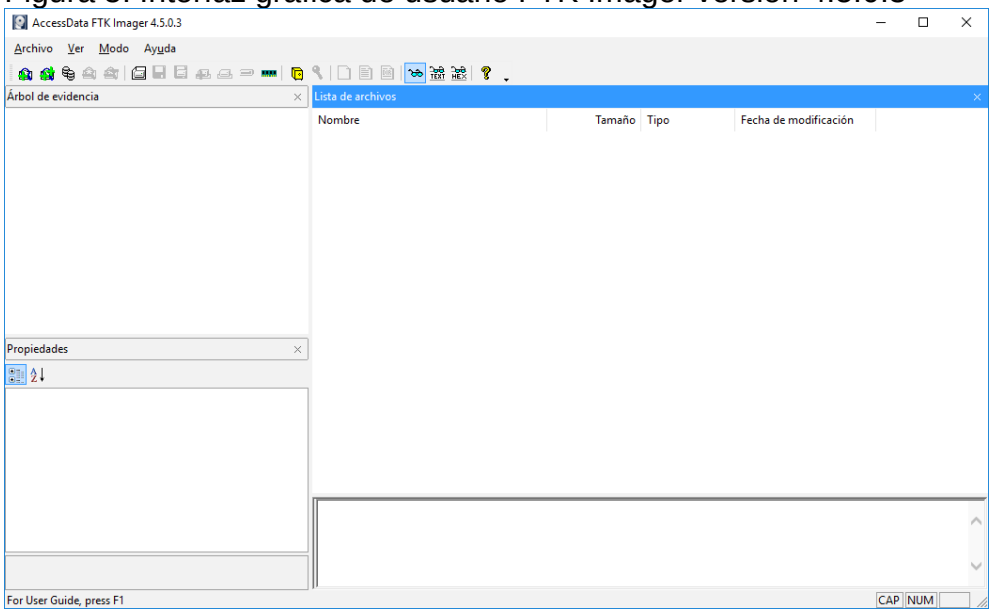
6.1.10 Reducción de Riesgos Jurídicos:

La utilización de imágenes forenses reduce los riesgos jurídicos al garantizar que la evidencia digital se recopile y maneje de manera apropiada. Esto puede prevenir problemas legales que podrían surgir si se modifica la evidencia o se viola la cadena de custodia.

6.2 Software para la generación de la imagen forense

La adquisición de imágenes forenses es el proceso de crear una copia exacta y forense de un dispositivo de almacenamiento o una parte de él, con el propósito de preservar y analizar la evidencia digital en investigaciones forenses. Para la obtención de dichas imágenes se optó por utilizar el software FTK IMAGER. Esta herramienta forense desarrollada por AccessData, una empresa ampliamente reconocida en el campo de la informática forense y la ciberseguridad. FTK Imager se utiliza para la adquisición y el análisis de datos en investigaciones forenses y es una parte integral del kit de herramientas forenses FTK (Forensic Toolkit)[49].

Figura 5. Interfaz gráfica de usuario FTK Imager versión 4.5.0.3



Fuente: Elaboración propia.

[49] FTK (Forensic Toolkit). 2023. [En línea] [Fecha de consulta: 05 de junio de 2023] Disponible en: https://www.forensiccomputers.com/accessdata-ftk-7.

Ésta es una herramienta especializada en este proceso y ofrece las siguientes características y capacidades:

6.2.1 Integridad de la Evidencia:

FTK Imager garantiza que la integridad de la evidencia digital se mantenga en todo momento. Durante la adquisición, crea una copia bit a bit de los datos almacenados en el dispositivo, lo que significa que cada bit de información se replica en la imagen forense sin alteraciones ni modificaciones. Esto es fundamental para preservar la evidencia en su estado original y asegurar que no se pueda cuestionar su autenticidad en un tribunal.

6.2.2. Copia de Dispositivos de Almacenamiento:

La herramienta permite la adquisición de imágenes forenses de diversos dispositivos de almacenamiento, que incluyen discos duros internos y externos, dispositivos USB, tarjetas de memoria, discos ópticos y más. Los investigadores pueden seleccionar la fuente de datos de la que desean obtener la imagen forense.

6.2.3. Creación de Copias en Formatos Estandarizados:

FTK Imager es capaz de crear imágenes forenses en formatos estandarizados, como Encase E01, Raw DD (copia bruta de disco), AFF (Avanced Forensic Format), y otros. Estos formatos son reconocidos en la comunidad forense y son compatibles con otras herramientas de análisis forense, lo que facilita el intercambio de evidencia y datos entre profesionales forenses.

6.3 Pruebas:

Las siguientes son las pruebas que se llevarán a cabo como parte del proceso de evaluación de herramientas forenses en un entorno controlado. Estas pruebas están diseñadas para evaluar diferentes aspectos de las herramientas y su capacidad para realizar tareas clave en la informática forense:

6.3.1 Prueba de Extracción de Datos:

Esta prueba se enfoca en evaluar la capacidad de las herramientas forenses para extraer todos los datos de los dispositivos de almacenamiento masivo especificados, que incluyen un disco duro interno de 2 TB, una tarjeta SD de 32 GB y una memoria USB de 64 GB. A continuación, se describen los criterios específicos que se utilizarán para evaluar esta prueba:

Número de archivos extraídos: Se contabilizará el número total de archivos extraídos de cada dispositivo de almacenamiento. Esto permitirá determinar si las herramientas pueden recuperar todos los archivos presentes en el dispositivo.

Número de archivos extraídos eliminados y/o recuperados: Se contabilizará el número total de archivos extraídos eliminados y/o recuperados de cada dispositivo de almacenamiento. Esto permitirá determinar la capacidad de recuperación de cada herramienta forense.

Tiempo de extracción: Se registrará el tiempo necesario para extraer los datos de cada dispositivo de almacenamiento. Esta métrica es esencial para evaluar la eficiencia de las herramientas en términos de velocidad de extracción.

6.3.2 Prueba de Recuperación de Datos:

En esta prueba, se evaluará la capacidad de las herramientas forenses para recuperar datos que han sido eliminados o dañados. Los dispositivos de almacenamiento mencionados anteriormente se utilizarán para esta prueba. A continuación, se detallan los criterios que se utilizarán para evaluar la eficacia de esta prueba:

Porcentaje de datos recuperados: Se calculará el porcentaje de datos que las herramientas son capaces de recuperar con éxito, en comparación con el conjunto total de datos eliminados o dañados en cada dispositivo.
Calidad de los datos recuperados: Se evaluará la integridad y la utilidad de los datos recuperados. Esto implica verificar si los archivos recuperados son accesibles y legibles.

Tiempo de recuperación: Se registrará el tiempo necesario para llevar a cabo el proceso de recuperación de datos en cada dispositivo. Esto es fundamental para determinar la eficiencia de las herramientas en la recuperación de datos.

6.3.3 Prueba de Análisis de Datos:

La prueba de análisis de datos se centrará en la capacidad de las herramientas para analizar los datos extraídos de los dispositivos de almacenamiento. Se utilizarán los mismos criterios de los dispositivos mencionados en pruebas anteriores. Los criterios de evaluación incluyen:
Facilidad de uso de las herramientas: Se evaluará la facilidad con la que los investigadores pueden utilizar las herramientas para analizar los datos. Esto incluye la capacidad de navegar, buscar y filtrar los datos de manera eficiente.
Robustez de las herramientas: Se determinará la capacidad de las herramientas para manejar una variedad de formatos de archivos y situaciones de datos. La robustez es esencial para garantizar que las herramientas sean versátiles en diferentes escenarios.
Precisión de los resultados del análisis: Se evaluará la precisión de los resultados de análisis generados por las herramientas. Esto implica verificar la identificación precisa de datos relevantes y la generación de informes con detalles precisos.

6.4 Herramientas

Cada herramienta tiene su conjunto de características y capacidades únicas, y se seleccionan para evaluar su idoneidad en diferentes aspectos de la informática forense. A continuación, se proporciona una descripción general de cada herramienta que se utilizará:

6.4.1 FTK: Forensic Toolkit Versión 7.1.0.290

Descripción: FTK (Forensic Toolkit) es una herramienta forense ampliamente utilizada que ofrece una amplia gama de características para la adquisición, análisis y presentación de evidencia digital. Está diseñada para ser una solución integral en investigaciones forenses[50].
Características Destacadas: FTK es conocido por su capacidad para adquirir datos de una variedad de dispositivos y medios de almacenamiento. Ofrece herramientas de búsqueda avanzada, análisis de metadatos y capacidades de informes personalizables. También incluye características de indexación y filtrado para facilitar la identificación de evidencia relevante.

6.4.2 AXIOM: All-in-One Forensics versión 6.2.0.31740

Descripción: AXIOM es una herramienta forense desarrollada por Magnet Forensics que se destaca por su enfoque integral para la recuperación y el análisis de evidencia digital. Ofrece capacidades avanzadas para la adquisición y el análisis de datos[51].
Características Destacadas: AXIOM es conocido por su capacidad para recuperar datos de dispositivos móviles, aplicaciones en la nube y medios de almacenamiento tradicionales. Ofrece análisis de registros de chat, imágenes, redes sociales entre otros. Además, presenta una interfaz de usuario intuitiva y funciones de generación de informes.

6.4.3 Wondershare Recoverit

Wondershare Recoverit es una herramienta destacada de recuperación de datos, compatible con una amplia gama de dispositivos de almacenamiento, desde discos duros hasta tarjetas de memoria y cámaras digitales. Su interfaz intuitiva facilita la recuperación de datos para usuarios de todos los niveles de experiencia. Ofrece

---

[50] FTK (Forensic Toolkit). 2023. [En línea] [Fecha de consulta: 05 de octubre de 2023] Disponible en: https://www.forensiccomputers.com/accessdata-ftk-7.
[51] Magnet forensics. 2023. [En línea] [Fecha de consulta: 08 de octubre de 2023] Disponible en: https://www.magnetforensics.com/?utm_source=Google&utm_medium=Search&utm_campaign=2023_homepage&gad=1&gclid=CjwKCAjw-IWkBhBTEiwA2exyO74FvM5MZjVO_mLo3d6nUXwFludzUHezDZDiwUXvk90O8p2PS0PPmRoC1PcQAvD_BwE.

dos modos de recuperación, rápido y completo, adaptándose a distintas situaciones de pérdida de datos.
Con algoritmos avanzados, Recoverit puede recuperar datos perdidos debido a eliminaciones accidentales, formateo, daño del sistema de archivos y otros escenarios desafiantes. La herramienta permite previsualizar archivos antes de la recuperación, brindando control y evitando la restauración innecesaria de datos. Su capacidad para abordar discos duros virtuales y recuperar datos desde la nube y máquinas virtuales amplía su utilidad en diversos entornos operativos[52].

6.4.4 AUTOPSY: Advanced Forensics Toolkit Versión 4.21.0

Descripción: AUTOPSY, también conocido como The Sleuth Kit y Autopsy, es una herramienta forense de código abierto que se utiliza para la adquisición y el análisis de datos. Aunque es de código abierto, ofrece un conjunto completo de funciones forenses[53].
Características Destacadas: AUTOPSY es conocido por su capacidad para analizar sistemas de archivos, recuperar datos de medios de almacenamiento y generar informes forenses detallados. También es apreciado por su comunidad de usuarios activa y su compatibilidad multiplataforma.

6.5 Resultados

En esta parte, se describe cómo se evaluarán y medirán los resultados de las pruebas realizadas en las herramientas forenses. Los resultados son fundamentales para tomar decisiones informadas sobre la elección de las herramientas más adecuadas para aplicaciones específicas en el campo de la informática forense. Los resultados se evaluarán en función de varios criterios clave:

6.5.1 Completitud de los datos extraídos:

Este criterio evaluará la capacidad de las herramientas para extraer datos de manera completa de los dispositivos de almacenamiento. Se medirá si las herramientas pueden recuperar todos los archivos y datos disponibles en los dispositivos de prueba. La completitud es esencial, ya que la falta de datos importantes puede afectar negativamente una investigación forense.

6.5.2 Efectividad de la recuperación de datos:

[52] Wondershare Recoverit. 2023. [En línea] [Fecha de consulta: 08 de noviembre de 2023] Disponible en: https://recoverit.wondershare.es/
[53] Autopsy. 2023. [En línea] [Fecha de consulta: 07 de junio de 2023] Disponible en: https://www.autopsy.com/.

Este criterio evaluará la capacidad de las herramientas para recuperar datos que han sido eliminados o dañados. Se medirá la efectividad de la recuperación en términos del porcentaje de datos recuperados en comparación con el conjunto total de datos eliminados o dañados. Una recuperación efectiva es crucial para la recuperación de evidencia importante en casos forenses.

6.5.3 Calidad del análisis de datos:

Este criterio evaluará la calidad de los resultados del análisis de datos generados por las herramientas. Se considerará si las herramientas proporcionan resultados precisos y significativos. La calidad del análisis es esencial para determinar la utilidad de las herramientas en la interpretación de la evidencia digital y la generación de informes forenses sólidos.

Los resultados de las pruebas se expresarán en términos cuantitativos y cualitativos, lo que permitirá una evaluación completa de las herramientas forenses y sus capacidades. Estos resultados serán documentados y presentados en informes detallados, lo que facilitará la comparación y la toma de decisiones informadas sobre qué herramientas son las más adecuadas para aplicaciones específicas en el campo de la informática forense.

7 REALIZACIÓN Y EJECUCIÓN DE PRUEBAS

7.1 DISCO DURO INTERNO 2TB

El primer dispositivo objeto de análisis corresponde a un disco duro interno marca Seagate de 2TB de capacidad, el cual se muestra en la siguiente imagen:

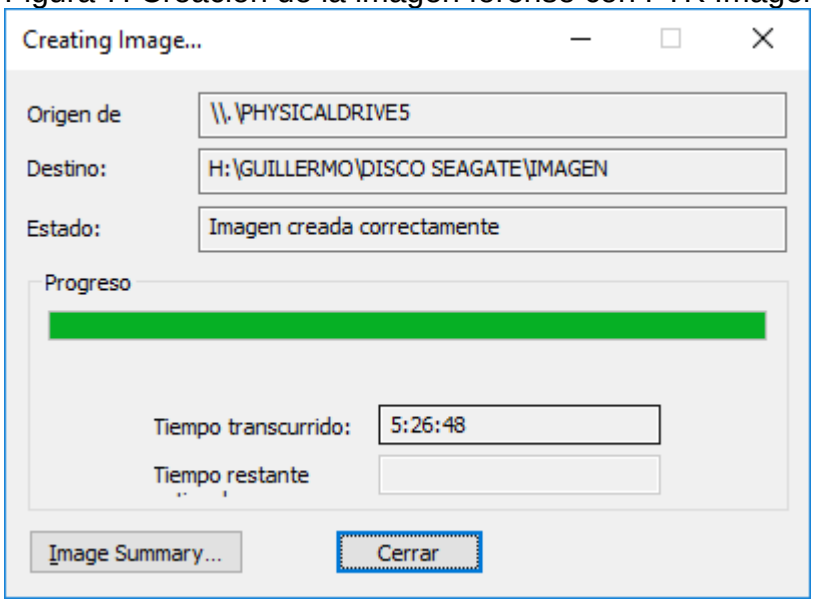
Figura 6. Disco duro interno de 2 TB marca Seagate.

Fuente: Elaboración propia.

7.1.1 OBTENCIÓN DE IMAGEN FORENSE

Inicialmente, se realiza la obtención de la imagen forense con la herramienta FTK Imager versión 4.5.0.3, en formato E01, como se muestra en la siguiente imagen:

Figura 7. Creación de la imagen forense con FTK Imager versión 4.5.0.3

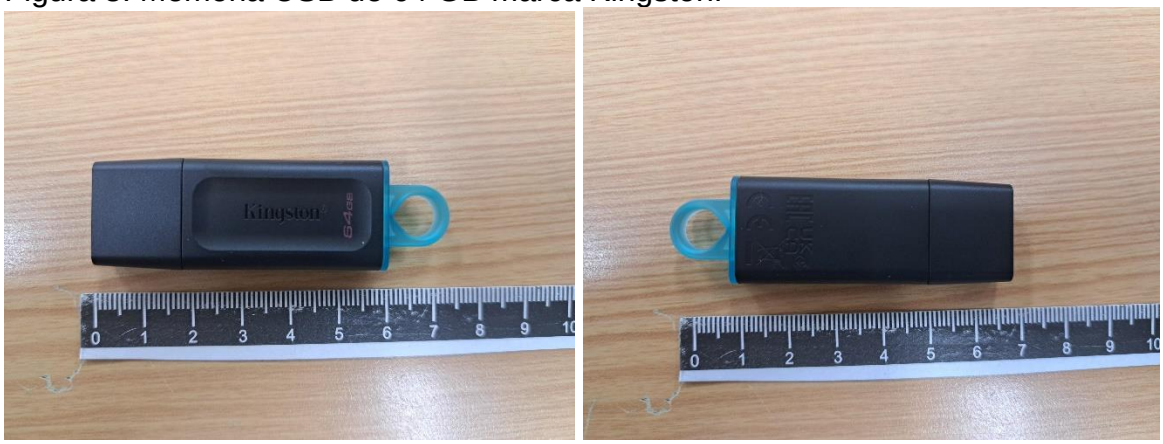


Fuente: Elaboración propia.

