

15-10-2025

# Adquisición de evidencias por software

HECHO POR: IZAN NAVARRO

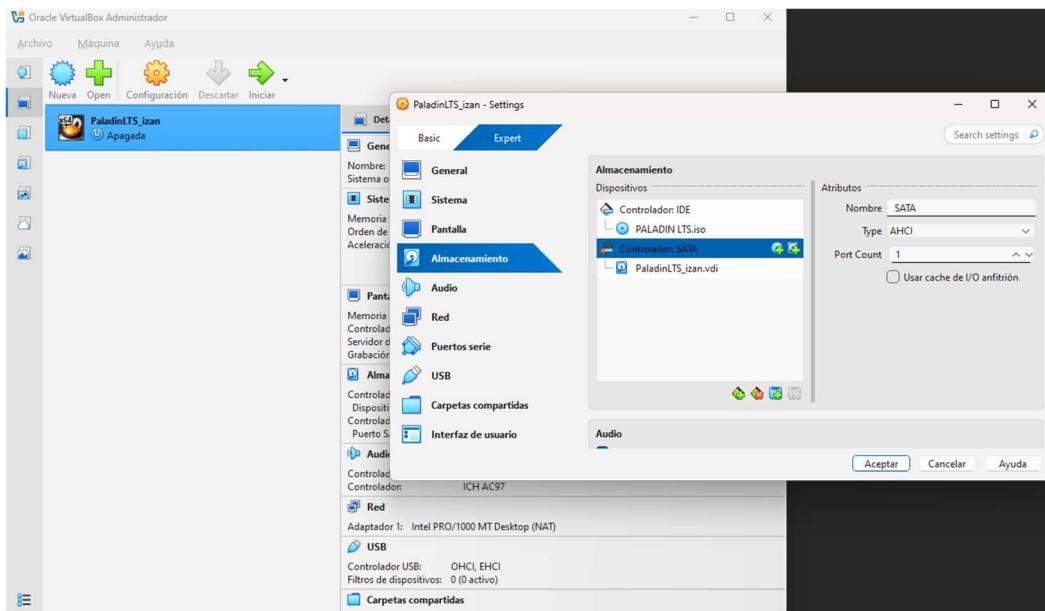
## Indice

<u>1.</u> Adquisición de evidencia con distribución Linux .....	2
2. Adquisición de evidencia con herramienta de software .....	7
3. Adquisición de evidencia con comandos .....	10

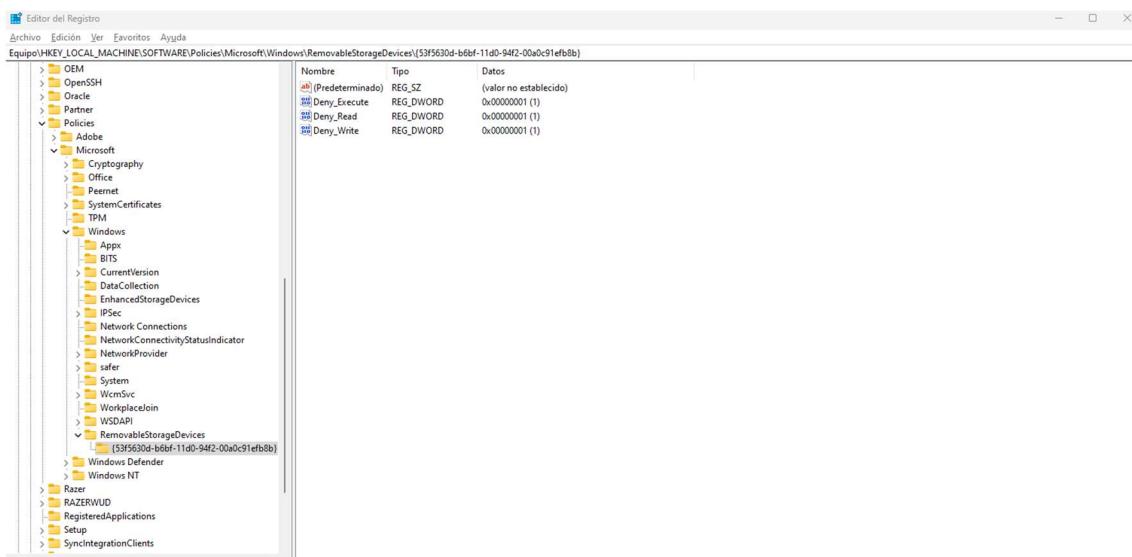
## PRACTICA 1

### 1. Adquisición de evidencia con distribución Linux

1) Creamos la VM y añadimos la iso de Paladin LTS.

