



INFORME DE LABORATORIO 02

INDIRA JOHANA FLÓREZ CÓRDOBA

Estudiante IX

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERIA

INGENIERIA DE TELECOMUNICACIONES E INFORMÁTICA

QUIBDÓ – CHOCÓ

2025



INFORME DE LABORATORIO 02

INDIRA JOHANA FLÓREZ CÓRDOBA

Estudiante IX

RAFAEL SANDOVAL MORALES

Docente

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERIA

INGENIERIA DE TELECOMUNICACIONES E INFORMÁTICA

QUIBDÓ – CHOCÓ

2025



TABLA DE CONTENIDO

1.	INTRODUCCIÓN	8
2.	OBJETIVOS	9
2.1	Objetivo general	9
2.2	Objetivos específicos.....	9
3.	ALCANCE.....	10
4.	CAPITULO 1 – ANALISIS FORENSE CON AUTOPSY EN KALI LINUX.....	11
4.1	Configuración de dispositivos USB en VirtualBox	11
4.2	Identificación de discos con el comando fdisk.....	11
4.3	Generación de hash forense de la memoria USB	12
4.4	Escritorio de Kali Linux con archivo forense	12
4.5	Verificación del hash forense generado	13
4.6	Creación de imagen forense con dd	13
4.7	Verificación de integridad de la imagen forense.....	14
4.8	Propiedades del archivo de imagen forense	14
4.9	Menú de aplicaciones de Kali Linux.....	15
4.10	Inicio de Autopsy desde terminal	16
4.11	Interfaz web de Autopsy Forensic Browser	17
4.12	Creación de nuevo caso forense	17
4.13	Asignación de permisos a la imagen forense.....	20
4.14	Configuración de importación de imagen forense.....	20
4.15	Módulo de análisis de archivos en Autopsy	22
4.16	Cálculo de hash MD5 para verificación de integridad	23



5.	CAPITULO 2 - INSTALACIÓN Y ANALISIS FORENSE CON AUTOPSY EN WINDOWS	25
5.1	Búsqueda en Google de Autopsy para Windows.....	26
5.2	Página oficial de descarga de Autopsy.....	26
5.3	Diálogo de descarga del archivo de instalación	27
5.4	Gestor de descargas del sistema.....	27
5.5	Instalación de Autopsy en Windows.....	28
5.6	Acceso directo de Autopsy en el escritorio.....	30
5.7	Inicio de Autopsy y Carga de Módulos.....	31
5.8	Creación de la carpeta donde se guardará la imagen forense.....	35
5.9	Transferencia de Imagen Forense desde Kali Linux a Windows.....	36
5.10	Selección del Archivo de Imagen Forense	37
6.	CAPITULO 3 – ANALISIS FORENSE CON FTK IMAGER EN WINDOWS...	43
6.1	Búsqueda y Selección de FTK Imager.....	43
6.2	Descarga desde el Sitio Oficial de Exterro.....	43
6.3	Confirmación de Descarga del Instalador	44
6.4	Verificación del Archivo Descargado	44
6.5	Instalación de FTK Imager.....	44
6.6	Inicio de FTK Imager.....	48
7.	CONCLUSIÓN.....	55
8.	BIBLIOGRAFIA	56



TABLA DE ILUSTRACIONES

Ilustración 1. Configuración de dispositivos USB.....	11
Ilustración 2. Identificación de discos.....	12
Ilustración 3. Generación de hash forense	12
Ilustración 4. Archivo hash forense	13
Ilustración 5. Verificación del hash forense generado	13
Ilustración 6. Creación de imagen forense.....	14
Ilustración 7. Verificación de integridad de la imagen forense	14
Ilustración 8. Ver propiedades de la imagen forense	14
Ilustración 9. Propiedades de la imagen forense	15
Ilustración 10. Menú de aplicaciones de Kali Linux.....	15
Ilustración 11. Inicio de Autopsy	16
Ilustración 12. Servicio Autopsy iniciado correctamente	16
Ilustración 13. Interfaz web de Autopsy	17
Ilustración 14. Creación de nuevo caso forense.....	18
Ilustración 15. Confirmación de creación del caso	18
Ilustración 16. Configuración de nuevo host forense	19
Ilustración 17. Host creado exitosamente	19
Ilustración 18. Interfaz de gestión de host sin imágenes.....	20
Ilustración 19. Permisos a la imagen forense.....	20
Ilustración 20. Importando imagen forense	21
Ilustración 21. Detalles de la imagen forense importada	21
Ilustración 22. Confirmación de imagen agregada exitosamente	22
Ilustración 23. Interfaz principal de análisis forense	22
Ilustración 24. Módulo de análisis de archivos en Autopsy.....	23
Ilustración 25. Análisis detallado de archivos	23
Ilustración 26. Interfaz principal de gestión de volúmenes en Autopsy	24
Ilustración 27. Cálculo de hash MD5.....	24
Ilustración 28. Hash MD5 calculado y almacenado exitosamente	24
Ilustración 29. Generar listas MD5 de archivos.....	25
Ilustración 30. Hashes MD5 de archivos específicos recuperados	25



Ilustración 31. Búsqueda del Software	26
Ilustración 32. Descarga desde la Página Oficial.....	26
Ilustración 33. Confirmación de Descarga.....	27
Ilustración 34. Verificación del Archivo Descargado.....	27
Ilustración 35. Inicio del Asistente de Instalación	28
Ilustración 36. Selección de la Carpeta de Destino.....	28
Ilustración 37. Confirmación para Instalar.....	29
Ilustración 38. Proceso de Instalación en Curso	29
Ilustración 39. Finalización de la Instalación.....	30
Ilustración 40. Software Instalado y Accesible.....	30
Ilustración 41. Inicio de Autopsy	31
Ilustración 42. Ventana Principal de Bienvenida.....	31
Ilustración 43. Creación de Nuevo Caso - Información Básica.....	32
Ilustración 44. Navegación para Seleccionar Directorio.....	32
Ilustración 45. Creación de la Carpeta de Análisis Forense.....	33
Ilustración 46. Confirmación de Información del Caso	33
Ilustración 47. Información Opcional del Examinador.....	34
Ilustración 48. Selección de Host para la Fuente de Datos	34
Ilustración 49. Selección del Tipo de Fuente de Datos	35
Ilustración 50. Seleccionar opción para crear la nueva carpeta	35
Ilustración 51. Crear nueva carpeta donde se guardará la imagen de que está en Kali	
Linux.....	36
Ilustración 52. Carpeta "imagen" creada.....	36
Ilustración 53. Transferencia de Imagen Forense desde Máquina Virtual.....	37
Ilustración 54. Selección del Archivo	37
Ilustración 55. Configuración de Parámetros de la Fuente de Datos	38
Ilustración 56. Selección de Módulos de Ingesta.....	38
Ilustración 57. Procesamiento Inicial de la Fuente de Datos	39
Ilustración 58. Finalización de la Adición de Fuente de Datos	39
Ilustración 59. Interfaz Principal de Análisis en Progreso.....	40
Ilustración 60. Estructura de la Fuente de Datos y Volúmenes	40



Ilustración 61. Análisis del Espacio No Asignado (vol1)	41
Ilustración 62. Contenido del Sistema de Archivos FAT32 (vol2).....	41
Ilustración 63. Vista Expandida de Archivos.....	42
Ilustración 64. Análisis de Hashes y Tipos MIME	42
Ilustración 65. Búsqueda en Google de FTK Imager.....	43
Ilustración 66. Formulario de descarga.....	43
Ilustración 67. Confirmación de descarga de FTK Imager	44
Ilustración 68. Archivo FTK Imager en la carpeta de descargas	44
Ilustración 69. Instalación de FTK Imager	45
Ilustración 70. Aceptación del Acuerdo de Licencia	45
Ilustración 71. Selección de Carpeta de Destino.....	46
Ilustración 72. Confirmación Final antes de la Instalación.....	46
Ilustración 73. Progreso de la Instalación	47
Ilustración 74. Finalización Exitosa de la Instalación.....	47
Ilustración 75. Interfaz Principal de FTK Imager	48
Ilustración 76. Selección del Tipo de Fuente de Evidencia	48
Ilustración 77. Navegación para Seleccionar Archivo de Imagen	49
Ilustración 78. Verificación de la Ruta de la Imagen Forense	49
Ilustración 79. Confirmación de la Ruta de la Imagen Forense.....	50
Ilustración 80. Estructura de Particiones de la Imagen	50
Ilustración 81. Contenido del Directorio Raíz FAT32.....	51
Ilustración 82. Análisis Detallado de Archivos	51
Ilustración 83. Lista Completa de Archivos Recuperados	52
Ilustración 84. Exportación de Resultados a CSV	52
Ilustración 85. Configuración de Exportación de Hash	53
Ilustración 86. Verificación del Archivo de Hash Exportado	53
Ilustración 87. Archivo hash	54



1. INTRODUCCIÓN

En este laboratorio se abordó la aplicación práctica de herramientas forenses especializadas como Autopsy y FTK Imager, ejecutadas tanto en entornos Kali Linux como Windows, con el fin de comprender los procedimientos de creación y verificación de imágenes forenses, así como la integridad de los datos mediante el uso de algoritmos hash.



2. OBJETIVOS

2.1 Objetivo general

Realizar el análisis forense de una memoria USB utilizando las herramientas Autopsy y FTK Imager en los sistemas operativos Kali Linux y Windows

2.2 Objetivos específicos

- Configurar el dispositivo USB dentro de VirtualBox para la captura y análisis forense.
- Generar y verificar los valores hash de la evidencia digital para asegurar su autenticidad e integridad.
- Crear una imagen forense bit a bit de la memoria USB empleando comandos de Kali Linux.
- Instalar e importar la imagen forense utilizando Autopsy.
- Instalar y ejecutar FTK Imager en Windows para examinar la misma evidencia.



3. ALCANCE

El presente informe abarca el proceso completo de análisis forense digital aplicado a una memoria USB, desde la configuración inicial del entorno virtual hasta la verificación final de los valores hash de los archivos examinados. Las actividades se desarrollan en dos sistemas operativos distintos los cuales son Kali Linux y Windows.

El alcance de esta práctica se limita a la fase de adquisición, preservación y análisis básico de evidencias digitales.



4. CAPITULO 1 – ANALISIS FORENSE CON AUTOPSY EN KALI LINUX

4.1 Configuración de dispositivos USB en VirtualBox

En el menú de dispositivos de VirtualBox, luego USB seleccionar el dispositivo "Generic Flash Card Reader/Writer" la cual es el nombre de nuestra memoria USB insertada (el nombre puede variar), esto permite que la memoria esté disponible dentro de la máquina virtual Kali Linux para el análisis forense.

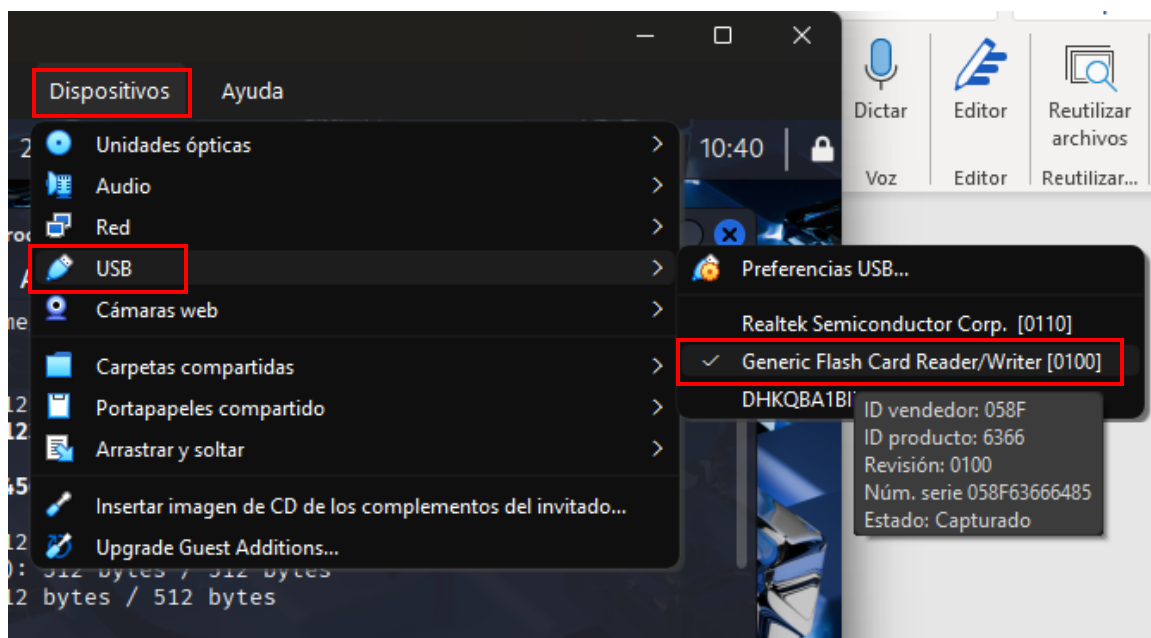


Ilustración 1. Configuración de dispositivos USB

4.2 Identificación de discos con el comando fdisk

En la terminal de Kali Linux ingresar al modo superusuario y luego ejecutar el comando **fdisk -l** para listar los discos disponibles. Se identifican dos dispositivos: **/dev/sda** (disco principal del sistema) y **/dev/sdb** (memoria USB de 3.75 GB conectada).



```
(brasil123@kali)-[~]
$ sudo su
[sudo] contraseña para brasil123:
(brasil123@kali)-[/home/brasil123]
# fdisk -l
Disk /dev/sda: 25 GiB, 26843545600 bytes, 52428800 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x0707ed0f

Device      Boot    Start        End    Sectors    Size Id Type
/dev/sda1   *          2048    49641471   49639424   23,7G 83 Linux
/dev/sda2             49643518   52426751    2783234    1,3G  f W95 Ext'd (LBA)
/dev/sda5             49643520   52426751    2783232    1,3G 82 Linux swap / Solaris

Disk /dev/sdb: 3,75 GiB, 4026531840 bytes, 7864320 sectors
Disk model: Card Reader
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x00000000
```

Ilustración 2. Identificación de discos

4.3 Generación de hash forense de la memoria USB

Con el comando `shasum /dev/sdb > /home/brasil123/Escritorio/hash_forense.sha1` se calcula y guarda el hash SHA1 de toda la memoria USB en un archivo.

```
(root@kali)-[/home/brasil123]
# shasum /dev/sdb > /home/brasil123/Escritorio/hash_forense.sha1
```

Ilustración 3. Generación de hash forense

4.4 Escritorio de Kali Linux con archivo forense

Vista del escritorio de Kali Linux mostrando el archivo generado durante el proceso forense.

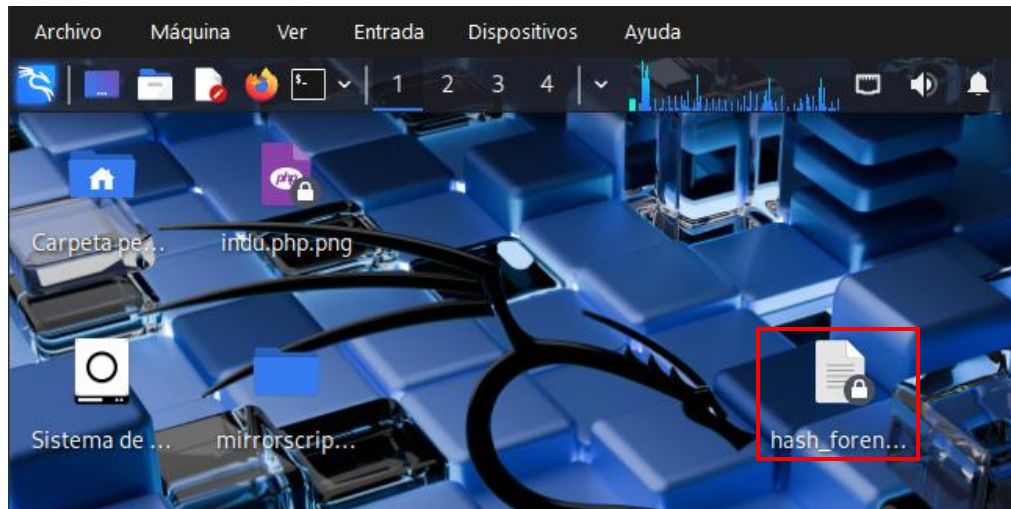


Ilustración 4. Archivo hash forense

4.5 Verificación del hash forense generado

Contenido del archivo **hash_forense.sha1** mostrando el hash SHA1 de la memoria USB, que servirá para verificar la integridad de la evidencia.

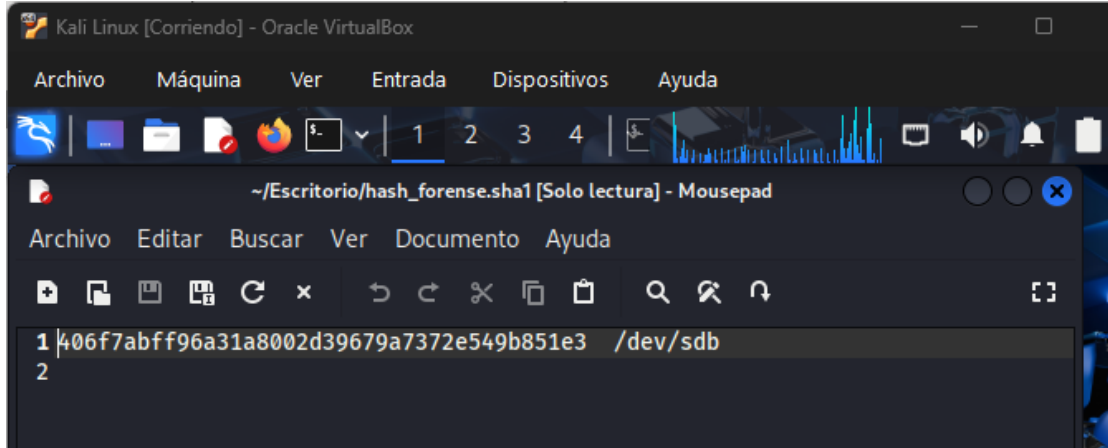


Ilustración 5. Verificación del hash forense generado

4.6 Creación de imagen forense con dd

Ejecutar **dd if=/dev/sdb of=/home/brasil123/Escritorio/imagen_usb_forense.dd** comando que crea una imagen forense bit-a-bit de toda la memoria USB.



```
(root@kali)-[/home/brasil123]
# dd if=/dev/sdb of=/home/brasil123/Escritorio/imagen_usb_forense.dd conv=noer
ror, sync
7864320+0 records in
7864320+0 records out
4026531840 bytes (4,0 GB, 3,8 GiB) copied, 945,278 s, 4,3 MB/s
```

Ilustración 6. Creación de imagen forense

4.7 Verificación de integridad de la imagen forense

Usamos el comando **shasum** a la imagen forense creada, confirmando que el hash SHA1 coincide exactamente con el original, validando la integridad de la imagen durante el proceso de análisis.

```
(root@kali)-[/home/brasil123]
# sha1sum /home/brasil123/Escritorio/imagen_usb_forense.dd
406f7abff96a31a8002d39679a7372e549b851e3 /home/brasil123/Escritorio/imagen_usb_f
orense.dd
```

Ilustración 7. Verificación de integridad de la imagen forense

4.8 Propiedades del archivo de imagen forense

Haciendo clic derecho se pueden ver las opciones disponibles para el archivo de imagen forense, incluyendo ver propiedades.

