Universidad Tecnológica del Cho
Diego Luis Córdoba

INFORME DE AUTORIA FORENSE CON AUTOPSY Y FTK EN LINUX Y WINDOWS

JOHAN CAMILO GARCIA CARO

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

PROGRAMA

INGENIERÍA TELECOMUNICACIONES E INFORMÁTICA

IX-NIVEL

SEGURIDAD Y AUDITORÍA DE REDES

QUIBDÓ, CHOCÓ, COLOMBIA

2025

TABLA DE CONTENIDO

TABLA DE IMÁGENES

INTRODUCION

En el campo de la seguridad y auditoría de redes, la autoría forense digital es un pilar fundamental para la investigación de incidentes y la recolección de evidencia. Este proceso requiere el uso de herramientas especializadas que permitan analizar sistemas de almacenamiento sin alterar la data original, garantizando la integridad de la prueba.

Este informe, desarrollado en el marco de la asignatura Seguridad y Auditoría de Redes, presenta una guía práctica del análisis forense realizado sobre una imagen de disco. El documento se enfoca en la aplicación de dos de las herramientas más reconocidas en la industria: **Autopsy** y **FTK Imager**.

A lo largo de los capítulos, se detalla el procedimiento completo, comenzando con la fase crucial de adquisición de evidencia en un entorno Linux. Esto incluye la identificación de dispositivos , el cálculo de hashes de verificación (SHA1) para asegurar la integridad , y la creación de una imagen forense bit a bit (.dd). Posteriormente, se demuestra cómo esta imagen es procesada y analizada en múltiples plataformas: primero con Autopsy en Linux (Capítulo 1) , luego con Autopsy en Windows (Capítulo 2) y finalmente con FTK Imager en Windows (Capítulo 3).

RESUMEN

El presente informe documenta un proceso de autoría forense digital aplicado a una imagen de disco (imagen_usb_forense.dd). El análisis se realiza utilizando dos herramientas clave, **Autopsy** y **FTK Imager**, en los sistemas operativos **Linux y Windows**.

El procedimiento inicia en Linux con la identificación del dispositivo USB de origen (/dev/sdb) , la generación de un hash SHA1 para garantizar su integridad y la adquisición de una imagen bit a bit mediante el comando dd. Posteriormente, se verifica la integridad de la imagen .dd creada comparando su hash.

El informe se divide en tres capítulos:

1. **Auditoría con Autopsy en Linux**
2. **Auditoría con Autopsy en Windows**
3. **Autoría con FTK Imager en Windows**

OBJETIVO GENERAL

Demostrar el proceso práctico de una autoría forense digital, desde la adquisición de una imagen de disco hasta su análisis detallado, utilizando las herramientas Autopsy y FTK Imager en los sistemas operativos Linux y Windows.

OBJETIVO ESPECIFICO

Realizar la adquisición forense bit a bit de un dispositivo de almacenamiento (USB) en un entorno Linux utilizando el comando dd.

Asegurar y verificar la integridad de la evidencia digital (tanto del dispositivo original como de la imagen) mediante la generación y comparación de valores hash (SHA1 y MD5).

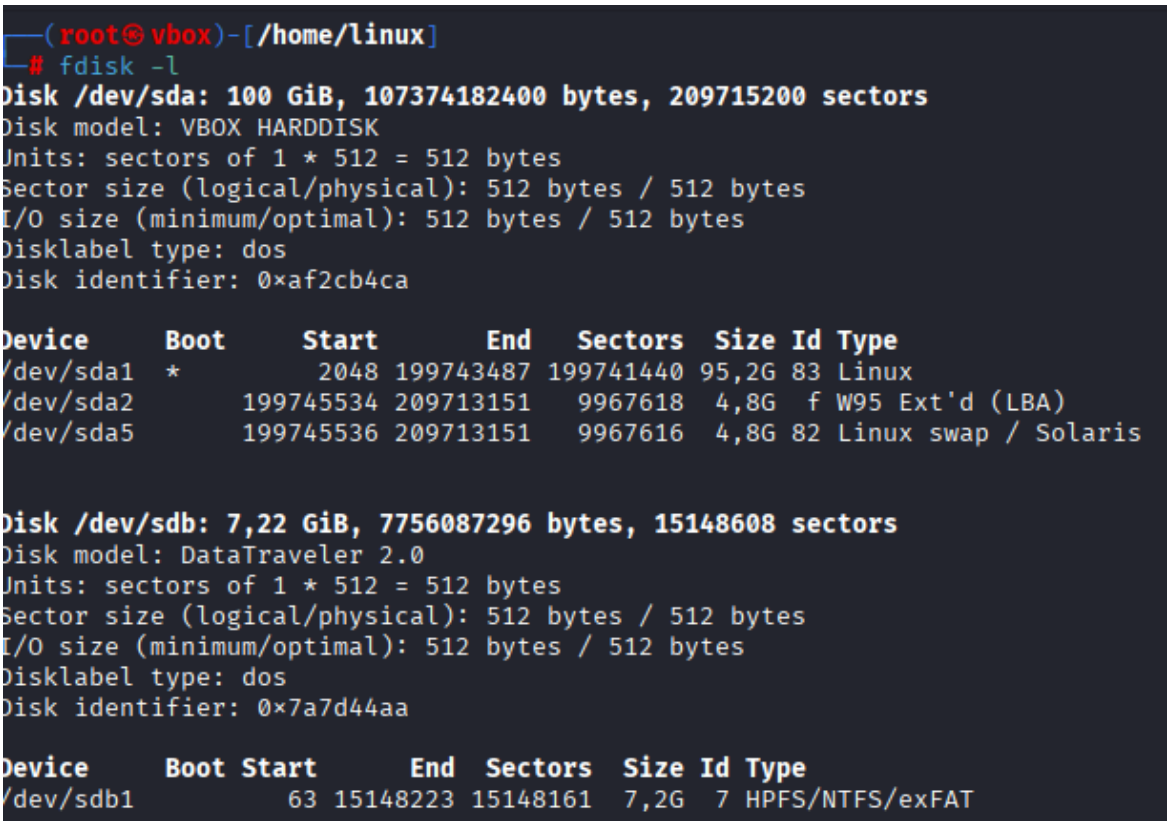
Detallar el procedimiento de análisis de la imagen forense con la herramienta Autopsy en el sistema operativo Linux, cubriendo la creación del caso, la importación de la evidencia y la revisión de archivos.

Documentar el proceso de instalación y configuración de Autopsy en Windows para el análisis de la misma imagen, incluyendo la configuración de módulos de ingesta (Ingest Modules).

Emplear la herramienta FTK Imager en Windows para cargar la imagen forense, explorar la estructura de particiones, listar archivos y examinar su contenido en una vista.

CAPITULO#1 AUDITORIA FORENSE CON AUTOPSY EN LINUX

En este paso se ejecuta el comando fdisk -l para identificar los discos y particiones disponibles en el sistema. Esta acción permite conocer la estructura del almacenamiento, los tipos de particiones y los tamaños de cada unidad, información fundamental antes de realizar un análisis forense o crear una imagen del disco.



imagenes 1 ejecucion del comando fdisk -l

En este paso se genera el valor **hash SHA1** del disco /dev/sdb, guardándolo en un archivo ubicado en el escritorio. Este procedimiento se realiza para garantizar la integridad de la evidencia digital, permitiendo comprobar posteriormente que la información analizada no ha sido alterada durante el proceso forense.

```
┌──(root㉿vbox)-[/home/linux]
└─# sha1sum /dev/sdb > /home/linux/Escritorio/hash_fore.sha1
```

imagenes 2 generación de hash_sha1

```
1 2944dc2f2059c1af88e3ea516126835939e07182  /dev/sdb
```

imagenes 3 hash_generado

En este paso se utiliza el comando dd para realizar una adquisición forense del dispositivo USB, copiando cada bit del disco original a un archivo de imagen (.dd). Las opciones conv noerror,sync aseguran que, aunque existan errores de lectura, el proceso continúe sin perder datos. Este paso es esencial para preservar la evidencia digital y trabajar posteriormente sobre una copia sin alterar el dispositivo original.

```
┌──(root㉿vbox)-[/home/linux]
└─# dd if=/dev/sdb of=/home/linux/Escritorio/imagen_usb_forense.dd conv=noerror,sync
15148608+0 records in
15148608+0 records out
7756087296 bytes (7,8 GB, 7,2 GiB) copied, 1354,46 s, 5,7 MB/s
```

imagenes 4 comando dd

En este paso se calcula el **hash SHA1** de la imagen forense (imagen_usb_forense.dd) para obtener una **huella digital única** del archivo. Este valor se utiliza posteriormente para comparar y verificar que la imagen no ha sido modificada durante el análisis. Es un paso fundamental dentro del proceso de **verificación de integridad** en la auditoría forense digital.

```
┌──(root㉿vbox)-[/home/linux]
└─# sha1sum /home/linux/Escritorio/imagen_usb_forense.dd
2944dc2f2059c1af88e3ea516126835939e07182  /home/linux/Escritorio/imagen_usb_forense.dd
```

imagenes 5 adquisición del análisis forense *de la USB*

En este paso se modifica el permiso de acceso del archivo de imagen forense mediante el comando chmod 777. Esto otorga permisos de lectura, escritura y ejecución a todos los usuarios, facilitando su manipulación durante el análisis. Sin embargo, en un entorno forense real, esta práctica debe hacerse con precaución para evitar alteraciones accidentales de la evidencia.