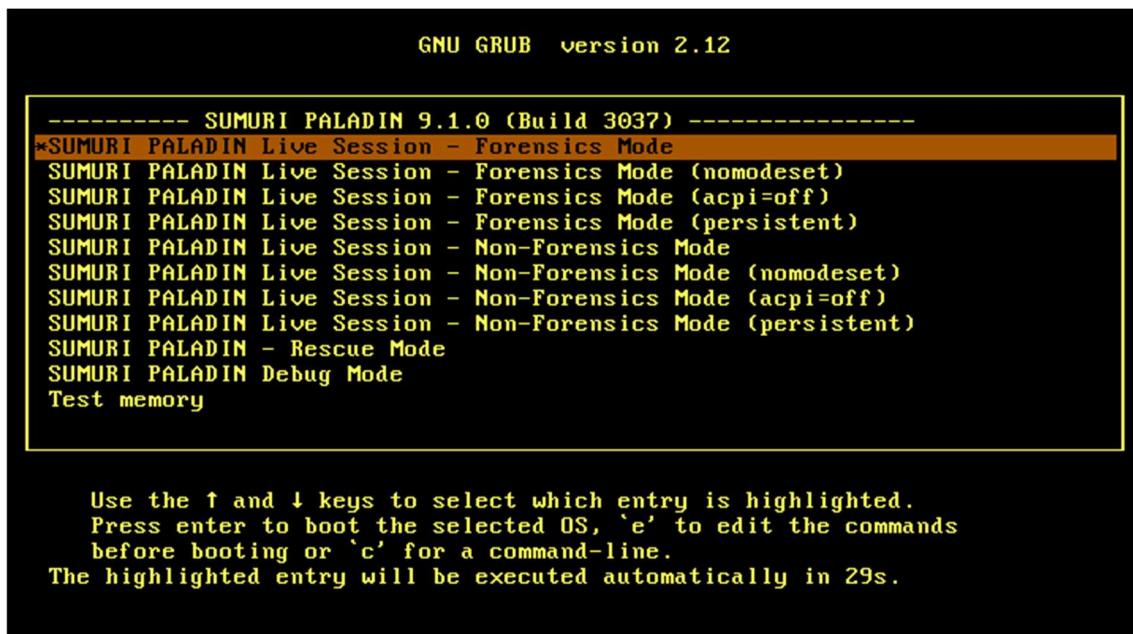


Al ser W11 Home no me funciona el gpedit.msc por lo que tuve que recurrir al "regedit" y crear la clave "RemovableStorageDevices" y crear los 3 datos de execute, read y write para poder denegar las acciones a los discos extraíbles.

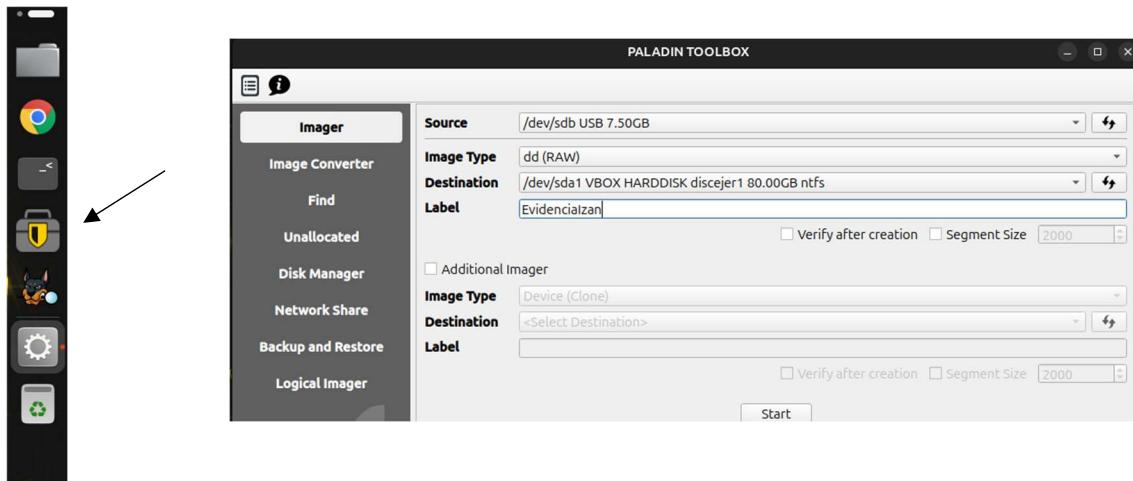


## PRACTICA 1

2) Seleccionamos la opción “Forensics Mode” y entramos a la VM PALADIN LTS.