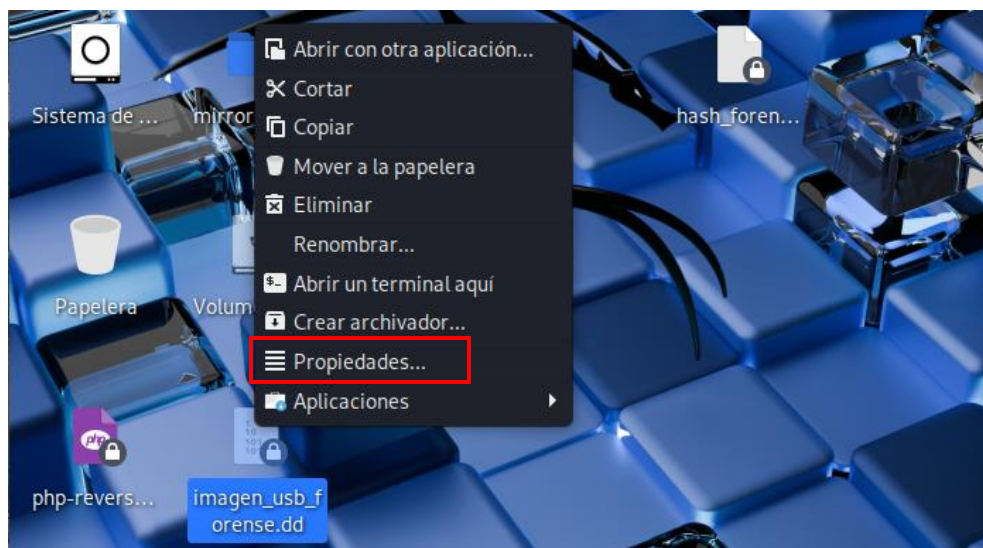


Ilustración 8. Ver propiedades de la imagen forense



Ventana de propiedades del archivo **imagen_usb_forense.dd** mostrando que tiene un tamaño de 3.8 GB, confirmando que se capturó completamente el contenido de la memoria USB.

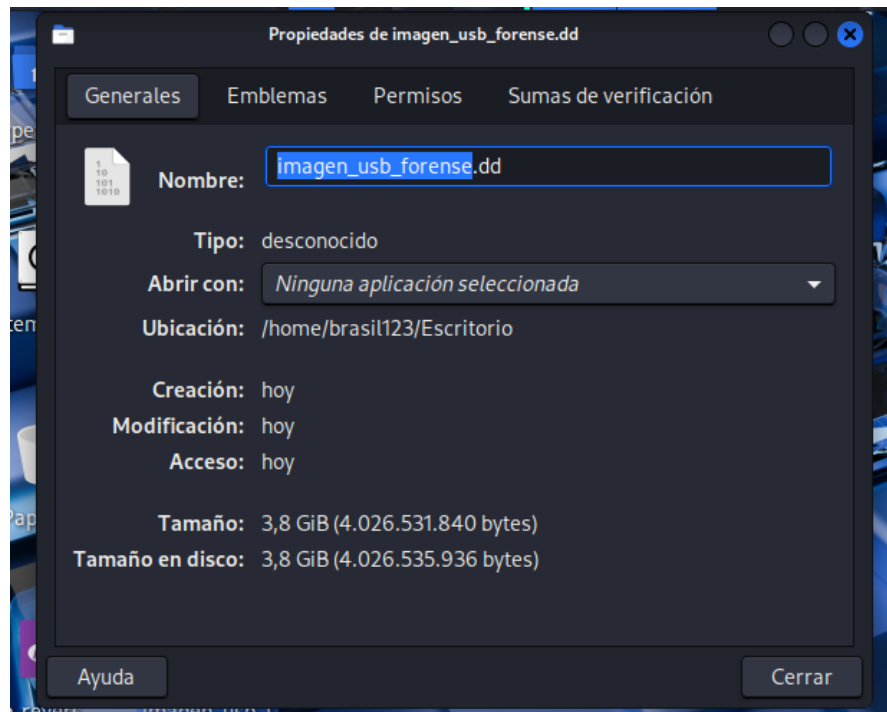


Ilustración 9. Propiedades de la imagen forense

4.9 Menú de aplicaciones de Kali Linux

En el menú de aplicaciones de Kali Linux buscar Autopsy, que será utilizada para el análisis de la evidencia.

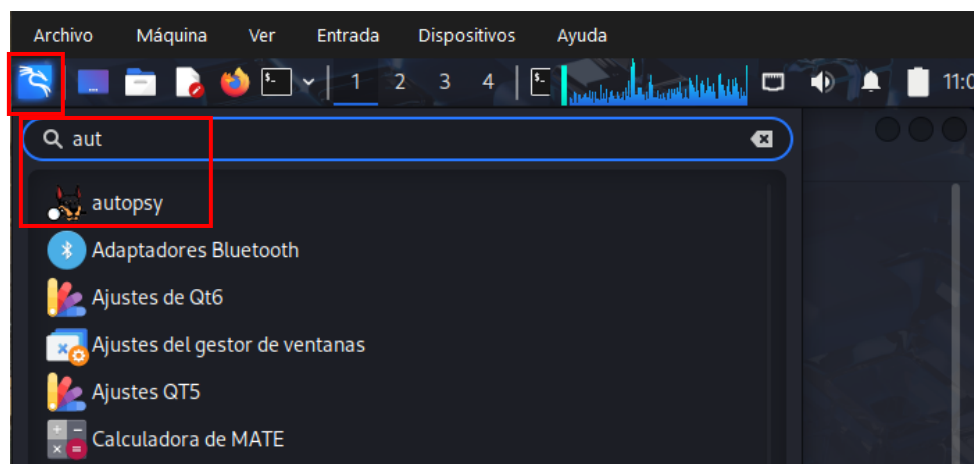


Ilustración 10. Menú de aplicaciones de Kali Linux



4.10 Inicio de Autopsy desde terminal

Terminal de Kali Linux mostrando la ejecución del comando **sudo autopsy** para iniciar la herramienta de análisis forense Autopsy. Posteriormente ingresar la contraseña de nuestro Kali.

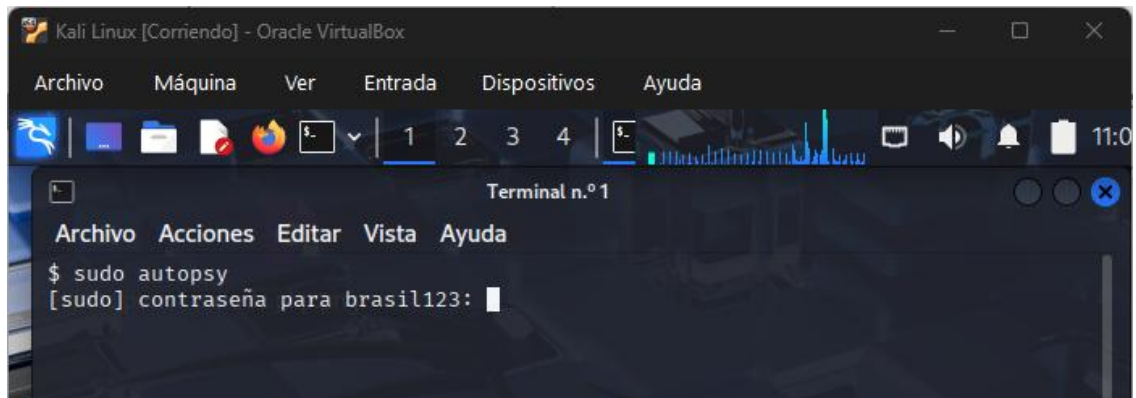


Ilustración 11. Inicio de Autopsy

Confirmación de que el servicio Autopsy se ha iniciado correctamente en el puerto 9999, proporcionando la URL **http://localhost:9999/autopsy** para acceder a la interfaz web.

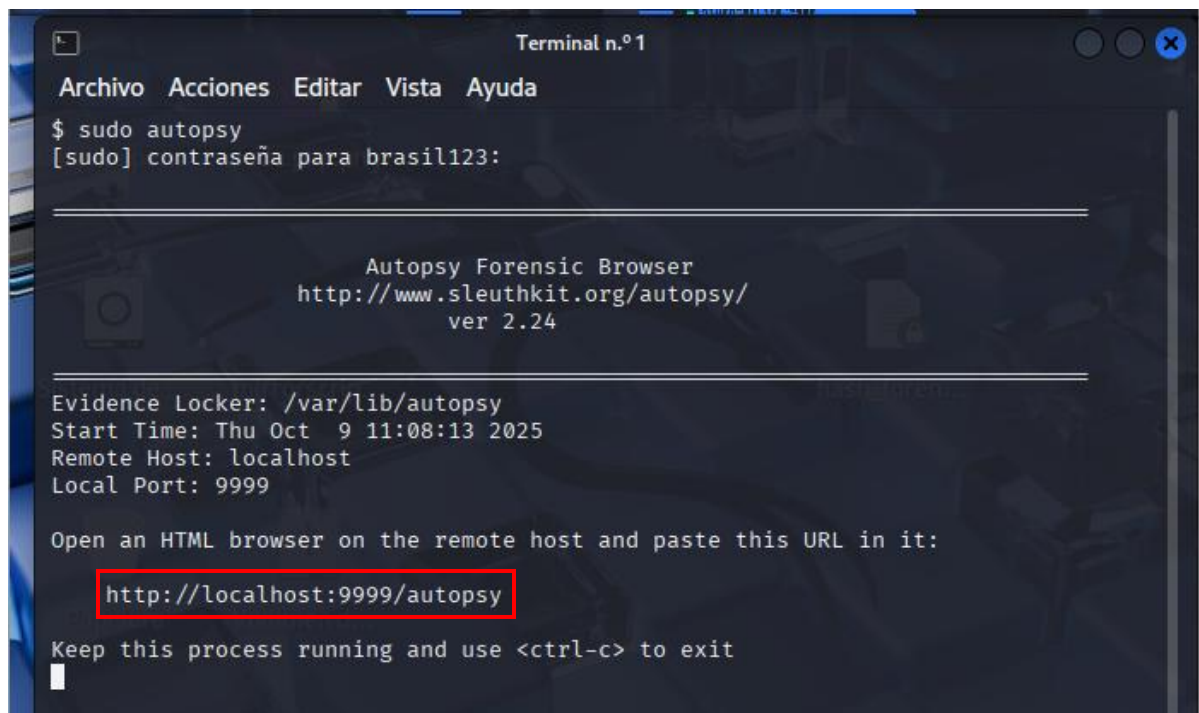


Ilustración 12. Servicio Autopsy iniciado correctamente



4.11 Interfaz web de Autopsy Forensic Browser

En el navegador de Kali Linux ingresamos la URL que nos proporcionó el servicio de Autopsy. Una vez hecho podemos ver la pantalla de advertencia inicial de Autopsy sobre JavaScript, seguida de la pantalla principal de la herramienta forense lista para comenzar el análisis haciendo clic en el link http que se muestra abajo del dibujo.

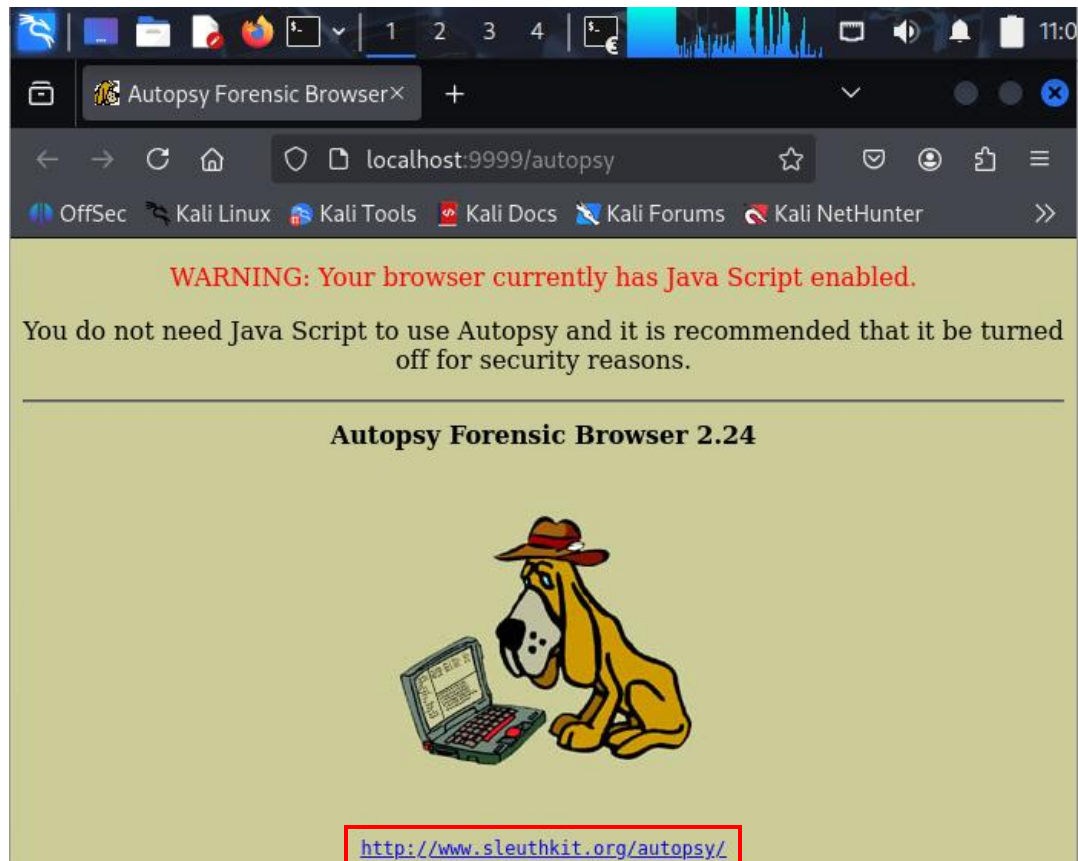


Ilustración 13. Interfaz web de Autopsy

4.12 Creación de nuevo caso forense

Ahora veremos un formulario para crear un nuevo caso forense, le pondremos el nombre de "miPrimerCaso1" con descripción "Análisis Forense USB Clase" y los investigadores Indira_Florez y Rosa_Elvira. Una vez llenados los campos damos clic en “**New Case**”.



CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. Indira_Florez	b. Rosa_Elvira
c.	d.
e.	f.
g.	h.
i.	j.

NEW CASE **CANCEL** **HELP**

Ilustración 14. Creación de nuevo caso forense

Mensaje de confirmación de que el caso "**miPrimerCaso1**" ha sido creado exitosamente, procediendo a la creación del host para el análisis haciendo clic en "**Add Host**".

Creating Case: miPrimerC

localhost:9999/autopsy?mod=0

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali Net

Creating Case: miPrimerCaso1

Case directory (/var/lib/autopsy/miPrimerCaso1/) created
Configuration file (/var/lib/autopsy/miPrimerCaso1/case.aut) created

We must now create a host for this case.

Please select your name from the list:

ADD HOST

Ilustración 15. Confirmación de creación del caso



Formulario para agregar un nuevo host el cual llevará el nombre de "MVKaliPIT11" con descripción "Portatil_HP" que representará el sistema bajo investigación.

ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

2. **Description:** An optional one-line description or note about this computer.

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

Ilustración 16. Configuración de nuevo host forense

Confirmación de que el host "MVKaliPIT11" ha sido agregado al caso, procediendo a importar la imagen forense para análisis haciendo clic en “Add Image”.

Adding host: MVKaliPIT11 to case miPrimerCaso1

Host Directory (/var/lib/autopsy/miPrimerCaso1/MVKaliPIT11/) created

Configuration file (/var/lib/autopsy/miPrimerCaso1/MVKaliPIT11/host.aut) created

We must now import an image file for this host

ADD IMAGE

Ilustración 17. Host creado exitosamente



Pantalla del host recién creado mostrando que no hay imágenes agregadas aún, hacemos clic en el botón "**ADD IMAGE FILE**" para importar la evidencia.

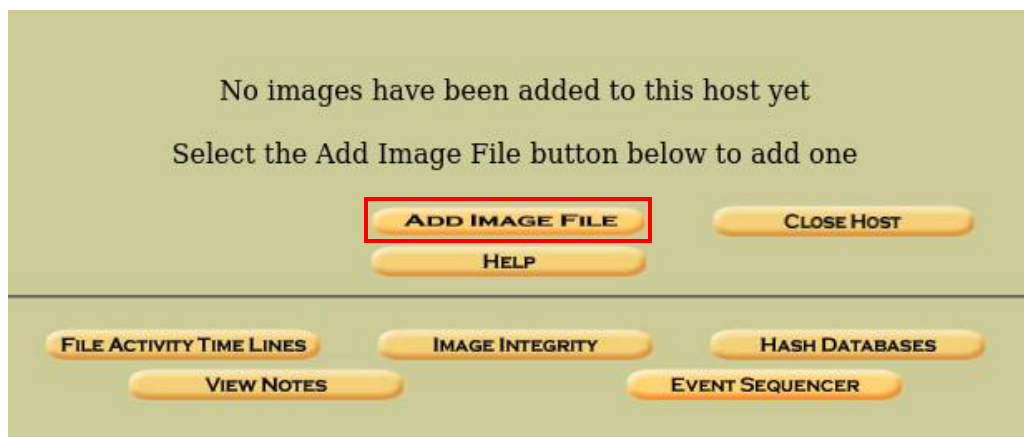


Ilustración 18. Interfaz de gestión de host sin imágenes

4.13 Asignación de permisos a la imagen forense

En una nueva terminal de Kali Linux en el modo superusuario ejecutamos el comando **chmod 777** sobre la imagen forense para asegurar que Autopsy tenga los permisos necesarios para acceder al archivo.

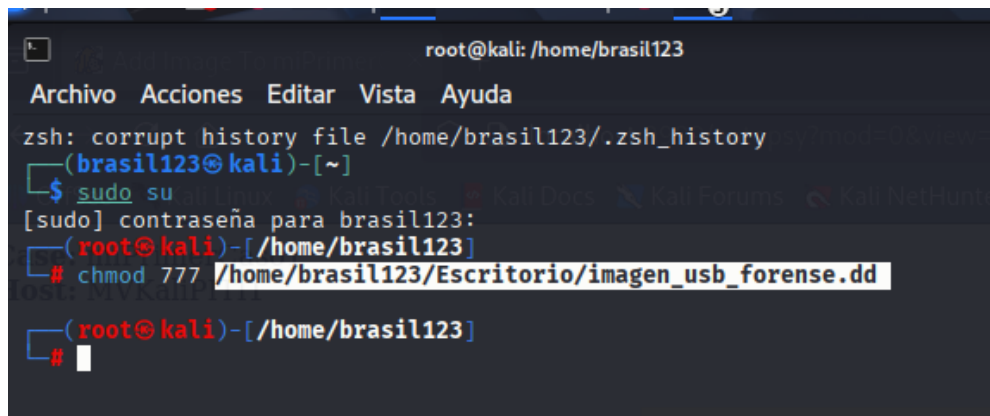


Ilustración 19. Permisos a la imagen forense

4.14 Configuración de importación de imagen forense

Formulario de Autopsy para importar la imagen forense, especificando la ruta de la imagen, seleccionando tipo "Disk" y método "Symlink". Luego damos clic en "Next".



1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

/home/brasil123/Escritorio/imagen_usb_forense.dd

2. Type
Please select if this image file is for a disk or a single partition.

☒ Disk ☐ Partition

3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

☒ Symlink ☐ Copy ☐ Move

NEXT

CANCEL **HELP**

Ilustración 20. Importando imagen forense

Pantalla que muestra los detalles de la imagen importada, incluyendo la partición FAT32 identificada y el rango de sectores (32 to 7864319). Luego hacemos clic en “Add”.

Image File Details

Local Name: images/imagen_usb_forense.dd

Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

☒ Ignore the hash value for this image.

☐ Calculate the hash value for this image.

☐ Add the following MD5 hash value for this image:

☐ Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: Win95 FAT32 (0x0c))

Sector Range: 32 to 7864319

Mount Point: C: File System Type: fat32

Ilustración 21. Detalles de la imagen forense importada



Mensaje de confirmación de que la imagen forense ha sido agregada exitosamente con ID img1, y los volúmenes correspondientes han sido identificados.

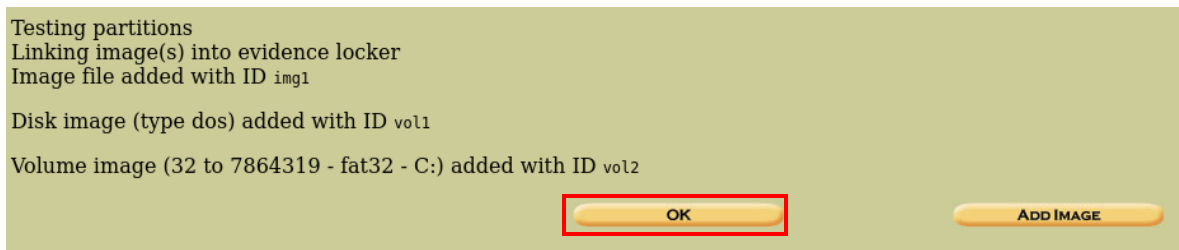


Ilustración 22. Confirmación de imagen agregada exitosamente

4.15 Módulo de análisis de archivos en Autopsy

Pantalla principal de Autopsy mostrando los volúmenes disponibles para análisis: el disco completo y la partición FAT32, listos para ser analizados.

