

2. CLONACIÓN CON HARDWARE Y MONTAJE DE IMÁGENES

Hecho por:
Izan Navarro

INDICE

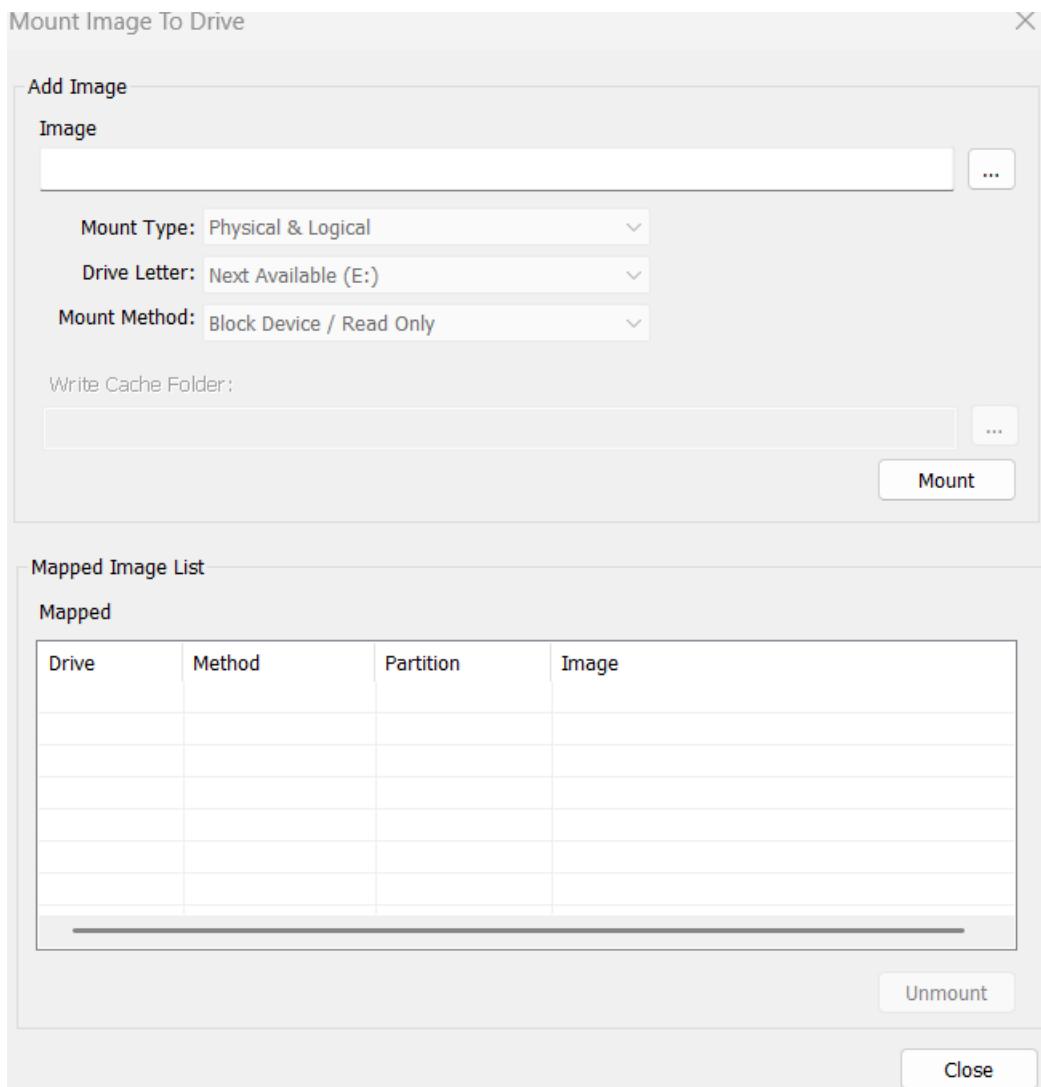
1. Montaje de imagen.....	3
2. Montaje de imagen Linux.....	8
3. Adquisición de evidencia mediante hardware.....	11