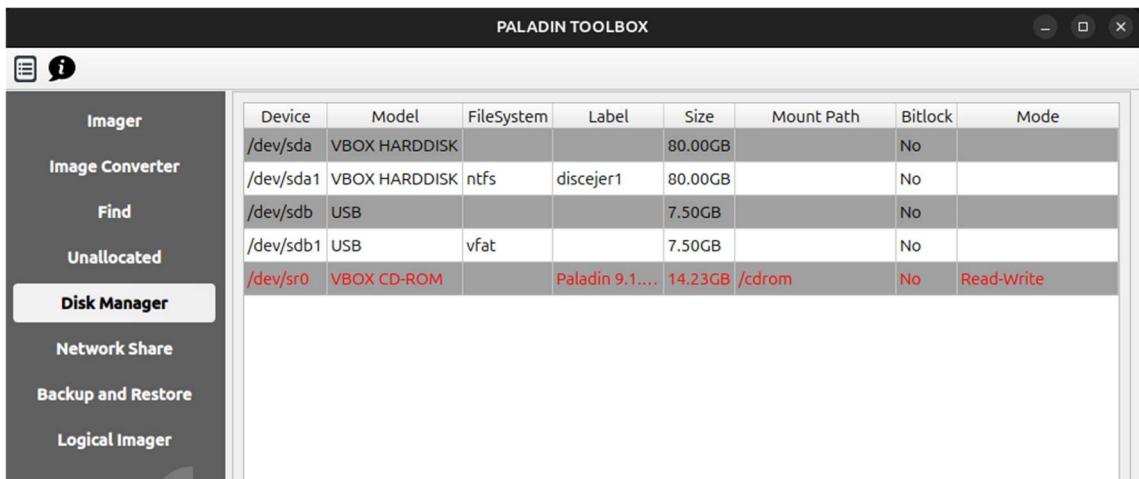


Una vez dentro de la VM seleccionamos el “paladin toolbox” que sale como icono de maleta a la izquierda



3) Dentro del toolbox tenemos el administrador de discos, el cual nos mostrará el DD de la MV como “HARDDISK”, el USB a crear imagen de evidencia como “dev/sdb”, en este caso de 7.5GB, y por último tendremos el primer dispositivo óptico del sistema.

## PRACTICA 1



- 4) Creamos la imagen en formato dd/RAW y seleccionamos Disco que analizar y Destino de la imagen. Esto generará archivos 000

Evid\_Izan.dd - Thunar

File Edit View Go Bookmarks Help

< > ⌂ ⌄ ⌅ ⌆ /media/discejer1/Evid\_Izan.dd/

Warning: you are using the root account. You may harm your system.

Places

- root
- Devices
- File System
- discejer1

Devices

- Evid\_Izan.dd.000
- Evid\_Izan.dd.complete.log
- Evid\_Izan.dd.log
- Evid\_Izan.dd.log.hashes
- Evid\_Izan.dd.process.log
- Evid\_Izan.dd.source\_info
- Evid\_Izan.dd.verify.log

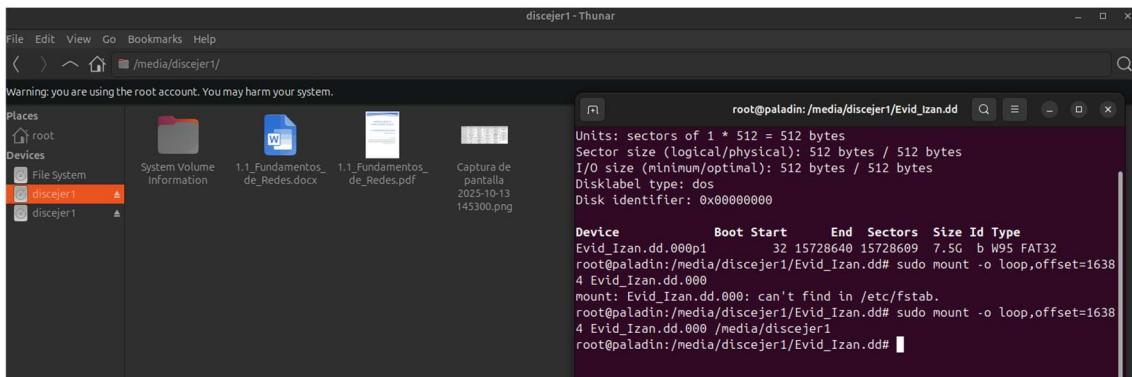
5)

```
root@paladin:/media/discejer1/Evid_Izan.dd# ls
Evid_Izan.dd.000          Evid_Izan.dd.log.hashes  Evid_Izan.dd.verify.log
Evid_Izan.dd.complete.log Evid_Izan.dd.process.log
Evid_Izan.dd.log          Evid_Izan.dd.source_info
root@paladin:/media/discejer1/Evid_Izan.dd# sudo fdisk -l Evid_Izan.dd.000
Disk Evid_Izan.dd.000: 7.5 GiB, 8053064192 bytes, 15728641 sectors
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

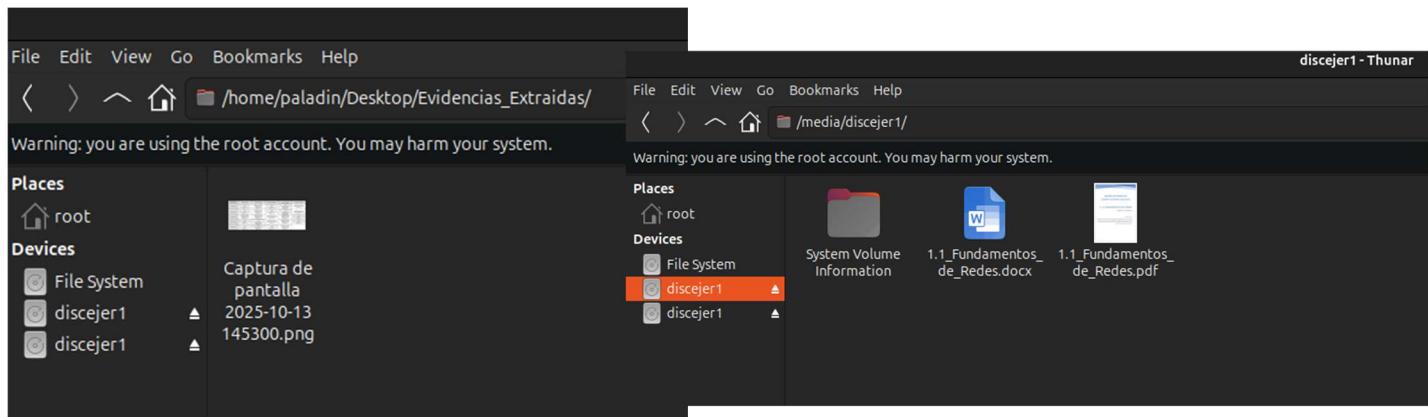
Device      Boot Start     End Sectors  Size Id Type
Evid_Izan.dd.000p1            32 15728640 15728609  7.5G b W95 FAT32
```