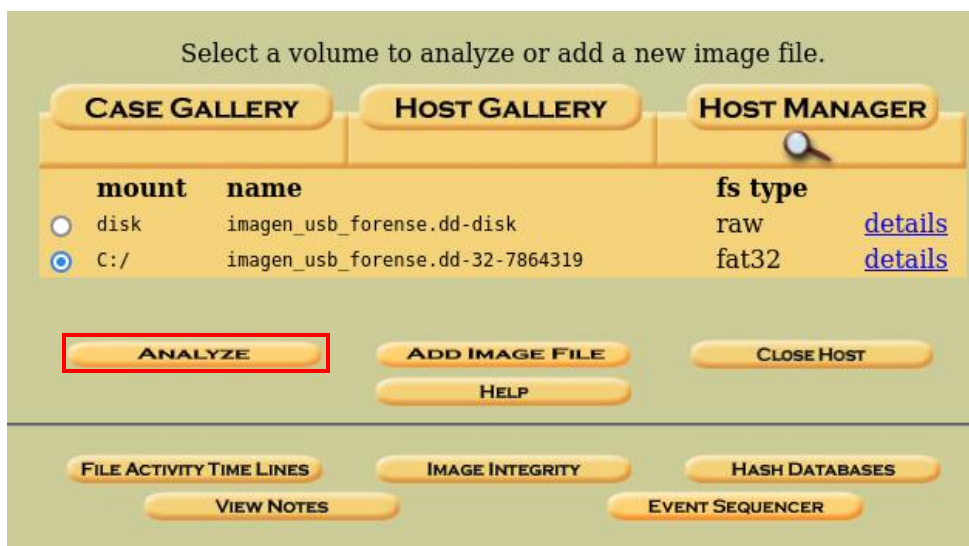


Ilustración 23. Interfaz principal de análisis forense

Esta imagen muestra la interfaz del módulo de Análisis de Archivos (File Analysis), donde se explora el contenido de la memoria USB previamente capturada. Se muestra los archivos recuperados de la imagen forense, también una lista detallada de todos los archivos existentes en la ubicación seleccionada, incluyendo sus nombres, tamaños, fechas de modificación y tipos.



FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE									
Current Directory: C:/									
Add Note GENERATE MDS LIST OF FILES									
DEL	Type	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	dir / in								
Error Parsing File (Invalid Characters?): V/V 125797382: \$OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0									
	v / v	\$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	491520	0	0	125797380
	v / v	\$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	491520	0	0	125797381
	v / v	\$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	125797379
✓	r / r	_magen.jpg	2025-09-05 18:06:20 (-05)	2025-10-02 00:00:00 (-05)	2025-10-02 11:32:45 (-05)	146105	0	0	12
✓	r / r	Articulo.docx	2025-09-17 09:03:14 (-05)	2025-10-02 00:00:00 (-05)	2025-10-02 11:32:37 (-05)	40834	0	0	7
	r / r	FECHA 1 LUNES.jpg	2025-08-20 16:04:56 (-05)	2025-10-02 00:00:00 (-05)	2025-10-02 11:40:21 (-05)	1315053	0	0	21

Ilustración 24. Módulo de análisis de archivos en Autopsy

En la sección inferior, la herramienta muestra una vista previa en miniatura de la imagen seleccionada y proporciona detalles técnicos del tipo de archivo, identificando correctamente el formato JPEG con metadatos EXIF que incluyen información sobre el fabricante (Apple), resolución y software de creación.

FILE ANALYSIS		KEYWORD SEARCH	FILE TYPE	IMAGE DETAILS	META DATA	DATA UNIT	HELP	CLOSE
							?	X
r / r	IMG_0001.JPG		2024-03-04 11:47:52 (-05)	2025-10-02 00:00:00 (-05)	2025-10-02 11:40:21 (-05)	2188388	0	
r / r	IMG_3422.mov		2025-09-28 22:02:56 (-05)	2025-10-02 00:00:00 (-05)	2025-10-02 11:40:22 (-05)	191534405	0	
r / r	ECOCM +v+		2025-10-02	2025-10-02	2025-10-02	766	0	

ASCII ([display](#) - [report](#)) * Hex ([display](#) - [report](#)) * ASCII Strings ([display](#) - [report](#)) * [Export](#) * [View](#) * [Add Note](#)

File Type: JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=12, manufacturer=Apple, model=orientation=upper-right. xresolution=176. yresolution=184. resolutionunit=2. software=15.8.1. datetime=2024:03:04]

C:/IMG_0001.JPG

Thumbnail:

[View Full Size Image](#)

Ilustración 25. Análisis detallado de archivos

4.16 Cálculo de hash MD5 para verificación de integridad

Pantalla principal de Autopsy mostrando los volúmenes disponibles para análisis

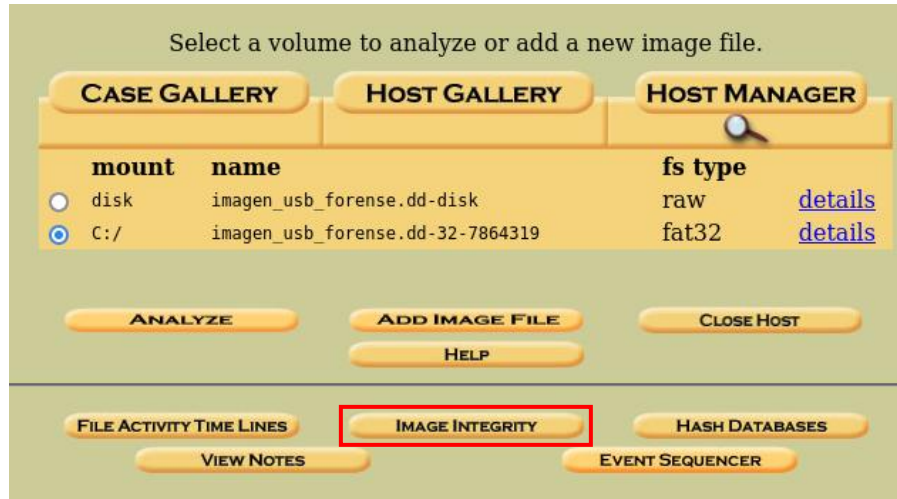


Ilustración 26. Interfaz principal de gestión de volúmenes en Autopsy

Proceso de cálculo de hash MD5 para la imagen forense "**imagen_usb_forense.dd**". Autopsy muestra una ventana de progreso indicando que está realizando el cálculo criptográfico.

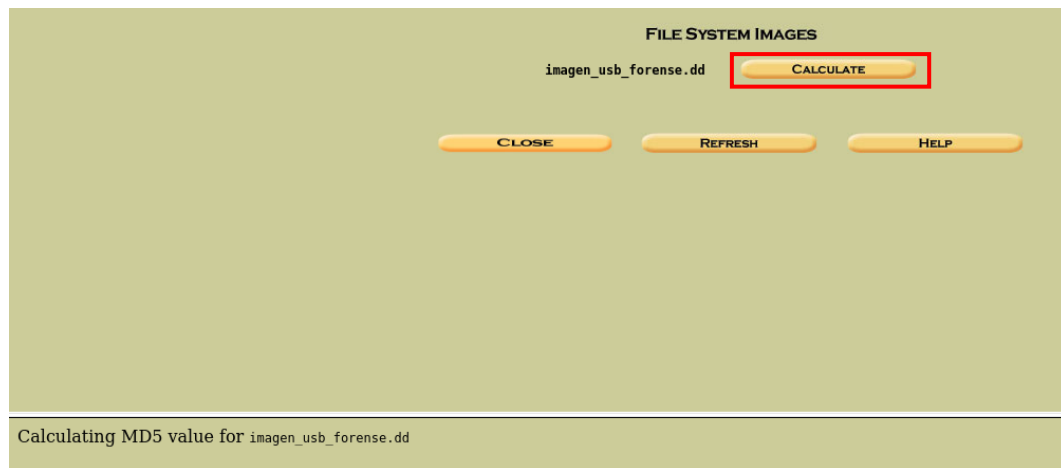


Ilustración 27. Cálculo de hash MD5

Resultado exitoso del cálculo de hash MD5, generando el valor único. El sistema confirma que el hash ha sido guardado en el archivo del host.

```
Calculating MD5 value for imagen_usb_forense.dd
MD5: 8675470A9267E672A4EA039C2838677F

Value saved to host file
```

Ilustración 28. Hash MD5 calculado y almacenado exitosamente



Volvemos a la interfaz del módulo de Análisis de Archivos que tiene la opción para generar listas MD5 de archivos y damos clic en ella.

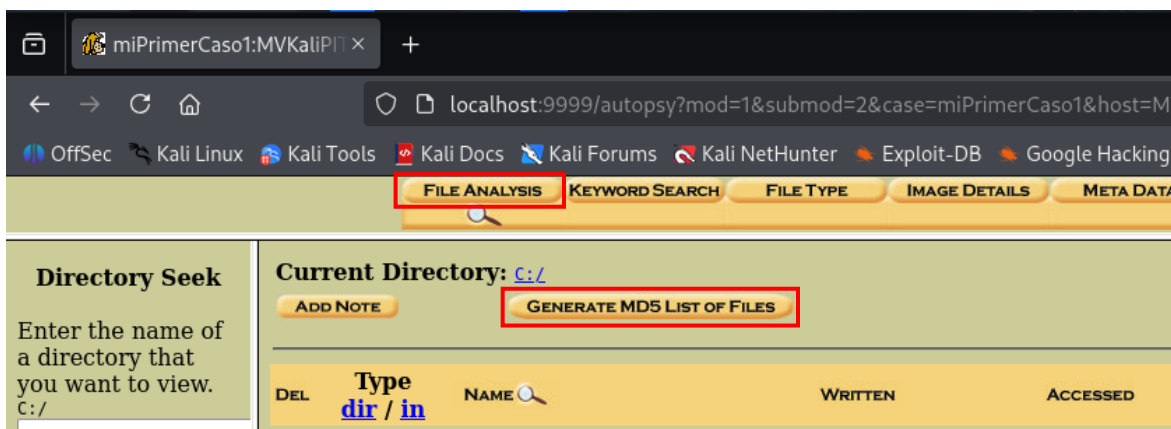


Ilustración 29. Generar listas MD5 de archivos

Resultados de la generación de hashes MD5 para los archivos específicos contenidos en la memoria USB. Se listan los valores hash únicos para cada archivo recuperado, incluyendo documentos importantes y archivos multimedia.

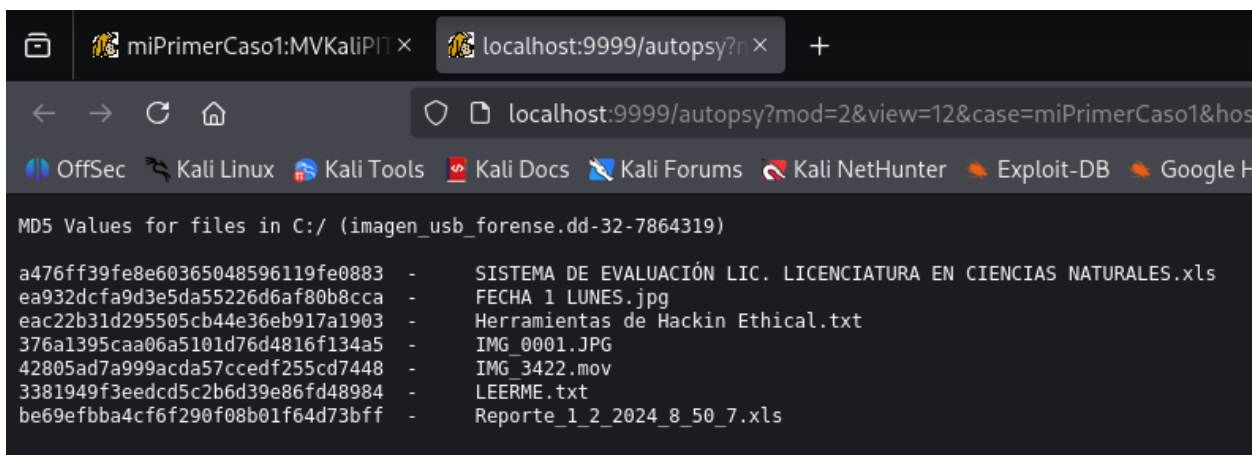


Ilustración 30. Hashes MD5 de archivos específicos recuperados

5. CAPITULO 2 - INSTALACIÓN Y ANALISIS FORENSE CON AUTOPSY EN WINDOWS



5.1 Búsqueda en Google de Autopsy para Windows

Se inició el procedimiento realizando una búsqueda en el navegador web con el término "autopsy win". El resultado principal dirigió a la página oficial de descarga de Autopsy.

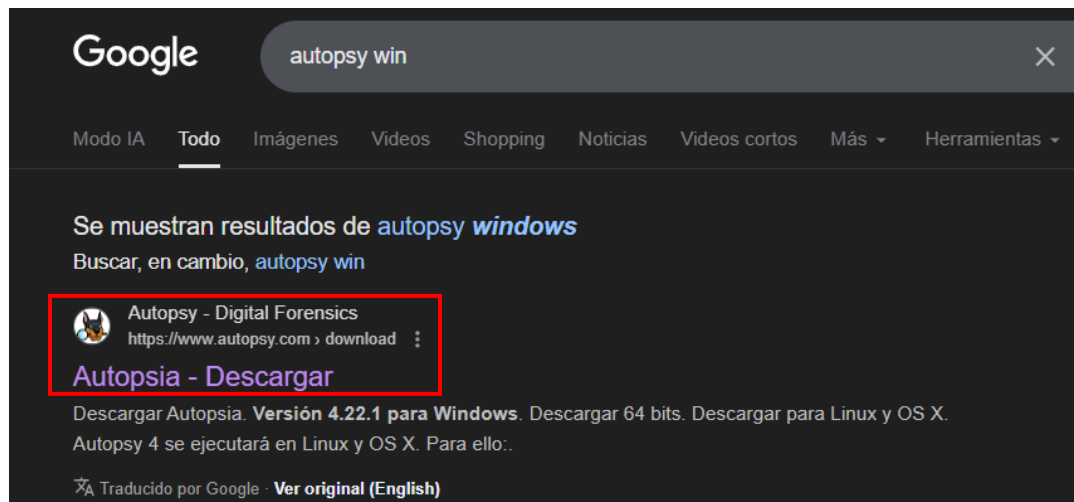


Ilustración 31. Búsqueda del Software

5.2 Página oficial de descarga de Autopsy

En la página web oficial de Autopsy, se seleccionó la versión 4.22.1 para Windows de 64 bits y se procedió a hacer clic en el enlace de descarga.

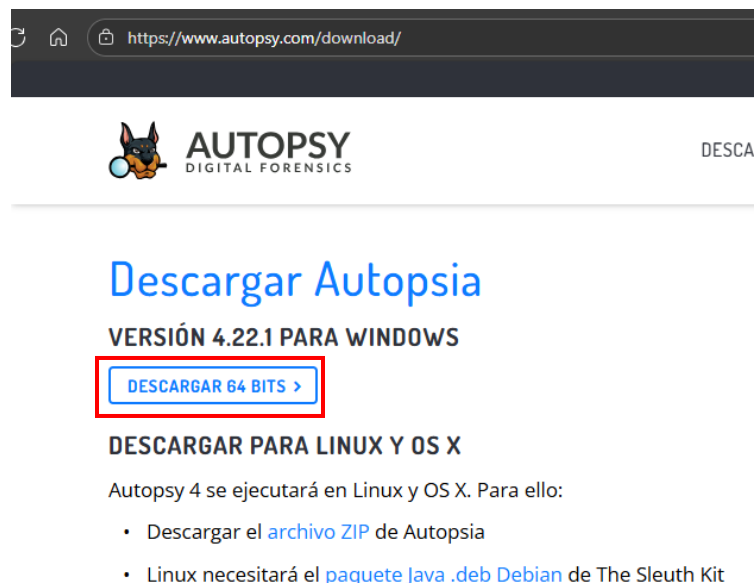


Ilustración 32. Descarga desde la Página Oficial



5.3 Diálogo de descarga del archivo de instalación

El navegador mostró un cuadro de diálogo preguntando qué acción realizar con el archivo "autopsy-4.22.1-64bit (1).msi". Se eligió la opción "Guardar" para descargar el instalador en el sistema.

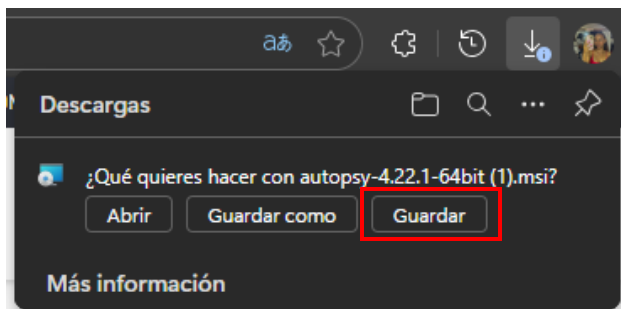


Ilustración 33. Confirmación de Descarga

5.4 Gestor de descargas del sistema

Se accedió a la carpeta "**Descargas**" del sistema para verificar que el archivo "autopsy-4.22.1-64bit (1).msi" se había descargado correctamente.

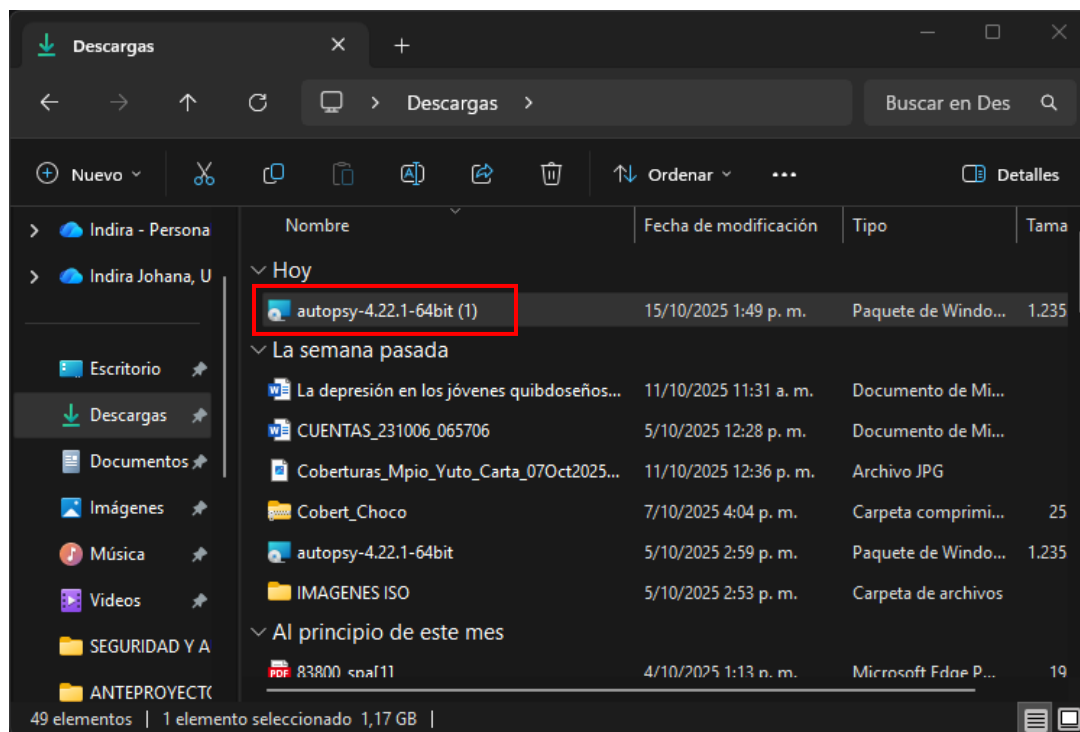


Ilustración 34. Verificación del Archivo Descargado



5.5 Instalación de Autopsy en Windows

Se ejecutó el archivo descargado, lo que abrió el Asistente de Instalación de Autopsy. En esta ventana de bienvenida, se hizo clic en "Next" para comenzar el proceso de instalación.