1. MONTAJE DE IMAGEN

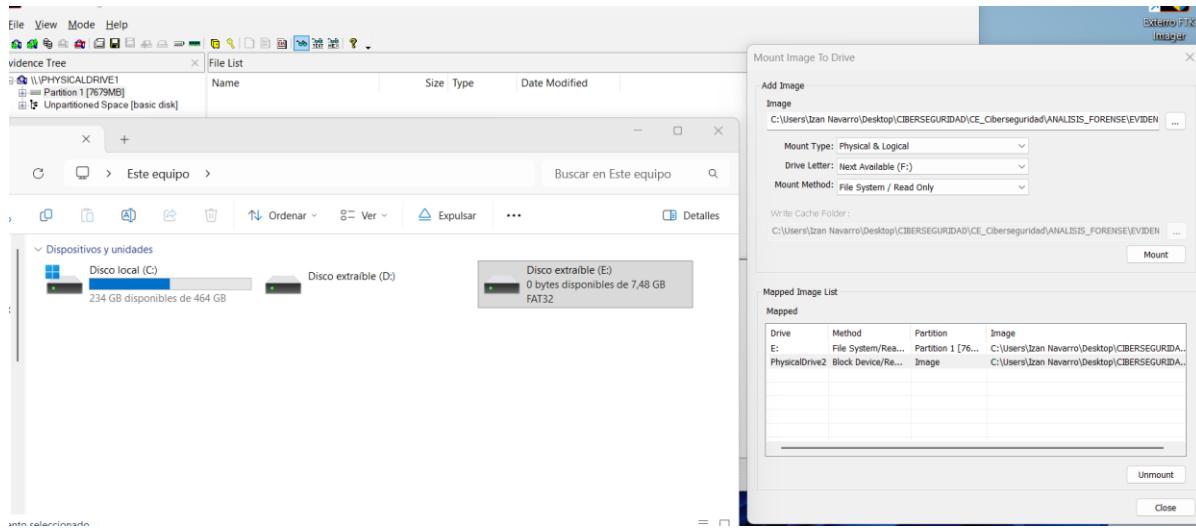
Elige cualquiera de las imágenes generadas en la práctica anterior y realiza las siguientes actividades con ella (puedes usar tanto FTK Imager como Arsenal image mounter)

1. Monta la imagen en modo de solo lectura (RO) para poder explorar el contenido de la imagen. Fíjate si hay varias particiones. Móntalas todas.

Seleccionamos “File > Image Mounting” y seleccionamos la imagen a montar para poder hacer en solo lectura (RO).



Nos aparecerá en nuevo disco duro con la imagen montada en read only:

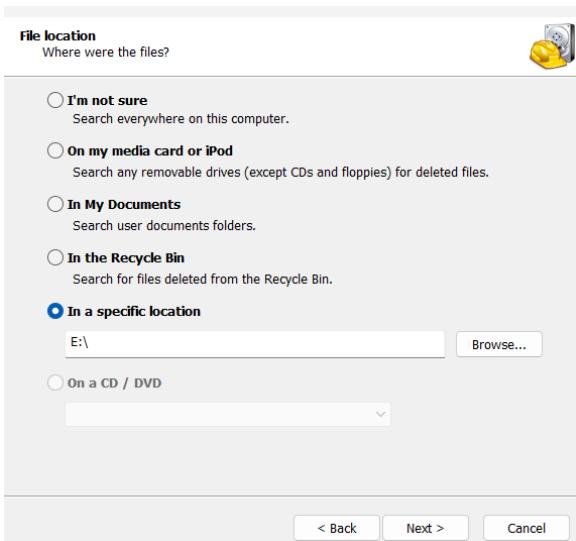


2. Utiliza cualquier herramienta Windows para recuperar archivos borrados (por ejemplo, Recuva <https://www.ccleaner.com/recuva>). ¿Has descubierto archivos eliminados?