## PRACTICA 1

Sí, se puede montar la imagen. He realizado el montaje mediante comandos ya que Paladin LTS no tiene herramienta de montaje por defecto



6) Extraemos un archivo del disco de forma gráfica arrastrando



7) NO ME DEJA USAR AUTOPSY, USO DEL COMANDO "fls -r -d -m / -o (Start)"

Así se listan los archivos borrados anteriormente.

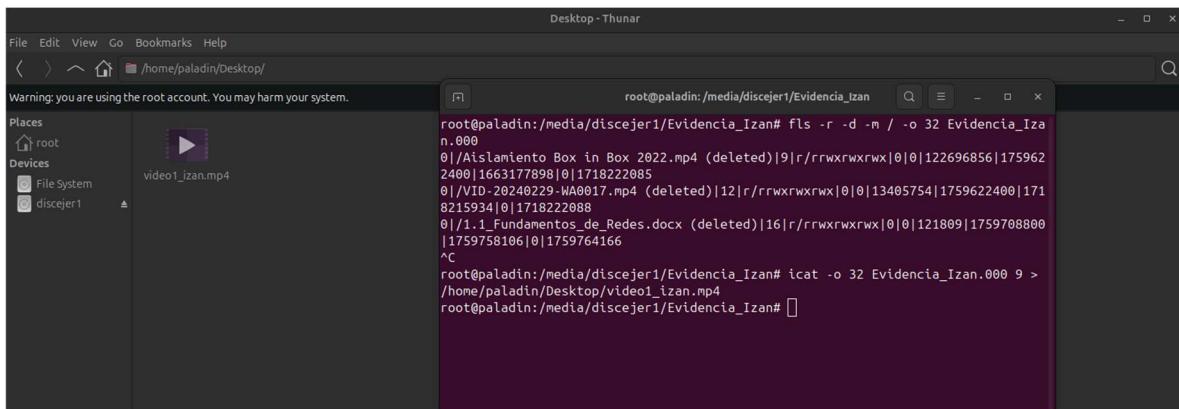
"mmls (evidencia)" lista las particiones. Nosotros estamos usando el Slot 2, con sector 032.

```
root@paladin:/media/discejer1/Evidencia_Izan# mmls Evidencia_Izan.000
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start          End          Length        Description
000:  Meta    000000000000  000000000000  00000000001  Primary Table (#0)
001:  -----  000000000000  00000000031   00000000032  Unallocated
002:  000:000  00000000032  0015728640    0015728609  Win95 FAT32 (0x0b)
root@paladin:/media/discejer1/Evidencia_Izan# fls -r -d -m / -o 32 Evidencia_Izan.000
0|/Aislamiento Box in Box 2022.mp4 (deleted)|9|r/rwrxrwxrwx|0|0|122696856|175962400|1663177898|0|1718222085
0|/VID-20240229-WA0017.mp4 (deleted)|12|r/rwrxrwxrwx|0|0|13405754|1759622400|1718215934|0|1718222088
0|/1.1_Fundamentos_de_Netw.docx (deleted)|16|r/rwrxrwxrwx|0|0|121809|1759708800|1759758106|0|1759764166
```