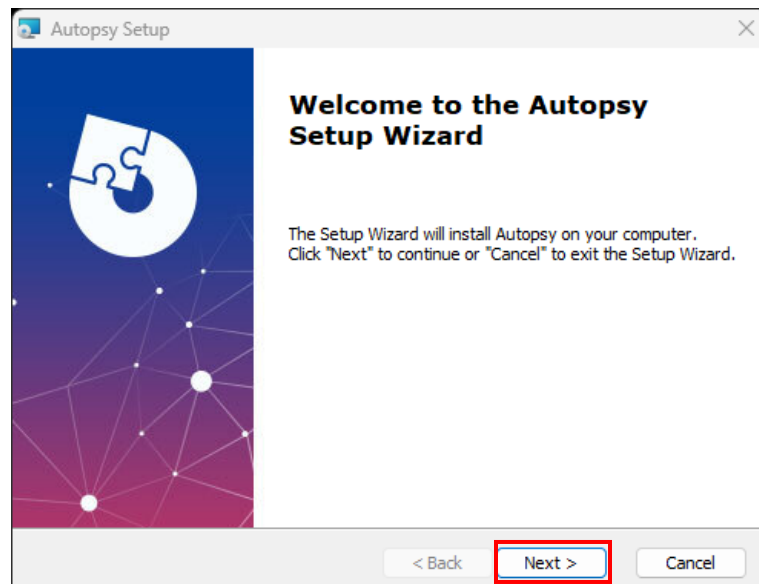


Ilustración 35. Inicio del Asistente de Instalación

El asistente presentó la opción de seleccionar la carpeta de instalación. Se mantuvo la ruta por defecto ("C:\Program Files\Autopsy-4.22.1") y se hizo clic en "Next" para continuar.

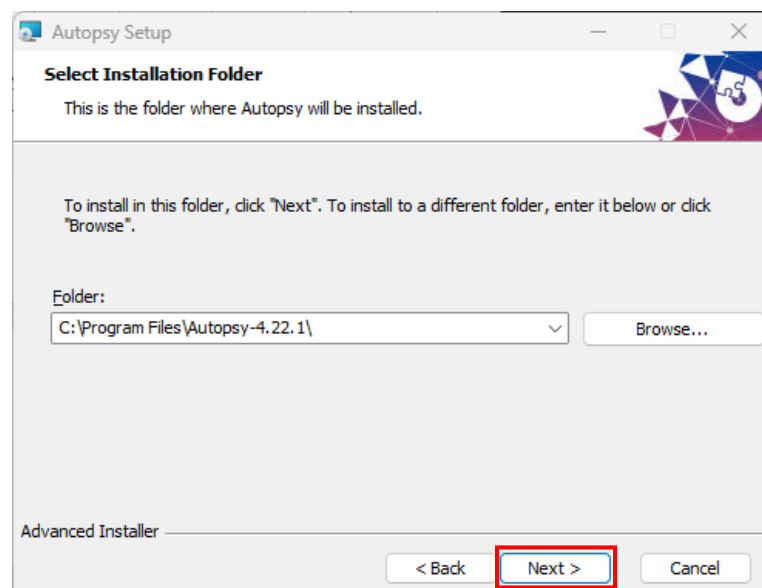


Ilustración 36. Selección de la Carpeta de Destino



En la ventana "Ready to Install", se hizo clic en el botón "Instalar" para iniciar la copia de archivos y la configuración del software.

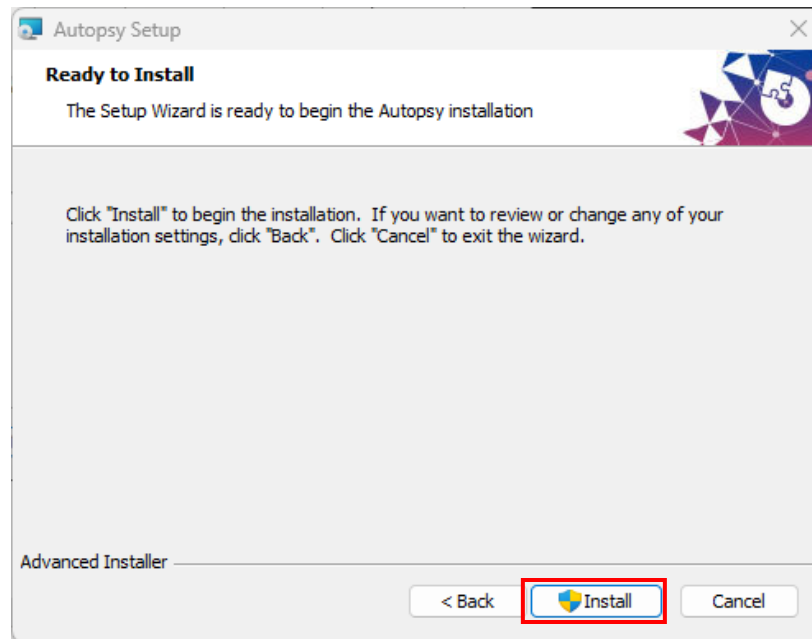


Ilustración 37. Confirmación para Instalar

Se esperó a que el proceso se completara.

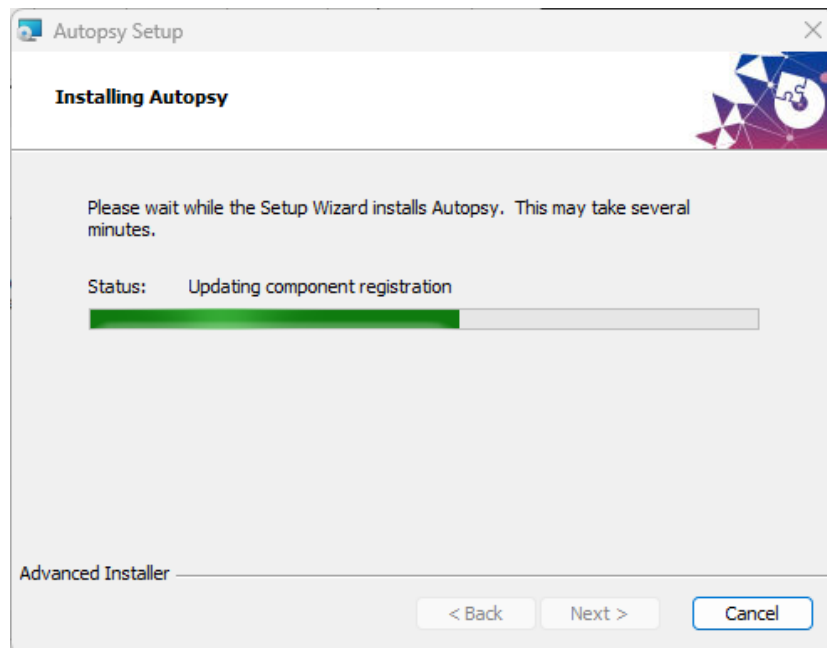


Ilustración 38. Proceso de Instalación en Curso



Al concluir el proceso, el asistente mostró la ventana "Completando el Asistente de Instalación de Autopsy". Se hizo clic en el botón "**Finalizar**" para salir del wizard.

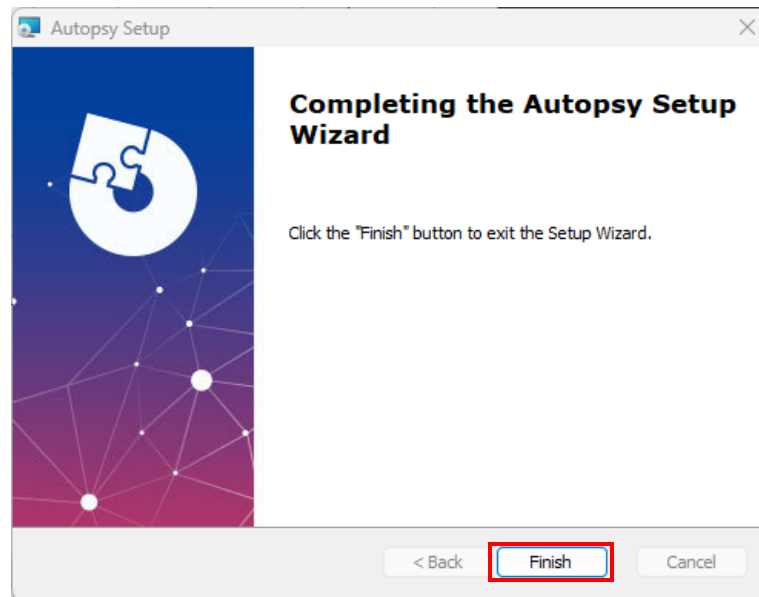


Ilustración 39. Finalización de la Instalación

5.6 Acceso directo de Autopsy en el escritorio

Como evidencia final de una instalación exitosa, se verificó que el acceso directo de "Autopsy 4.22.1" estaba disponible en el escritorio, listo para ser ejecutado.

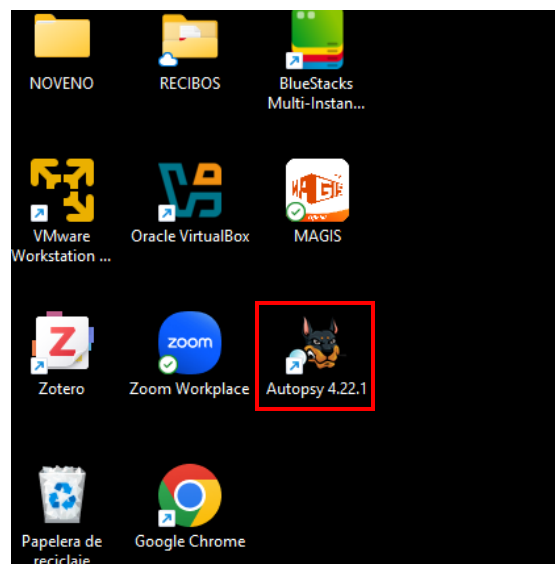


Ilustración 40. Software Instalado y Accesible



5.7 Inicio de Autopsy y Carga de Módulos

Se ejecutó la aplicación Autopsy, mostrando la pantalla inicial con el lema "OPEN EXTENSIBLE FAST". La aplicación inició el proceso de carga y activación de sus módulos de análisis forense.

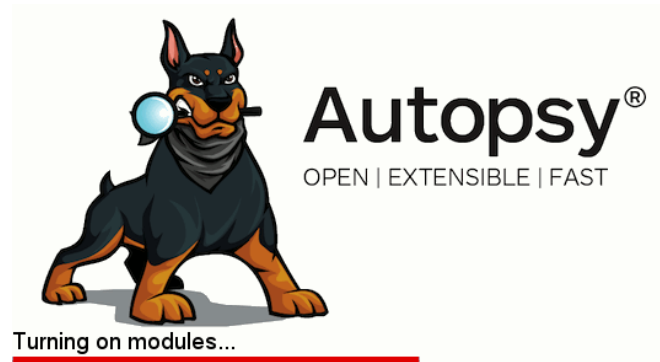


Ilustración 41. Inicio de Autopsy

Al abrir Autopsy, se presentó la ventana principal de bienvenida con las opciones para crear un nuevo caso "**New Case**", abrir un caso reciente "**Open Recent Case**" o abrir un caso existente "**Open Case**".

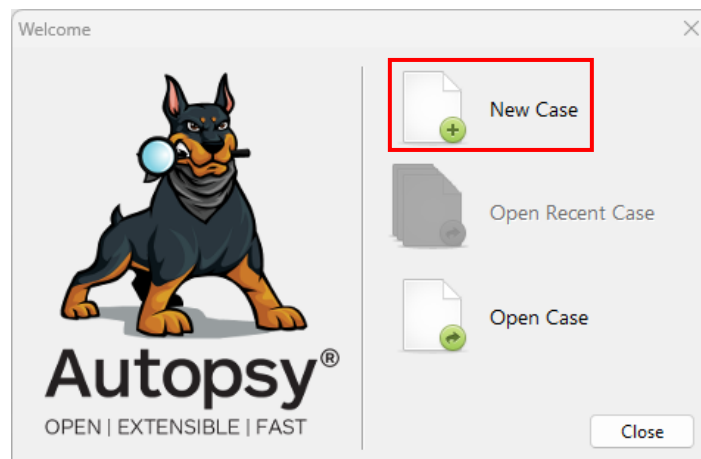


Ilustración 42. Ventana Principal de Bienvenida

Se seleccionó "**New Case**" y se procedió a llenar la información básica del caso. Se definió el nombre del caso y el directorio base donde se almacenarían los datos, manteniendo la opción "Single-User" seleccionada.

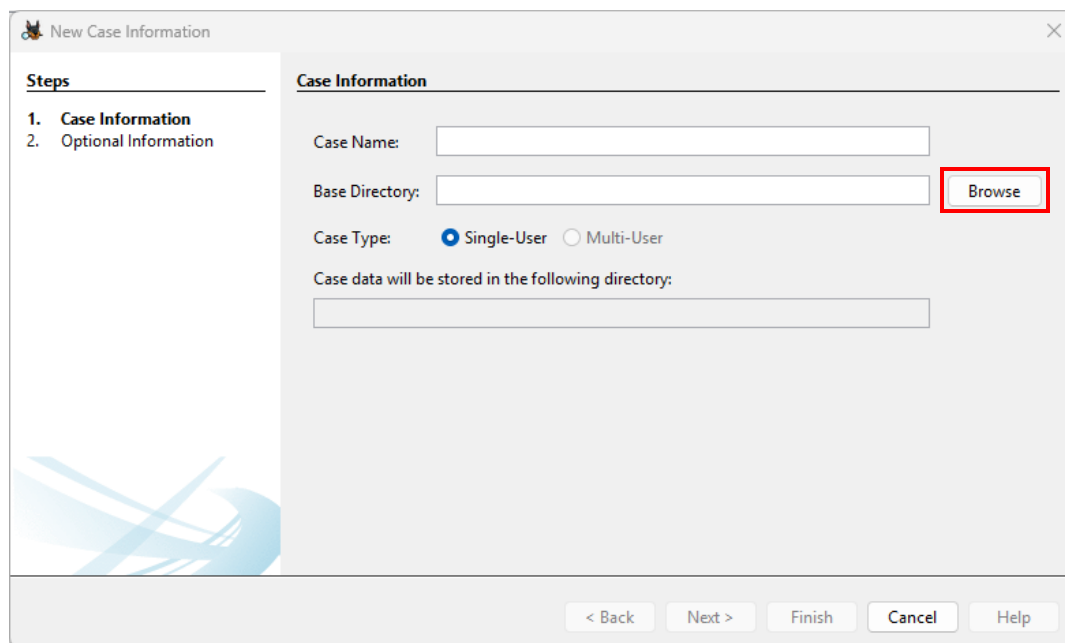


Ilustración 43. Creación de Nuevo Caso - Información Básica

Al hacer clic en "**Browse**" para seleccionar el directorio base, se abrió una ventana de navegación de archivos mostrando las unidades y carpetas disponibles en el sistema, incluyendo el disco local (C:).

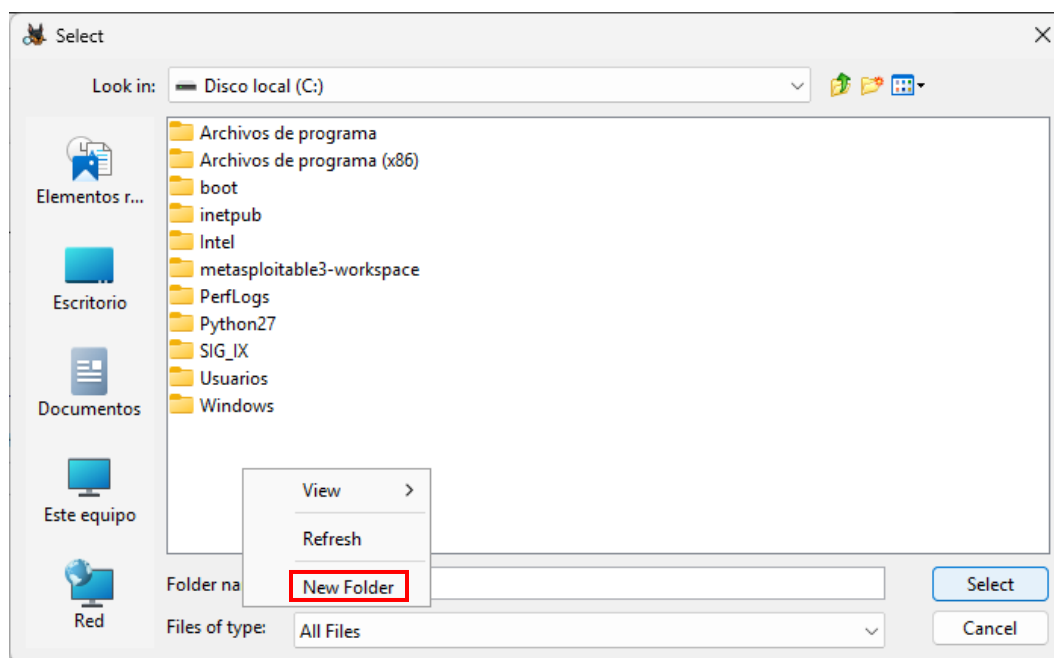


Ilustración 44. Navegación para Seleccionar Directorio



En la ventana de navegación, se creó la carpeta "**Analisis_Forens**" como ubicación para almacenar todos los datos relacionados con el caso forense, haciendo clic derecho y seleccionando la opción "**New Folder**" para crear la carpeta.

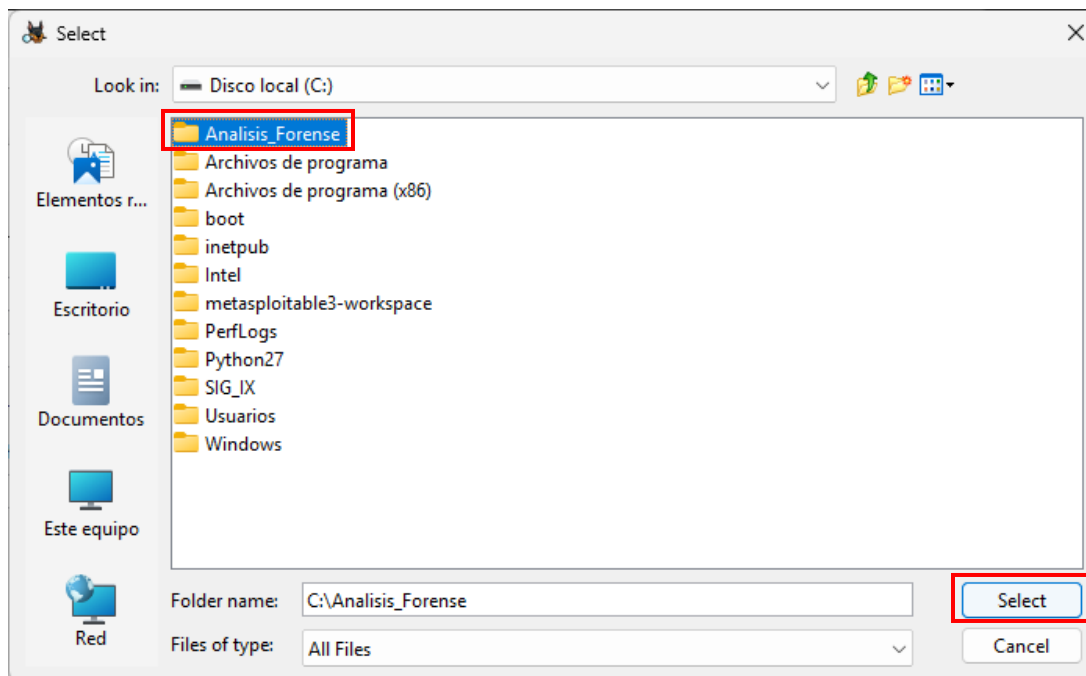


Ilustración 45. Creación de la Carpeta de Análisis Forense

Se verificó y confirmó la información del caso creado, mostrando el nombre "**MiPrimerCaso**" y la ruta de almacenamiento "**C:\Analisis_Forens\MiPrimerCaso**".