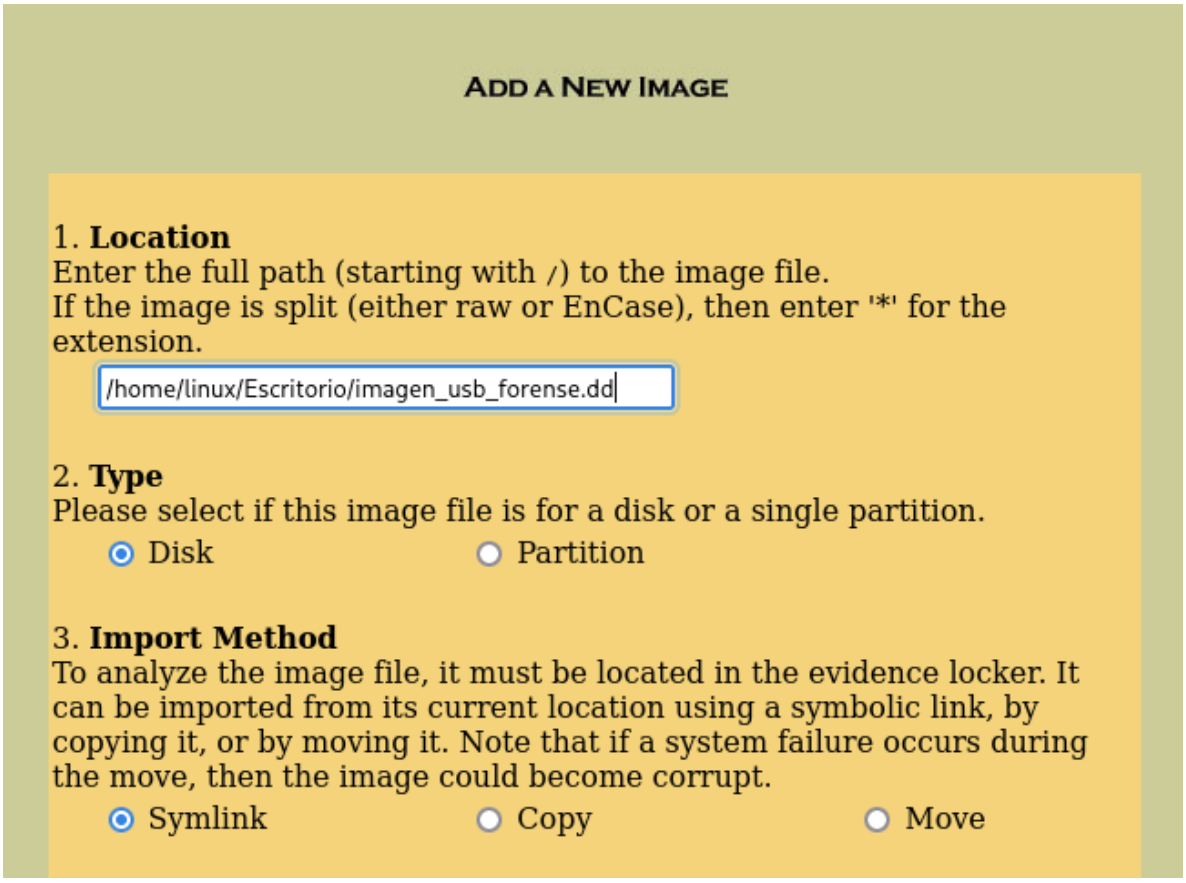
```
┌──(root㉿vbox)-[/home/linux]
└─# chmod 777 /home/linux/Escritorio/imagen_usb_forense.dd
```

imagenes 6 permisos

En este paso se observa el proceso de **creación de un host dentro de un caso en Autopsy**, donde el sistema genera automáticamente el **directorio y archivo de configuración** correspondientes. Este paso permite vincular la evidencia digital con un equipo específico para su análisis. Finalmente, se indica que el siguiente paso es **importar la imagen forense** obtenida previamente, lo cual se hace mediante el botón **Add Image.**

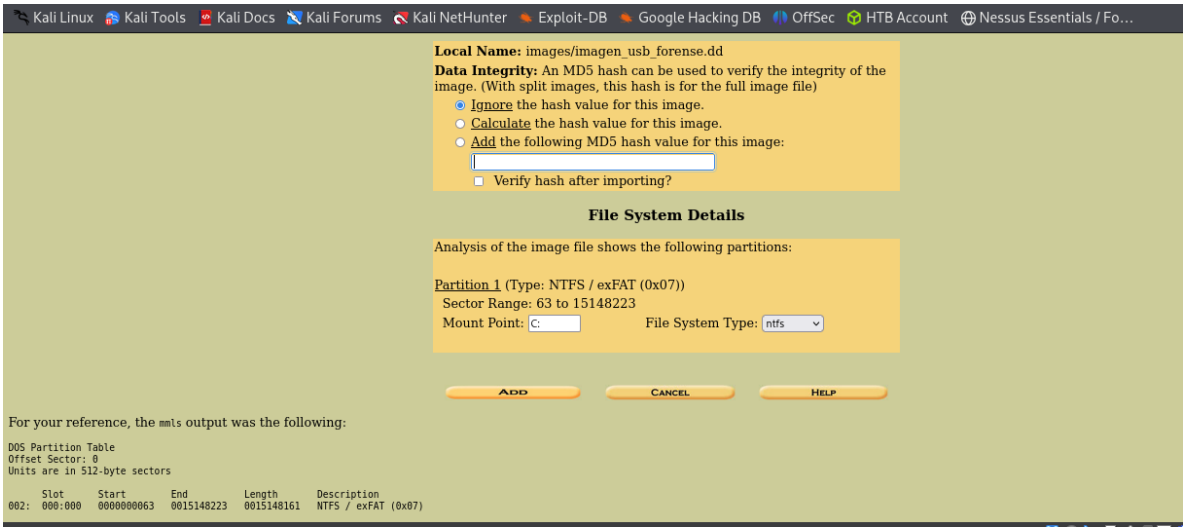
imagenes 7 creacion de un host

En este paso se realiza la importación de la evidencia digital en Autopsy. Se especifica la ubicación del archivo de imagen (/home/Linux/Escritorio/imagen_usb_forense.dd), indicando que se trata de un disco completo (Disk) y seleccionando el método de importación Symlink, que crea un enlace simbólico sin alterar el archivo original. Este paso es fundamental para comenzar el análisis forense sobre la copia creada, preservando la integridad de la evidencia.



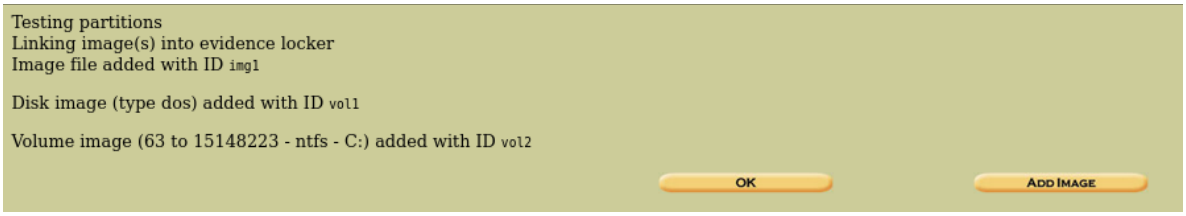
imagenes 8 nueva imagen

En este paso se observa cómo Autopsy analiza la imagen forense imagen_usb_forense.dd, detectando automáticamente el **sistema de archivos NTFS** y la **partición** correspondiente. Además, se configura la opción para **calcular o verificar el hash MD5**, lo que garantiza que la imagen no haya sido alterada durante el proceso de importación. Este paso confirma la **integridad de la evidencia** y prepara el entorno para iniciar el análisis detallado del contenido del disco.



imagenes 9 sistema de archivo

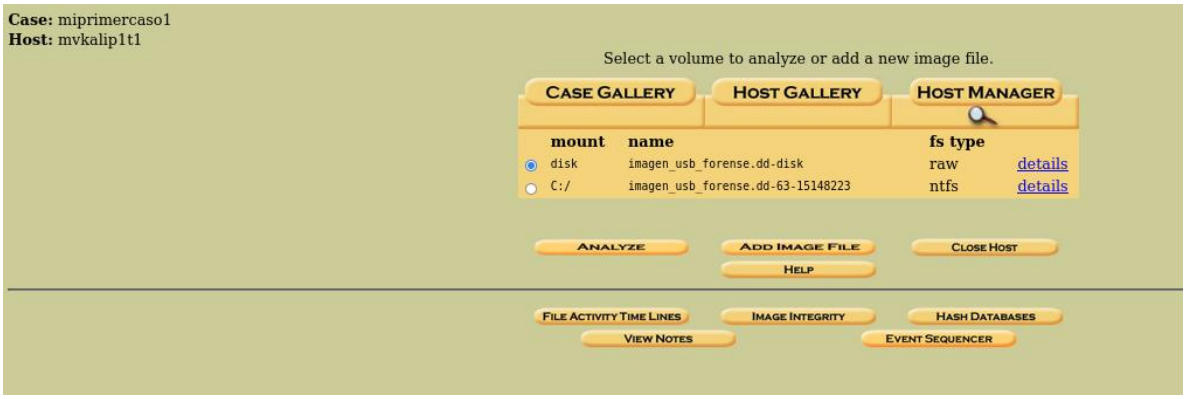
En este paso se confirma que la imagen de disco y su volumen asociado fueron añadidos exitosamente al evidencie locker (repositorio de evidencias) de Autopsy. El sistema asigna identificadores únicos (vol1 y vol2) a cada elemento, lo que permite gestionarlos y analizarlos de forma organizada. Este paso marca el inicio formal del análisis forense, ya que la evidencia queda registrada y disponible para su exploración dentro del caso.



imagenes 10 asociación exitosa

En esta imagen se observa la interfaz del programa Autopsy, utilizada en el análisis forense digital. Aquí se ha cargado un caso denominado “miprimercaso1” y un host identificado como “mvkalip1t1”.