7.2 MEMORIA USB 64 GB

El segundo dispositivo objeto de análisis corresponde a una memoria USB marca Kingston de 64GB de capacidad, el cual se muestra en la siguiente imagen:

Figura 8. Memoria USB de 64 GB marca Kingston.

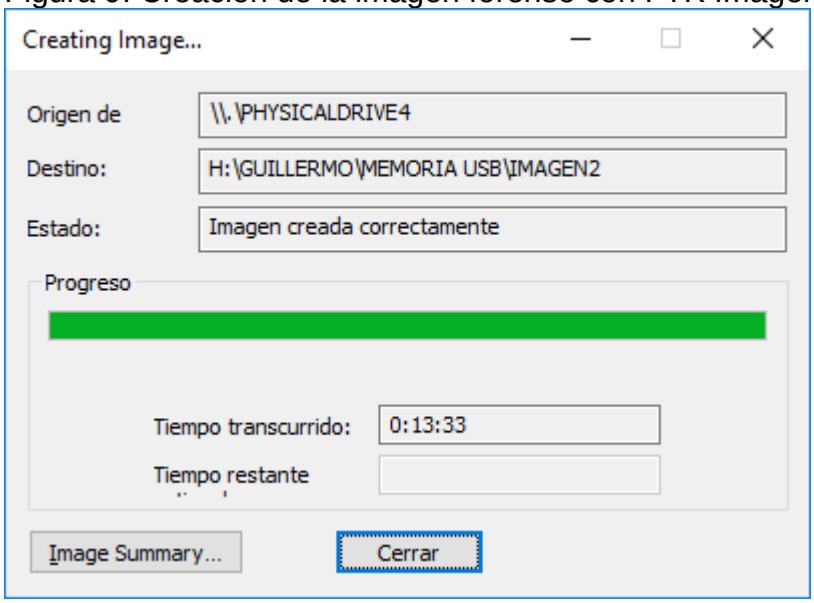


Fuente: Elaboración propia.

7.2.1 OBTENCIÓN DE IMAGEN FORENSE

Inicialmente, se realiza la obtención de la imagen forense con la herramienta FTK Imager versión 4.5.0.3, en formato E01, como se muestra en la siguiente imagen:

Figura 9. Creación de la imagen forense con FTK Imager versión 4.5.0.3

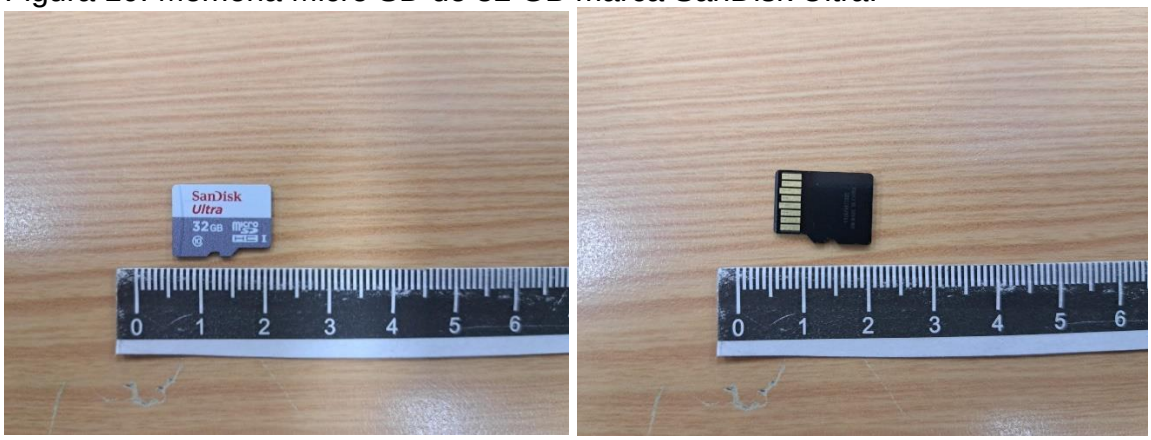


Fuente: Elaboración propia.

7.3 MEMORIA MICRO SD 32 GB

El tercer dispositivo objeto de análisis corresponde a una memoria MICROSD marca SanDisk Ultra de 32GB de capacidad, el cual se muestra en la siguiente imagen:

Figura 10. Memoria Micro SD de 32 GB marca SanDisk Ultra.

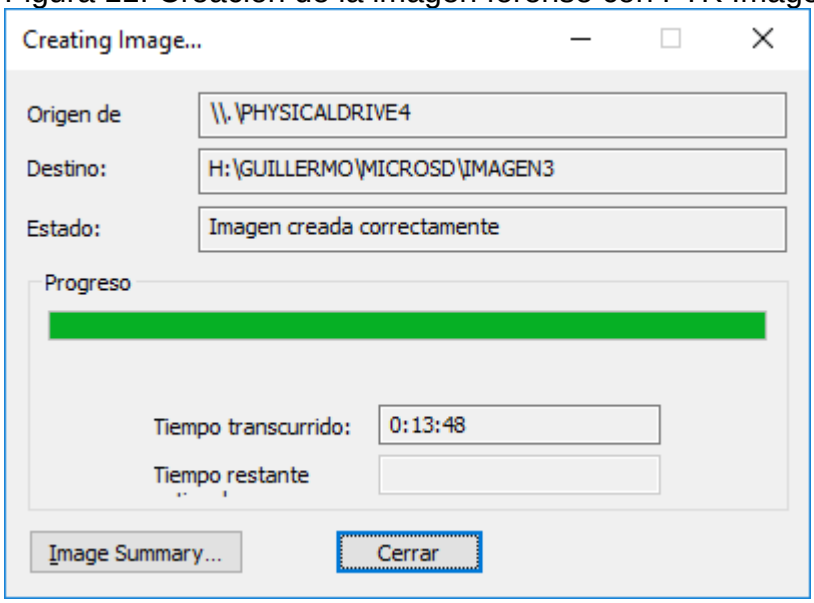


Fuente: Elaboración propia.

7.3.1 OBTENCIÓN DE IMAGEN FORENSE

Inicialmente, se realiza la obtención de la imagen forense con la herramienta FTK Imager versión 4.5.0.3, en formato E01, como se muestra en la siguiente imagen:

Figura 11. Creación de la imagen forense con FTK Imager versión 4.5.0.3



Fuente: Elaboración propia.

7.4 PROCESAMIENTO DE IMAGENES FORENSES

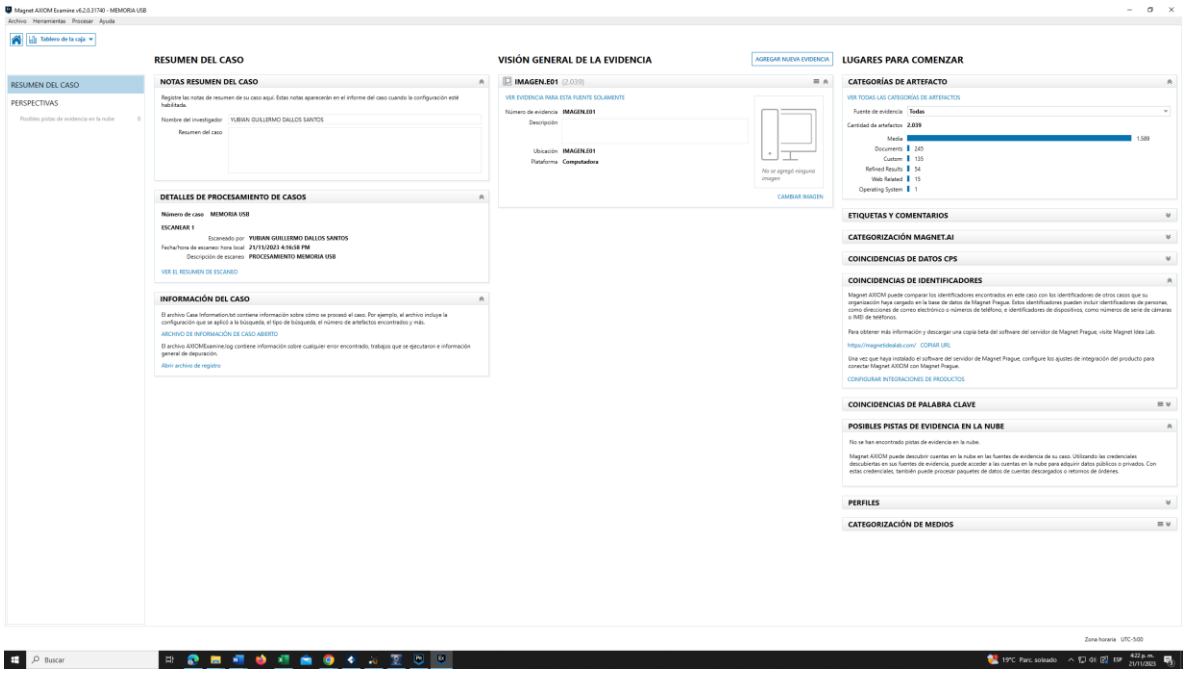
7.4.1 PROCESAMIENTO DE IMAGEN FORENSE DE MEMORIA USB 64 GB

Inicialmente, se realiza el procesamiento de la imagen forense de la unidad MEMORIA USB 64 GB en cada una de las herramientas forenses seleccionadas (FTK, AXIOM, ENCASE Y AUTOPSY).

7.4.1.1 PROCESAMIENTO DE IMAGEN FORENSE DE MEMORIA USB 64 GB EN AXIOM

Al realizar el procesamiento de la imagen forense de la MEMORIA USB de 64 GB en la herramienta AXIOM, el resultado es el siguiente:

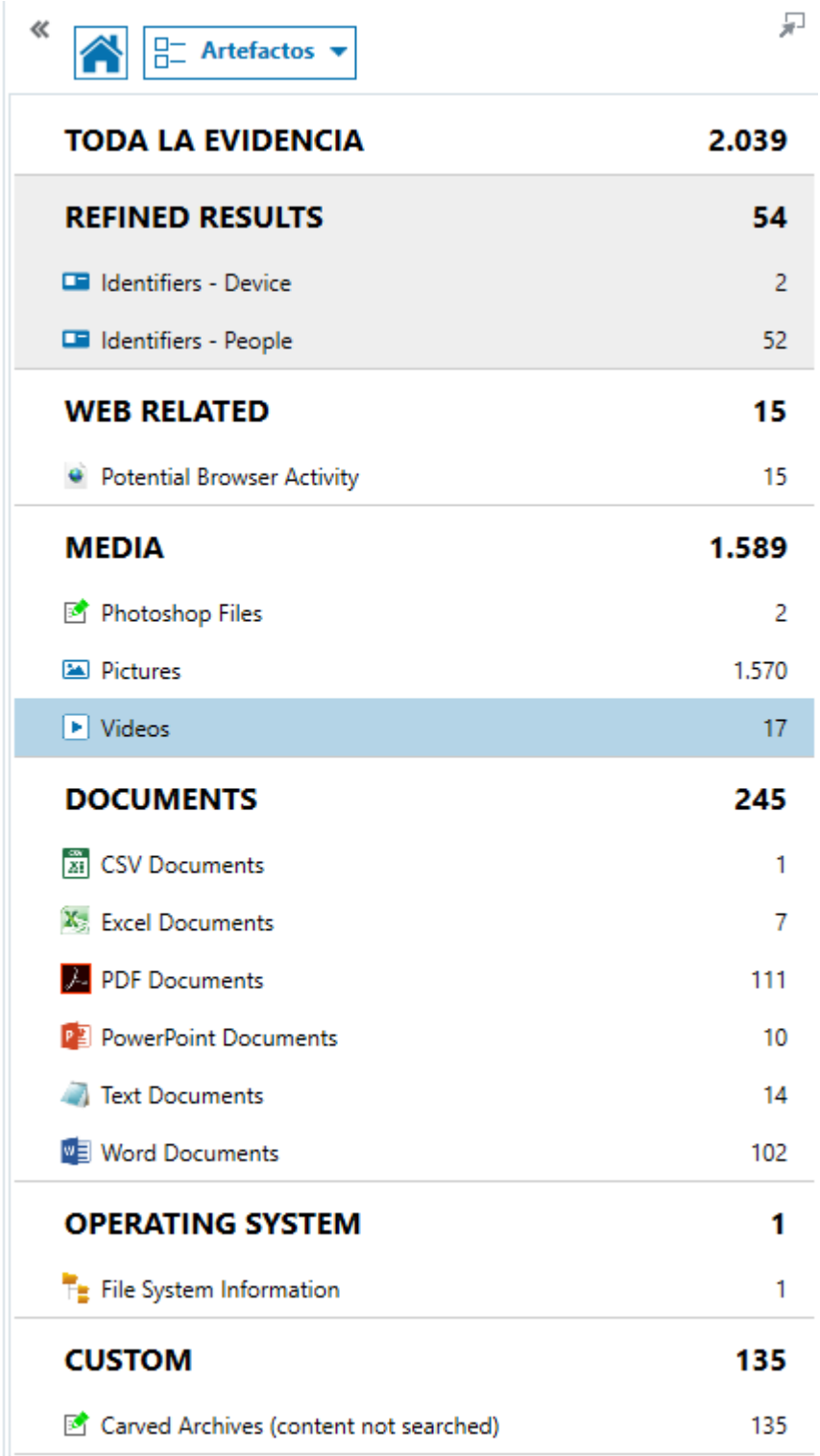
Figura 12. Procesamiento de la imagen forense de la MEMORIA USB de 64 GB en la herramienta AXIOM.



Fuente: Elaboración propia.

Luego del procesamiento de la imagen, la herramienta muestra la totalidad de archivos contenidos en el dispositivo, tanto los existentes como los recuperados, como se muestra en la siguiente imagen:

Figura 13. Archivos existentes y recuperados del dispositivo MEMORIA USB de 64 GB en la herramienta AXIOM.

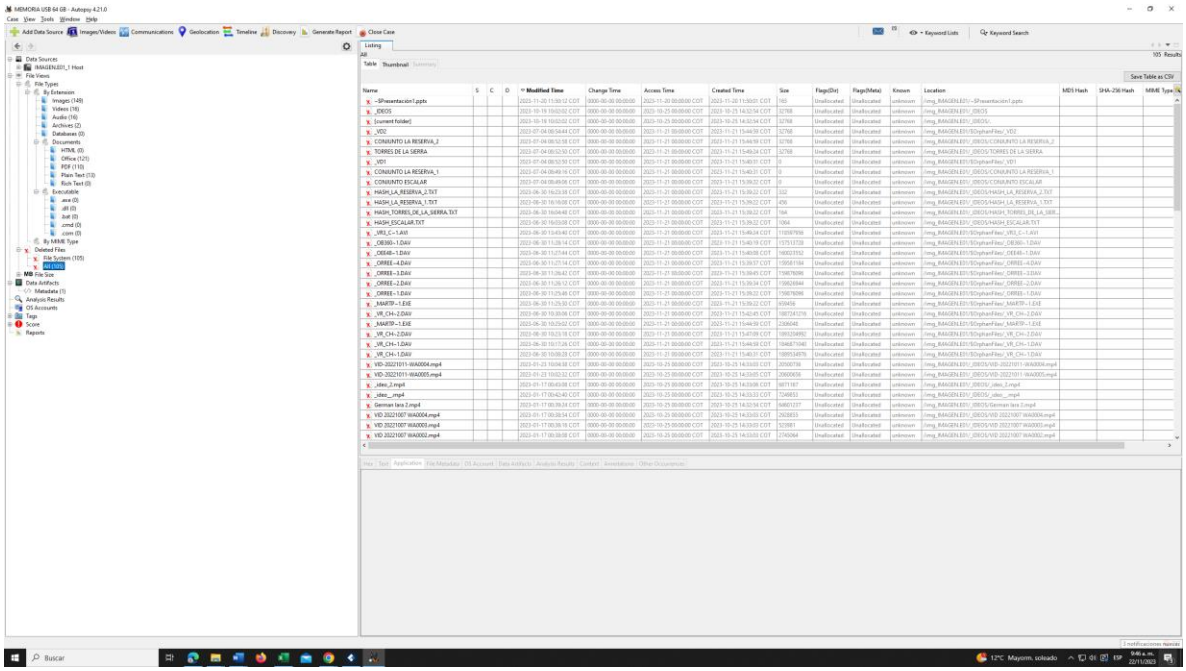


Fuente: Elaboración propia.