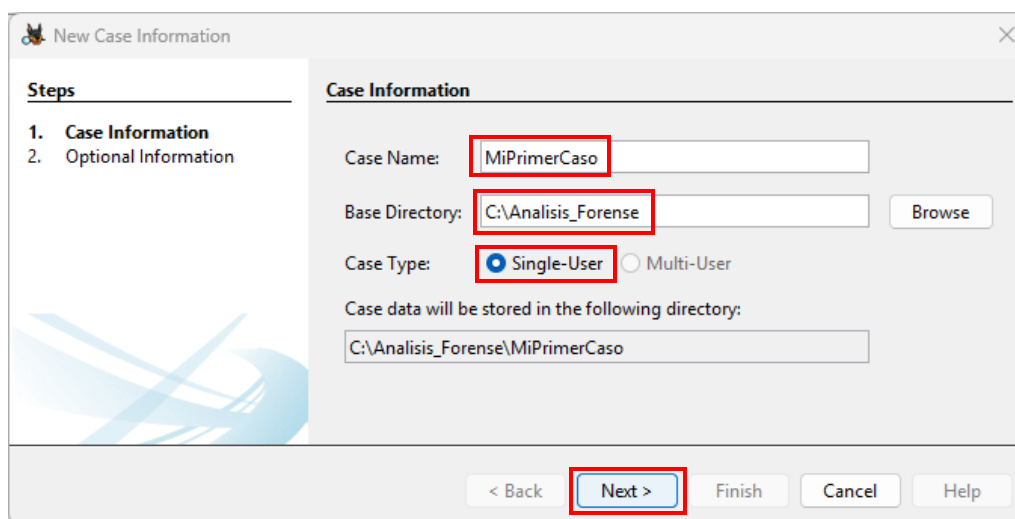


Ilustración 46. Confirmación de Información del Caso



Se completó la información opcional del examinador, incluyendo nombre, teléfono, correo electrónico y notas del caso. También se asignó un número de caso (01) para fines de documentación y trazabilidad.

Ilustración 47. Información Opcional del Examinador

Al agregar una fuente de datos, se configuró la opción de host seleccionando **"Generate new host name based on data source name"** para organizar los datos dentro del caso.

Ilustración 48. Selección de Host para la Fuente de Datos



Se eligió el tipo de fuente de datos "**Disk Image or VM File**" para cargar una imagen forense previamente creada.

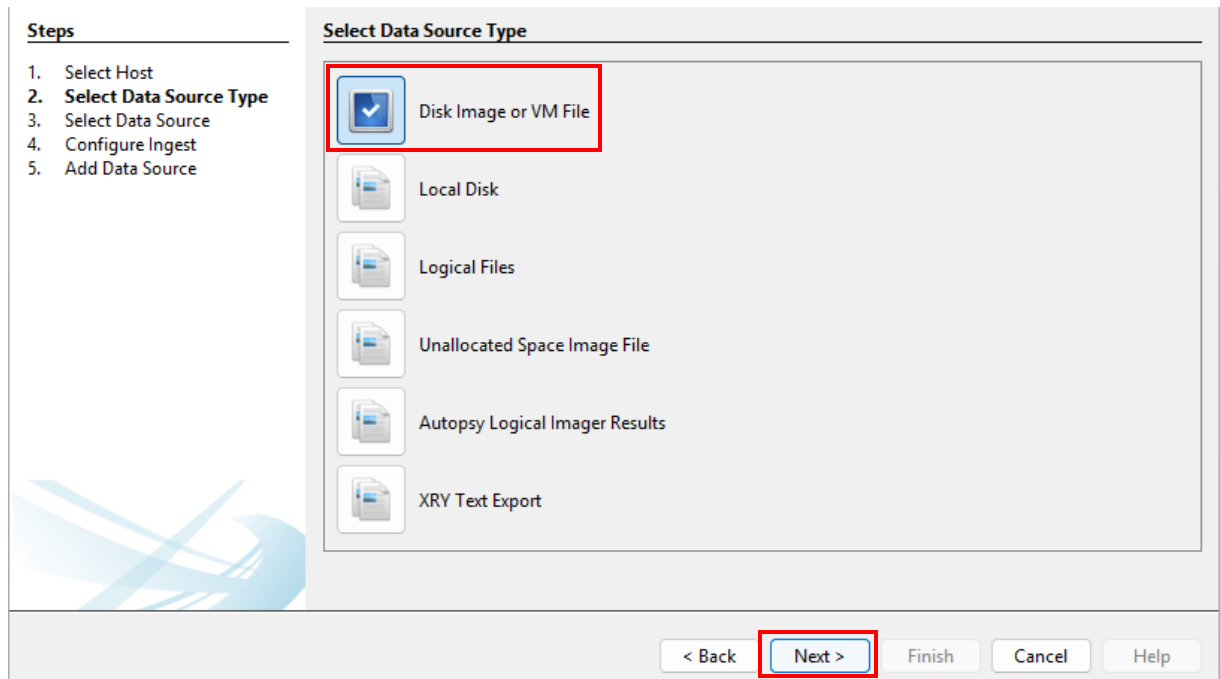


Ilustración 49. Selección del Tipo de Fuente de Datos

5.8 Creación de la carpeta donde se guardará la imagen forense

En la estructura de carpetas generada automáticamente para el caso "**MiPrimerCaso**" se va a crear una carpeta llamada "**imagen**" para guardar la imagen que se encuentra en Kali Linux en esa carpeta, haciendo clic derecho, seleccionando "**Nuevo**" y luego "**Carpeta**".

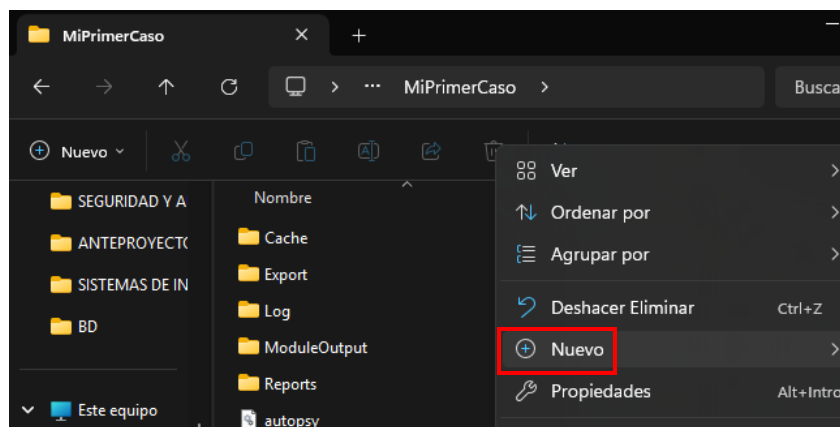


Ilustración 50. Seleccionar opción para crear la nueva carpeta

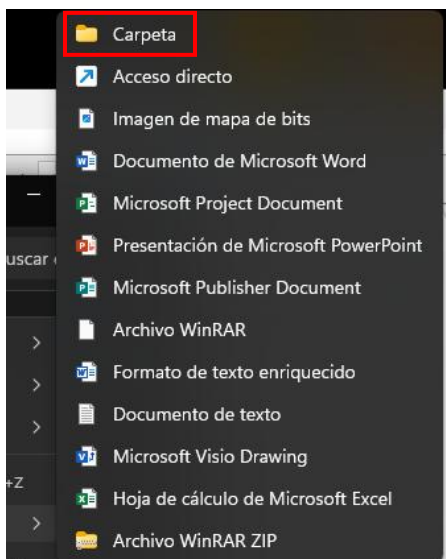


Ilustración 51. Crear nueva carpeta donde se guardará la imagen de que está en Kali Linux

Confirmando la correcta creación de la carpeta “imagen”.

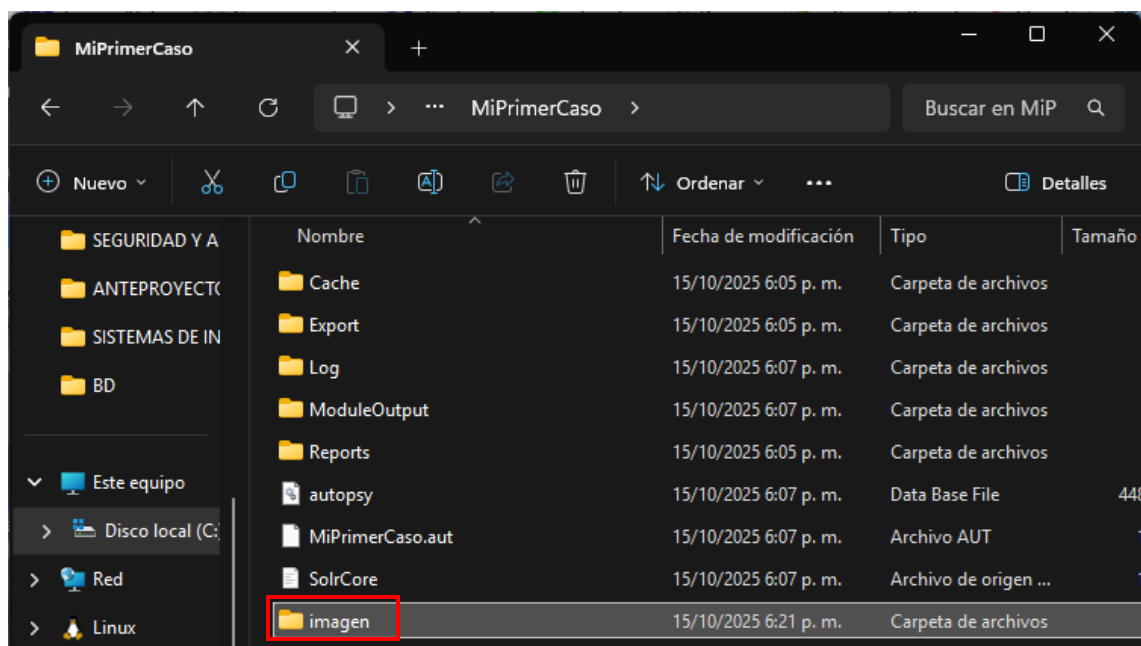


Ilustración 52. Carpeta "imagen" creada

5.9 Transferencia de Imagen Forense desde Kali Linux a Windows



Se capturó el proceso de copia del archivo de la imagen forense "imagen_usb_forense.dd" desde la máquina virtual Kali Linux hacia la carpeta "Imagen" que está en Windows, mostrando el progreso de la transferencia de 3.8 GB.

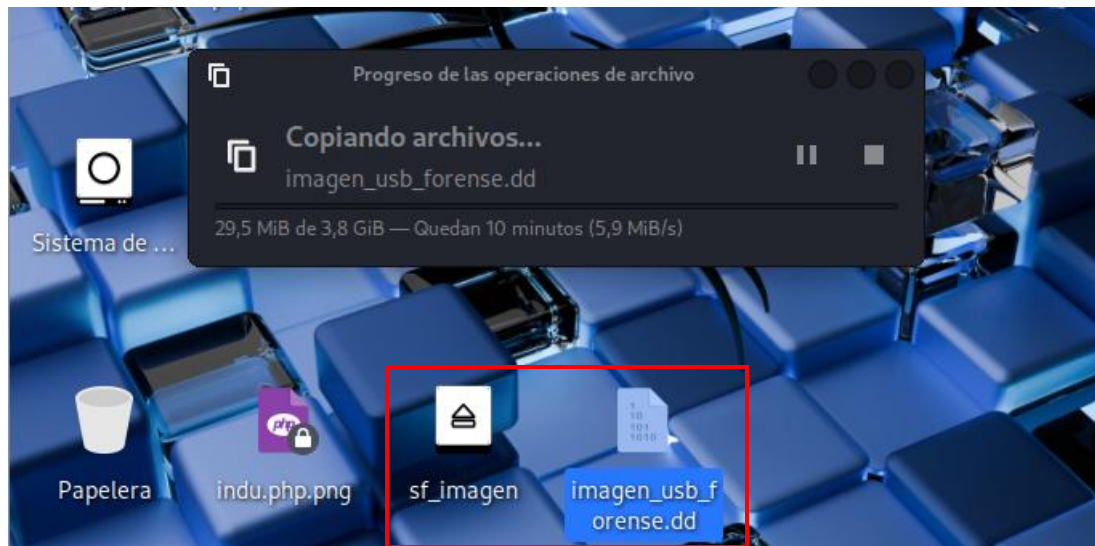


Ilustración 53. Transferencia de Imagen Forense desde Máquina Virtual

5.10 Selección del Archivo de Imagen Forense

En Autopsy, se navegó hasta la ubicación del archivo de imagen forense "imagen_usb_forense.dd" y se procedió a seleccionarlo para agregarlo como fuente de datos al caso.

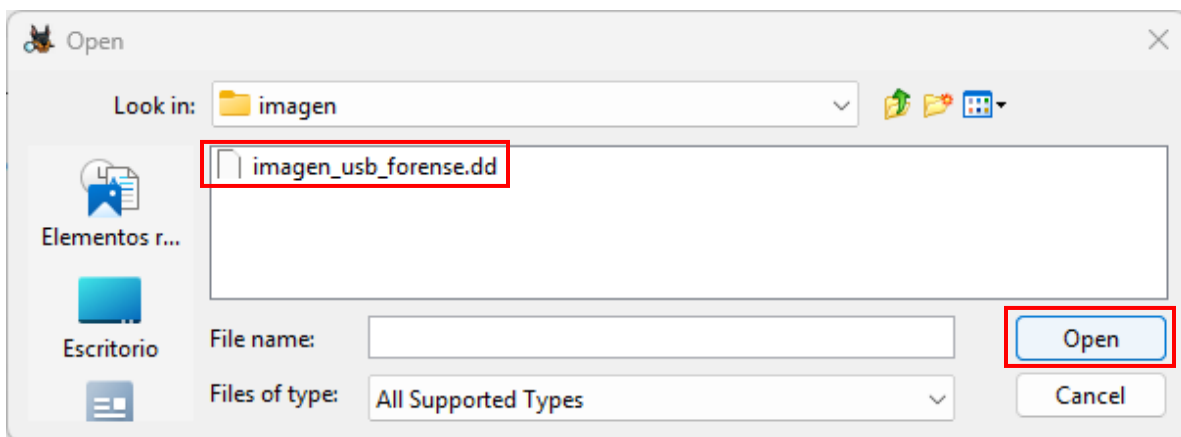


Ilustración 54. Selección del Archivo



Se configuraron los parámetros específicos para la fuente de datos, incluyendo la zona horaria (America/Bogota) y opciones de tamaño de sector.

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path: C:\Analisis_Forense\MiPrimerCaso\imagen\imagen_usb_forense.dd Browse

☐ Ignore orphan files in FAT file systems

Time zone: (GMT-5:00) America/Bogota

Sector size: Auto Detect

Bitlocker Password (optional):

Hash Values (optional):

MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

< Back **Next >** Finish Cancel Help

Ilustración 55. Configuración de Parámetros de la Fuente de Datos

Se configuraron los módulos de análisis que se ejecutarían sobre la imagen.

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

Run ingest modules on: All Files, Directories, and Unallocated Space

☒ PhotoRec Carver

☒ Virtual Machine Extractor

☒ Data Source Integrity

☐ Android Analyzer (aLEAPP)

☐ Cyber Triage Malware Scanner

☐ DJI Drone Analyzer

☐ Plaso

☒ YARA Analyzer

☐ iOS Analyzer (iLEAPP)

☒ GPX Parser

☐ Android Analyzer

Select All Deselect All History

The selected module has no per-run settings.

Extracts Android system and third-party app data.

Global Settings

< Back **Next >** Finish Cancel Help

Ilustración 56. Selección de Módulos de Ingesta



Autopsy inició el procesamiento de la fuente de datos, mostrando un mensaje indicando que este proceso podría tomar tiempo dependiendo del tamaño de la imagen.

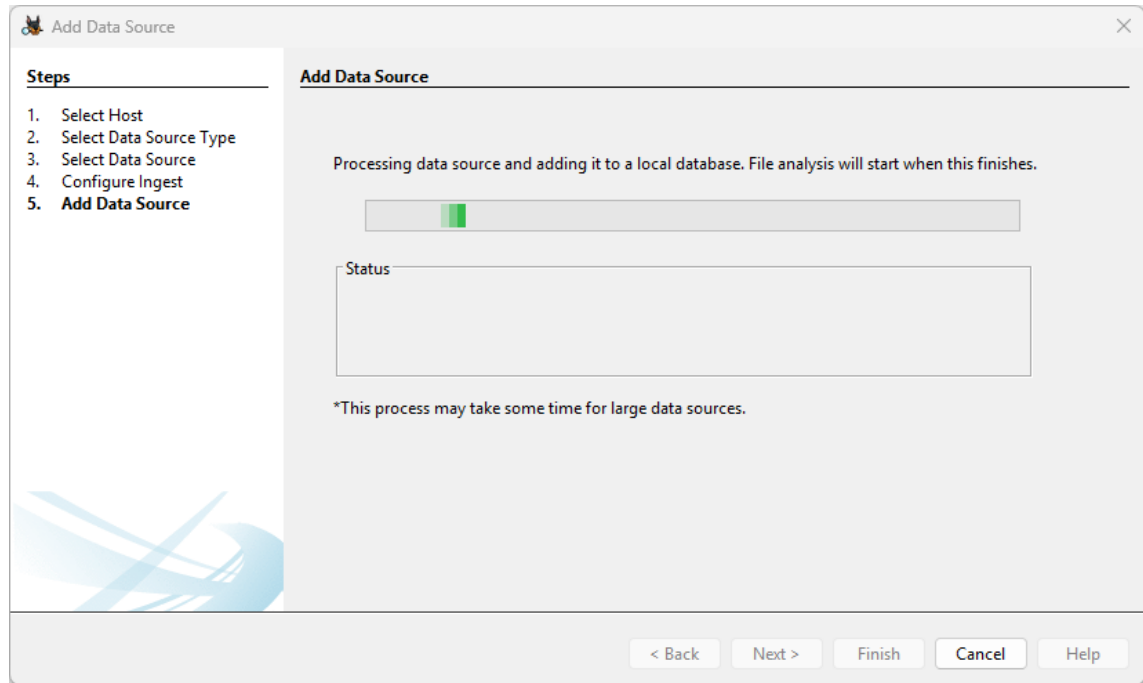


Ilustración 57. Procesamiento Inicial de la Fuente de Datos

Se confirmó que la fuente de datos fue añadida exitosamente a la base de datos local y que el análisis de archivos estaba comenzando automáticamente.

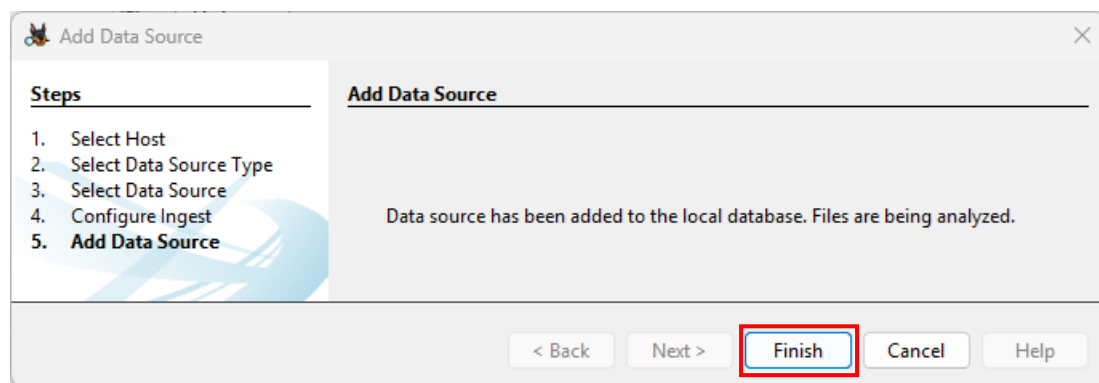


Ilustración 58. Finalización de la Adición de Fuente de Datos

Se muestra la interfaz principal de Autopsy con la barra de progreso al 100% indicando la finalización del procesamiento inicial.