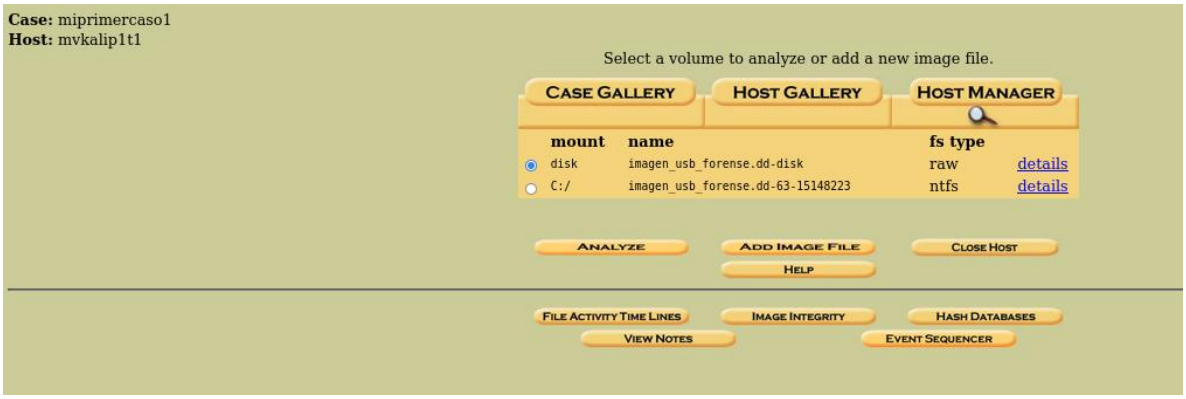
Se muestran los volúmenes o imágenes de disco agregadas para su estudio: una con formato raw y otra con sistema de archivos NTFS. Desde esta ventana se puede seleccionar la imagen a analizar, verificar su integridad, consultar detalles, o acceder a herramientas adicionales como el análisis de línea de tiempo, bases de datos de hashes y secuenciador de eventos.



imagenes 11 interfaz de autopsy

En este paso se muestra nuevamente la interfaz del programa Autopsy, donde se gestiona el análisis de evidencias digitales dentro de un caso forense.
Aquí se observan los volúmenes asociados al caso “miprimercaso1” y al host “mvkalip1t1”, con dos imágenes forenses cargadas: una con formato raw y otra con sistema de archivos NTFS.

Desde esta pantalla se puede seleccionar la imagen a analizar, consultar detalles técnicos, añadir nuevos archivos de imagen o cerrar el host. Además, se ofrecen herramientas complementarias como verificación de integridad, líneas de tiempo de actividad y base de datos de hashes para profundizar en el examen de los datos.

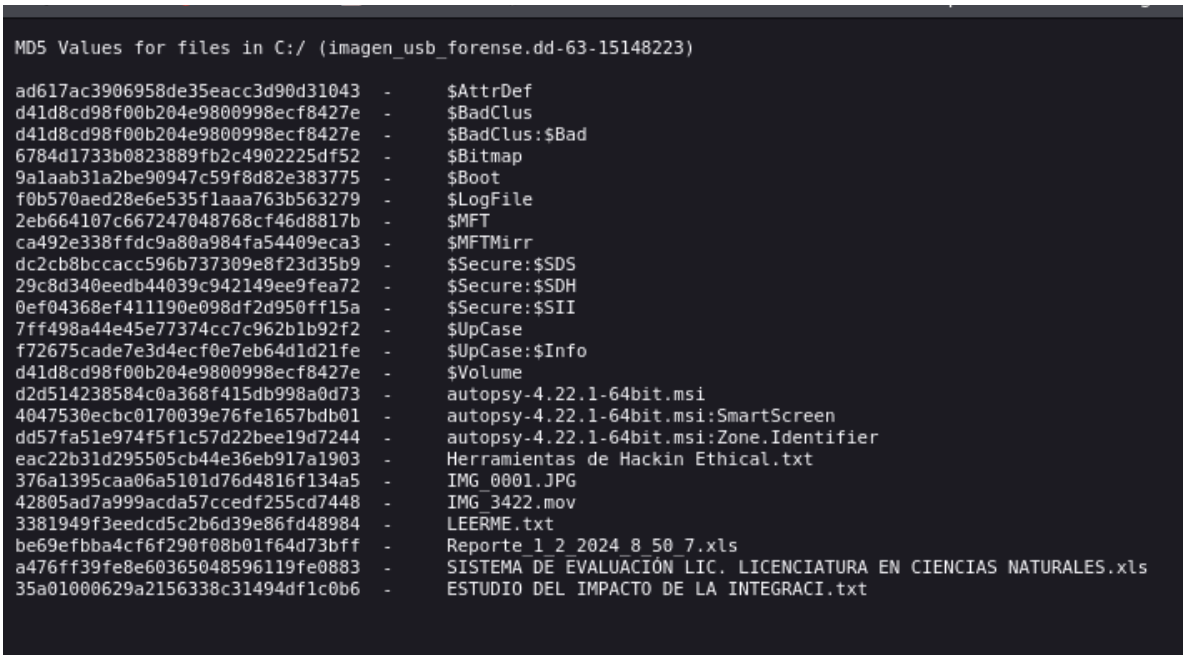


imagenes 12 gestión de análisis

En este paso se observa el resultado del **cálculo de valores hash MD5** para los archivos contenidos en la imagen forense **“imagen_usb_forense.dd”**, ubicada en la unidad C:/.

Cada archivo listado tiene asociado su respectivo hash MD5, el cual permite verificar la integridad y autenticidad de los datos durante el análisis forense digital.

Entre los archivos identificados se encuentran documentos de texto, hojas de cálculo, instaladores y archivos multimedia (como .JPG y .MOV).
Esta información es esencial para detectar posibles alteraciones, duplicados o modificaciones en los archivos extraídos de la evidencia.



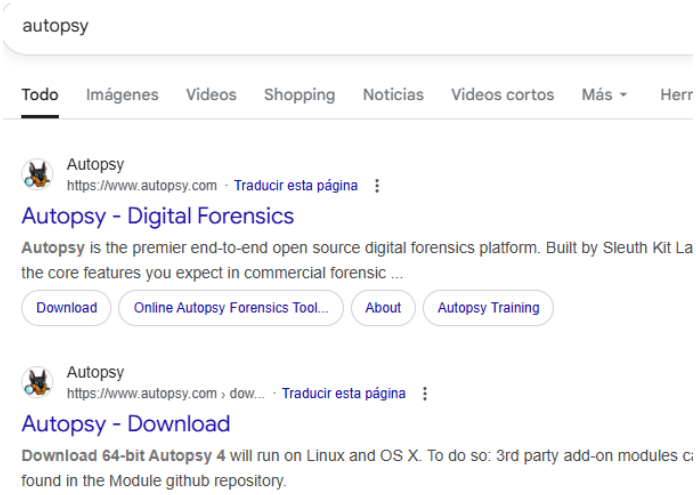
```
MD5 Values for files in C:/ (imagen_usb_forense.dd-63-15148223)

ad617ac3906958de35eacc3d90d31043  -     $AttrDef
d41d8cd98f00b204e9800998ecf8427e  -     $BadClus
d41d8cd98f00b204e9800998ecf8427e  -     $BadClus:$Bad
6784d1733b0823889fb2c4902225df52  -     $Bitmap
9a1aab31a2be90947c59f8d82e383775  -     $Boot
f0b570aed28e6e535f1aaa763b563279  -     $LogFile
2eb664107c667247048768cf46d8817b  -     $MFT
ca492e338ffdc9a80a984fa54409eca3  -     $MFTMirr
dc2cb8bccacc596b737309e8f23d35b9  -     $Secure:$SDS
29c8d340eedb44039c942149ee9fea72  -     $Secure:$SDH
0ef04368ef411190e098df2d950ff15a  -     $Secure:$SII
7ff498a44e45e77374cc7c962b1b92f2  -     $UpCase
f72675cade7e3d4ecf0e7eb64d1d21fe  -     $UpCase:$Info
d41d8cd98f00b204e9800998ecf8427e  -     $Volume
d2d514238584c0a368f415db998a0d73  -     autopsy-4.22.1-64bit.msi
4047530ecbc0170039e76fe1657bdb01  -     autopsy-4.22.1-64bit.msi:SmartScreen
dd57fa51e974f5f1c57d22bee19d7244  -     autopsy-4.22.1-64bit.msi:Zone.Identifier
eac22b31d295505cb44e36eb917a1903  -     Herramientas de Hackin Ethical.txt
376a1395caa06a5101d76d4816f134a5  -     IMG_0001.JPG
42805ad7a999acda57ccedf255cd7448  -     IMG_3422.mov
3381949f3eedcd5c2b6d39e86fd48984  -     LEERME.txt
be69efbba4cf6f290f08b01f64d73bff  -     Reporte_1_2_2024_8_50_7.xls
a476ff39fe8e60365048596119fe0883  -     SISTEMA DE EVALUACIÓN LIC. LICENCIATURA EN CIENCIAS NATURALES.xls
35a01000629a2156338c31494df1c0b6  -     ESTUDIO DEL IMPACTO DE LA INTEGRACI.txt
```