## PRACTICA 1

Así se recuperan archivos borrados anteriormente: “icat -o <start\_sector> /ruta/a/imagen\_completa.dd 12 > /ruta/de/salida/archivo\_recuperado”



8) EXCEL RELLENADO (comandos de ayuda para conocer información de la imagen dd/RAW)

```
root@paladin:/media/discejer1/Evidencia_Izan# udevadm info --query=all --name=/dev/sdb | grep -i serial
E: ID_SERIAL=ASolid_USB_02122023-0:0
```

```
Disk /dev/sda: 80 GiB, 85899345920 bytes, 167772160 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: gpt
Disk identifier: 53A7B8B0-D5C9-4344-A5A7-C69AA30782BF
```

Device	Start	End	Sectors	Size	Type
/dev/sda1	2048	167770111	167768064	80G	Microsoft basic data

```
root@paladin:/media/discejer1# udevadm info --query=all --name=/dev/sda | grep -i serial
E: ID_SERIAL=VBOX_HARDDISK_VBbcf8520d-a5cabf0a
E: ID_SERIAL_SHORT=VBbcf8520d-a5cabf0a
root@paladin:/media/discejer1#
```

```
root@paladin:/media/discejer1# date -u
Mon Oct 13 21:15:01 UTC 2025
```

```
dc3dd 7.2.646 started at 2025-10-13 18:40:54 +0000
compiled options:
command line /usr/bin/dc3dd if=/dev/sdb hash=md5 hash=sha1
of=/media/discejer1/Evidencia_Izan/Evidencia_Izan.000
log=/media/discejer1/Evidencia_Izan/Evidencia_Izan.log
hlog=/media/discejer1/Evidencia_Izan/Evidencia_Izan.log.hashes bufsz=512k
input results for device `/dev/sdb':
 7a4eb2ff2990afbcfb2941082ffbb599 (md5)
 906d0f9fcdb85127c2520655db259183d83566bc7 (sha1)
output results for file `/media/discejer1/Evidencia_Izan/Evidencia_Izan.000':
dc3dd completed at 2025-10-13 18:59:13 +0000
```