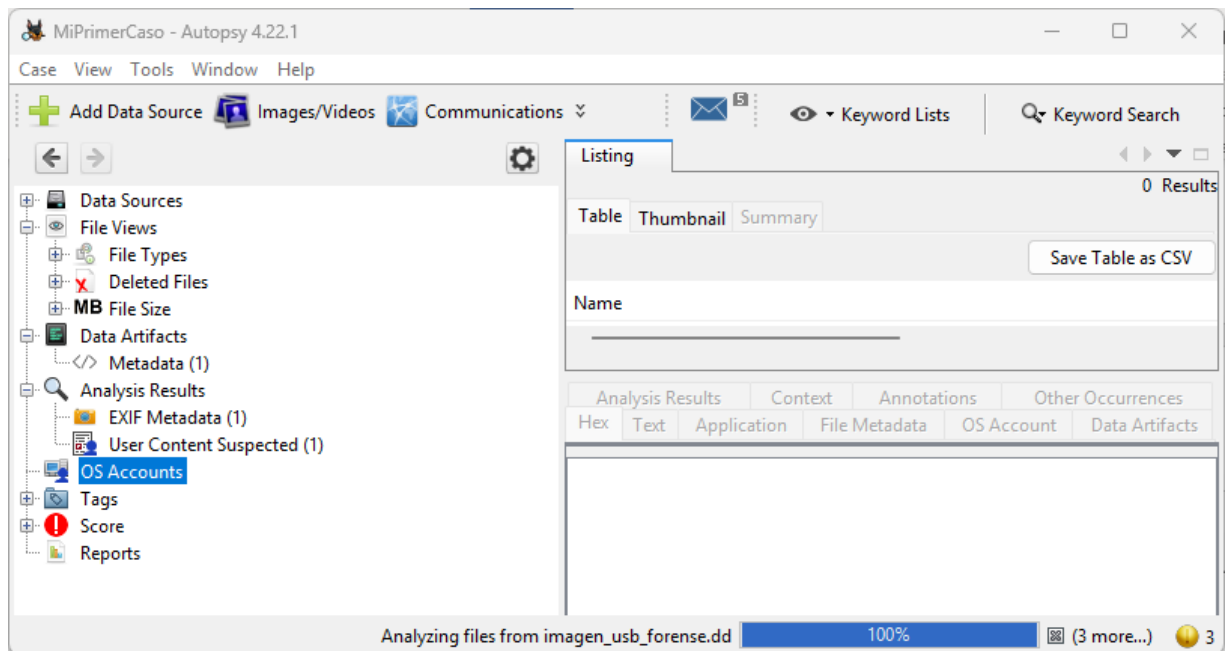


Ilustración 59. Interfaz Principal de Análisis en Progreso

Se visualiza la estructura de la imagen forense "**imagen_usb_forense.dd**" cargada en Autopsy. La imagen contiene dos volúmenes: **vol1** y **vol2**.

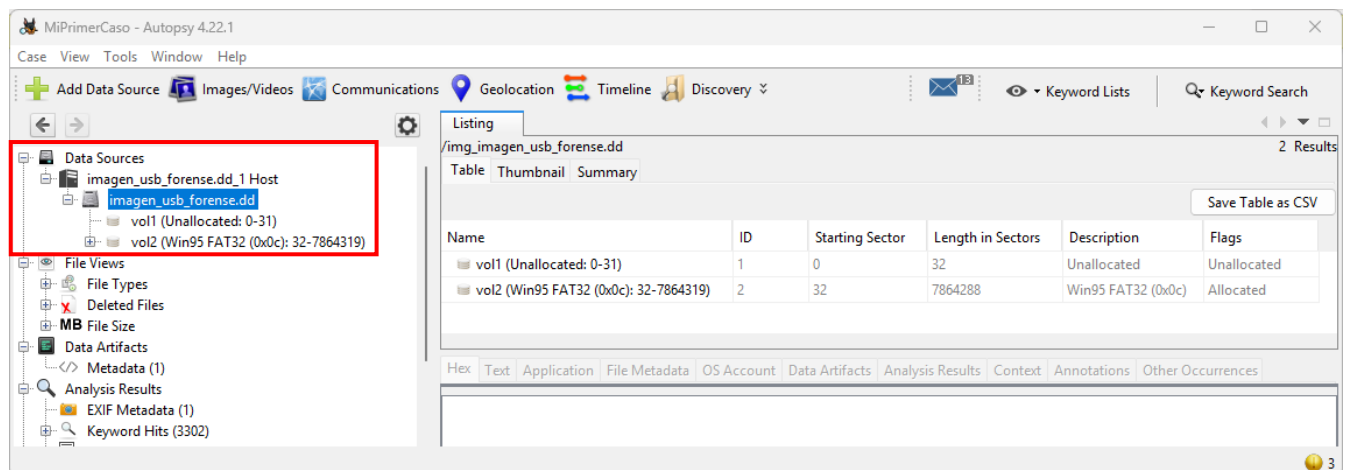


Ilustración 60. Estructura de la Fuente de Datos y Volúmenes

Se examina el volumen no asignado (vol1) donde se identifica un fragmento de datos denominado "Unalloc_3_0_16384" con tamaño de 16.384 bytes. Todos los timestamps de este



fragmento aparecen como "0000-00-00 00:00:00", lo que es característico de espacio no asignado que no contiene metadatos de sistema de archivos.

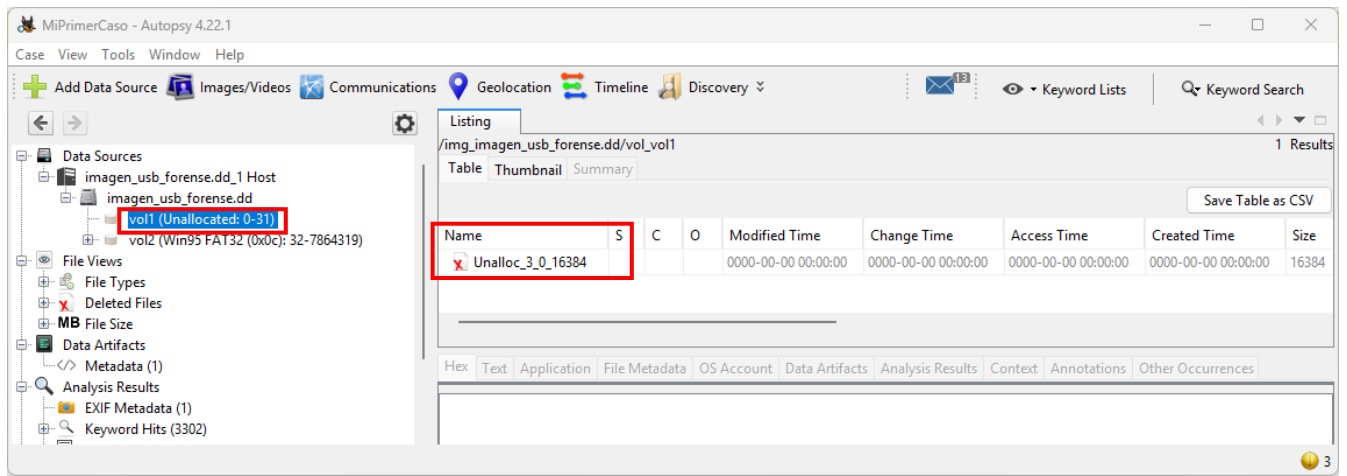


Ilustración 61. Análisis del Espacio No Asignado (vol1)

Se muestra el contenido del volumen FAT32 con 17 archivos recuperados. Entre los archivos identificados se encuentran: "X_imagen.jpg", "X_Articulo.docx", "FECHA 1 LUNES.jpg", "Herramientas de Hacking Ethical.txt", "IMG_0001.JPG", "IMG_3422.mov", y documentos PDF como "PROPUESTA DE ANTEPROYECTO.pdf". Los metadatos muestran fechas de modificación entre 2021 y 2025.

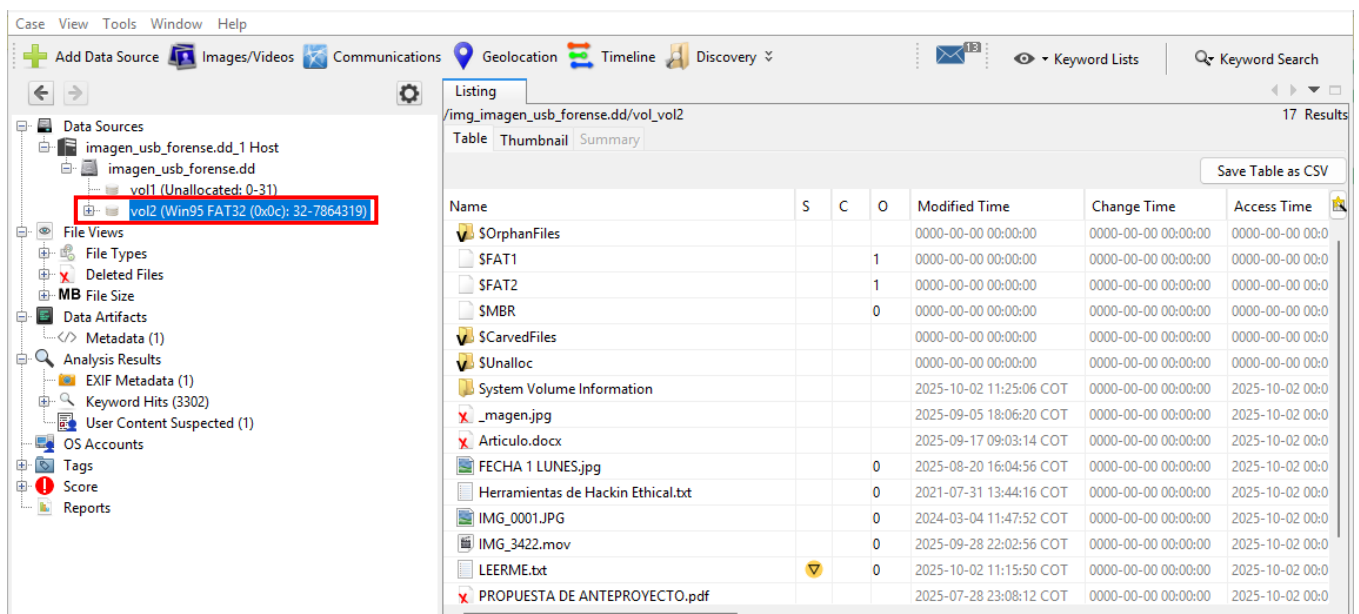


Ilustración 62. Contenido del Sistema de Archivos FAT32 (vol2)



Se presenta una vista detallada de los archivos del volumen FAT32.

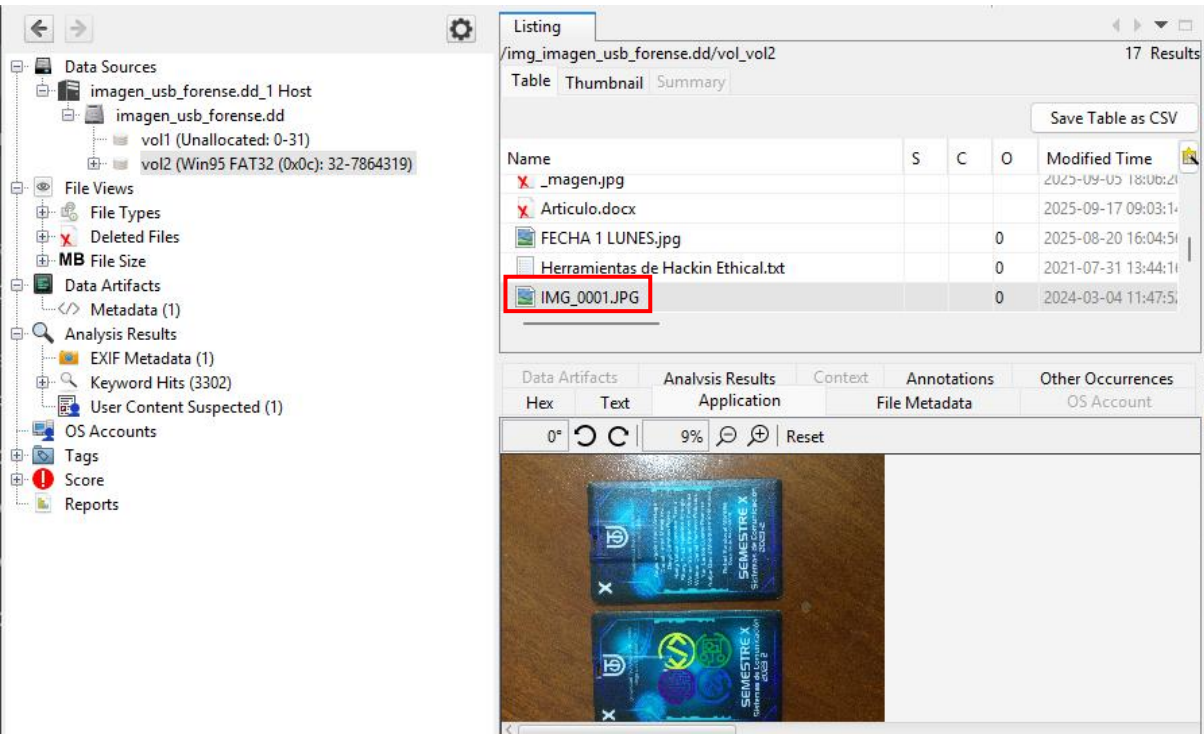


Ilustración 63. Vista Expandida de Archivos

Se realiza un análisis forense avanzado mostrando los valores hash (MD5 y SHA-256) de los archivos recuperados, junto con sus tipos MIME identificados.

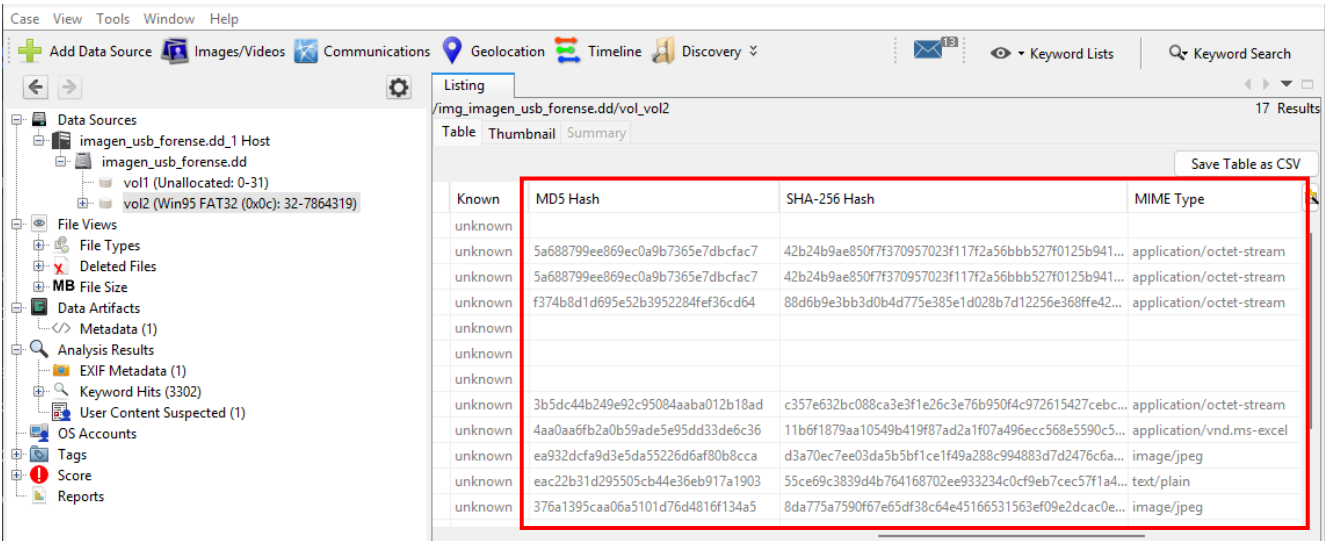


Ilustración 64. Análisis de Hashes y Tipos MIME



6. CAPITULO 3 – ANALISIS FORENSE CON FTK IMAGER EN WINDOWS

6.1 Búsqueda y Selección de FTK Imager

Se realizó una búsqueda en Google con el término "ftk imager 4.7.1 superior" para descargar la herramienta. El resultado principal dirigió al sitio oficial de Exterro.

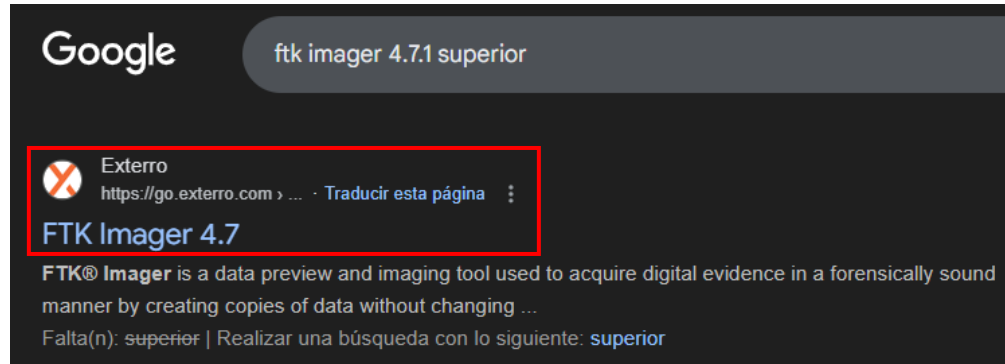


Ilustración 65. Búsqueda en Google de FTK Imager

6.2 Descarga desde el Sitio Oficial de Exterro

En la página oficial de Exterro, se accedió al formulario de descarga de FTK Imager versión 4.7. Se completó el formulario con los datos personales y profesionales requeridos.

exterro

GET STARTED WITH FTK IMAGER 4.7!

FTK® Imager is a data preview and imaging tool used to acquire digital evidence in a forensically sound manner by creating copies of data without changing the original in any way. The latest version supports the AFF4 format and execution on portable drives.

With FTK Imager you can:

- ✓ Create forensic images of entire local hard drives, CDs and DVDs, thumb drives and other USB devices—or just the files and folders you need.
- ✓ Preview the contents of forensic images stored on local machines or network drives.

Fill out the form to download FTK Imager 4.7

* First Name
Indira Johana

* Last Name
Flórez Córdoba

* Business Email
indirajohana3@gmail.com

* Organization Name
UTCH

* Job Title
Análisis forense

* Company Country
Colombia

Ilustración 66. Formulario de descarga



6.3 Confirmación de Descarga del Instalador

El navegador mostró el diálogo de descarga, se seleccionó la opción "**Guardar**" para proceder con la descarga del instalador en el sistema.

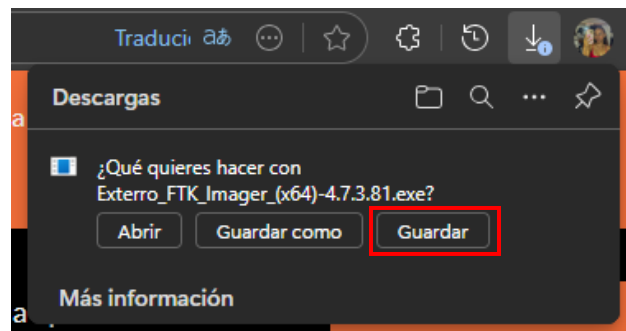


Ilustración 67. Confirmación de descarga de FTK Imager

6.4 Verificación del Archivo Descargado

Se accedió a la carpeta de "**Descargas**" del sistema para verificar que el archivo se había descargado correctamente.

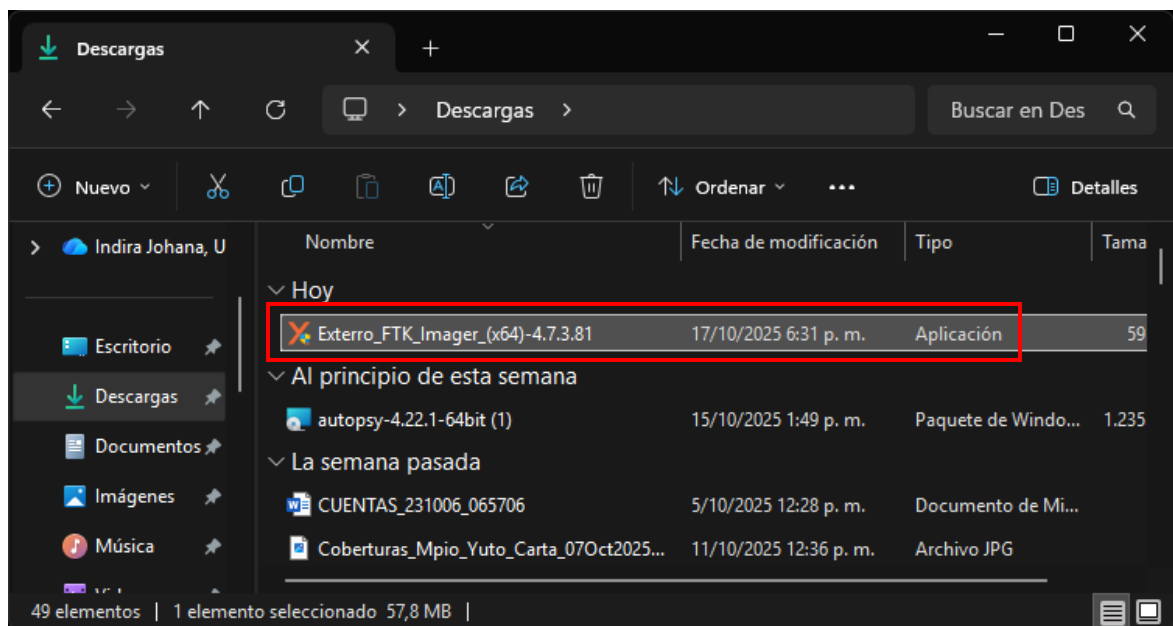


Ilustración 68. Archivo FTK Imager en la carpeta de descargas

6.5 Instalación de FTK Imager



Se ejecutó el archivo descargado, lo que inició el InstallShield Wizard para FTK Imager. Se presentó la pantalla de bienvenida y se hizo clic en "**Next**" para comenzar la instalación.