imagenes 13 archivos hash_md5

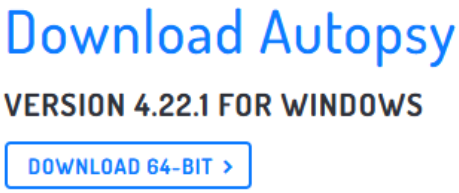
CAPITULO #2 AUDITORIA FORENSE CON AUTOPSY EN WINDOWS

Busqueda de autopsy en google



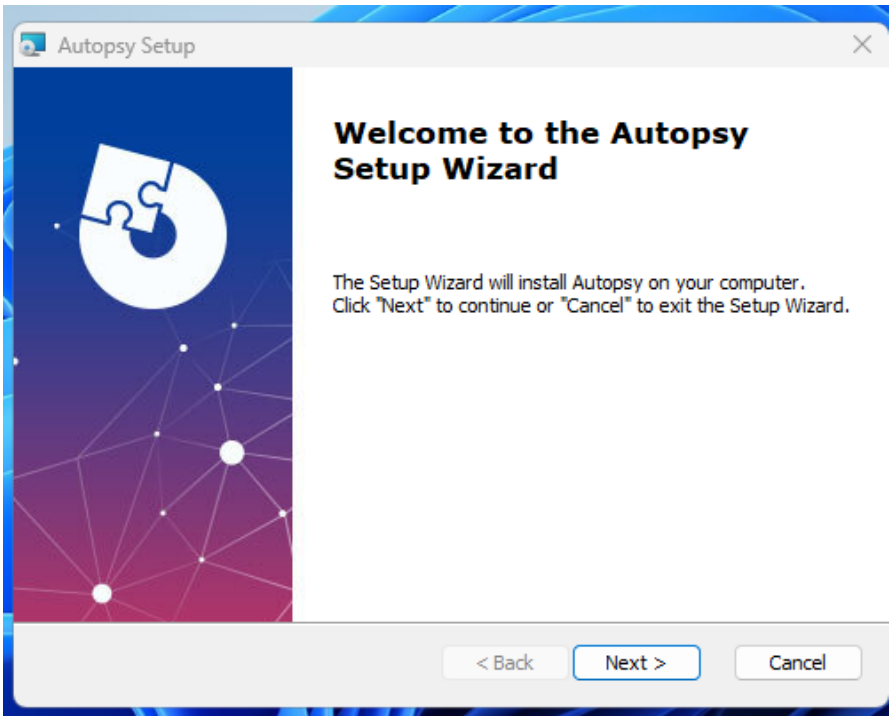
imagenes 14 descarga de autopsy

Botón de descarga de autopsy



imagenes 15 botón de descarga de autopsy

paso de la instalacion de autopsy



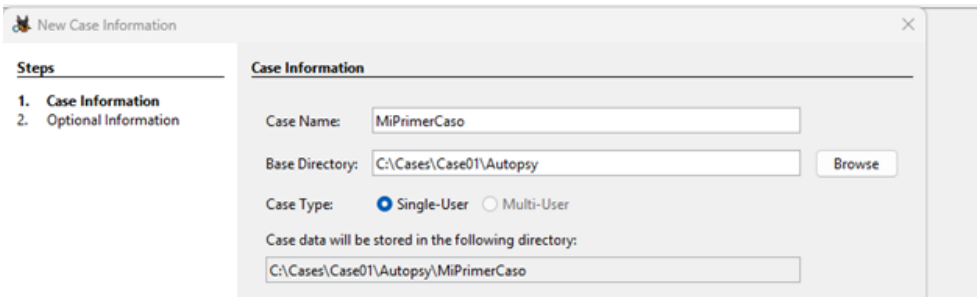
imagenes 16 instalacion de autopsy

Creacion de nuevo caso

imagenes 17creacion de un nuevo caso

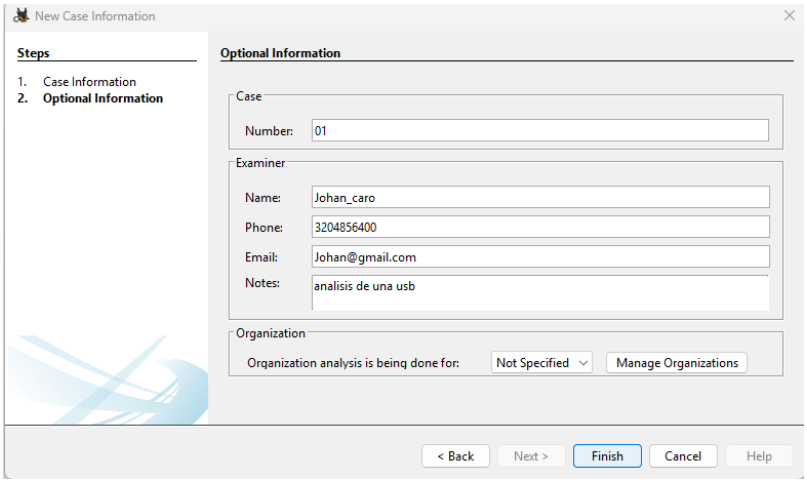
En este paso se muestra la ventana de creación de un nuevo caso en Autopsy, donde se configuran los datos iniciales del análisis forense.

Se define el **nombre del caso (Mi Primer Caso)**, la **ruta base** donde se almacenará la información y el **tipo de caso**, que en este ejemplo es **Single-User** (usuario único).



imagenes 18 configuracion del nuevo caso

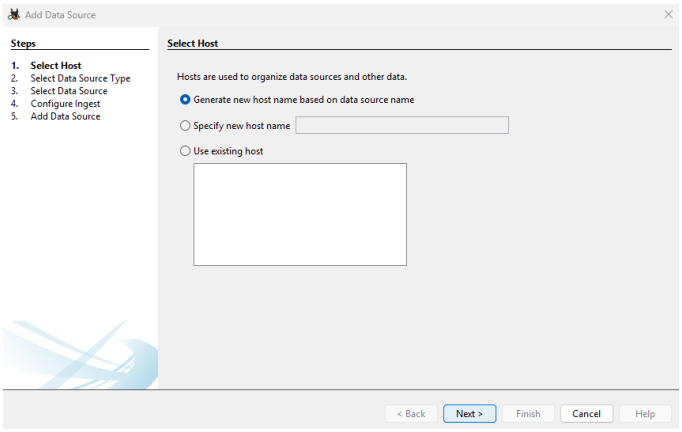
En este paso se observa la segunda parte del proceso de creación de un nuevo caso en Autopsy, correspondiente a la sección de información opcional.
Aquí se registran los datos del examinador como nombre, número de teléfono, correo electrónico y notas del caso, además del número de caso y la organización (si aplica).



imagenes 19 segunda parte de la creacion del caso

En este paso se muestra la ventana de selección del host dentro del proceso de agregar una fuente de datos en Autopsy.
Aquí se define si el programa debe generar automáticamente un nombre de host basado en la fuente de datos, especificar un nombre nuevo, o utilizar un host existente.