1) Instalamos Recuva:



2) Elegimos el disco a recuperar archivos, en mi caso el E: y seleccionamos “all Files” y activamos la opción de Deep Scan:



Thank you, Recuva is now ready to search for your files

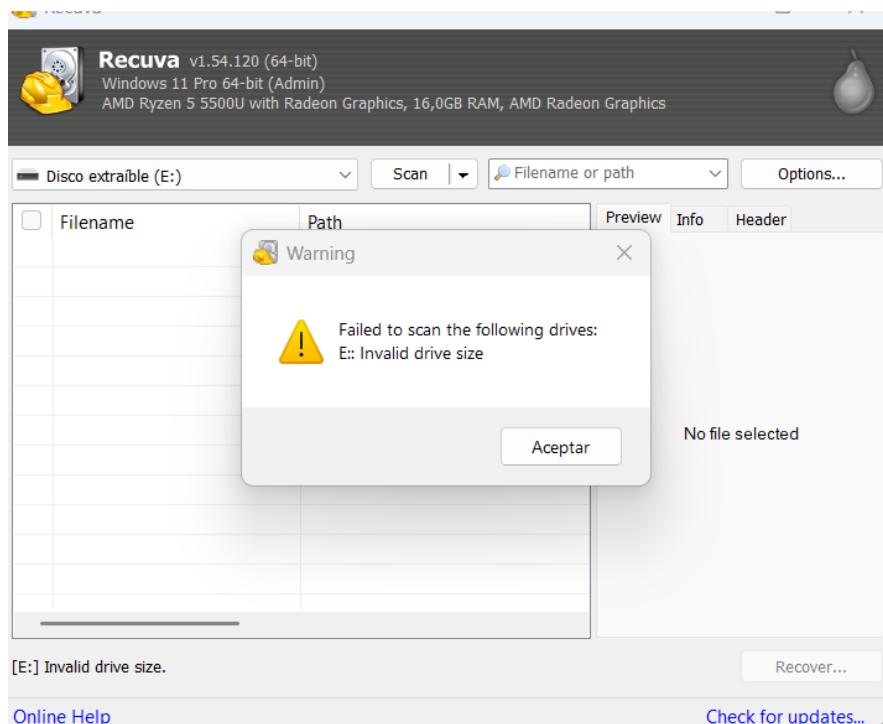
After the search is complete you will see a list of the files Recuva has found. Simply check the files you would like to recover and click the Recover button.

Check this box if previous scans have failed to find your files. Note that this may take over an hour on a large drive.

Enable Deep Scan

Click Start to begin the search.

3) Intento Scanear la imagen en Recuva y siempre me salta este Mensaje:



Pero en cambio sí que puedo entrar dentro de la imagen y ver los archivos dentro de la carpeta “root”:

Nombre	Fecha de modificación	Tipo	Tamaño
System Volume Information	12/06/2024 21:54	Carpeta de archivos	
1.1_Fundamentos_de_NeRedes	06/10/2025 21:45	Documento de Mi...	539 KB
1.1_Fundamentos_de_NeRedes	13/10/2025 17:57	Microsoft Edge PD...	1.862 KB
Captura de pantalla 2025-10-13 145300	13/10/2025 16:53	Archivo PNG	630 KB

3. Utiliza ahora PhotoRec para hacer carving sobre la imagen y observa el resultado, ¿Has descubierto más archivos o los mismos que en el punto anterior? Explica el motivo del resultado de esta comparación.

1) Arrancamos “photorec_win.exe” y seleccionamos nuestro DD:

```

PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media and choose 'Proceed' using arrow keys:
Disk \\.\PhysicalDrive0 - 500 GB / 465 GiB (R0) - WD Blue SN580 500GB
Disk \\.\PhysicalDrive1 - 8053 MB / 7680 MiB (R0) - ASolid USB
Drive E: - 8036 MB / 7663 MiB (R0) - Callback Technologies Virtual Storage

-[Proceed ] [ Quit ]

Note: Serial number 0000000005^F^X
Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has an incorrect size, check HD jumper settings and BIOS
detection, and install the latest OS patches and disk drivers.