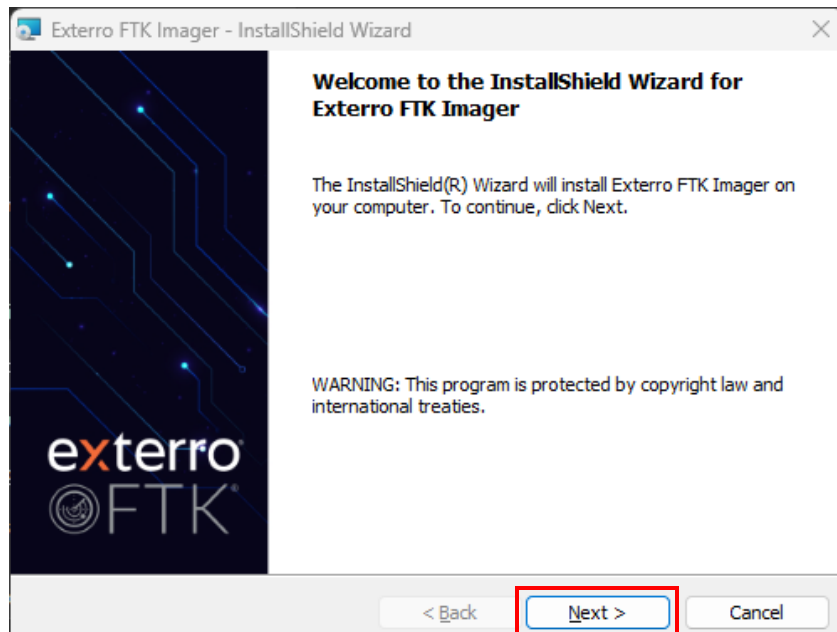


Ilustración 69. Instalación de FTK Imager

Se presentó el Acuerdo de Licencia y se seleccionó la **opción "Acepto los términos del acuerdo de licencia"** para poder continuar con la instalación del software forense.

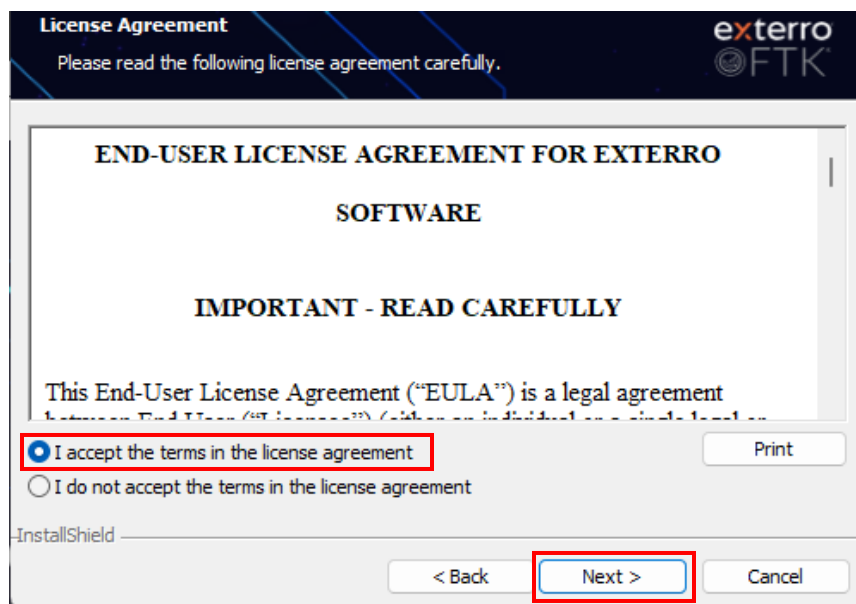


Ilustración 70. Aceptación del Acuerdo de Licencia



El asistente de instalación mostró la carpeta destino predeterminada para la instalación: "C:\Program Files\AccessData". Se mantuvo esta ubicación por defecto y se marcó la opción adicional **"Add Installation File path in Windows Defender Exclusion List"** para evitar interferencias del antivirus durante el uso de la herramienta forense.

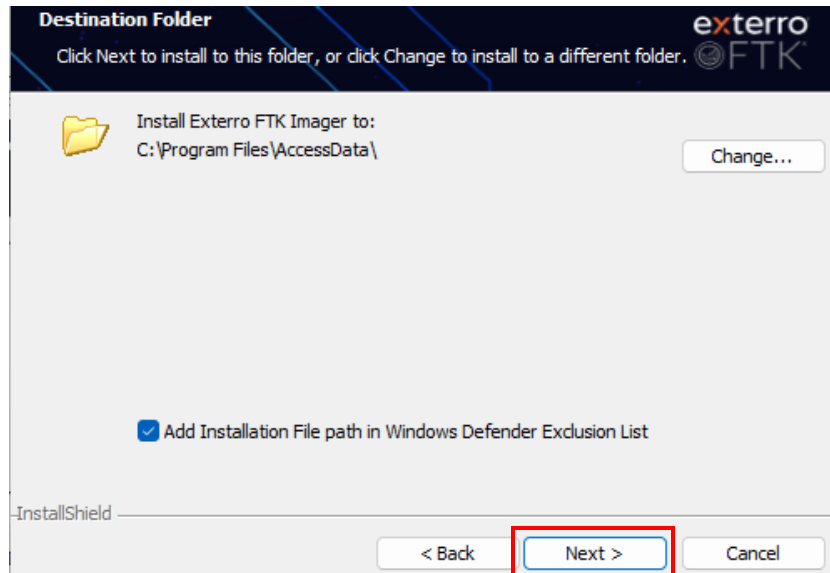


Ilustración 71. Selección de Carpeta de Destino

Ventana de confirmación final donde se hizo clic en el botón **"Install"** para iniciar el proceso de instalación propiamente dicho.

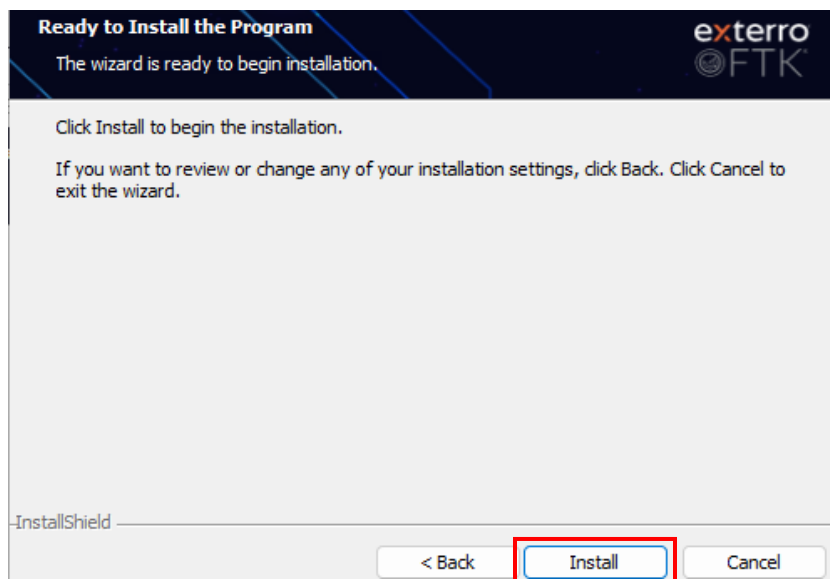


Ilustración 72. Confirmación Final antes de la Instalación



Progreso de la instalación, indicando el estado actual **"Registering product"**. Este proceso tomó varios minutos mientras el sistema copiaba los archivos necesarios y configuraba los registros del sistema.

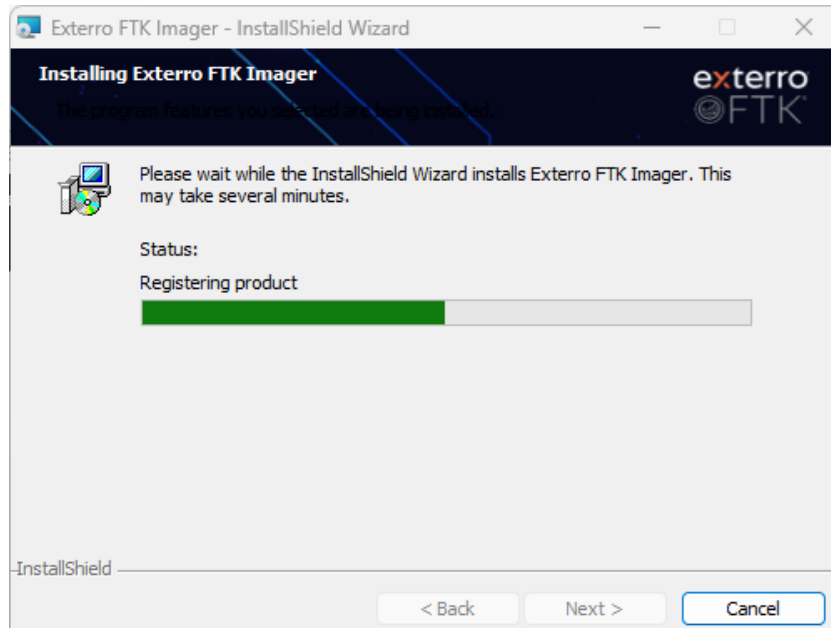


Ilustración 73. Progreso de la Instalación

Finalización exitosa de la instalación. Se marcó la opción **"Launch Exterro FTK Imager"** para ejecutar automáticamente la aplicación al hacer clic en **"Finish"**.

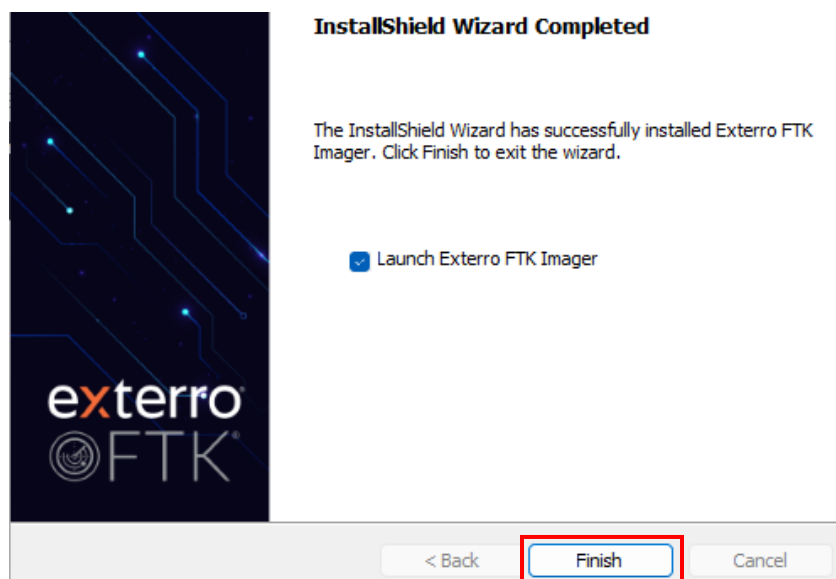


Ilustración 74. Finalización Exitosa de la Instalación



6.6 Inicio de FTK Imager

Se inició la aplicación FTK Imager, mostrando la interfaz principal con el árbol de evidencia, lista de archivos y opciones para manejar fuentes de contenido personalizadas

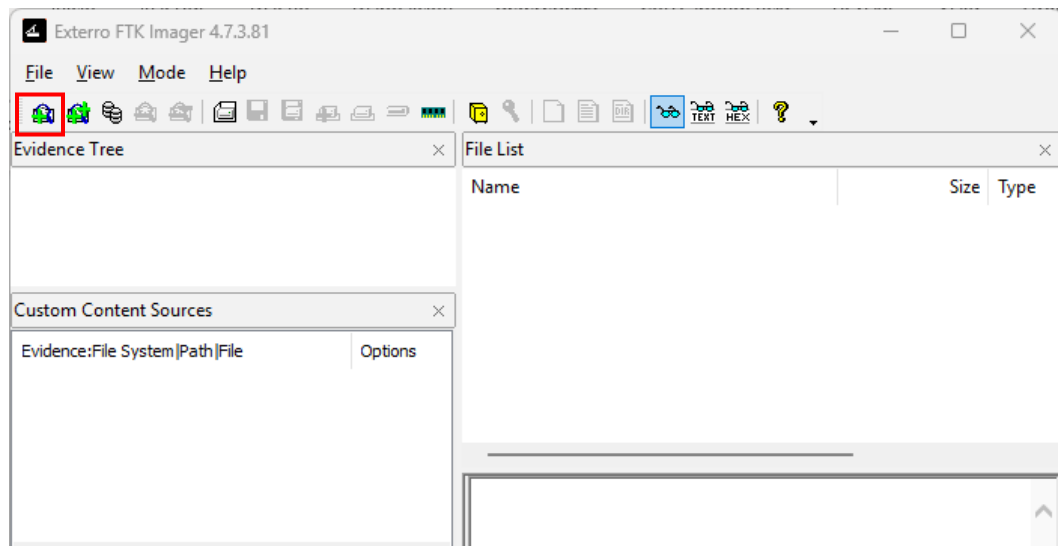


Ilustración 75. Interfaz Principal de FTK Imager

Al agregar una nueva evidencia, se seleccionó la opción "**Image File**" como tipo de fuente de evidencia, indicando que se trabajaría con una imagen forense previamente creada.

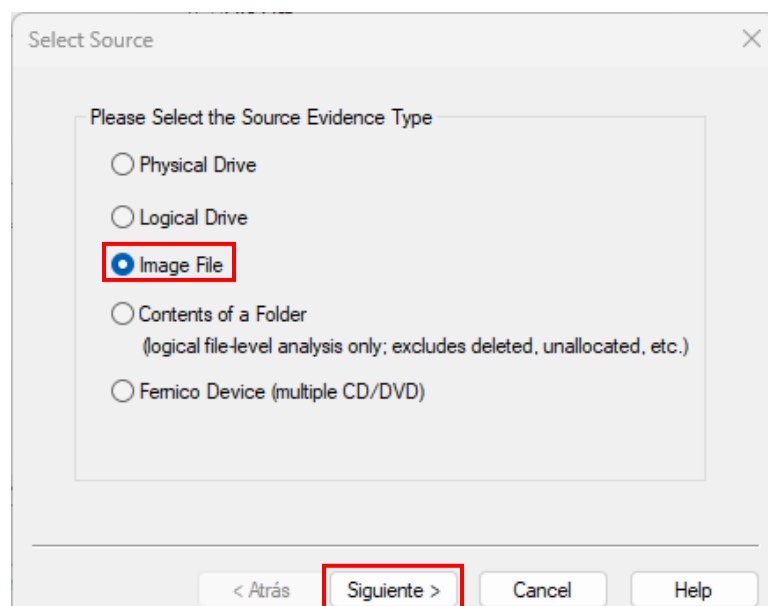


Ilustración 76. Selección del Tipo de Fuente de Evidencia



Se utilizó el botón "**Browse**" para navegar hasta la ubicación del archivo de imagen forense "**imagen_usb_forense.dd**".

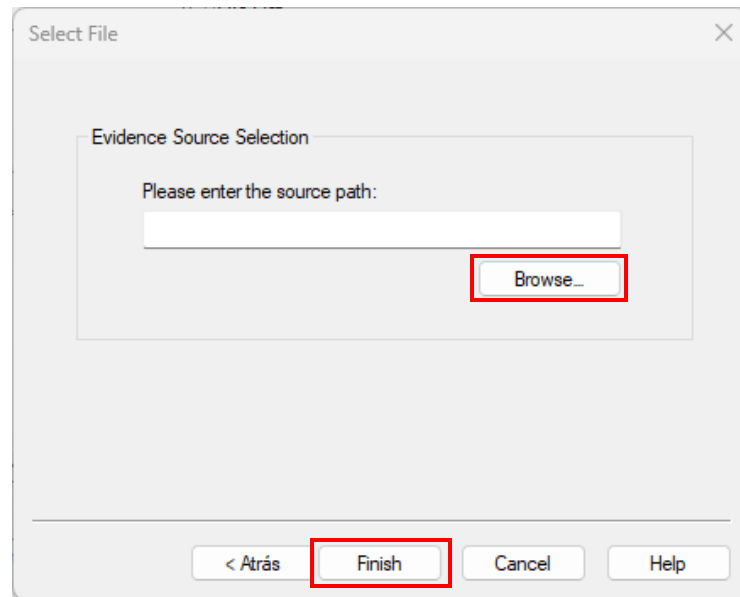


Ilustración 77. Navegación para Seleccionar Archivo de Imagen

Se verificó la ruta del archivo de imagen forense.

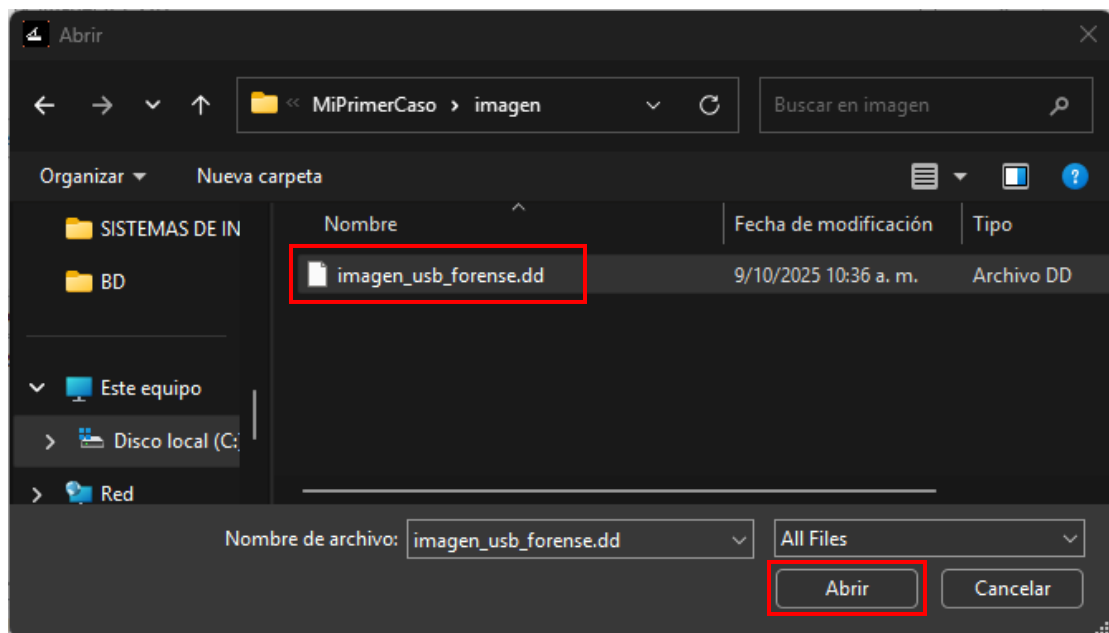


Ilustración 78. Verificación de la Ruta de la Imagen Forense



Se confirmó la ruta completa del archivo de imagen forense.