7.4.1.2 PROCESAMIENTO DE IMAGEN FORENSE DE MEMORIA USB 64 GB EN AUTOPSY

Al realizar el procesamiento de la imagen forense de la MEMORIA USB en la herramienta AUTOPSY, el resultado es el siguiente:

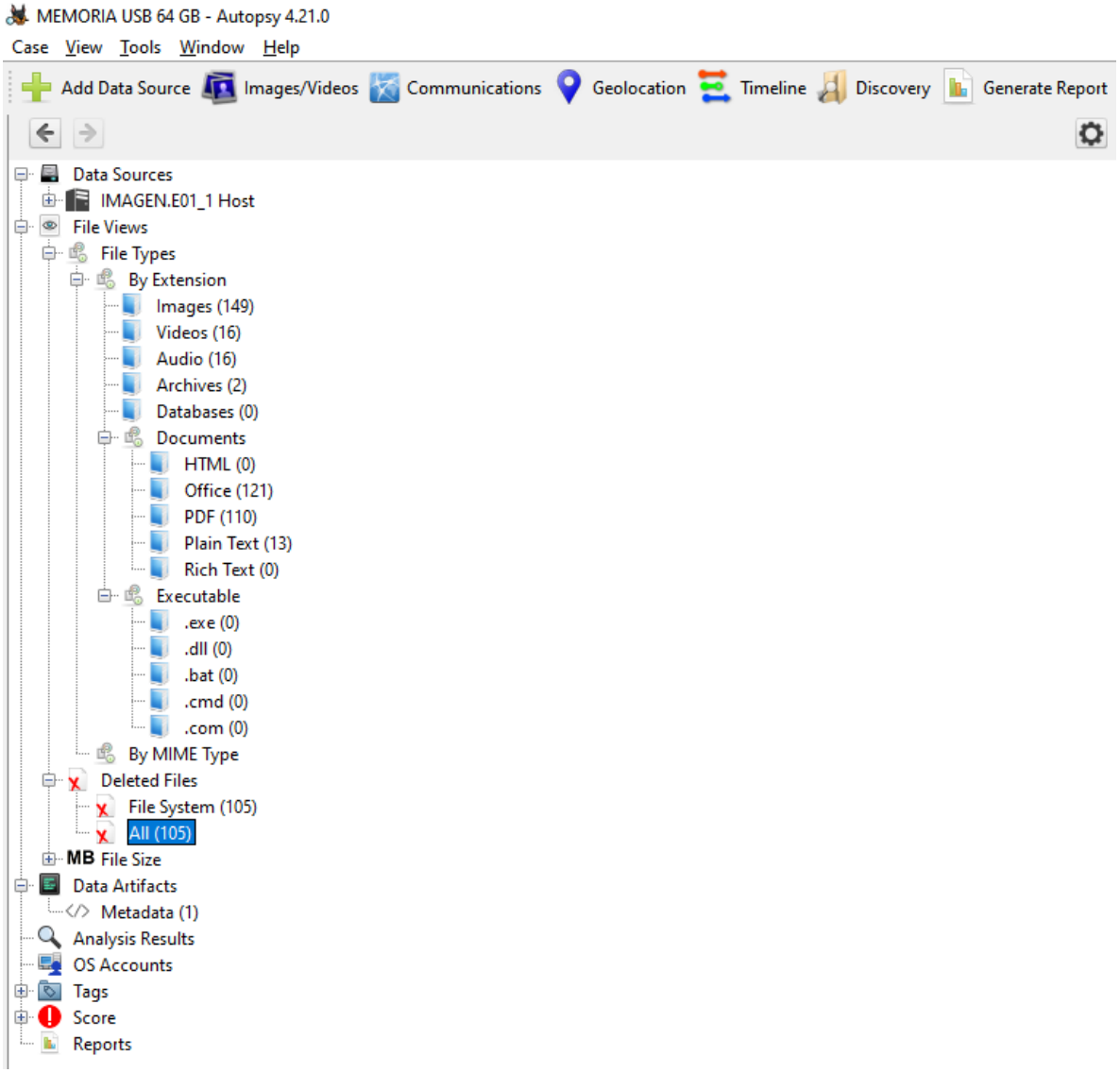
Figura 14. Procesamiento de la imagen forense de la MEMORIA USB en la herramienta AUTOPSY.



Fuente: Elaboración propia.

Luego del procesamiento de la imagen, la herramienta muestra la totalidad de archivos contenidos en el dispositivo, tanto los existentes como los recuperados, como se muestra en la siguiente imagen:

Figura 15. Archivos existentes y recuperados del dispositivo MEMORIA USB en la herramienta AUTOPSY.

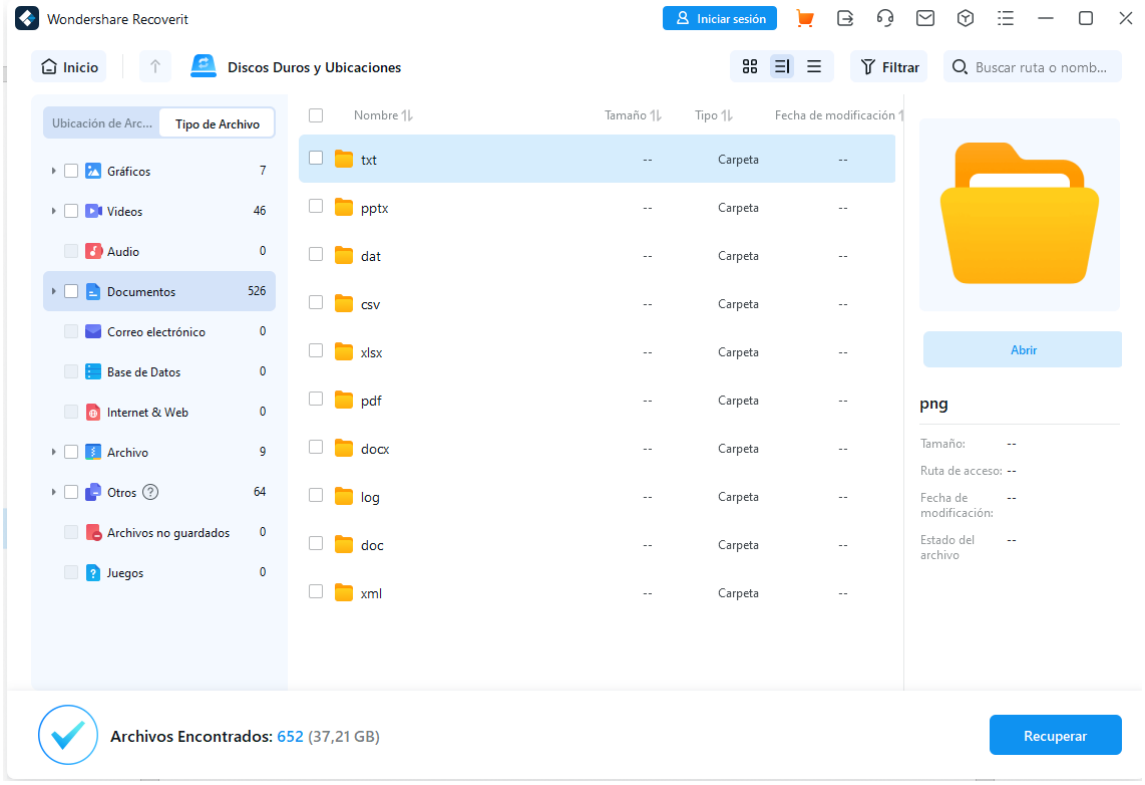


Fuente: Elaboración propia.

7.4.1.3 PROCESAMIENTO DE IMAGEN FORENSE DE MEMORIA USB DE 64 GB EN WONDERSHARE RECOVERIT

Al realizar el procesamiento de la imagen forense de la MEMORIA USB en la herramienta WONDERSHARE RECOVERIT, el resultado es el siguiente:

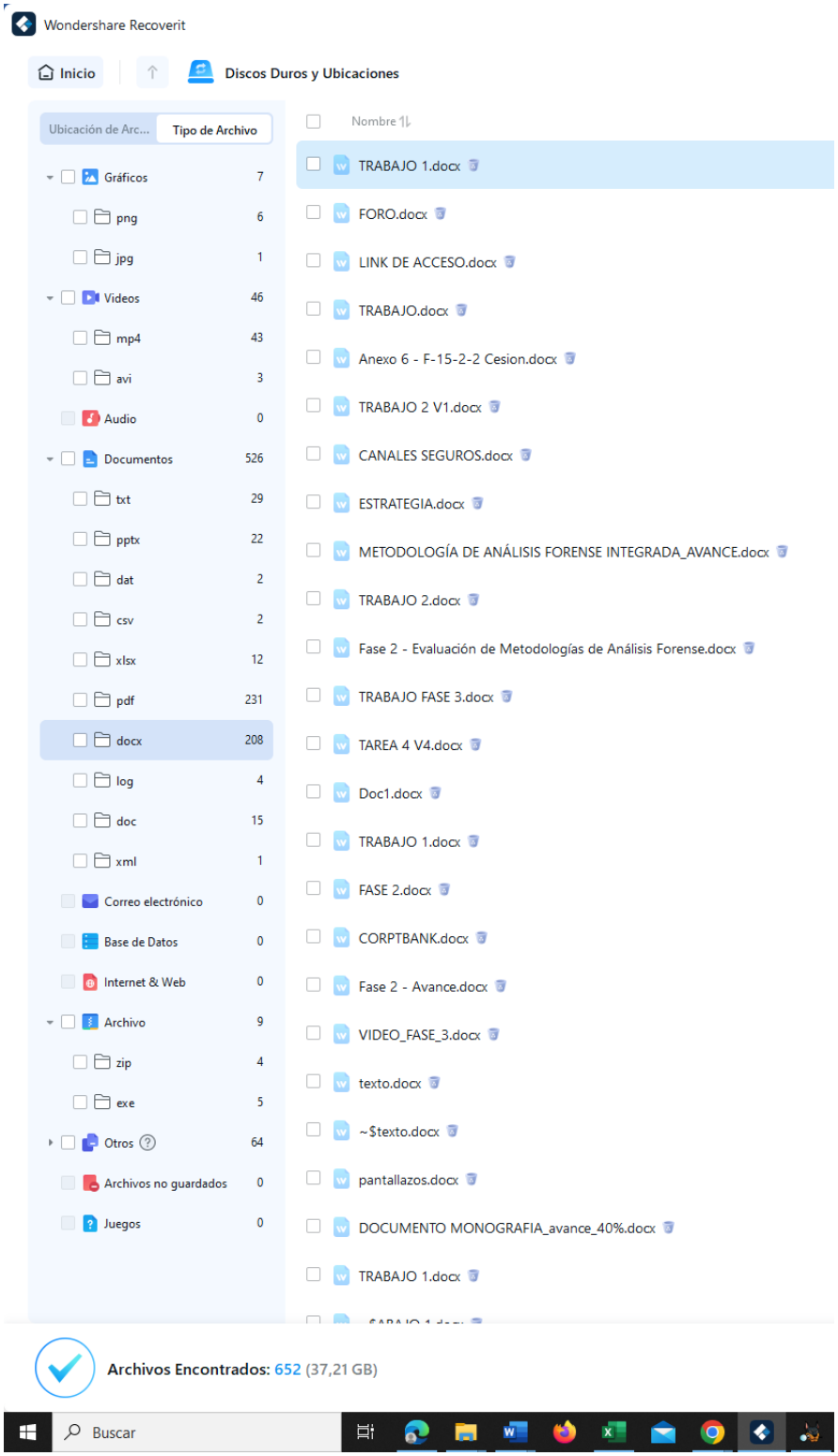
Figura 16. Procesamiento de la imagen forense de la MEMORIA USB en la herramienta WONDERSHARE RECOVERIT.



Fuente: Elaboración propia.

Luego del procesamiento de la imagen, la herramienta muestra la totalidad de archivos contenidos en el dispositivo, tanto los existentes como los recuperados, como se muestra en la siguiente imagen:

Figura 17. Archivos existentes y recuperados del dispositivo MEMORIA USB en la herramienta WONDERSHARE RECOVERIT.

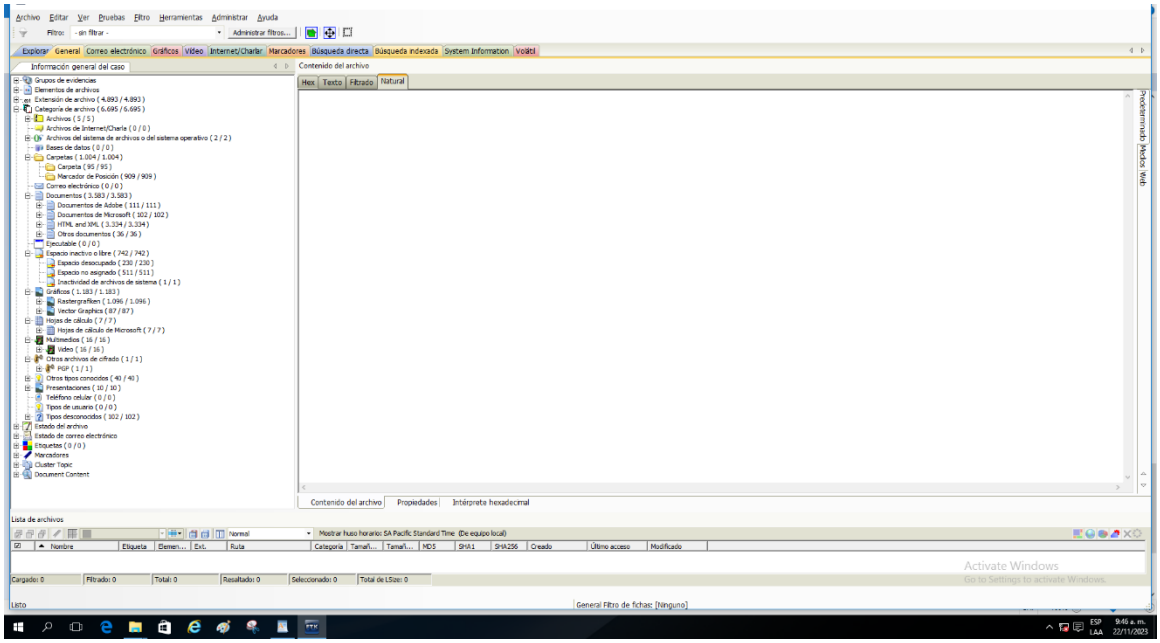


Fuente: Elaboración propia.

7.4.1.4 PROCESAMIENTO DE IMAGEN FORENSE DE MEMORIA USB DE 64 GB EN FTK (Forensic Toolkit)

Al realizar el procesamiento de la imagen forense de la MEMORIA USB en la herramienta FTK, el resultado es el siguiente:

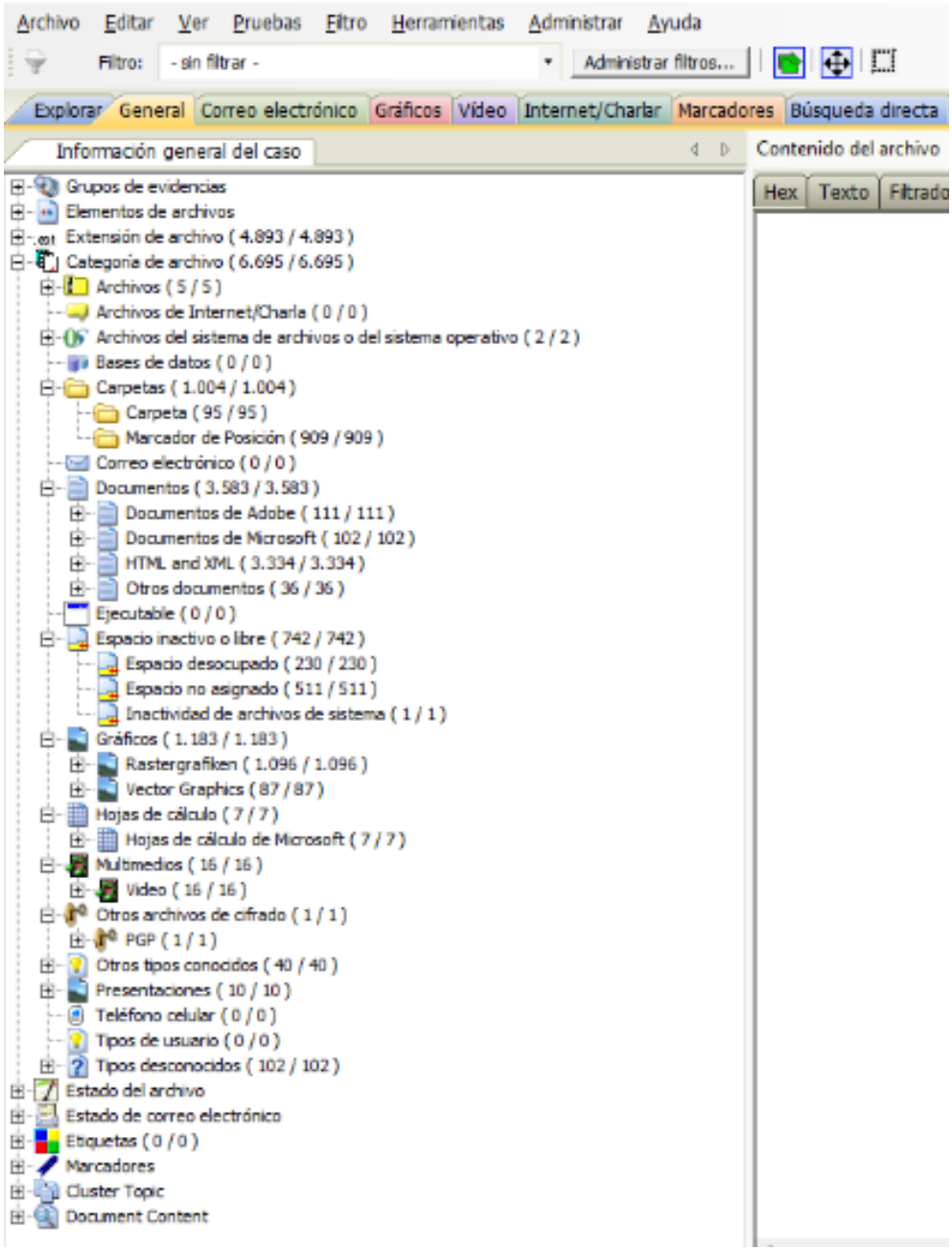
Figura 18. Procesamiento de la imagen forense de la MEMORIA USB en la herramienta FTK.