```

2) Dentro, seleccionamos “whole disk” y de formato “Other”:

```

C:\Users\Izan Navarro\Downloads\testdisk-7.3-WIP.win64\testdisk-7.3-WIP\photorec_win.exe

PhotoRec 7.3-WIP, Data Recovery Utility, September 2025
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

P Unknown          0   0   1 245247   0 32   15695840

To recover lost files, PhotoRec needs to know the filesystem type where the
file were stored:
[ ext2/ext3 ] ext2/ext3/ext4 filesystem
>[ Other ] FAT/NTFS/HFS+/ReiserFS...

```

3) Seleccionamos un espacio del equipo donde recuperar los datos borrados y no borrados de la imagen creada, en mi caso “C:/Recuperados”:

```

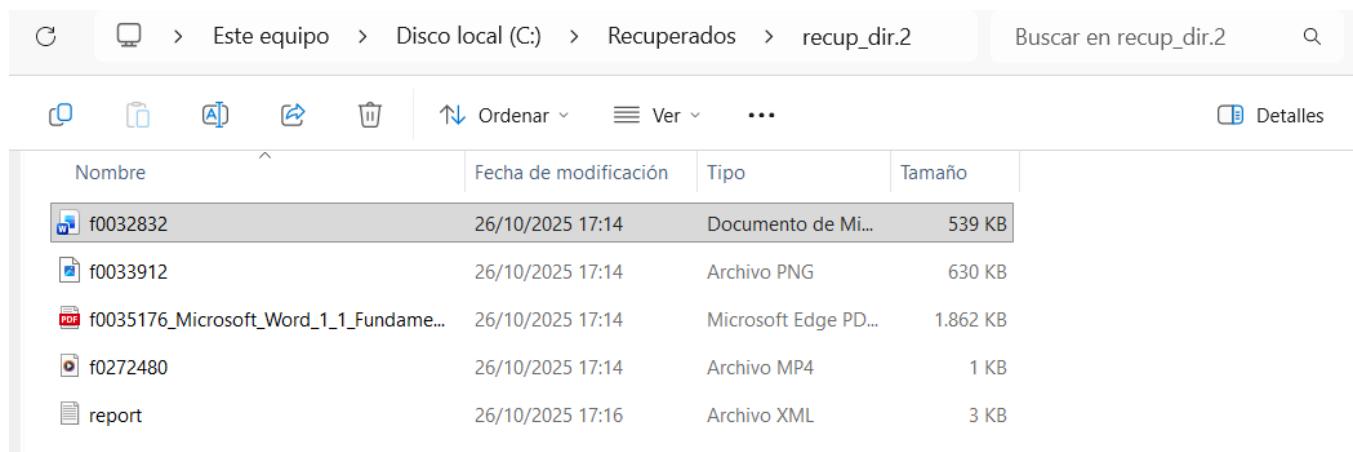
Disk \\.\PhysicalDrive1 - 8053 MB / 7680 MiB (RO) - ASolid USB
      Partition          Start          End    Size in sectors
      No partition       0            0        1      979   15 61    15728641 [Whole disk]

Destination /cygdrive/c/Recuperados/recup_dir

Pass 1 - Reading sector 2997144/15728641, 4 files found
Elapsed time 0h00m21s - Estimated time to completion 0h01m29
mov: 1 recovered
png: 1 recovered
zip: 1 recovered
pdf: 1 recovered

```

- 4) Una vez terminado se nos creará una carpeta “recup_dir.X” donde nos aparecerán los elementos borrados y no borrados de la Imagen o USB
Evidencia:



The screenshot shows a Windows File Explorer interface. The path is displayed as: This PC > Local Disk (C:) > Recuperados > recuper_dir.2. A search bar at the top right contains the text "Buscar en recuper_dir.2". Below the search bar is a toolbar with icons for back, forward, refresh, and file operations. To the right of the toolbar is a "Details" button. The main area displays a table of recovered files:

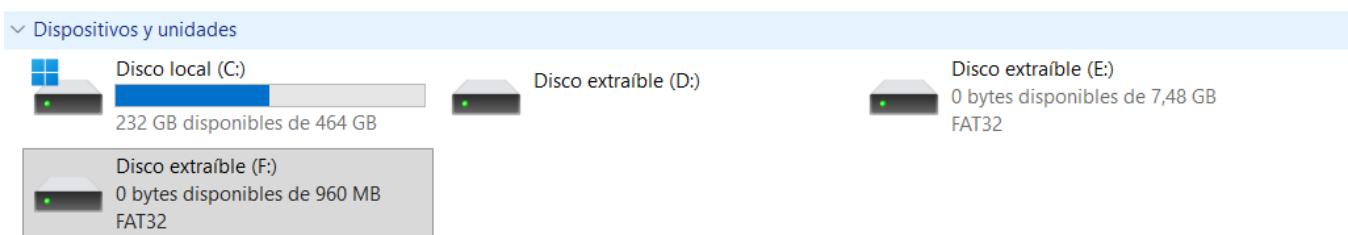
Nombre	Fecha de modificación	Tipo	Tamaño
f0032832	26/10/2025 17:14	Documento de Mi...	539 KB
f0033912	26/10/2025 17:14	Archivo PNG	630 KB
PDF f0035176_Microsoft_Word_1_1_Fundame...	26/10/2025 17:14	Microsoft Edge PD...	1.862 KB
f0272480	26/10/2025 17:14	Archivo MP4	1 KB
report	26/10/2025 17:16	Archivo XML	3 KB

2. MONTAJE DE IMAGEN LINUX

Adjunta a esta práctica hay una imagen de una adquisición de un disco con sistema Linux. La tarea es montar la imagen (siempre en modo RO) y responder a algunas preguntas. Para ello sigue estos pasos:

1. Monta la imagen en un sistema Windows con la misma herramienta que el punto anterior (FTK Imager o Arsenal image mounter)

Montamos la imagen como “System File/Read Only” con la letra F:



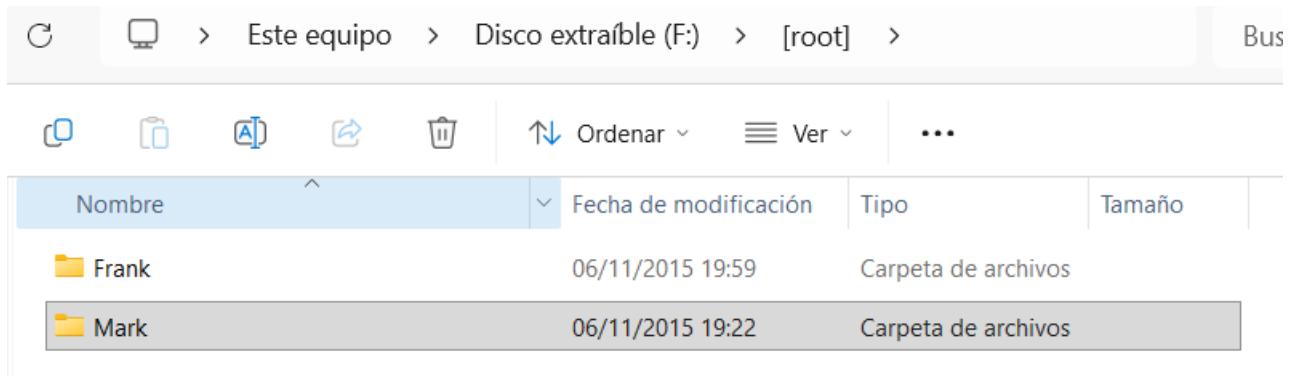
2. Despues de montarla, ¿puedes acceder al sistema de archivos? En caso afirmativo pasa directamente al punto 5. En caso negativo, ¿Por qué crees que no puedes acceder al sistema de archivos?