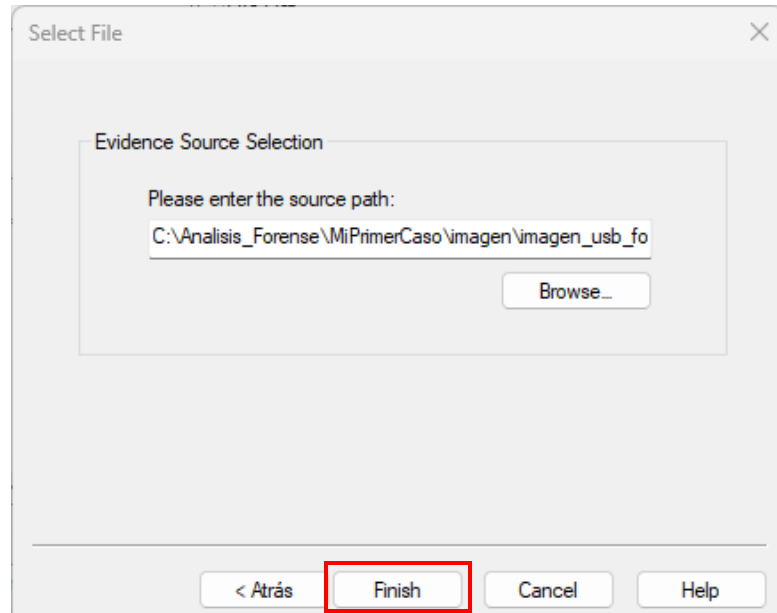


Ilustración 79. Confirmación de la Ruta de la Imagen Forense

FTK Imager mostró la estructura de la imagen forense, identificando "**Partition 1 [3839MB]**" con sistema de archivos **FAT32** y espacio no particionado.

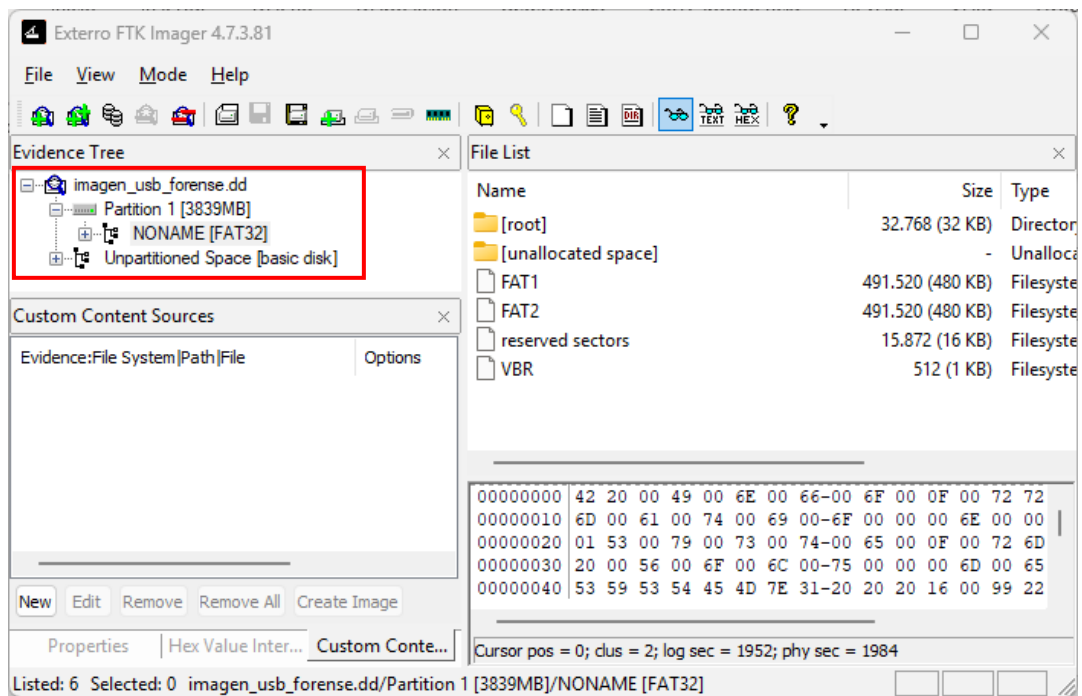


Ilustración 80. Estructura de Particiones de la Imagen



Se examinó el contenido del directorio raíz de la partición FAT32, identificando 18 elementos.

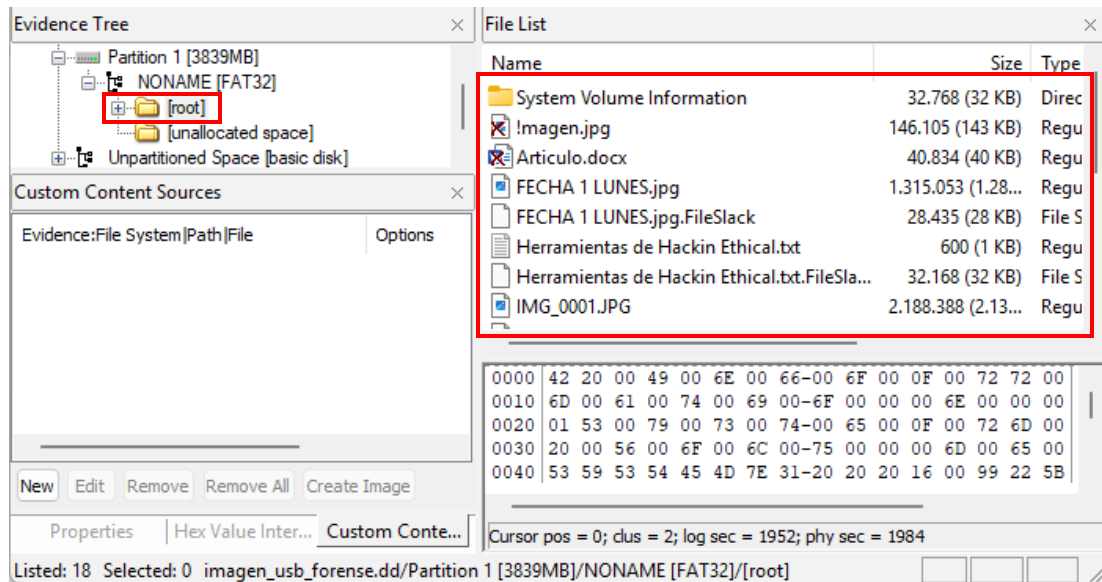


Ilustración 81. Contenido del Directorio Raíz FAT32

Se visualizó la lista detallada de archivos mostrando los archivos regulares. Se seleccionó específicamente "IMG_0001.JPG" para su análisis, mostrando su tamaño de 2.13 MB.

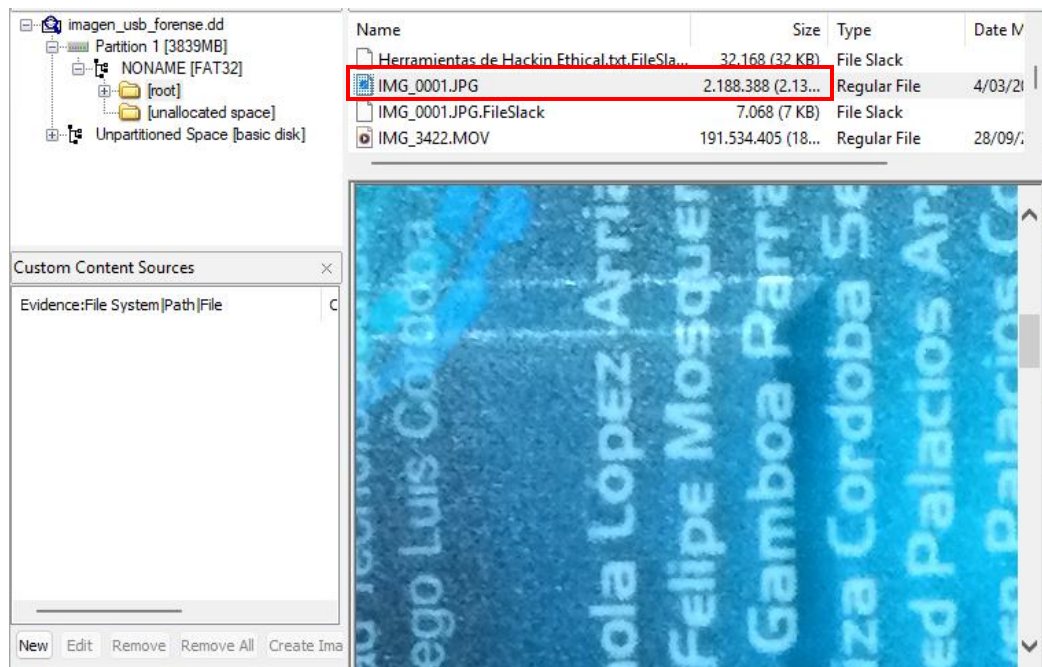


Ilustración 82. Análisis Detallado de Archivos



Se seleccionaron todos los archivos en el sistema de archivos FAT32, incluyendo documentos PDF, archivos Excel, imágenes JPEG, video MOV y archivos de texto para guardar los hash.

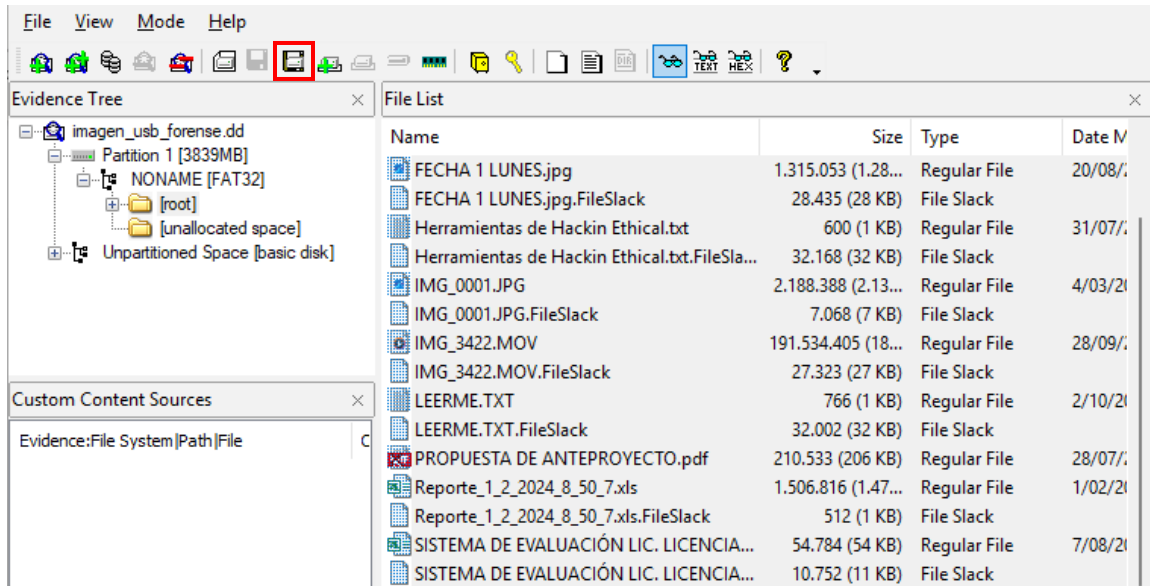


Ilustración 83. Lista Completa de Archivos Recuperados

Se inició el proceso de exportación de los resultados del análisis para documentar los hallazgos forenses en un formato estructurado y procesable.

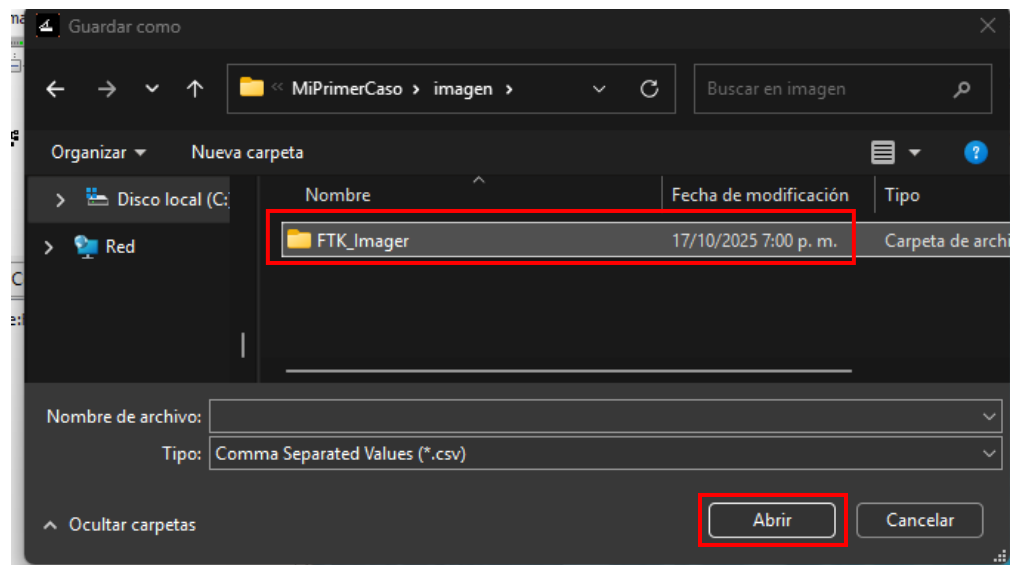


Ilustración 84. Exportación de Resultados a CSV



Se configuró la exportación específicamente para generar un archivo de valores hash, seleccionando el formato CSV y asignando el nombre "hash" al archivo de salida.

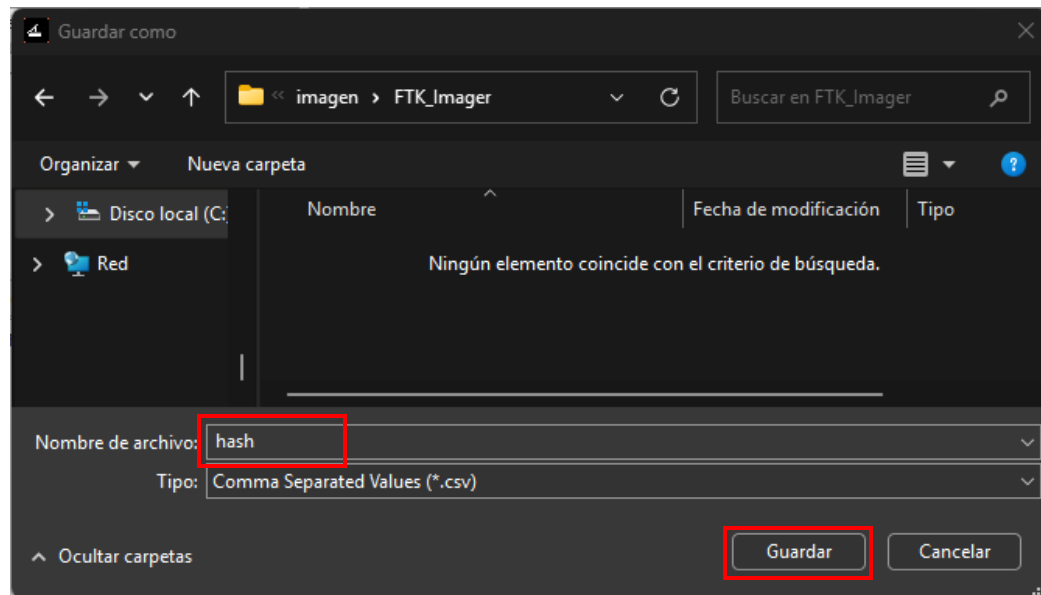


Ilustración 85. Configuración de Exportación de Hash

Se confirmó la creación exitosa del archivo "**hash.csv**" en la carpeta "**FTK_Imager**", validando que la exportación de los valores hash de los archivos analizados se completó correctamente.

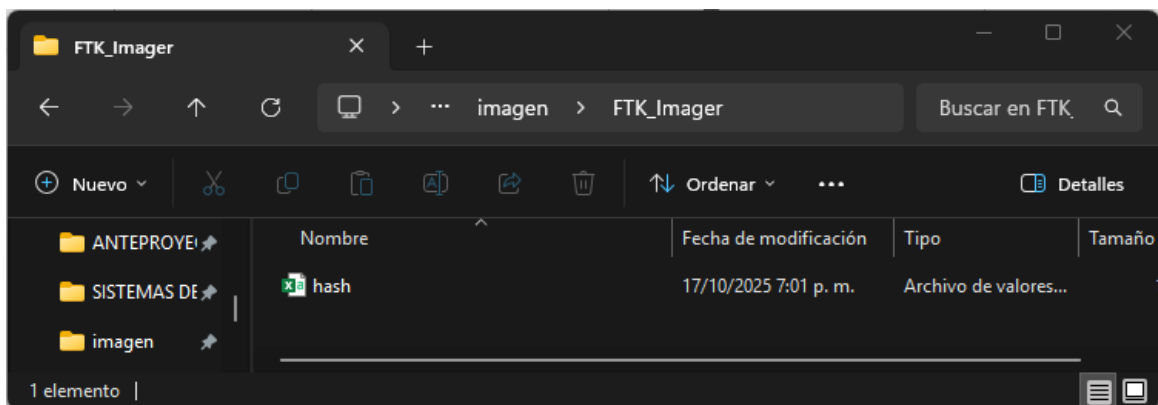


Ilustración 86. Verificación del Archivo de Hash Exportado

Archivo hash abierto.

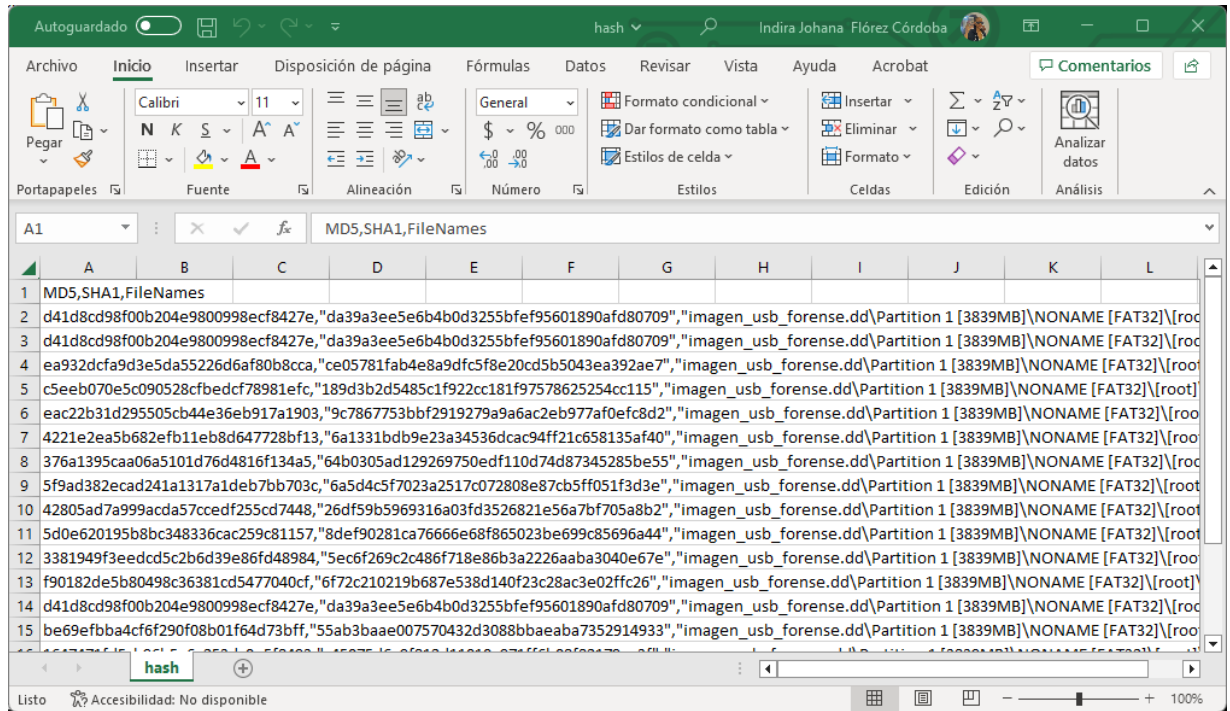


Ilustración 87. Archivo hash



7. CONCLUSIÓN

El uso de Autopsy y FTK Imager facilitó la identificación, clasificación y verificación de archivos contenidos en la memoria USB, demostrando la eficiencia de ambas herramientas en entornos operativos distintos.

Asimismo, se confirmó que los valores hash obtenidos antes y después del proceso coincidieron, validando la preservación íntegra de los datos.



8. BIBLIOGRAFIA

Morales, R. S. (25). *INFORME DE LABORATORIO 02*. Quibdó, Colombia: Universidad Tecnología del Chocó Diego Luis Córdoba. Recuperado el 16 de 10 de 2025