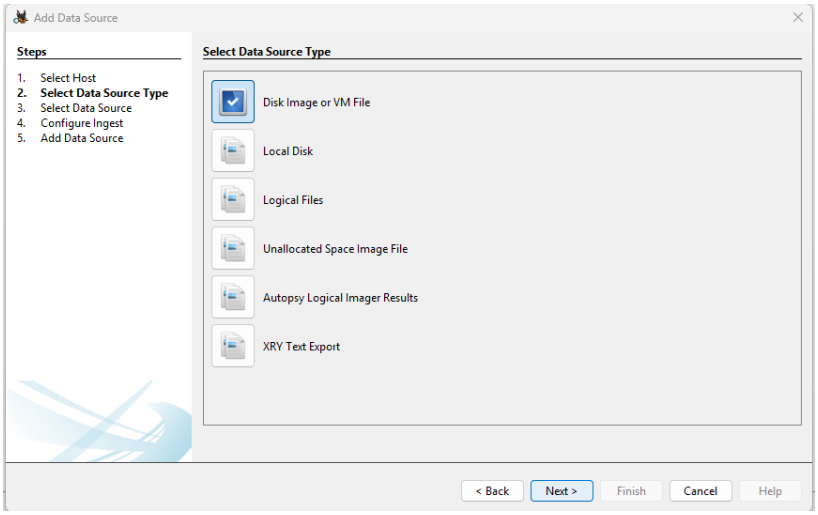
El host sirve para organizar las fuentes de datos y evidencias dentro de un mismo caso, facilitando la gestión y el análisis de los diferentes dispositivos o imágenes que se examinan.



imagenes 20 ventana de selecion del host

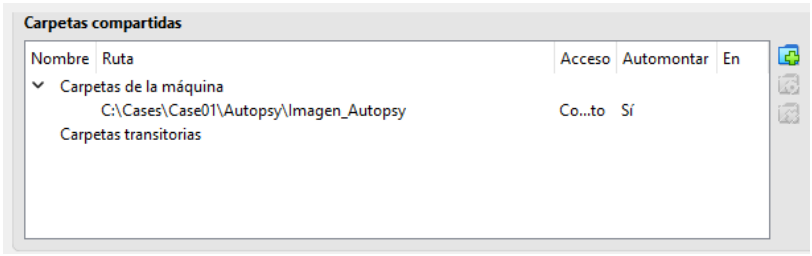
En este paso se observa la ventana de selección del tipo de fuente de datos en el programa Autopsy, una parte esencial del proceso de análisis forense digital.

Aquí el usuario debe elegir qué tipo de evidencia se va a examinar. En este caso, está seleccionada la opción “Disk Image or VM File”, que permite analizar una imagen de disco o un archivo de máquina virtual.



imagenes 21 ventana de selecion de la fuente de los datos

Creacion de la carpeta compartida

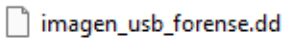


imagenes 22 carpeta compartida

Imagen USB forense.dd

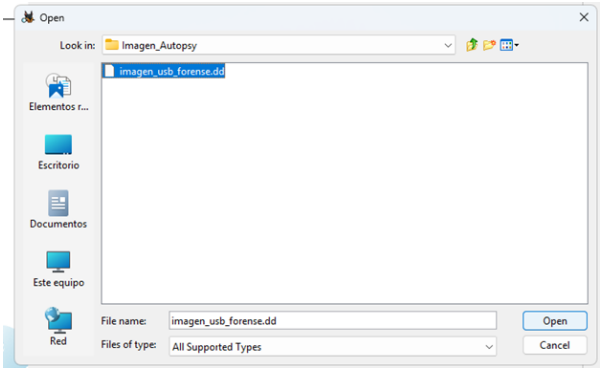
imagenes 23 imagen forense

Archivo de la imagen



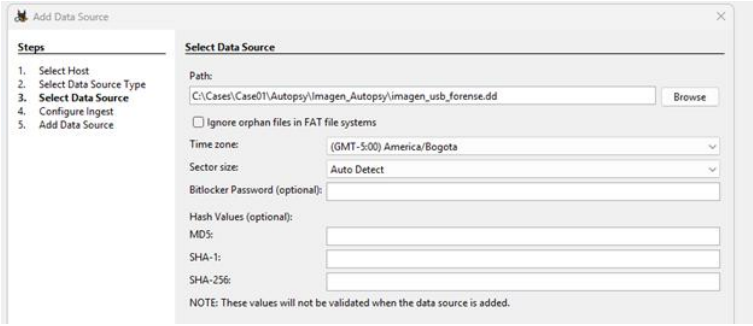
imagenes 24 archivo forense

En este paso se muestra la ventana del explorador de archivos de Autopsy, donde se selecciona la imagen forense que será analizada.
El archivo escogido es imagen_usb_forense.dd, el cual representa una copia exacta (bit a bit) de un dispositivo USB u otro medio de almacenamiento digital.



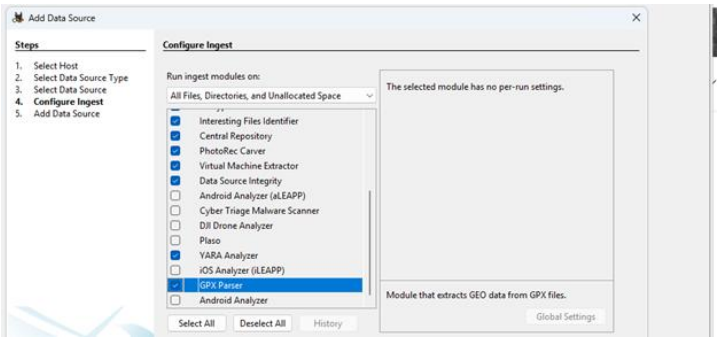
imagenes 25 selecion de la imagen forense

En este paso se observa la ventana de selección de la fuente de datos en Autopsy, donde se configura la imagen forense que será analizada.
Aquí se especifica la ruta del archivo (imagen_usb_forense.dd), la zona horaria (en este caso, GMT-5:00 América/Bogotá), el tamaño del sector y los valores hash opcionales (MD5, SHA-1, SHA-256), que sirven para verificar la integridad de la evidencia.



imagenes 26 configuracion de la imagen forense

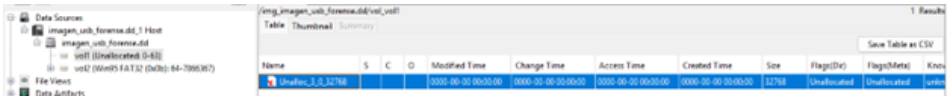
En este paso se aprecia la ventana de configuración de módulos de análisis (Ingest Modules) en Autopsy, correspondiente a una fase clave del proceso forense.
Aquí el usuario puede seleccionar qué módulos se ejecutarán sobre la imagen forense, como el análisis de archivos interesantes, metadatos EXIF, base de datos central, escáner de malware, o análisis GPS, entre otros.



imagenes 27 configuracion de módulos de análisis

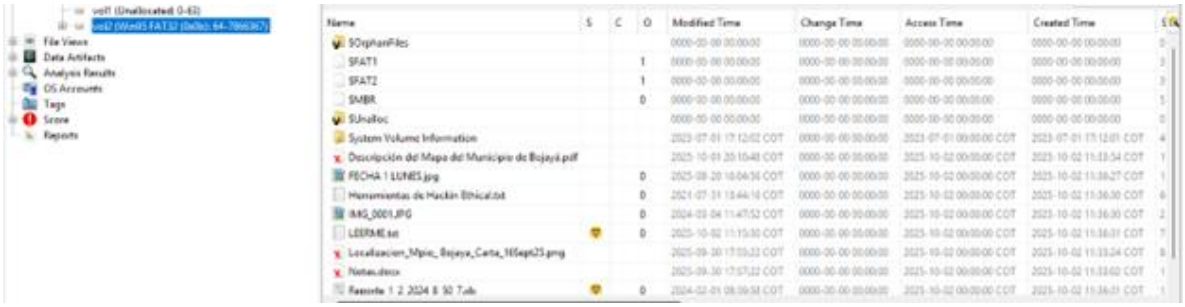
en este paso se muestra una interfaz de análisis que parece pertenecer a un visor de registros o cliente de correo electrónico, centrado en el directorio "megan.smith.framework". En el panel derecho se observa una tabla con información técnica sobre componentes del sistema, destacando una entrada con estado bloqueado (ícono rojo), método de entrada tipo DLL, y fecha de modificación 28 de marzo de 2023.

Esta información sugiere la detección de un posible componente sospechoso o alterado, lo cual es relevante en investigaciones de seguridad informática o auditorías forenses.



imagenes 28 visor de registros

en este paso se muestra una vista del directorio de archivos dentro de un entorno de análisis forense digital. Se ha accedido a la carpeta usr/Downloads/4-01, donde se listan múltiples archivos relevantes, como imágenes, documentos técnicos y mapas. Cada archivo incluye campos de metadatos como fecha de modificación, acceso, creación y cambio. Sin embargo, todos los valores aparecen en ceros, lo que sugiere que los metadatos podrían estar corruptos o no disponibles, una situación común cuando se trabaja con copias forenses o sistemas alterados. Esta información es clave para reconstruir la actividad del usuario y validar la integridad de los archivos.



imagenes 29 directorio de archivos

en este paso se muestra una tabla de análisis forense correspondiente al dispositivo USB examinado, específicamente en la ruta /img_imagen_usb_forense.dd/vol_vol2. Se presentan columnas clave como Flags, MD5 Hash, SHA-256 Hash, y MIME Type, que permiten identificar el estado de asignación de los archivos (por ejemplo, asignado o no asignado), verificar su integridad mediante valores hash, y clasificar su tipo de contenido (imagen, texto, binario, etc.). Esta información es esencial para validar la autenticidad de los archivos y detectar posibles manipulaciones o archivos ocultos durante una investigación digital.