Fuente: Elaboración propia.

Luego del procesamiento de la imagen, la herramienta muestra la totalidad de archivos contenidos en el dispositivo, tanto los existentes como los recuperados, como se muestra en la siguiente imagen:

Figura 19. Archivos existentes y recuperados del dispositivo MEMORIA USB en la herramienta FTK.



Fuente: Elaboración propia.

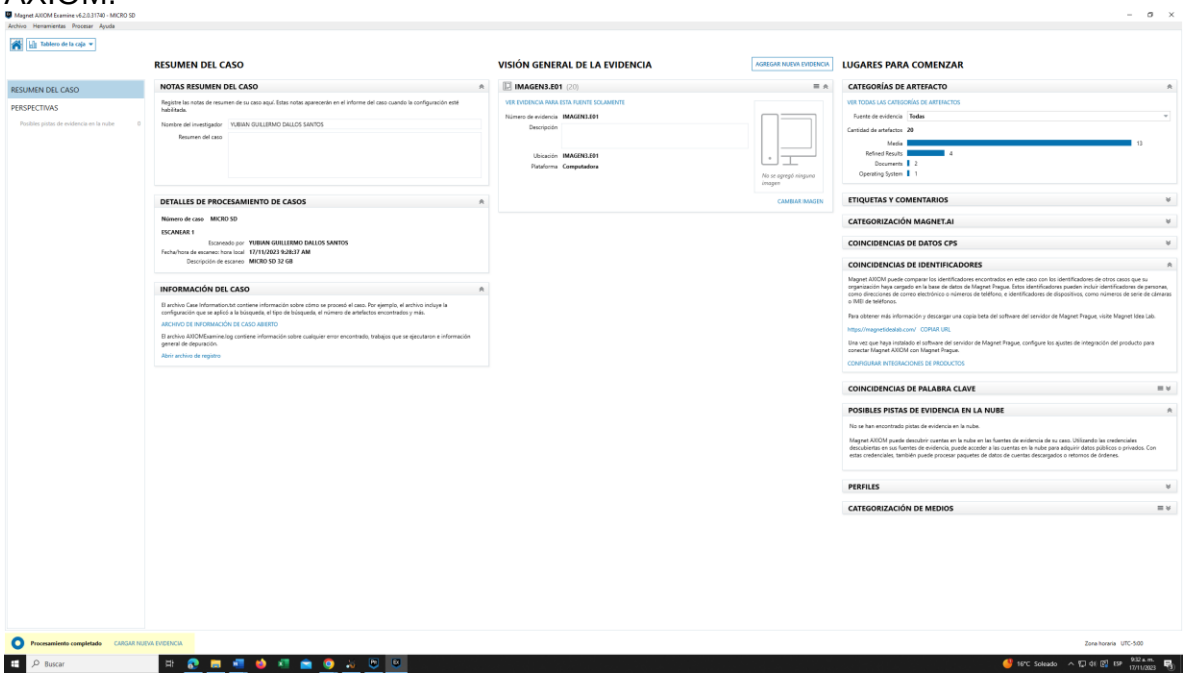
7.4.2 **PROCESAMIENTO DE IMAGEN FORENSE DE MICRO SD 32 GB**

Inicialmente, se realiza el procesamiento de la imagen forense de la unidad MICRO SD en cada una de las herramientas forenses seleccionadas (FTK, AXIOM, ENCASE Y AUTOPSY).

7.4.2.1 PROCESAMIENTO DE IMAGEN FORENSE DE MICRO SD DE 32 GB EN AXIOM

Al realizar el procesamiento de la imagen forense de la MICRO SD en la herramienta AXIOM, el resultado es el siguiente:

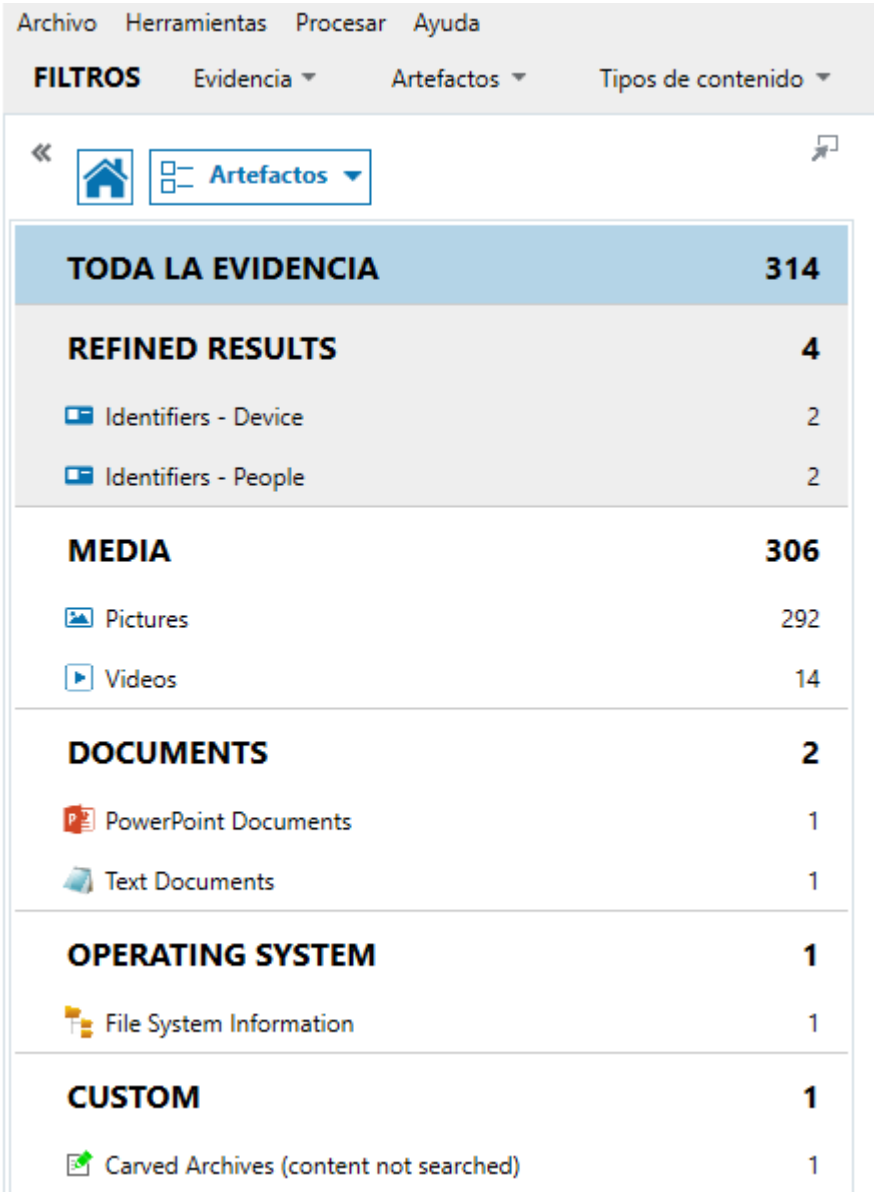
Figura 20. Procesamiento de la imagen forense de la MICRO SD en la herramienta AXIOM.



Fuente: Elaboración propia.

Luego del procesamiento de la imagen, la herramienta muestra la totalidad de archivos contenidos en el dispositivo, tanto los existentes como los recuperados, como se muestra en la siguiente imagen:

Figura 21. Archivos existentes y recuperados del dispositivo MICRO SD en la herramienta AXIOM.

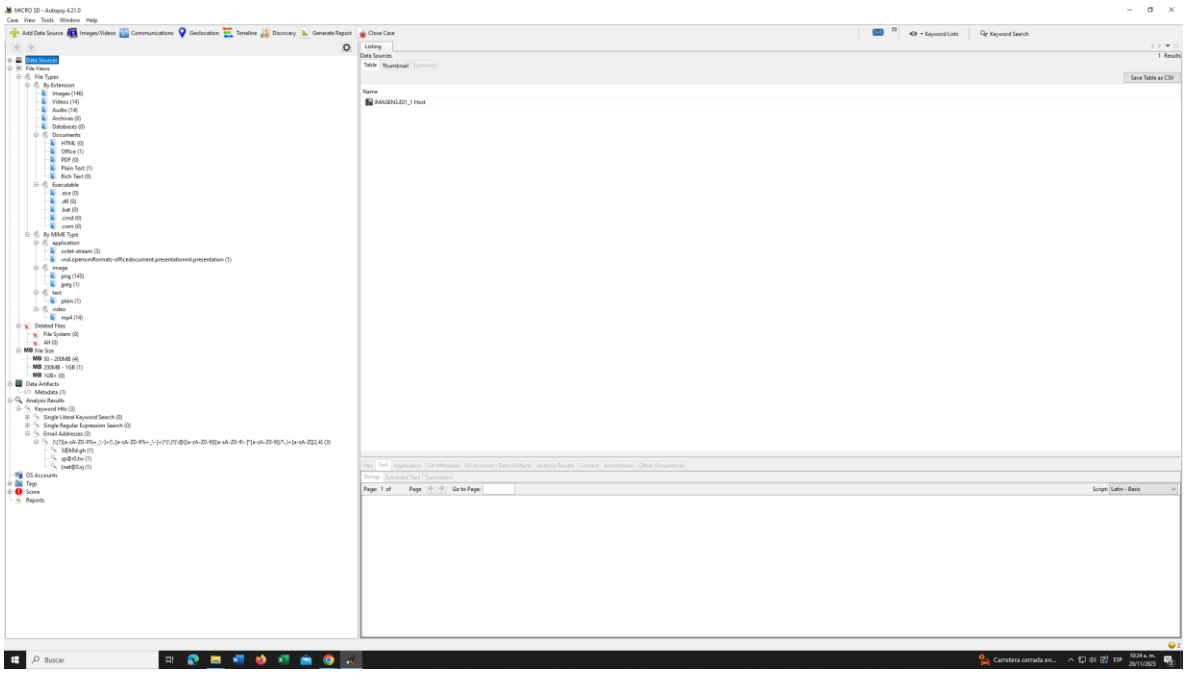


Fuente: Elaboración propia.

7.4.2.2 PROCESAMIENTO DE IMAGEN FORENSE DE MICRO SD DE 32 GB EN AUTOPSY

Al realizar el procesamiento de la imagen forense de la MICRO SD en la herramienta AUTOPSY, el resultado es el siguiente:

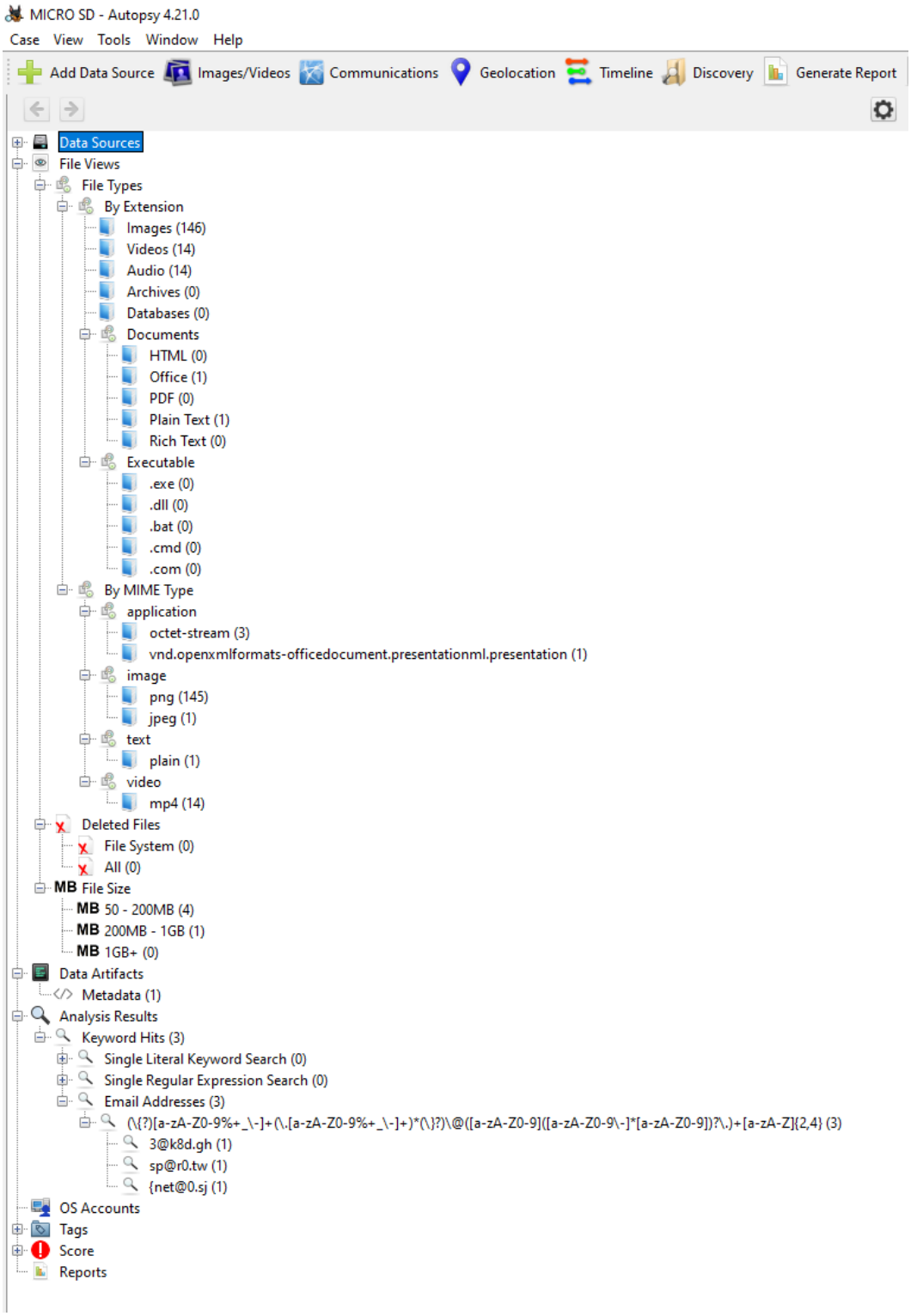
Figura 22. Procesamiento de la imagen forense de la MICRO SD en la herramienta AUTOPSY.



Fuente: Elaboración propia.

Luego del procesamiento de la imagen, la herramienta muestra la totalidad de archivos contenidos en el dispositivo, tanto los existentes como los recuperados, como se muestra en la siguiente imagen:

Figura 23. Archivos existentes y recuperados del dispositivo MICRO SD en la herramienta AUTOPSY.

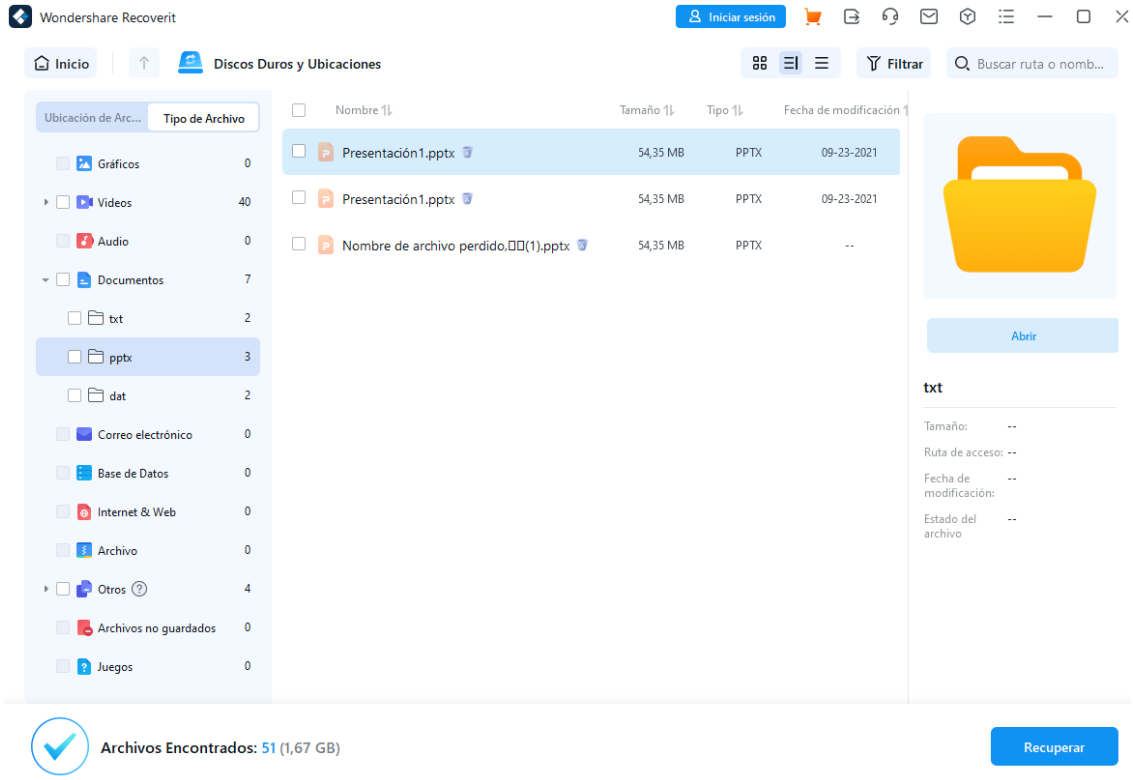


Fuente: Elaboración propia.