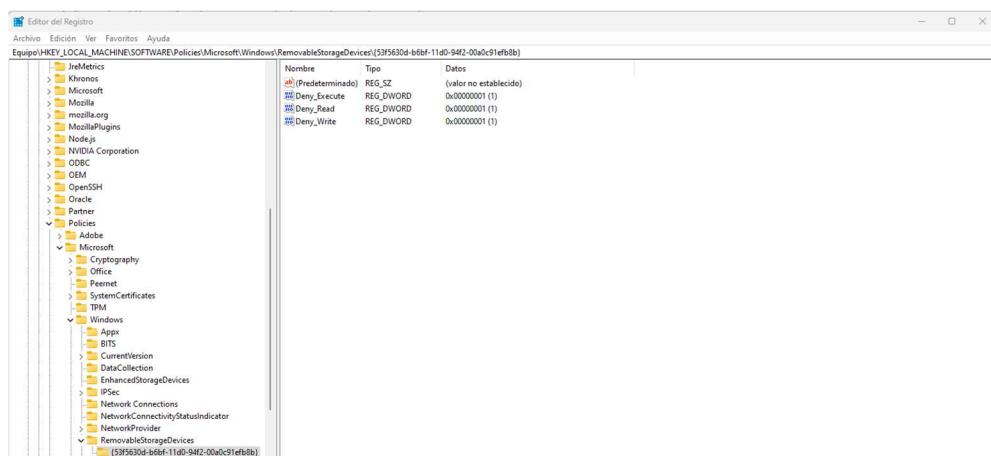
## PRACTICA 1

### 2. Adquisición de evidencia con herramienta de software

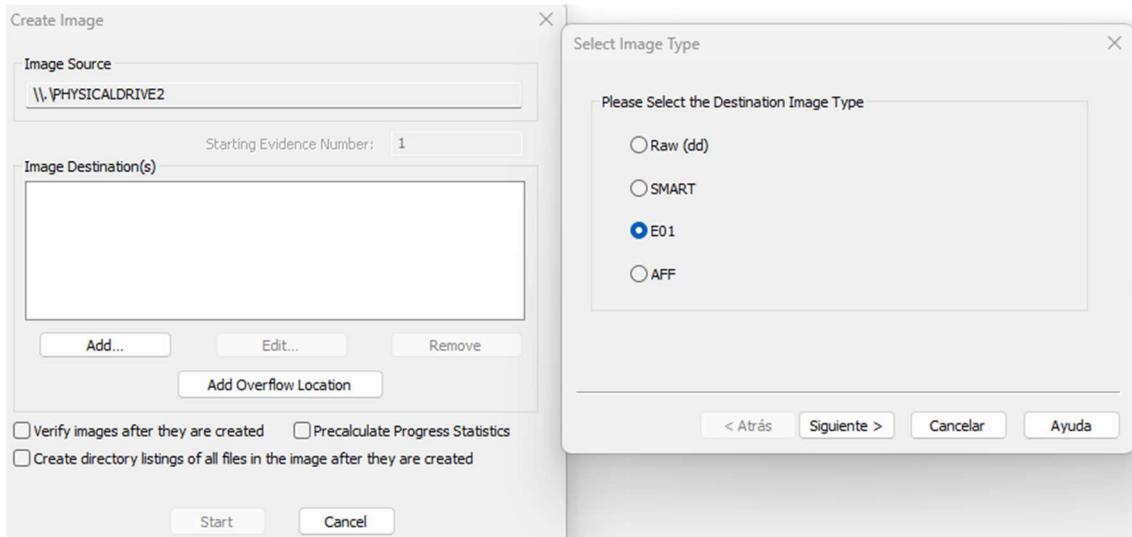
1) Instalamos el FTK Imager y seleccionamos el icono creado en el escritorio.



2) Configuración mediante “regedit” para poder Denegar acceso, lectura y ejecución a dispositivos extraíbles en un W10.



3) Arrancamos el FTK y le damos a la opción “File > Create Image Disk” y nos saltarán estas pantallas. Creamos una imagen en formato E01 como copia.



## PRACTICA 1

Evidence Item Information

Case Number:	001
Evidence Number:	001
Unique Description:	USB
Examiner:	Izan Navarro
Notes:	USB from a Crime

[< Atrás](#) [Siguiente >](#) [Cancel](#) [Help](#)

4) Creamos una segunda imagen del disco en un formato dd/Raw y lo guardamos dentro del escritorio

The screenshot shows the FTK Imager interface. On the left, there's a sidebar with tabs for 'Creating', 'Image Source', 'Destination', 'Status', and 'Progress'. The 'Creating' tab is active, showing a progress bar at 100%. The main area has tabs for 'Evidence Tree' and 'File List'. Under 'Evidence Tree', it shows 'A:\PHYSICALDRIVE2'. A 'Create Image' dialog box is open, with 'Image Source' set to 'A:\PHYSICALDRIVE2' and 'Image Destination(s)' set to 'C:\Users\Izan\Desktop\PROYECTOS DE GITHUB'. Below this, a 'Select Image Type' dialog box is open, with 'Raw (dd)' selected. At the bottom of the interface, there are buttons for 'New', 'Edit', 'Remove', 'Remove All', 'Create Image', 'Properties', 'Hex Value Inter...', 'Custom Conte...', and 'For User Guide, press F1'. A 'Cancel' button is also present.

**Select Image Type**

Please Select the Destination Image Type

- Raw (dd)
- SMART
- E01
- AFF

**Create Image**

Image Source  
A:\PHYSICALDRIVE2

Starting Evidence Number: 1

Image Destination(s)  
C:\Users\Izan\Desktop\PROYECTOS DE GITHUB

Add... Edit... Remove Add Overflow Location

Verify images after they are created  Precalculate Progress Statistics   
Create directory listings of all files in the image after they are created

**Select Image Destination**

Image Destination Folder  
C:\Users\Izan\Desktop\PROYECTOS DE GITHUB [Browse](#)

Image Filename (Excluding Extension)  
Evidencia

Image Fragment Size (MB)  
For Raw, E01, and AFF formats: 0 = do not fragment 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest) 0

Use AD Encryption

[< Atrás](#) [Finish](#) [Cancel](#) [Help](#)

File List

A:\PHYSICALDRIVE2

New Edit Remove Remove All Create Image Properties Hex Value Inter... Custom Conte... For User Guide, press F1 Cancel

dd 14/10/2025 23:18 Carpeta de archivos

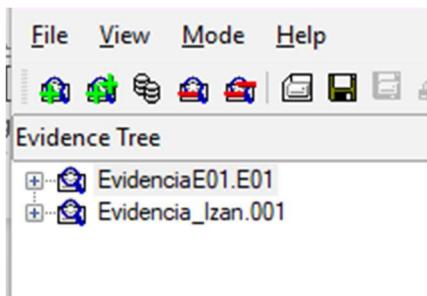
E01 14/10/2025 23:20 Carpeta de archivos

**Evidencia**

	Evidencia	14/10/2025 10:07	Archivo WinRAR 1.536.000 KB
	Evidencia.001	14/10/2025 10:08	Archivo de valores... 17 KB
	Evidencia.001	14/10/2025 10:09	Documento de te... 2 KB
	Evidencia.002	14/10/2025 10:07	Archivo 002 1.536.000 KB
	Evidencia.003	14/10/2025 10:08	Archivo 003 1.536.000 KB
	Evidencia.004	14/10/2025 10:08	Archivo 004 1.536.000 KB
	Evidencia.005	14/10/2025 10:08	Archivo 005 1.536.000 KB
	Evidencia.006	14/10/2025 10:08	Archivo 006 184.321 KB

## PRACTICA 1

- 5) Verificación de hashes entre 01 y dd mediante la opción “File > Verify Disk” en ambas imágenes.