Flags(Dir)	Flags(Meta)	Known	MD5 Hash	SHA-256 Hash	MIME Type
Allocated	Allocated	unknown			
Allocated	Allocated	unknown	045776a6163054651fbeba5678fa4285	419a9a5c1dac6a0f4db417356f7163b901e86b153c17d4c...	application/octet-stream
Allocated	Allocated	unknown	045776a6163054651fbeba5678fa4285	419a9a5c1dac6a0f4db417356f7163b901e86b153c17d4c...	application/octet-stream
Allocated	Allocated	unknown	eb86354b83081752a48f29b9389066ac	0e59571558b820da819707e655c64705c46520819fc6ef45...	application/octet-stream
Allocated	Allocated	unknown			
Allocated	Allocated	unknown			
Unallocated	Unallocated	unknown	cd33588981ec9d8818c5a6c47cffed1a	a9a71fb7c26b754e390333a8ddc68fa0a73aeb00f015cde...	application/octet-stream
Allocated	Allocated	unknown	ea932dcfa9d3e5da55226d6af80b8cca	d3a70ec7ee03da5b5bf1ce1f49a288c994883d7d2476c6a...	image/jpeg
Allocated	Allocated	unknown	eac22b31d295505cb44e36eb917a1903	55ce69c3839d4b764168702ee933234c0cf9eb7cec57f1a4...	text/plain
Allocated	Allocated	unknown	376a1395caa06a5101d76d4816f134a5	8da775a7590f67e65df38c64e45166531563ef09e2dcac0e...	image/jpeg
Allocated	Allocated	unknown	3381949f3eedcd5c2b6d39e86fd48984	572d315a03649417fb289aed6b425d8a5af346f70e404519...	text/plain
Unallocated	Unallocated	unknown	232de1b6ec01ee8b407175684fba12e6	5b1a6bc2b627fb6a81364cafec91d1a8f43569cdcec7c50...	application/octet-stream

imagenes 30 tabla de análisis forense

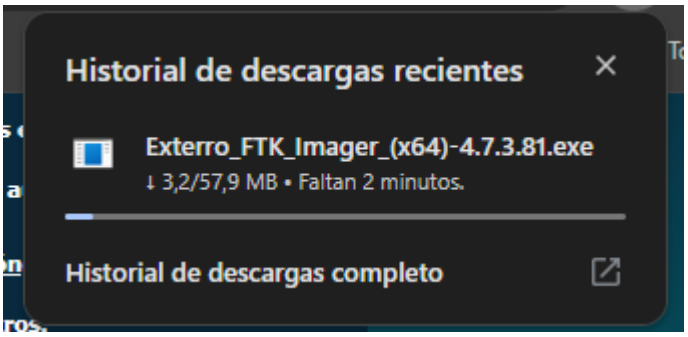
CAPITULO#3 AUTORIA FORENSE CON FTK IMAGER EN WINDOWS

Descarga de la herramienta ftk imager

Requisitos para la descarga

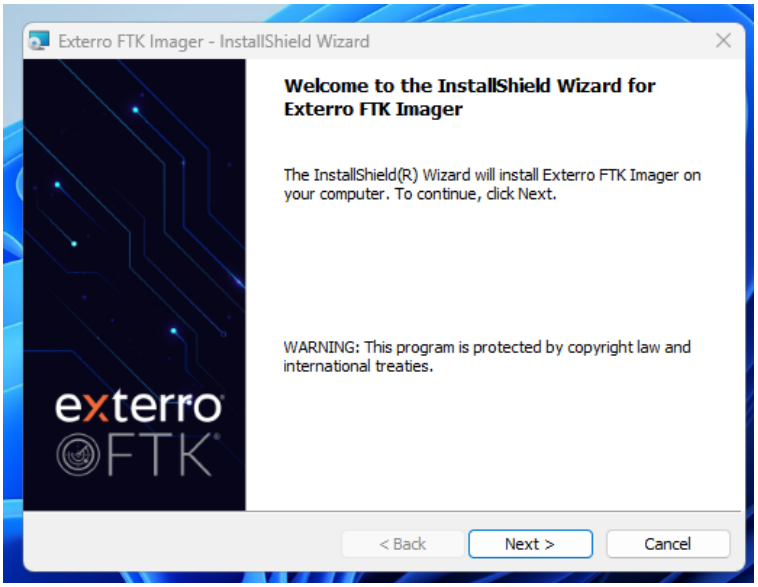
imagenes 31 requisitos para la descarga de FTK

Descarga de la herramienta



imagenes 32 descarga de FTK

Instalacion de la herramienta FTK IMAGER

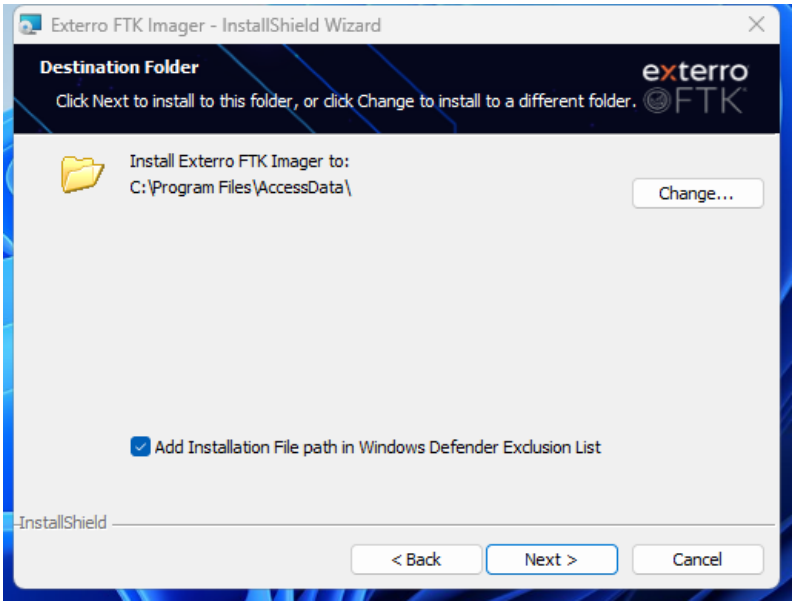


imagenes 33 instalacion de FTK

Aceptación de la licencia

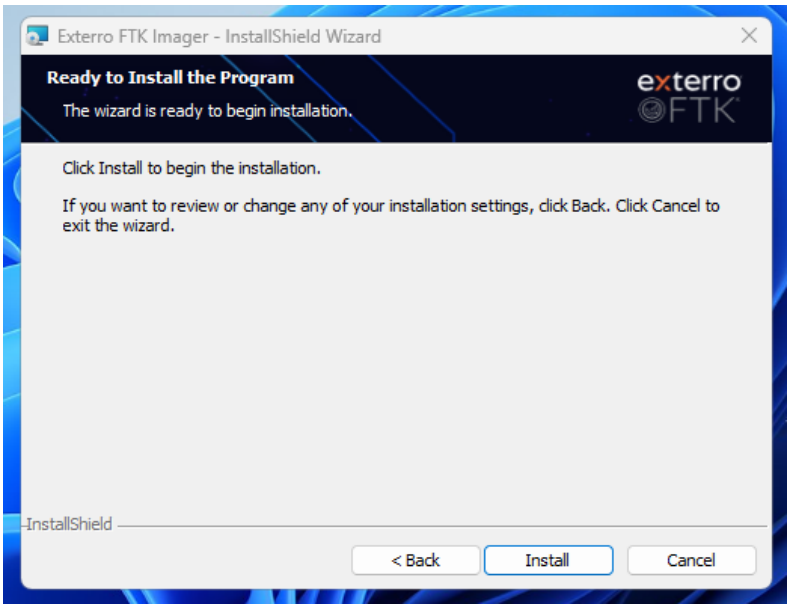
imagenes 34 aceptación de licencia

Se eligió la ruta predeterminada para instalar el programa.



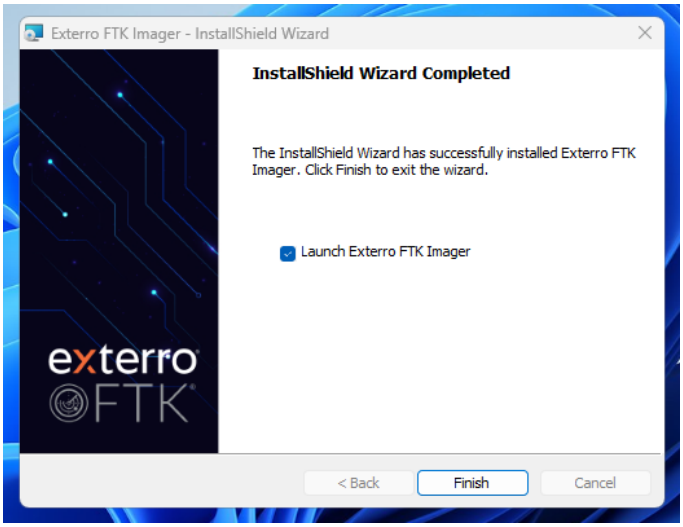
imagenes 35 elección de ruta

El asistente de instalación muestra que todo está listo para comenzar la instalación del programa Exterro FTK Imager.