7.4.2.3 PROCESAMIENTO DE IMAGEN FORENSE DE MICRO SD DE 32 GB EN WONDERSHARE RECOVERIT

Al realizar el procesamiento de la imagen forense de la MICRO SD en la herramienta WONDERSHARE RECOVERIT, el resultado es el siguiente:

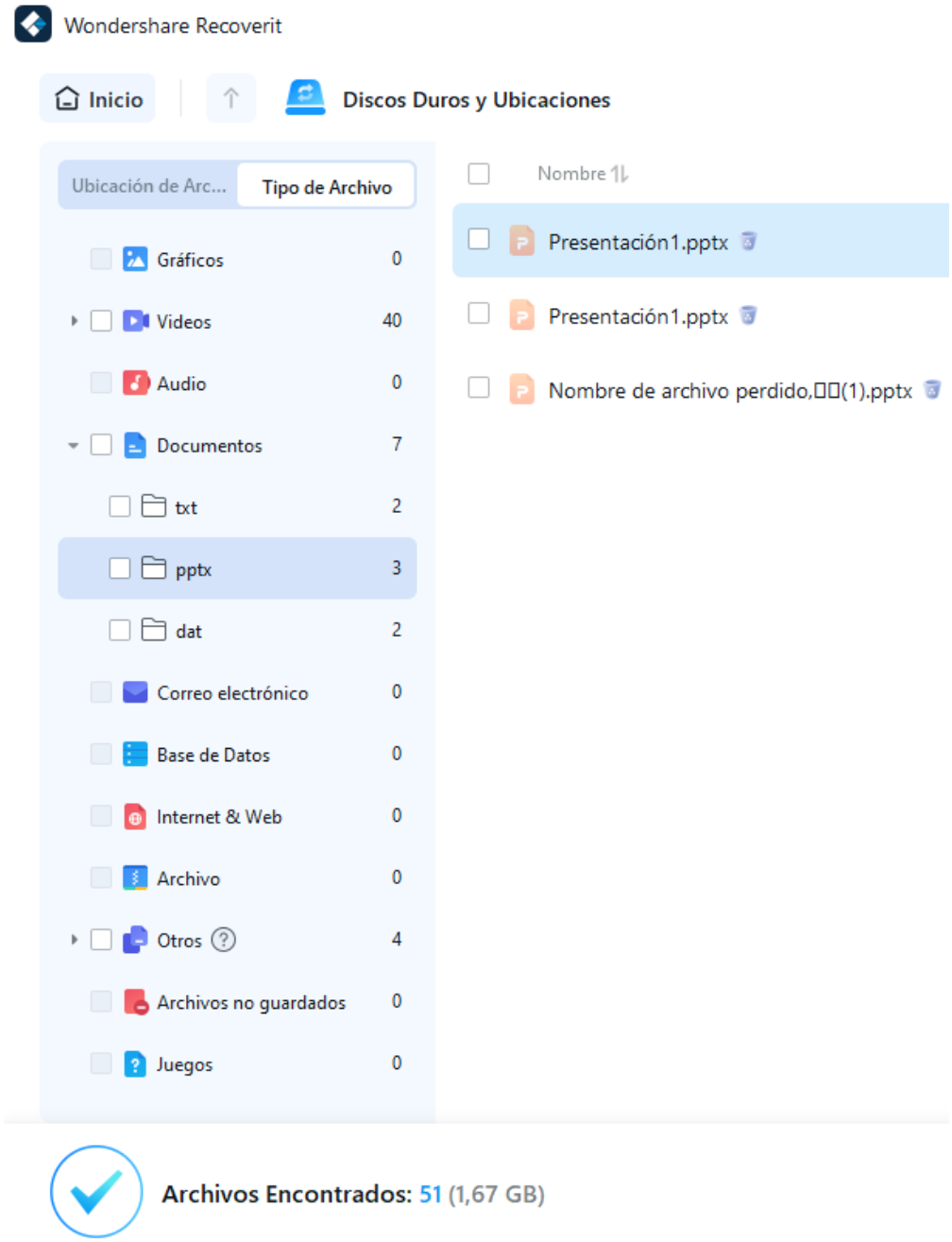
Figura 24. Procesamiento de la imagen forense de la MICRO SD en la herramienta WONDERSHARE RECOVERIT.



Fuente: Elaboración propia.

Luego del procesamiento de la imagen, la herramienta muestra la totalidad de archivos contenidos en el dispositivo, tanto los existentes como los recuperados, como se muestra en la siguiente imagen:

Figura 25. Archivos existentes y recuperados del dispositivo MICRO SD en la herramienta WONDERSHARE RECOVERIT.

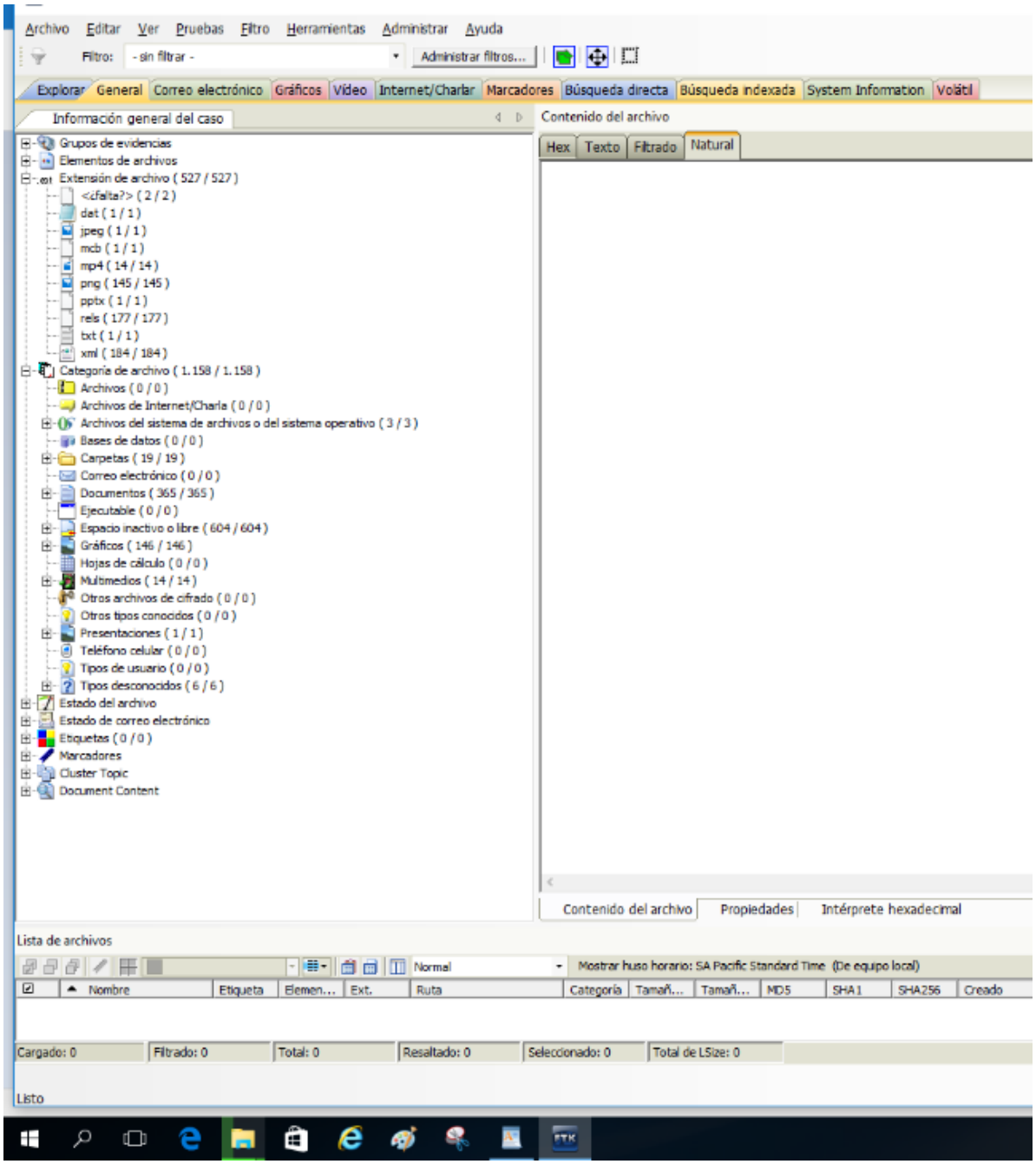


Fuente: Elaboración propia.

7.4.2.4 PROCESAMIENTO DE IMAGEN FORENSE DE MICRO SD DE 32 GB EN FTK (Forensic Toolkit)

Al realizar el procesamiento de la imagen forense de la MICRO SD en la herramienta FTK, el resultado es el siguiente:

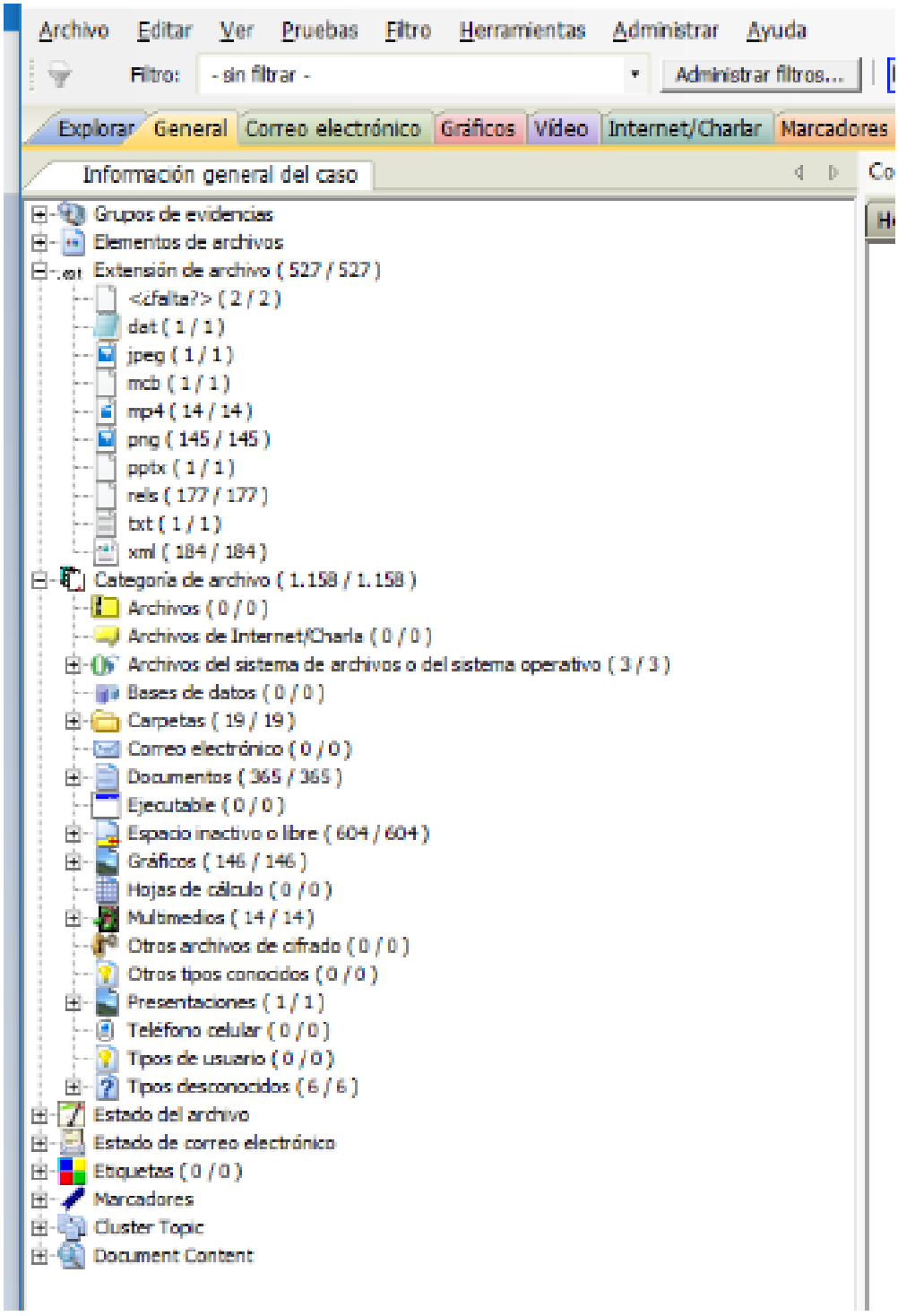
Figura 26. Procesamiento de la imagen forense de la MICRO SD en la herramienta FTK.



Fuente: Elaboración propia.

Luego del procesamiento de la imagen, la herramienta muestra la totalidad de archivos contenidos en el dispositivo, tanto los existentes como los recuperados, como se muestra en la siguiente imagen:

Figura 27. Archivos existentes y recuperados del dispositivo MICRO SD en la herramienta FTK.



Fuente: Elaboración propia.

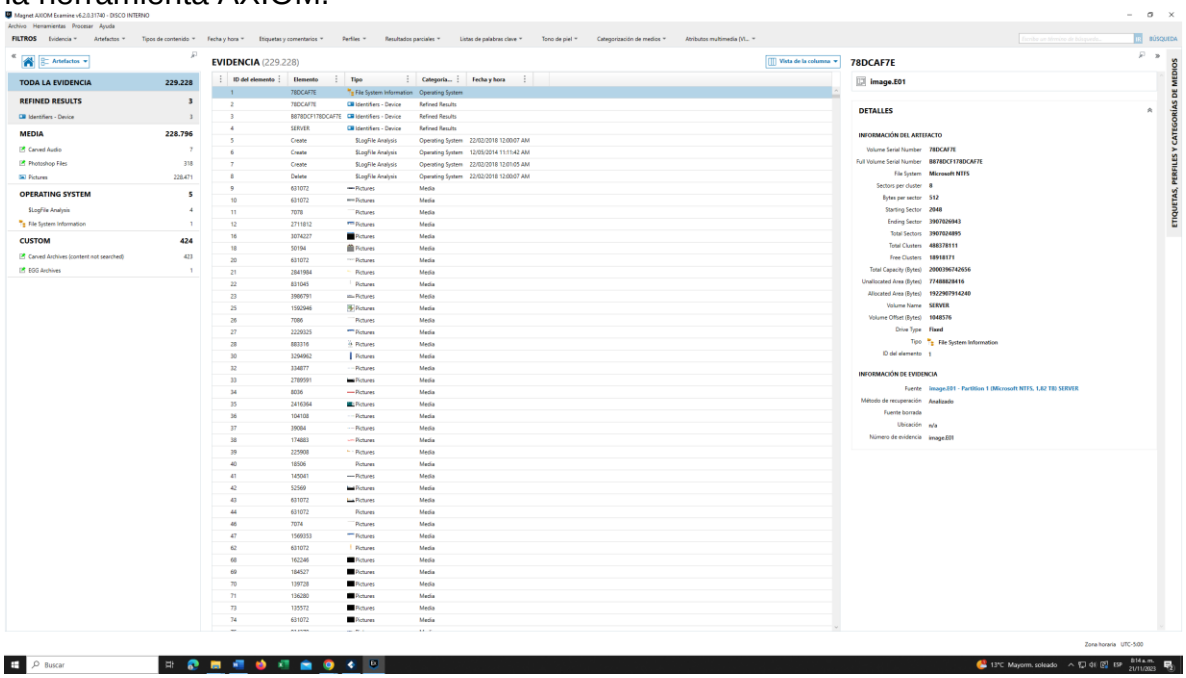
7.4.3 PROCESAMIENTO DE IMAGEN FORENSE DE DISCO DURO INTERNO 2 TB

Inicialmente, se realiza el procesamiento de la imagen forense de la unidad DISCO DURO INTERNO en cada una de las herramientas forenses seleccionadas (FTK, AXIOM, ENCASE Y AUTOPSY).