No hay diferencias encontradas ya que los hashes son idénticos

Two windows titled "Drive/Image Verify Results" are shown side-by-side, comparing the hash verification results for two evidence files. Both windows show identical results for MD5 and SHA1 hashes, indicating a perfect match.

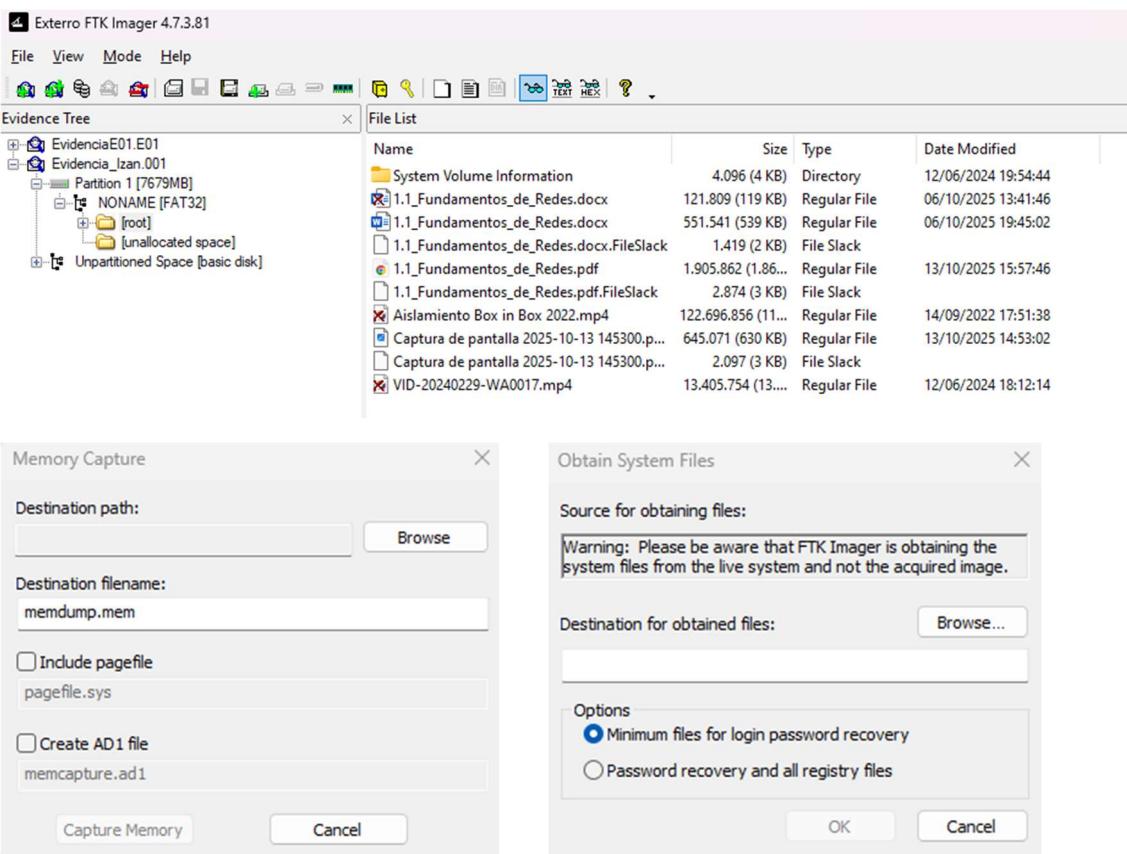
Name	Evidencia_Izan.001	EvidenciaE01.E01
Sector count	15728641	15728641
MD5 Hash		
Computed hash	ac8ad0cd85023095abb16122249f5eba	ac8ad0cd85023095abb16122249f5eba
Report Hash	ac8ad0cd85023095abb16122249f5eba	ac8ad0cd85023095abb16122249f5eba
Verify result	Match	Match
SHA1 Hash		
Computed hash	ab3e6dbe14663e47b8f0fb1009bf287b813ac	ab3e6dbe14663e47b8f0fb1009bf287b813ac
Report Hash	ab3e6dbe14663e47b8f0fb1009bf287b813ac	ab3e6dbe14663e47b8f0fb1009bf287b813ac
Verify result	Match	Match
Bad Blocks List		
Bad block(s) in image	No bad blocks found in image	No bad blocks found in image

- 6) FTK Imager permite:

- **Visualizar el contenido de discos o imágenes forenses** sin modificarlos, garantizando la integridad de la evidencia.
- Extraer archivos específicos, **calcular y verificar hashes (MD5, SHA1, SHA256)** y **generar informes automáticos** con toda la información del proceso.
- Admite varios formatos de imagen (**E01, RAW, AFF, SMART**) y ofrece una herramienta para **capturar la memoria RAM** del sistema.