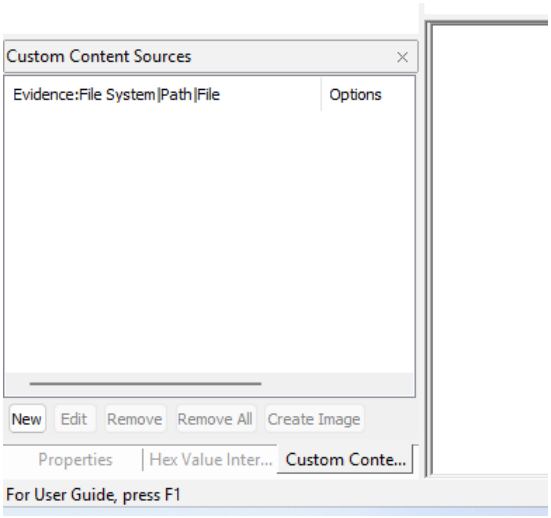
imagenes 36 inicio de instalacion de FTK

Finalizacion de la instalacion



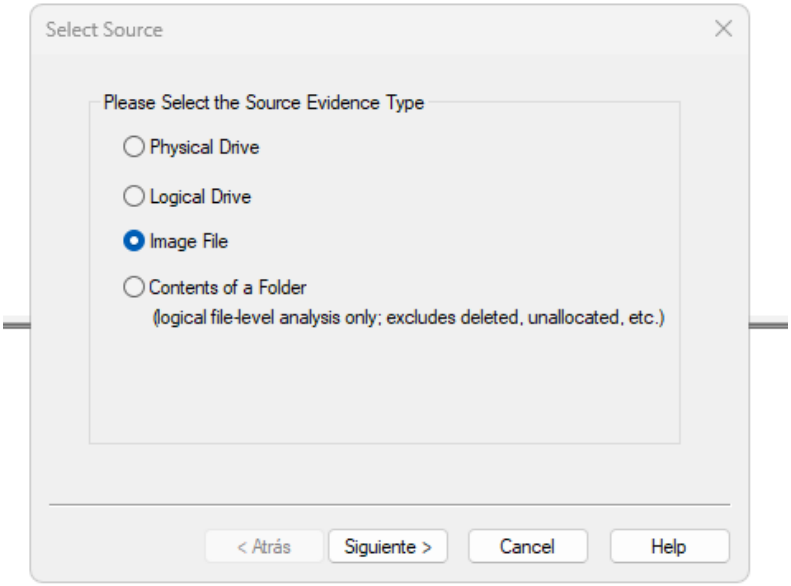
imagenes 37 finalizacion de instalacion

Dentro del entorno del software, se añadió una fuente personalizada de contenido tipo “File SystemPathFile”, lo que permite trabajar con archivos específicos del sistema como evidencia digital. Se habilitaron funciones para editar, eliminar y generar imágenes forenses a partir de estas fuentes.



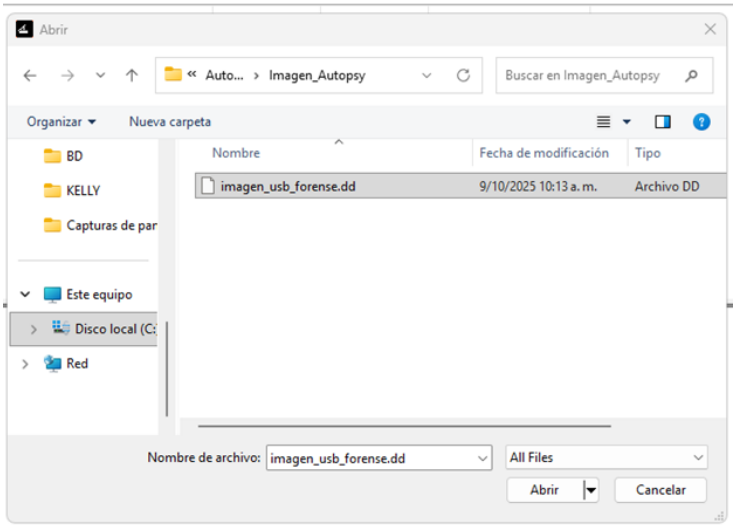
imagenes 38 fuente de personalización

se accedió a la ventana Select Source, donde se seleccionó la opción Image File como fuente de evidencia. Esta elección permite trabajar con imágenes forenses previamente generadas, facilitando el análisis sin necesidad de acceder directamente a discos físicos o lógicos.



imagenes 39 ventana Select source

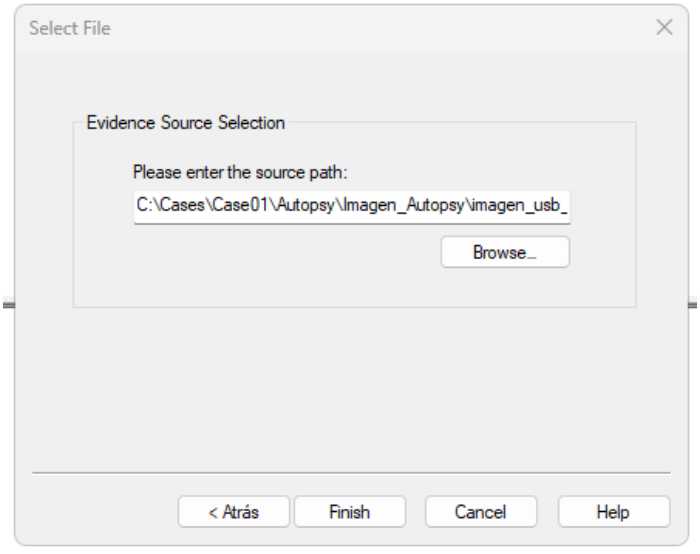
Se seleccionó el archivo desde la carpeta “Imagen_Autopsy”. Este archivo corresponde a una imagen forense en formato DD, lista para ser analizada dentro del entorno del software.



imagenes 40 selecion del archivo

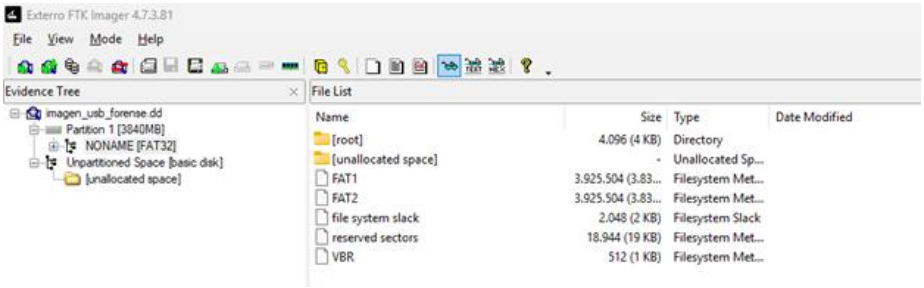
Se ingresó manualmente la ruta de acceso al archivo de evidencia:

Este paso permite al software localizar y preparar el archivo para su análisis, asegurando que se trabaje con la evidencia correcta.



imagenes 41 ingreso a la ruta

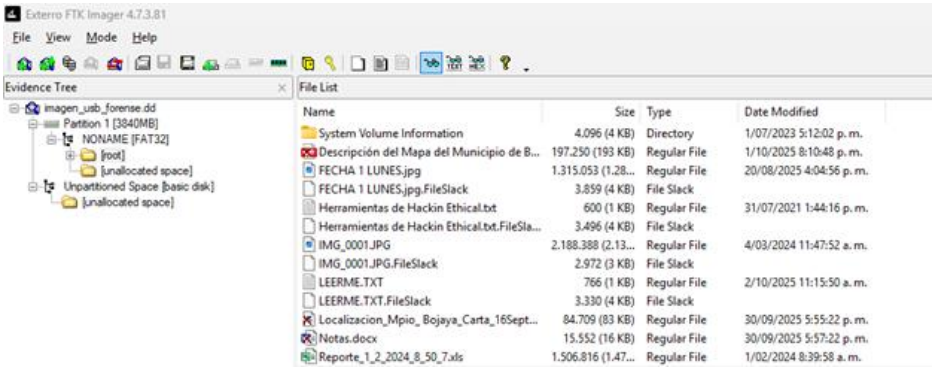
Se cargó el archivo en FTK Imager, visualizando su estructura interna. En el panel de evidencia se identificó una partición FAT32 con espacio no particionado y áreas no asignadas. El panel de archivos mostró metadatos del sistema de archivos, sectores reservados, espacio slack y directorios raíz, elementos clave para el análisis forense.



imagenes 42 visualización del archivo

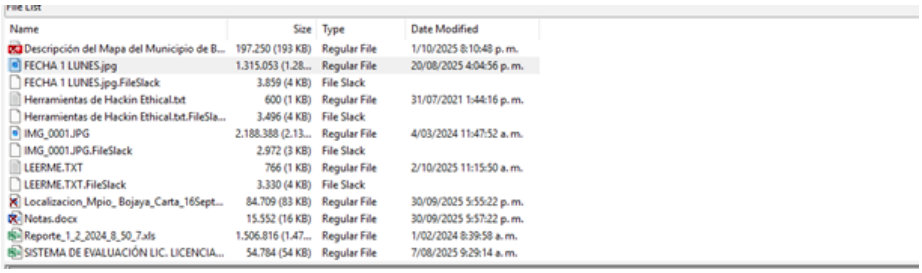
Se examinó la imagen imagen_usb_forense.dd, que contenía una partición activa en formato NTFS. Se accedió a archivos relevantes como:

- Imágenes (IMG_0001.JPG, FECHA 1 LUNES.jpg)
- Documentos (LEEME.TXT, Reporte_1_2_2021_5_0_7.xls)
- Archivos del sistema (System Volume Información)



imagenes 43 examinación de la imagen

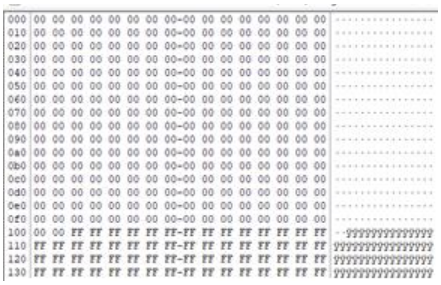
Se accedió a archivos relevantes dentro de la partición NTFS, incluyendo imágenes , documentos y archivos especializados como y , relacionados con herramientas de edición y localización geográfica. Los archivos presentan fechas de modificación que permiten establecer una línea temporal útil para la investigación.