7.4.3.1 PROCESAMIENTO DE IMAGEN FORENSE DE DISCO DURO INTERNO EN AXIOM

Al realizar el procesamiento de la imagen forense de la DISCO DURO INTERNO en la herramienta AXIOM, el resultado es el siguiente:

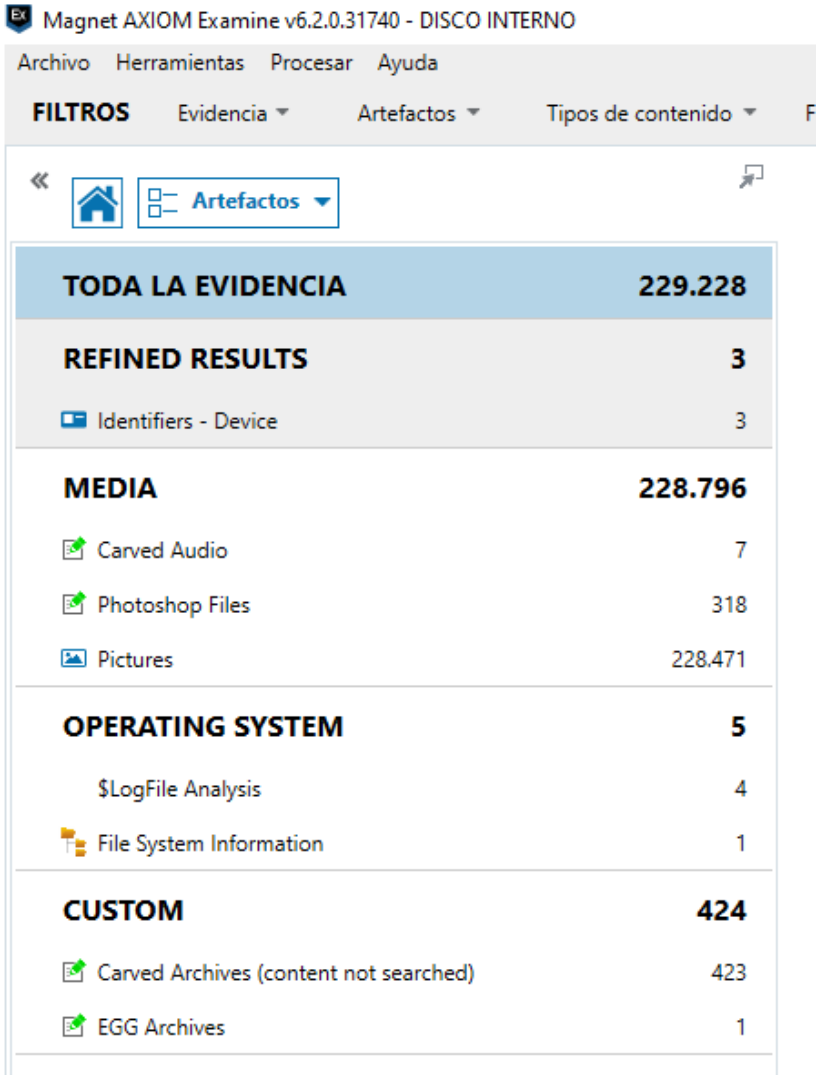
Figura 28. Procesamiento de la imagen forense de la DISCO DURO INTERNO en la herramienta AXIOM.



Fuente: Elaboración propia.

Luego del procesamiento de la imagen, la herramienta muestra la totalidad de archivos contenidos en el dispositivo, tanto los existentes como los recuperados, como se muestra en la siguiente imagen:

Figura 29. Archivos existentes y recuperados del dispositivo DISCO DURO INTERNO en la herramienta AXIOM.

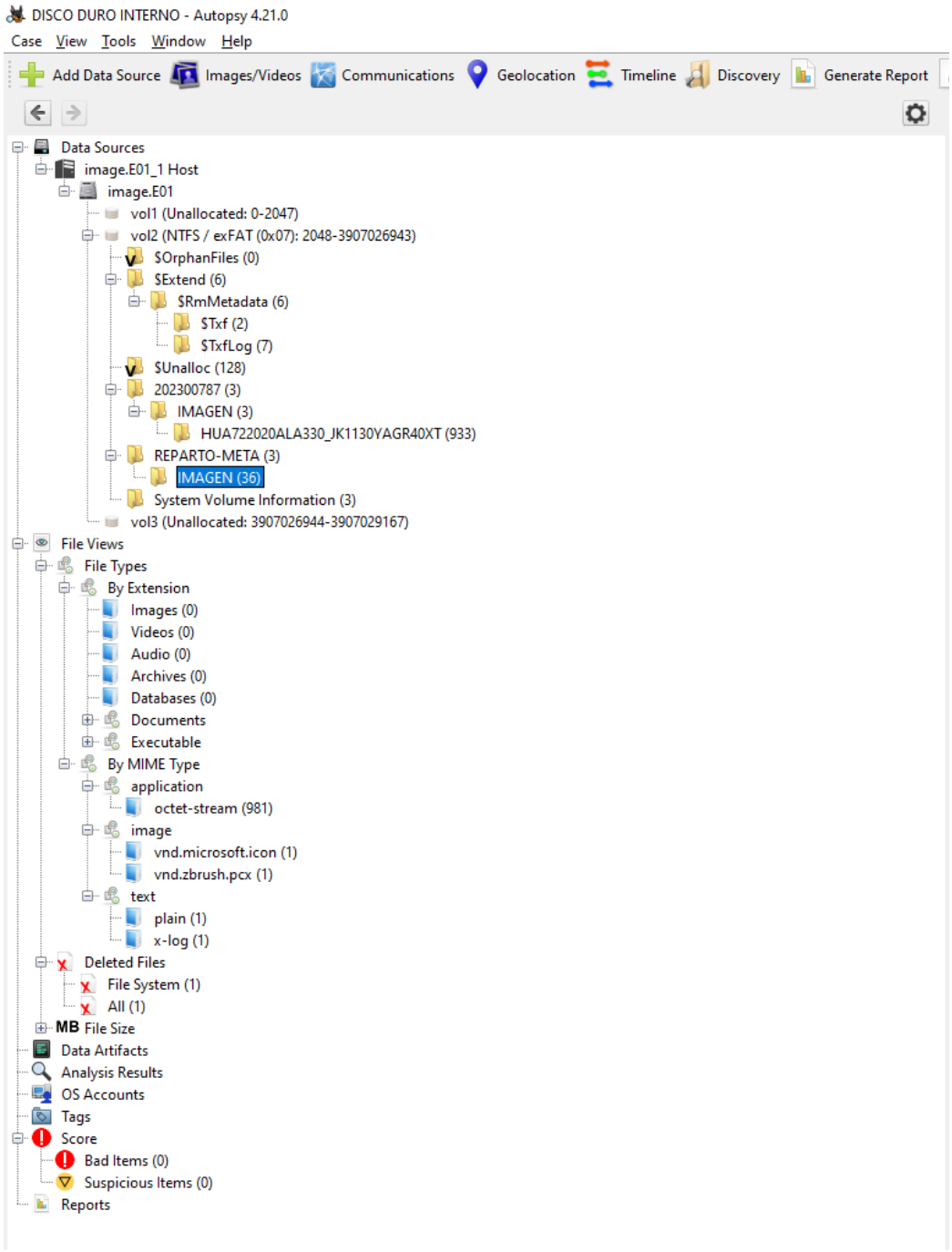


Fuente: Elaboración propia.

7.4.3.2 PROCESAMIENTO DE IMAGEN FORENSE DE DISCO DURO INTERNO EN AUTOPSY

Al realizar el procesamiento de la imagen forense de la DISCO DURO INTERNO en la herramienta AUTOPSY, el resultado es el siguiente:

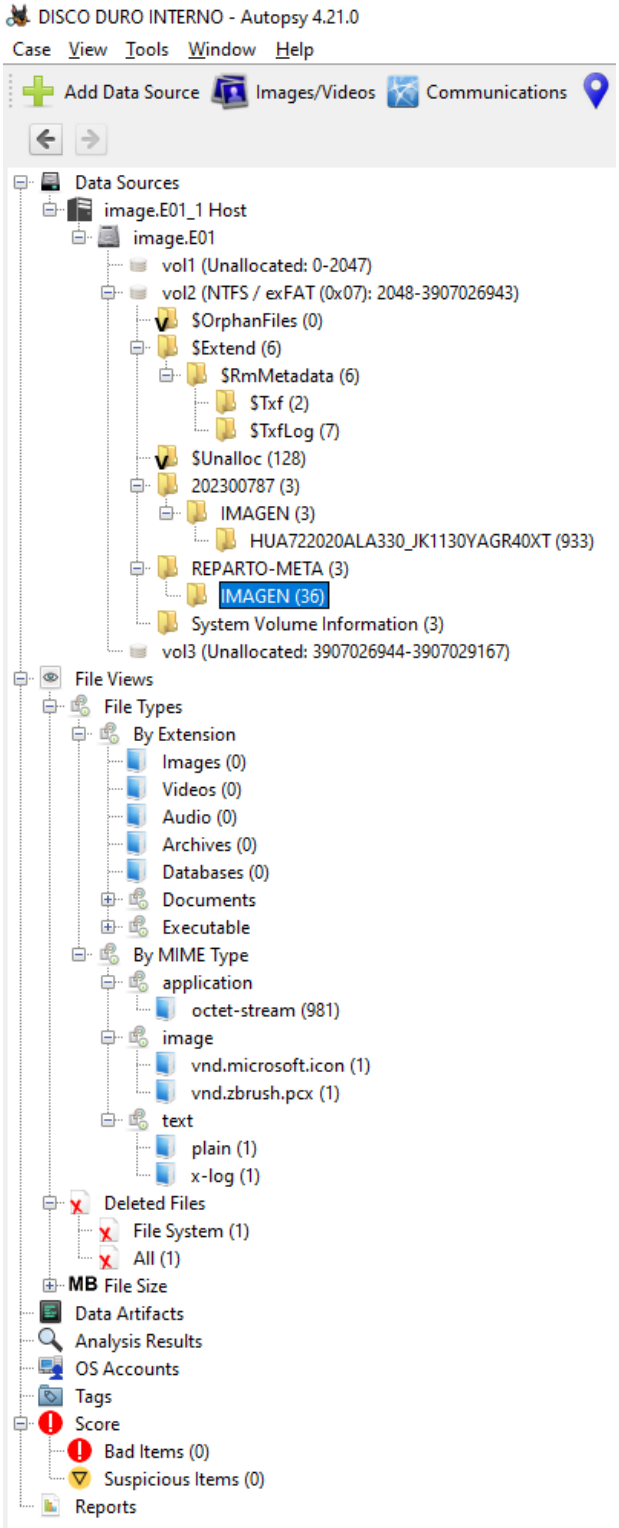
Figura 30. Procesamiento de la imagen forense de la DISCO DURO INTERNO en la herramienta AUTOPSY.



Fuente: Elaboración propia.

Luego del procesamiento de la imagen, la herramienta muestra la totalidad de archivos contenidos en el dispositivo, tanto los existentes como los recuperados, como se muestra en la siguiente imagen:

Figura 31. Archivos existentes y recuperados del dispositivo DISCO DURO INTERNO en la herramienta AUTOPSY.

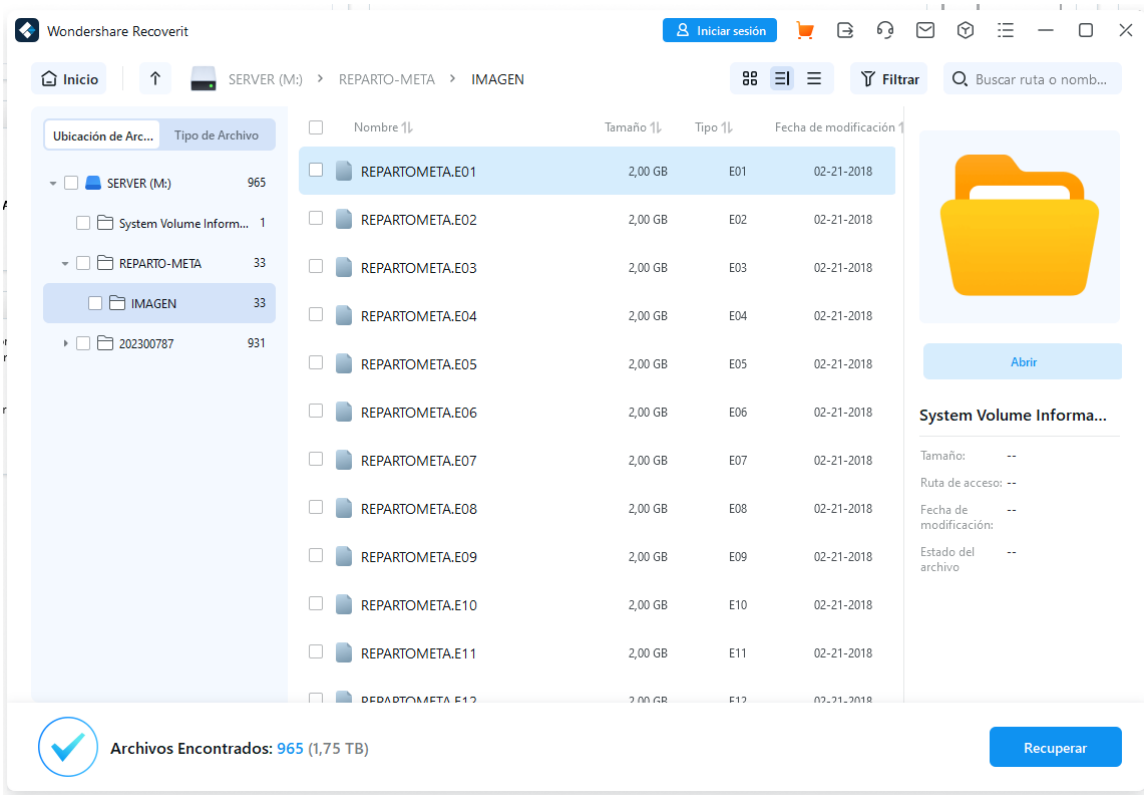


Fuente: Elaboración propia.

7.4.3.3 PROCESAMIENTO DE IMAGEN FORENSE DE DISCO DURO INTERNO EN WONDERSHARE RECOVERIT

Al realizar el procesamiento de la imagen forense de la DISCO DURO INTERNO en la herramienta WONDERSHARE RECOVERIT, el resultado es el siguiente:

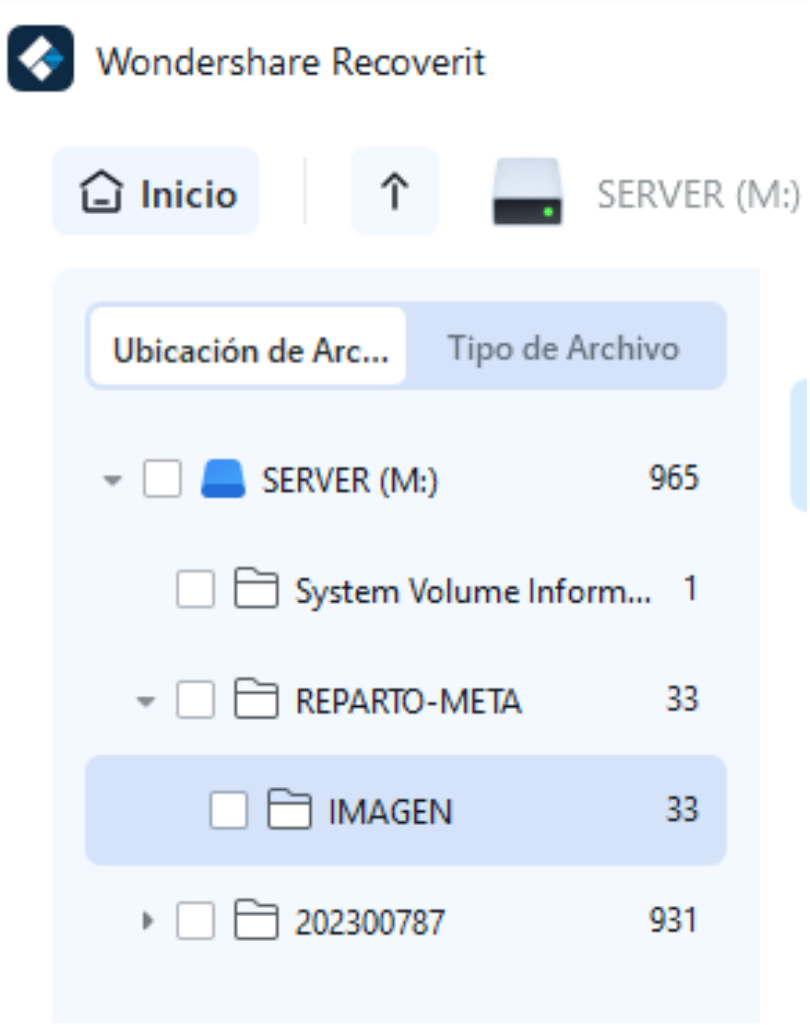
Figura 32. Procesamiento de la imagen forense de la DISCO DURO INTERNO en la herramienta WONDERSHARE RECOVERIT.



Fuente: Elaboración propia.

Luego del procesamiento de la imagen, la herramienta muestra la totalidad de archivos contenidos en el dispositivo, tanto los existentes como los recuperados, como se muestra en la siguiente imagen:

Figura 33. Archivos existentes y recuperados del dispositivo DISCO DURO INTERNO en la herramienta WONDERSHARE RECOVERIT.