Estos son algunos apartados de la app que se muestran de forma visual:

## PRACTICA 1



### 3. Adquisición de evidencia con comandos

1) Identificamos el USB con “`sudo fdisk -l`”

```
Disk /dev/sdb: 7.5 GiB, 8053064192 bytes, 15728641 sectors
Disk model: USB
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

Device      Boot Start    End  Sectors  Size Id Type
/dev/sdb1            32 15728640 15728609  7.5G  b W95 FAT32
root@paladin:/home/paladin#
```

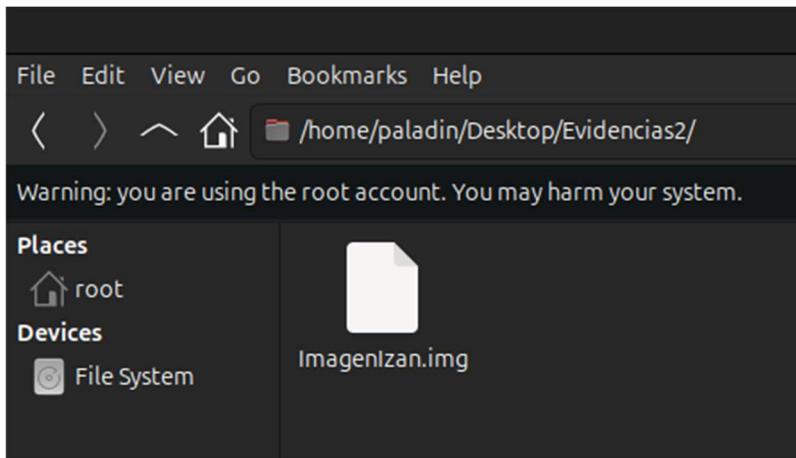
Ejecutamos el comando que crea el .dd “`sudo dd if=/dev/sdb of=/ruta/donde/guardar/usb.img bs=4M status=progress conv=sync`”

```
root@paladin:/home/paladin# sudo dd if=/dev/sdb of=/home/paladin/Desktop/Evidencias/imagenComandos.img bs=4M status=progress conv=sync
977272832 bytes (977 MB, 932 MiB) copied, 12 s, 81.3 MB/s
```

- `if=/dev/sdb` → dispositivo de entrada (tu USB).
- `of=/ruta/donde/guardar/usb.img` → archivo de salida (la imagen).
- `bs=4M` → tamaño de bloque de 4 MB (más rápido que el default).

## PRACTICA 1

- status=progress → muestra el progreso de la copia.
- conv=sync → rellena bloques incompletos con ceros para mantener la integridad.



2) Usamos el comando “**sha256sum /ruta/donde/guardar/usb.img**” para calcular el sha256 de la imagen.

```
root@paladin:/home/paladin/Desktop/Evidencia1# sha256sum Imagen_1.img  
1810545d38e3ab87c72a82e8db54112ab5778a78c5905a1859964b49e0140a48 Imagen_1.img
```

**Durante este proceso la VM Paladin LTS se quedaba bloqueada y he tenido que cortar la imagen al principio para poder seguir con los pasos (en un principio tendría que salirme el mismo hash que los ejercicios anteriores)**

3) Se realizó la adquisición forense del dispositivo USB mediante el comando dd, con el fin de generar una copia bit a bit de todos los sectores del medio:

```
sudo dd if=/dev/sdb of=/home/usuario/usb.img bs=4M status=progress conv=sync
```

La imagen resultante (usb.img) contiene todos los datos originales del USB, incluyendo archivos visibles, eliminados y el espacio libre.

Posteriormente, se calculó el hash de la imagen generada para garantizar su integridad:

```
sha256sum /home/usuario/usb.img
```

Al comparar el valor de hash de la imagen anterior completa del mismo USB, los resultados hubiesen sido idénticos (si no fuera por culpa del bloqueo de la VM), lo cual confirma que la copia es fiel al original.

**Herramienta elegida: sha256sum**

Motivo: Es una herramienta integrada en Linux, rápida, confiable y basada en un algoritmo criptográfico seguro (SHA-256). Permite verificar fácilmente la integridad de los datos sin requerir software adicional.