Name	Size	Type	Date Modified
Descripción del Mapa del Municipio de B...	197.250 (193 KB)	Regular File	1/10/2025 8:10:48 p. m.
FECHA 1 LUNES.jpg	1.315.053 (1.28...	Regular File	20/08/2025 4:04:56 p. m.
FECHA 1 LUNES.jpg.FileSlack	3.859 (4 KB)	File Slack	
Herramientas de Hackin Ethical.txt	600 (1 KB)	Regular File	31/07/2021 1:44:16 p. m.
Herramientas de Hackin Ethical.txt.FileSla...	3.496 (4 KB)	File Slack	
IMG_0001.JPG	2.188.388 (2.13...	Regular File	4/03/2024 11:47:52 a. m.
IMG_0001.JPG.FileSlack	2.972 (3 KB)	File Slack	
LEERME.TXT	766 (1 KB)	Regular File	2/10/2025 11:15:50 a. m.
LEERME.TXT.FileSlack	3.330 (4 KB)	File Slack	
Localizacion_Mpio_ Bojaya_Carta_16Sept...	84.709 (83 KB)	Regular File	30/09/2025 5:55:22 p. m.
Notas.docx	15.552 (16 KB)	Regular File	30/09/2025 5:57:22 p. m.
Reporte_1_2_2024_8_50_7.xls	1.506.816 (1.47...	Regular File	1/02/2024 8:39:58 a. m.
SISTEMA DE EVALUACIÓN LIC. LICENCIA...	54.784 (54 KB)	Regular File	7/08/2025 9:29:14 a. m.

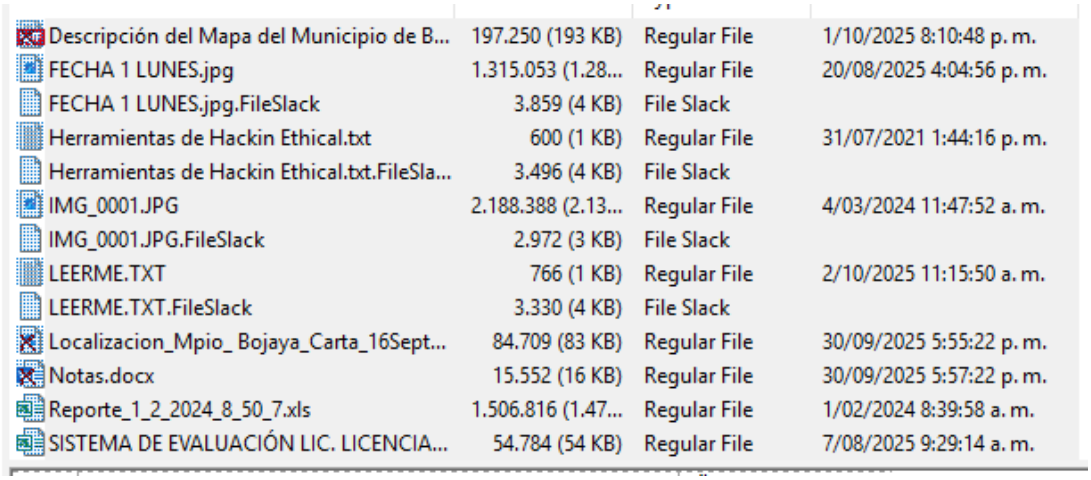
imagenes 44 archivos relevantes

Se examinó el contenido binario de un archivo o segmento de memoria mediante vista hexadecimal. Se observaron bloques de bytes nulos seguidos por valores , cuya representación ASCII corresponde al carácter y análisis permite identificar patrones, delimitadores o posibles estructuras ocultas en el archivo, útiles para tareas de recuperación, validación o detección de manipulación.



imagenes 45 contenido binario

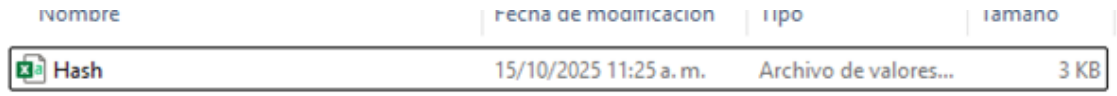
Se inspeccionó un directorio adicional que contenía archivos relacionados con actividades administrativas, técnicas y educativas. Se identificaron imágenes, hojas de cálculo, documentos de texto y archivos de herramientas, con fechas que abarcan desde 2023 hasta 2025.



Descripción del Mapa del Municipio de B...	197.250 (193 KB)	Regular File	1/10/2025 8:10:48 p. m.
FECHA 1 LUNES.jpg	1.315.053 (1.28...	Regular File	20/08/2025 4:04:56 p. m.
FECHA 1 LUNES.jpg.FileSlack	3.859 (4 KB)	File Slack	
Herramientas de Hackin Ethical.txt	600 (1 KB)	Regular File	31/07/2021 1:44:16 p. m.
Herramientas de Hackin Ethical.txt.FileSla...	3.496 (4 KB)	File Slack	
IMG_0001.JPG	2.188.388 (2.13...	Regular File	4/03/2024 11:47:52 a. m.
IMG_0001.JPG.FileSlack	2.972 (3 KB)	File Slack	
LEERME.TXT	766 (1 KB)	Regular File	2/10/2025 11:15:50 a. m.
LEERME.TXT.FileSlack	3.330 (4 KB)	File Slack	
Localizacion_Mpio_ Bojaya_Carta_16Sept...	84.709 (83 KB)	Regular File	30/09/2025 5:55:22 p. m.
Notas.docx	15.552 (16 KB)	Regular File	30/09/2025 5:57:22 p. m.
Reporte_1_2_2024_8_50_7.xls	1.506.816 (1.47...	Regular File	1/02/2024 8:39:58 a. m.
SISTEMA DE EVALUACIÓN LIC. LICENCIA...	54.784 (54 KB)	Regular File	7/08/2025 9:29:14 a. m.

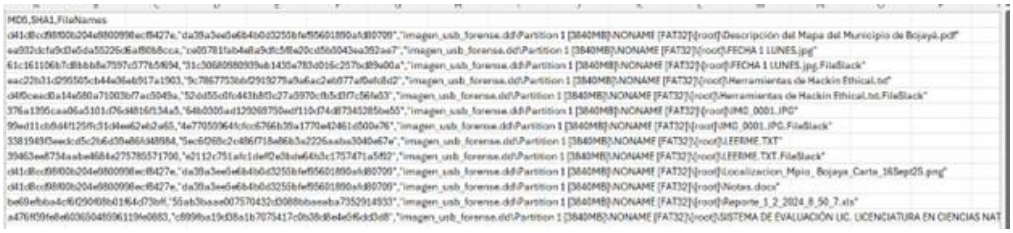
imagenes 46 archivos administrativos

Archivo hash



imagenes 47 archivo hash

Contenido del archivo hash



imagenes 48 contenido del archivo hash

CONCLUSIÓN

A través de la ejecución de este informe, se ha demostrado con éxito la metodología completa para realizar una autoría forense digital utilizando las herramientas Autopsy y FTK Imager en entornos Linux y Windows.

Se estableció un procedimiento forense sólido, iniciando con la etapa crítica de adquisición en Linux. Se utilizó el comando dd para una copia bit a bit y shalsum para generar hashes SHA1 , asegurando así la integridad de la evidencia original y de la imagen creada, un paso fundamental en cualquier investigación.

Se comprobó que tanto **Autopsy** (en ambas plataformas) como **FTK Imager** son capaces de procesar y analizar eficazmente la imagen forense (.dd) generada. Ambas herramientas permitieron la exploración de las particiones (detectando NTFS y FAT32) y la identificación de archivos relevantes, como documentos, imágenes y hojas de cálculo.

El análisis con Autopsy en Windows destacó la capacidad de los módulos de ingesta para procesar datos automáticamente , aunque también reveló anomalías en los metadatos (timestamps en cero), un hallazgo importante. Por su parte, FTK Imager demostró ser una herramienta robusta para la visualización de la estructura del disco y el análisis a bajo nivel, como la vista.