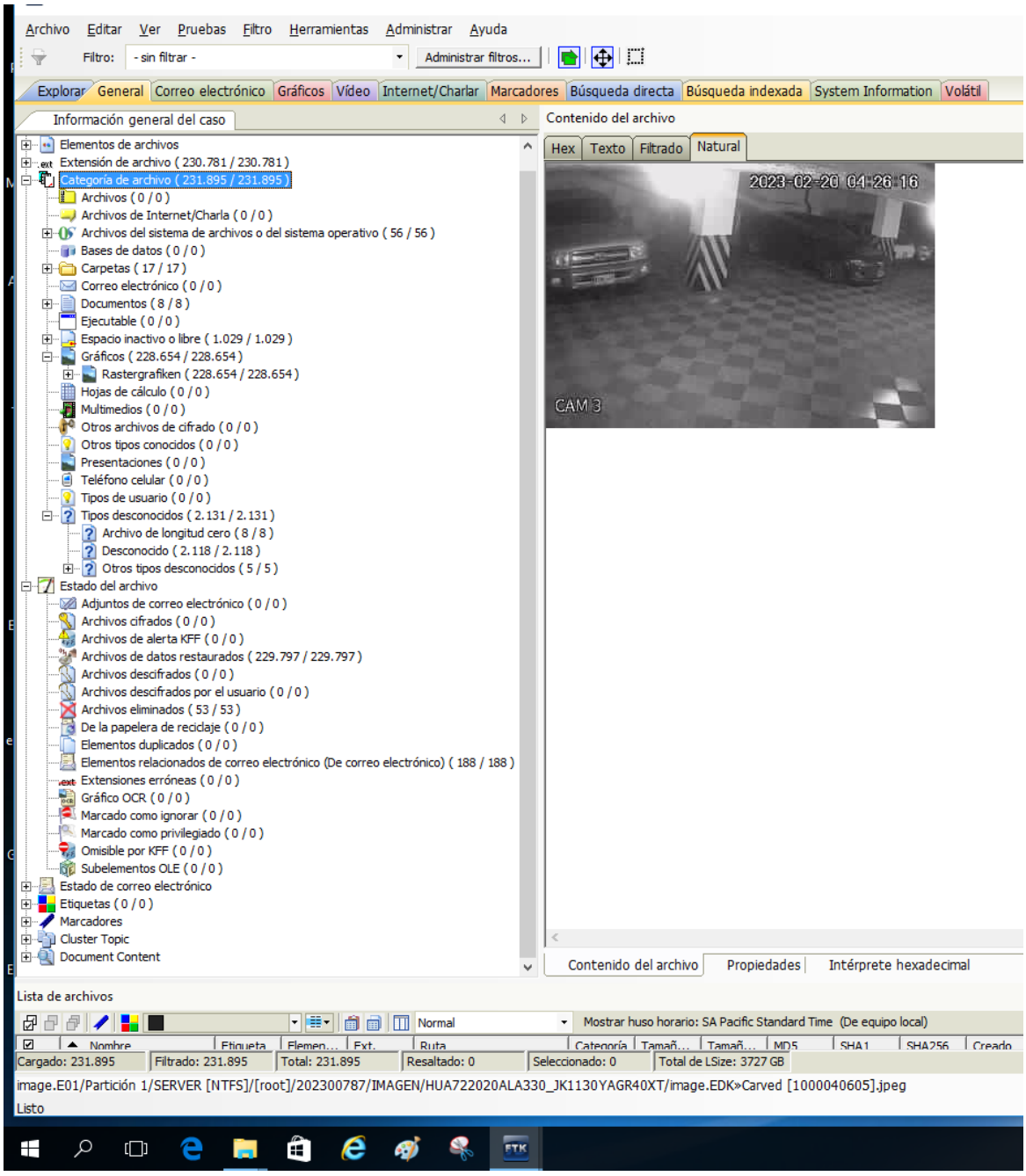


Fuente: Elaboración propia.

7.4.3.4 PROCESAMIENTO DE IMAGEN FORENSE DE DISCO DURO INTERNO EN FTK (Forensic Toolkit)

Al realizar el procesamiento de la imagen forense de la DISCO DURO INTERNO en la herramienta FTK, el resultado es el siguiente:

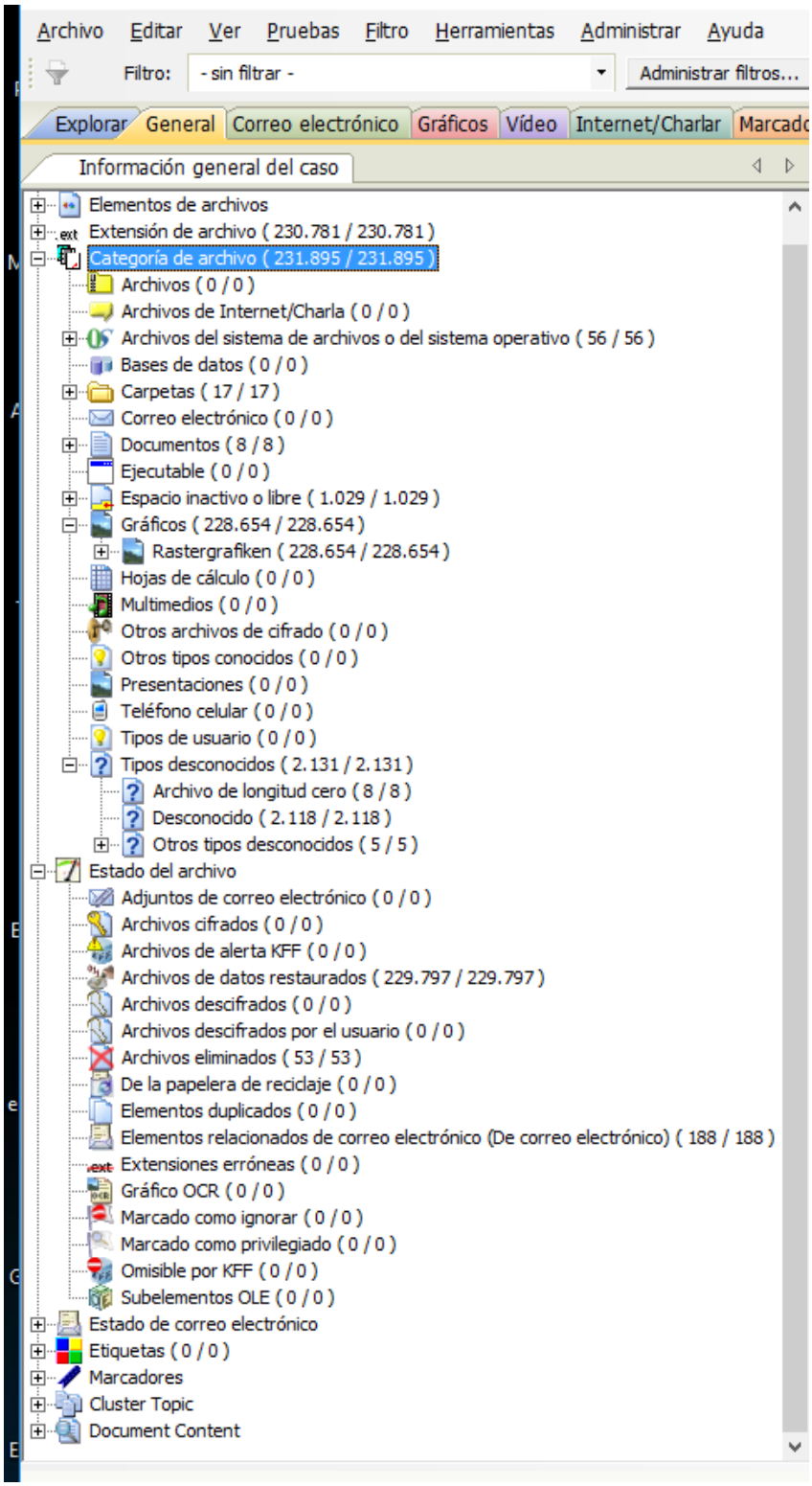
Figura 34. Procesamiento de la imagen forense de la DISCO DURO INTERNO en la herramienta FTK.



Fuente: Elaboración propia.

Luego del procesamiento de la imagen, la herramienta muestra la totalidad de archivos contenidos en el dispositivo, tanto los existentes como los recuperados, como se muestra en la siguiente imagen:

Figura 35. Archivos existentes y recuperados del dispositivo DISCO DURO INTERNO en la herramienta FTK.



Fuente: Elaboración propia.

7.5 Análisis de Resultados

En esta parte, se evalúan los resultados de las pruebas realizadas con las herramientas forenses. Los resultados son evaluados en función de los siguientes criterios:

7.5.1 Completitud de los datos extraídos:

Este criterio evalúa la eficacia de las herramientas en la extracción integral de datos desde los dispositivos de almacenamiento. Se analiza si estas herramientas son capaces de recuperar la totalidad de archivos y datos presentes en los dispositivos bajo evaluación. La integralidad resulta fundamental, dado que la ausencia de datos relevantes podría tener un impacto perjudicial en una investigación forense.

7.5.2 Efectividad de la recuperación de datos:

Este criterio analiza la robustez de las herramientas para restaurar información que ha sido eliminada o deteriorada. Se evalúa la eficacia de la recuperación mediante el porcentaje de datos recuperados en relación con el total de datos eliminados o dañados. Una recuperación exitosa resulta fundamental para la obtención de pruebas significativas en investigaciones forenses.

7.5.3 Calidad del análisis de datos:

Este criterio evalúa la calidad de los resultados obtenidos a través del análisis de datos generados por las herramientas. Se examina si estas herramientas producen resultados precisos y de relevancia. La calidad del análisis juega un papel crucial en la evaluación de la efectividad de las herramientas para interpretar la evidencia digital y generar informes forenses sólidos.

Los resultados de las pruebas se expresan en términos cuantitativos y cualitativos, lo que permite una evaluación completa de las herramientas forenses y sus capacidades.

7.6 Análisis de resultados en Memoria USB 64 GB

La siguiente tabla muestra un comparativo de las diferentes herramientas forenses utilizadas para el procesamiento de la imagen en formato E01 obtenida de la unidad correspondiente a la Memoria USB de 64 GB de capacidad, en dicha tabla se muestra un comparativo de cantidad de archivos extraídos, cantidad de archivos recuperados y el tiempo estimado en el proceso de procesamiento y recuperación de información de cada una de las herramientas forenses:

Tabla 1. Comparativo de las herramientas forenses en Memoria USB 64 GB.

MEMORIA USB 64 GB			
HERRAMIENTA	**ARCHIVOS EXTRAIDOS**	**ARCHIVOS RECUPERADOS**	**TIEMPO ESTIMADO (HH:MM:SS)**
AXIOM	2039	135	0:32:23
AUTOPSY	533	105	0:43:42
Wondershare Recoverit	652	13	0:12:29
FTK (Forensic Toolkit)	4237	342	0:11:51

Fuente: Elaboración propia.

En este análisis es importante destacar que en herramientas como AXIOM y FTK un alto porcentaje de los elementos extraídos corresponde a espacio libre o no asignado en la unidad, marcadores de posición o archivos tipo .xml (son archivos de texto que utilizan un formato de codificación estándar para almacenar y transportar datos). Este tipo de archivos no se registran en herramientas como AUTOPSY y Wondershare Recoverit.

7.7 Análisis de resultados en Memoria MICRO SD 32 GB

La siguiente tabla muestra un comparativo de las diferentes herramientas forenses utilizadas para el procesamiento de la imagen en formato E01 obtenida de la unidad correspondiente a la Memoria MICRO SD de 32 GB de capacidad, en dicha tabla se muestra un comparativo de cantidad de archivos extraídos, cantidad de archivos recuperados y el tiempo estimado en el proceso de procesamiento y recuperación de información de cada una de las herramientas forenses:

Tabla 2. Comparativo de las herramientas forenses en Memoria MICRO SD 32 GB.

MEMORIA MICRO SD 32 GB			
HERRAMIENTA	**ARCHIVOS EXTRAIDOS**	**ARCHIVOS RECUPERADOS**	**TIEMPO ESTIMADO (MINUTOS)**
AXIOM	314	1	0:21:33
AUTOPSY	340	0	0:28:17
Wondershare Recoverit	51	0	0:10:55
FTK (Forensic Toolkit)	1158	1	0:08:19

Fuente: Elaboración propia.

7.8 Análisis de resultados en Disco duro interno de 2TB

La siguiente tabla muestra un comparativo de las diferentes herramientas forenses utilizadas para el procesamiento de la imagen en formato E01 obtenida de la unidad correspondiente a Disco duro interno de 2 TB de capacidad, en dicha tabla se

muestra un comparativo de cantidad de archivos extraídos, cantidad de archivos recuperados y el tiempo estimado en el proceso de procesamiento y recuperación de información de cada una de las herramientas forenses:

Tabla 3. Comparativo de las herramientas forenses en Disco duro interno 2 TB.

DISCO DURO INTERNO 2TB			
HERRAMIENTA	**ARCHIVOS EXTRAIDOS**	**ARCHIVOS RECUPERADOS**	**TIEMPO ESTIMADO (MINUTOS)**
AXIOM	229228	227456	22:15:26
AUTOPSY	2075	933	45:19:54
Wondershare Recoverit	965	48	08:07:52
FTK (Forensic Toolkit)	231895	229797	33:15:46

Fuente: Elaboración propia.

Un punto importante para destacar es que herramientas como AXIOM, AUTOPSY y FTK permiten desde su interfaz realizar la generación de un REPORTE o INFORME con la información que se requiera extraer, a diferencia de la herramienta Wondershare Recoverit que no cuenta con esta opción.

7.9 Análisis Comparativo

El siguiente cuadro muestra un comparativo de las herramientas forenses utilizadas en los dispositivos de almacenamiento masivo descritos:

Cuadro 1. Comparativo de herramientas forenses utilizadas en dispositivos de almacenamiento masivo

Herramienta	AXIOM	AUTOPSY	Wondershare Recoverit	FTK (Forensic Toolkit)
Operatividad	Compleja	Media	Sencilla	Compleja
Características	Soporta una amplia gama de formatos de archivos, sistemas de archivos y dispositivos de almacenamiento.	Soporta una amplia gama de formatos de archivos, sistemas de archivos y dispositivos de almacenamiento.	Soporta una amplia gama de formatos de archivos, pero no todos los sistemas de archivos.	Soporta una amplia gama de formatos de archivos, sistemas de archivos y dispositivos de almacenamiento.
Efectividad	Alta	Media	Baja	Alta
Tiempo de procesamiento	Largo	Mediano	Corto	Largo
Tipo	Pago	Libre	Pago - Versión libre limitada	Pago
Recurso de Máquina requerido	Procesador: Intel Core i5 o superior, 16 GB de RAM, 1 TB de almacenamiento	Procesador: Intel Core i3 o superior, 8 GB de RAM, 500 GB de almacenamiento	Procesador: Intel Core i3 o superior, 4 GB de RAM, 250 GB de almacenamiento	Procesador: Intel Core i7 o superior, 32 GB de RAM, 2 TB de almacenamiento

Fuente: Elaboración propia.

7.9.1 Operatividad

La operatividad de una herramienta forense se refiere a su facilidad de uso y aprendizaje. Las herramientas forenses complejas, como AXIOM y FTK, requieren un nivel de experiencia y conocimientos técnicos para su uso. Las herramientas forenses sencillas, como AUTOPSY y Wondershare Recoverit, son más fáciles de usar y aprender, pero ofrecen menos características y opciones.

7.9.2 Características

Las características de una herramienta forense se refieren a sus capacidades y funcionalidades. Las herramientas forenses avanzadas, como AXIOM y FTK, ofrecen una amplia gama de características, incluyendo:

- Soporte para una amplia gama de formatos de archivos, sistemas de archivos y dispositivos de almacenamiento.
- Capacidades de análisis forense, como la recuperación de datos eliminados, la identificación de malware y la reconstrucción de eventos.
- Herramientas de informes y generación de evidencia.

Las herramientas forenses básicas, como AUTOPSY y Wondershare Recoverit, ofrecen un conjunto de características más limitado.

7.9.3 Efectividad

La efectividad de una herramienta forense se refiere a su capacidad para recuperar datos de forma completa y precisa. Las herramientas forenses avanzadas, como AXIOM y FTK, son más efectivas que las herramientas forenses básicas, como AUTOPSY y Wondershare Recoverit.

7.9.4 Tiempo de procesamiento

El tiempo de procesamiento de una herramienta forense se refiere al tiempo que tarda en extraer y recuperar datos de un dispositivo de almacenamiento. Las herramientas forenses complejas, como AXIOM y FTK, pueden tardar más tiempo en procesar datos que las herramientas forenses básicas, como AUTOPSY y Wondershare Recoverit.

7.9.5 Precio

El precio de una herramienta forense se refiere a su costo de adquisición. Las herramientas forenses avanzadas, como AXIOM y FTK, son de tipo comercial y de carácter pago, AUTOPSY es una herramienta de uso libre y Wondershare Recoverit cuenta con una versión libre que es limitada en cuanto a su funcionalidad y una versión premium que es de carácter pago.

7.9.6 Recurso de máquina requeridos

Los requisitos de hardware específicos de cada herramienta pueden variar según la versión de la herramienta y las características que se utilicen. Es importante consultar la documentación de la herramienta para obtener información específica sobre los requisitos de hardware.

Las herramientas forenses más complejas, como AXIOM y FTK, requieren más recursos de máquina que las herramientas forenses más sencillas, como AUTOPSY y Wondershare Recoverit. Esto se debe a que las herramientas forenses complejas deben procesar más datos y realizar cálculos más complejos.

Los recursos de máquina específicos que pueden ser necesarios para las herramientas forenses incluyen:

Procesador: La potencia del procesador determina la velocidad a la que la herramienta puede procesar datos.
RAM: La cantidad de RAM determina la cantidad de datos que la herramienta puede almacenar en la memoria a la vez.
Almacenamiento: El espacio de almacenamiento determina la cantidad de datos que la herramienta puede procesar y almacenar.

En general, las herramientas forenses analizadas presentan una buena efectividad en la extracción y recuperación de datos en dispositivos de almacenamiento masivo. Sin embargo, existen diferencias en términos de operatividad, características y efectividad.

AXIOM es la herramienta más completa, con una amplia gama de funciones y características que la hacen ideal para una variedad de tareas forenses. Es la herramienta más operativa, con una interfaz intuitiva y fácil de usar. También es la más efectiva, con una tasa de recuperación muy alta.

AUTOPSY es una herramienta especializada en la investigación forense de sistemas informáticos. Es una herramienta potente y flexible, pero puede ser compleja de usar para usuarios sin experiencia. Su tasa de recuperación es buena, pero no tan alta como la de AXIOM.

Wondershare Recoverit es una herramienta especializada en la recuperación de datos eliminados o perdidos. Es una herramienta fácil de usar, pero su gama de funciones es limitada. Su tasa de recuperación es regular, y puede no ser adecuada para casos complejos.

FTK (Forensic Toolkit) es una herramienta completa y flexible, con una gama de funciones similar a la de AXIOM. Es una herramienta operativa, pero su interfaz puede ser menos intuitiva que la de AXIOM. Su tasa de recuperación es muy buena, y es una buena opción para usuarios con experiencia.

En general, las herramientas forenses AXIOM y FTK (Forensic Toolkit) son las más efectivas en la extracción y recuperación de datos en dispositivos de almacenamiento masivo en equipos personales. Estas herramientas son complejas, pero ofrecen una amplia gama de características y soporte para una amplia gama de formatos de archivos, sistemas de archivos y dispositivos de almacenamiento.

La herramienta AUTOPSY es también una herramienta efectiva, pero es menos compleja que AXIOM y FTK. AUTOPSY ofrece un buen soporte para una amplia gama de formatos de archivos, sistemas de archivos y dispositivos de almacenamiento.

La herramienta Wondershare Recoverit es una herramienta que es adecuada para usuarios que necesitan recuperar datos de forma rápida y sencilla. Sin embargo, Wondershare Recoverit no ofrece el mismo nivel de efectividad que las otras herramientas forenses.

8 CONCLUSIONES

- Selección de Herramientas Forenses: Durante la investigación, se ha identificado que la elección de las herramientas forenses es un paso crítico en el proceso de extracción y recuperación de datos. El conocimiento adquirido sobre herramientas como FTK, AXIOM, WONDERSHARE RECOVERIT y AUTOPSY ha revelado su importancia en el campo. Estas herramientas ofrecen funcionalidades variadas que permiten a los investigadores adaptarse a diversas situaciones y, por lo tanto, aportan flexibilidad y eficacia a la resolución de casos forenses.

- La planificación de pruebas en la investigación forense de extracción y recuperación de datos en dispositivos de almacenamiento masivo se ha revelado como un componente esencial para el éxito de la investigación. Durante el proceso de planificación y ejecución de pruebas, se ha reconocido la importancia de la meticulosidad y la atención al detalle en la evaluación de las herramientas forenses seleccionadas. La planificación adecuada de pruebas garantiza la efectividad de las herramientas, la confiabilidad de los resultados y el cumplimiento de los estándares legales y éticos. Además, la planificación de pruebas proporciona una oportunidad única para identificar desafíos específicos y obstáculos que pueden surgir durante una investigación forense real. Estas pruebas permiten a los investigadores anticipar posibles problemas y adaptar sus estrategias en consecuencia.

- Comprobación de la Efectividad en Pruebas realizadas: Las pruebas realizadas proporcionaron una valiosa lección: la necesidad de validar las herramientas forenses en condiciones controladas y en situaciones de la vida real. Esta validación asegura que las herramientas seleccionadas cumplan con los estándares requeridos y demuestren su efectividad en la adquisición y análisis de evidencia digital. Los hallazgos de estas pruebas son fundamentales para garantizar la calidad y confiabilidad de la investigación forense.

- Cumplimiento de Normas y Regulaciones Forenses: La investigación destacó la importancia del cumplimiento de normas y regulaciones en el proceso de investigación forense. La adhesión a estándares legales y éticos es esencial para garantizar la integridad de la evidencia y la defensa de los derechos individuales. Esta nueva comprensión subraya la responsabilidad del investigador en seguir prácticas sólidas de cadena de custodia y garantizar la legalidad de las pruebas recopiladas.

- Contribución a la Resolución de Casos Judiciales: El trabajo realizado, desde la selección de herramientas hasta la realización de pruebas, aporta de manera significativa a la resolución de casos judiciales. La adquisición y el análisis efectivos de evidencia digital son fundamentales para proporcionar pruebas sólidas que respalden el proceso legal. Esto, a su vez, contribuye a la justicia y a la resolución de crímenes, lo que es de suma importancia para la sociedad en su conjunto.

9 RECOMENDACIONES

- La elección de la herramienta forense adecuada dependerá de las necesidades específicas del caso. Para casos complejos o que requieran una gran gama de funciones, Axiom es la mejor opción. Para casos más sencillos o que requieran una herramienta especializada, Autopsy o FTK (Forensic Toolkit) pueden ser buenas opciones. Para casos de recuperación de datos eliminados o perdidos, Wondershare Recoverit puede ser una buena opción para un análisis rápido.
- Investigación Continua de Herramientas Forenses: Dado que el campo de la informática forense evoluciona constantemente, se recomienda mantenerse al día con las últimas herramientas y tecnologías forenses. La investigación futura debe centrarse en la evaluación y adopción de nuevas herramientas que se desarrollen, ya que podrían ofrecer ventajas adicionales en términos de eficacia y capacidad de recuperación de datos.
- Desarrollo de Normas y Guías: Para promover la integridad y la calidad de las investigaciones forenses, se sugiere que se continúe trabajando en el desarrollo de normas y guías específicas para la extracción y recuperación de datos en dispositivos de almacenamiento masivo. Estas normas pueden servir como referencia para garantizar la consistencia y la adhesión a mejores prácticas en el campo.
- Formación y Certificación Profesional: Dado que el éxito en la investigación forense depende en gran medida del conocimiento y las habilidades de los profesionales, se recomienda que las organizaciones y los investigadores busquen oportunidades de formación y certificación en informática forense. Estas certificaciones garantizarán que los investigadores estén bien preparados para abordar casos forenses de manera efectiva y hagan un uso adecuado de las diferentes herramientas forenses disponibles.
- Énfasis en la Ética y la Integridad: Se sugiere que se haga hincapié en la ética y la integridad en la investigación forense. Esto incluye el respeto de la privacidad de las personas y el cumplimiento de las leyes y regulaciones aplicables. La capacitación continua sobre ética y la supervisión de casos son esenciales para mantener una conducta profesional y legal.
- Colaboración y Comunicación Interdisciplinaria: En el ámbito forense, la colaboración entre diferentes disciplinas es clave. Se recomienda fomentar la comunicación y la colaboración interdisciplinaria entre expertos en informática, criminología, medicina legal y otras áreas. Esto permitirá un enfoque más completo y eficiente en la resolución de casos forenses complejos.

.

BIBLIOGRAFÍA

Aguilera, P. Redes seguras - Seguridad informática. 2011. Editex. Madrid. [En línea]. [Fecha de consulta: octubre 2023]. Disponible en: https://books.google.com.ec/books?id=Mgvm3AYIT64C&printsec=frontcover&hl=es#v=onepage&q&f=false

Astudillo, S., y Morales, G. 2018. Software y dispositivos utilizados en la computación forense. [En línea]. [Fecha de consulta: septiembre 2023]. Disponible en: https://repository.unicatolica.edu.co/bitstream/handle/20.500.12237/994/SOFTWARE_DISPOSITIVOS_UTILIZADOS_COMPUTACI%c3%93N_FORENSE.pdf?sequence=1&isAllowed=y

CAINE 8 Best Linux Distros for Forensics & Pentesting [En línea] [Fecha de consulta: 02 de abril de 2024] Disponible en: https://www.esecurityplanet.com/products/open-source-distros-for-pentesting-and-forensics/

Campoli, G. Manual Básico de Cateo y Aseguramiento de Evidencia Digital. 2006. México. [En línea]. [Fecha de consulta: octubre 2023]. Disponible en: https://www.derechopenalenlared.com/libros/manual-basico-cateo-aseguramiento-evidencia-digital.pdf

Cano, J. Introducción a la informática forense: Una disciplina técnico-legal. 2006. Revista Sistemas, Asociación Colombiana de Ingenieros de Sistemas (ACIS). Vol.96, pp. 64-73. Disponible en: http://52.0.140.184/typo43/fileadmin/Revista_96/dos.pdf

Casey, E. Evidencia Digital y Delitos Informáticos: Ciencia Forense, Computadoras y Internet. 2014. Academic Press.

Castañeda F., Rojas V., Villanueva N., Evaluación de herramientas para análisis forense orientado a discos duros. 2009. México.

Castillo, C., Romero, A., Cano, J. Análisis Forense Orientado a Incidentes en Teléfonos Celulares GSM: Una Guía Metodológica. 2008. Conf. XXXIV Conferencia Latinoamericana de Informática, Centro Latinoamericano de Estudios en Informática (CLEI).

Castro, Romero M., La informática Forense desde un enfoque práctico. 2020. [En línea]. [Fecha de consulta abril de 2023] Manabí, Ecuador. Disponible en: https://gc.scalahed.com/recursos/files/r161r/w26124w/LA_INFORMATICA_FORENSE_DESDE_UN_ENFOQUE_PRACTICO_compressed.pdf

Chicano Tejada, Esther. Gestión de incidentes de seguridad informática (MF0488_3). Antequera, Málaga. IC Editorial. 2015. [En línea]. [Fecha de consulta: octubre 2023]. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/44101?page=276. ISBN: 978-84-16207-15-2.

Cortés de la Rosa B., Manejo de evidencia digital en dispositivos de almacenamiento pendrive usb aplicando la norma ISO/IEC 27037:2012. 2014. Pasto.

Cuervo K., Comparación de diferentes herramientas para el análisis forense en dispositivos extraíbles de tipo flash drive. 2015. Universidad Santo Tomás, Tunja-Colombia.

Dallos, Y. Revisión de efectividad de herramientas forenses en la extracción y recuperación de datos en dispositivos de almacenamiento masivo de equipos personales. 2023. Repositorio UNAD. Continuación en la elaboración de Trabajo de grado.

Darahuge, M. Manual de Informática Forense. 2011. Errepar. Buenos Aires.

Di iorio, Ana Haydee. Guía Integral de Empleo de la Informática Forense en el Proceso Penal. 2015. Universidad FASTA. Mar del Plata. Argentina.

Domínguez, F. L. Introducción a la informática forense. 2013. Grupo Editorial RAMA.

Estrada, A. C. La informática forense y los delitos informáticos. 2010. Revista Pensamiento Americano, 81-88. [En línea]. [Fecha de consulta: octubre 2023]. https://www.academia.edu/27115286/
La_inform%C3%A1tica_forense_y_los_delitos_inform%C3%A1ticos

Gallego, J. C., y Folgado, L. Gestión de discos (Montaje y mantenimiento de equipos). 2011. Editex.

Gómez, H. H. S. Informática Forense. 2009. [En línea]. [Fecha de consulta: octubre 2023]. https://docplayer.es/4758786- Informatica-forense-hernan-herrera-sebastian-gomez.html

Guerra M., Análisis Forense Informático. 2021. RA-MA Editorial. ISBN: 978-84-1897-124-2. Madrid.

Hoog, A. iPhone Forensics: Annual Report on iPhone Forensic Industry. 2009. Chicago Electronic Discovery.

Huanca V., Metodología de análisis forense digital para la extracción de datos almacenados en dispositivos móviles basados en sistema operativo android. 2014. La Paz.

INFO-LAB. Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense. 2016. Universidad FASTA, Ministerio Público Fiscal de la Provincia de Buenos Aires y la Municipalidad de General Pueyrredon. Buenos Aires. Argentina.

Kent K., et al. SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. 2006. [En línea]. [Fecha de consulta: 09 de octubre 2023]. Disponible en: https://tsapps.nist.gov/ publication/get_pdf.cfm?pub_id=50875

Kruse, II, W. G., & Heiser, J. G. Informática Forense: Fundamentos para la Respuesta a Incidentes. 2002. Addison-Wesley Professional.

Lázaro, F. Introducción a la informática forense. 2014. [En línea]. [Fecha de consulta 12 de octubre de 2023]. Paracuellos de Jarama, Madrid, RAMA Editorial. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/106250?page=246

Leigland, R. A Formalization of Digital Forensics. International Journal of Digital Evidence. 2004. University of Idaho. Volume 3, Issue 2. [En línea]. [Fecha de consulta: octubre 2023]. http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B8472CD1D2- 8F98- 8F7597844CF74DF8.pdf.

LMO Campos, E. Gomes y HP Martins, Experiencia forense en dispositivos de almacenamiento USB Flash Drive: procedimientos y técnicas para evidencia. 2016. en IEEE Latin America Transactions , vol. 14, núm. 7, págs. 3427-3433, doi: 10.1109/TLA.2016.7587651.

López Delgado, Miguel. Análisis Forense Digital. 2007. [En Línea]. [Fecha de consulta: octubre, 2023]. Disponible en: https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

Maras, M. H. Forense Digital: Delitos Informáticos, Leyes y Evidencias. 2012. Jones & Bartlett Publishers.

Marcella, A. J., & Greenfield, L. Forense Cibernética: Manual de Campo para la Recolección, Examen y Preservación de Evidencias de Delitos Informáticos. 2004. CRC Press.

McKemmish, R. Examen Forense de Documentos: Principios y Práctica. 2018. CRC Press.

Mena, Y. Algoritmos HASH y vulnerabilidad a ataques. Revista de Información, Tecnología y Sociedad, 108. 2009. [En línea]. [Fecha de consulta: octubre 2023].

http://www.revistasbolivianas.org.bo/scielo. php?script=sci_arttext&pid=S1997-40442009000200026&lng=es&nrm=iso

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Evidencia Digital: Seguridad y privacidad de la información. 2016. Colombia.

Nelson, B., Phillips, A., & Steuart, C. Guía de Informática Forense e Investigaciones. 2014. Cengage Learning.
Organización de los Estados Americanos. Habilidades de Análisis Forense Informático. 2023. [En línea]. [Fecha de consulta: octubre 2023]. Disponible en: http://www.oas.org/juridico/english/cyb_mex_forense.pdf

Padmanabhan R., K. Lobo, M. Ghelani, D. Sujan y M. Shirole, «Comparative Analysis of Commercial and Open Source Mobile Device Forensic Tools,» IEEE, 2016.

Padula, E. J.; Fogliato, N.; Casco, M. Análisis Digital Forense, Conceptos y Aplicaciones. 2016. Facultad de Ciencias Exactas, Ingeniería. Universidad Nacional de Rosario. Rosario, Santa Fe. Argentina.

Pollitt, M. M. Implementación de la Preparación Forense Digital: De un Enfoque Reactivo a uno Proactivo. 2007. Digital Investigation, 4(3-4), 104-111.

Prosise, C., Mandia, K., & Pepe, M. Respuesta a Incidentes y Forense Informático. 2003. McGraw-Hill Education.

Quick, D. Investigación de Delitos Informáticos: Manual para Investigadores Corporativos. 2010. CRC Press.

Reith, M., Carr, C., & Gunsch, G. Un Examen de los Modelos Forenses Digitales. 2002. International Journal of Digital Evidence.

Roatta S., M.E. Casco, M. Fogliato. El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012. 2020. Facultad Tecnología Informática / Universidad Abierta Interamericana. Argentina.

Rodríguez M. Recuperación de información en discos duros. 2007. México.

Rogers, C. Investigaciones Forenses en Dispositivos Móviles: Guía de Recolección, Análisis y Presentación de Evidencias. 2016. Syngress.

Salem N., Iqbal F. y Alfandi O., «An Approach for the Validation of File Recovery Functions in Digital Forensics' Software Tools,» IEEE, 2014.

Sansevero, R. & Castellote, M. & Podestá, A. & Greco, F. & Constanzo, B. & Waimann, J. & Di Iorio, A. & Laboratory, Info-Lab. La recuperación de la información y la informática forense: Una propuesta de proceso unificado. 2012. Argentina.

Wondershare Recoverit. 2023. [En línea] [Fecha de consulta: 08 de noviembre de 2023] Disponible en: https://recoverit.wondershare.es/