Una vez entro al disco Extraible F me sale esta ruta de directorios:

A file browser interface showing the contents of the mounted Linux image at the path /root. An arrow points to the [root] folder. The table lists the files and their details:

📁 [root]	06/11/2015 19:21	Carpeta de archivos
📁 [unallocated space]		Carpeta de archivos
📄 bad blocks	06/11/2015 18:05	Archivo 4 KB
📄 block bitmap		Archivo 32 KB
📄 boot record		Archivo 1 KB
📄 group descriptor table		Archivo 20 KB
📄 inode bitmap		Archivo 32 KB
📄 inode table		Archivo 15,360 KB
📄 superblock		Archivo 20 KB

Dentro de “root” tengo todos los datos de la Imagen (pero ns si es eso lo que pide la actividad):



Como veo que así no se debería listar el sistema de archivos lo voy a hacer en linux.

3. Monta ahora la imagen en un sistema Linux usando un terminal (puedes usar Paladin o tu distribución favorita).

1) Instalamos las librerías necesarias para poder montar una imagen por terminal:

```
izan@Izan-Ubuntu20:~/Descargas$ sudo apt install kpartx mount
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Paquetes sugeridos:
  nfs-common
Se instalarán los siguientes paquetes NUEVOS:
  kpartx
Se actualizarán los siguientes paquetes:
  mount
```

2)

```
izan@Izan-Ubuntu20:~/Descargas/Imagen ejercicio 2$ sudo kpartx -av Linux\ Financial\ Case.001
add map loop7p1 (253:0): 0 1966080 linear 7:7 2048
izan@Izan-Ubuntu20:~/Descargas/Imagen ejercicio 2$
```

Creamos una carpeta para montar la imagen y hacerla con “-o ro” que es read Only:

```
izan@Izan-Ubuntu20:~/Descargas/Imagen ejercicio 2$ sudo mkdir /mnt/linuxImage
izan@Izan-Ubuntu20:~/Descargas/Imagen ejercicio 2$ sudo mount -o ro /dev/mapper/
loop7p1 /mnt/linuxImage
izan@Izan-Ubuntu20:~/Descargas/Imagen ejercicio 2$
```

4. Después de montarla, ¿puedes acceder al sistema de archivos? En caso afirmativo pasa directamente al punto 5. En caso negativo, ¿Por qué crees que no puedes acceder al sistema de archivos?

Visualizamos la imagen montada y esta vez tenemos toda la información de la evidencia bien estructurada

```
Izan@Izan-Ubuntu20:~/Descargas/Imagen ejercicio 2$ ls -l /mnt/linuxImage/
total 8
drwxrwxr-x 2 2002 2002 4096 nov  6  2015 Frank
drwxrwxr-x 4 1001 1001 4096 nov  6  2015 Mark
```

5. ¿Cuántas carpetas encuentras y cuáles son sus nombres?

Encontramos como en la imagen anterior 2 carpetas llamadas “Frank” y “Mark”.

6. Examina las carpetas y sus nombres. ¿Qué tipo de contenido tienen? ¿Qué datos están almacenando ¿Datos de ventas, de compras, de otra cosa?

Dentro de la Carpeta “Mark” encontraremos 2 carpetas adicionales “Finance_Confidential” con un archivo “Earning.xls” y después una carpeta “Transport” con un archivo “Presentation.ppt”.

```
Izan@Izan-Ubuntu20:~/Descargas/Imagen ejercicio 2$ ls -l /mnt/linuxImage/Mark/
total 8
drwxrwxr-x 2 1001 1001 4096 nov 13 2015 Finance_Confidential
drwxrwxr-x 2 1001 1001 4096 nov  6 2015 Transport
Izan@Izan-Ubuntu20:~/Descargas/Imagen ejercicio 2$ ls -l /mnt/linuxImage/Mark/Finance_Confidential/
total 4
-rw-rw-r-- 1 1001 1001 43 nov 13 2015 Earning.xls
Izan@Izan-Ubuntu20:~/Descargas/Imagen ejercicio 2$ ls -l /mnt/linuxImage/Mark/Transport/
total 180
-rw-rw---- 1 1001 1001 180224 nov  6 2015 Presentation.ppt
Izan@Izan-Ubuntu20:~/Descargas/Imagen ejercicio 2$ █
```

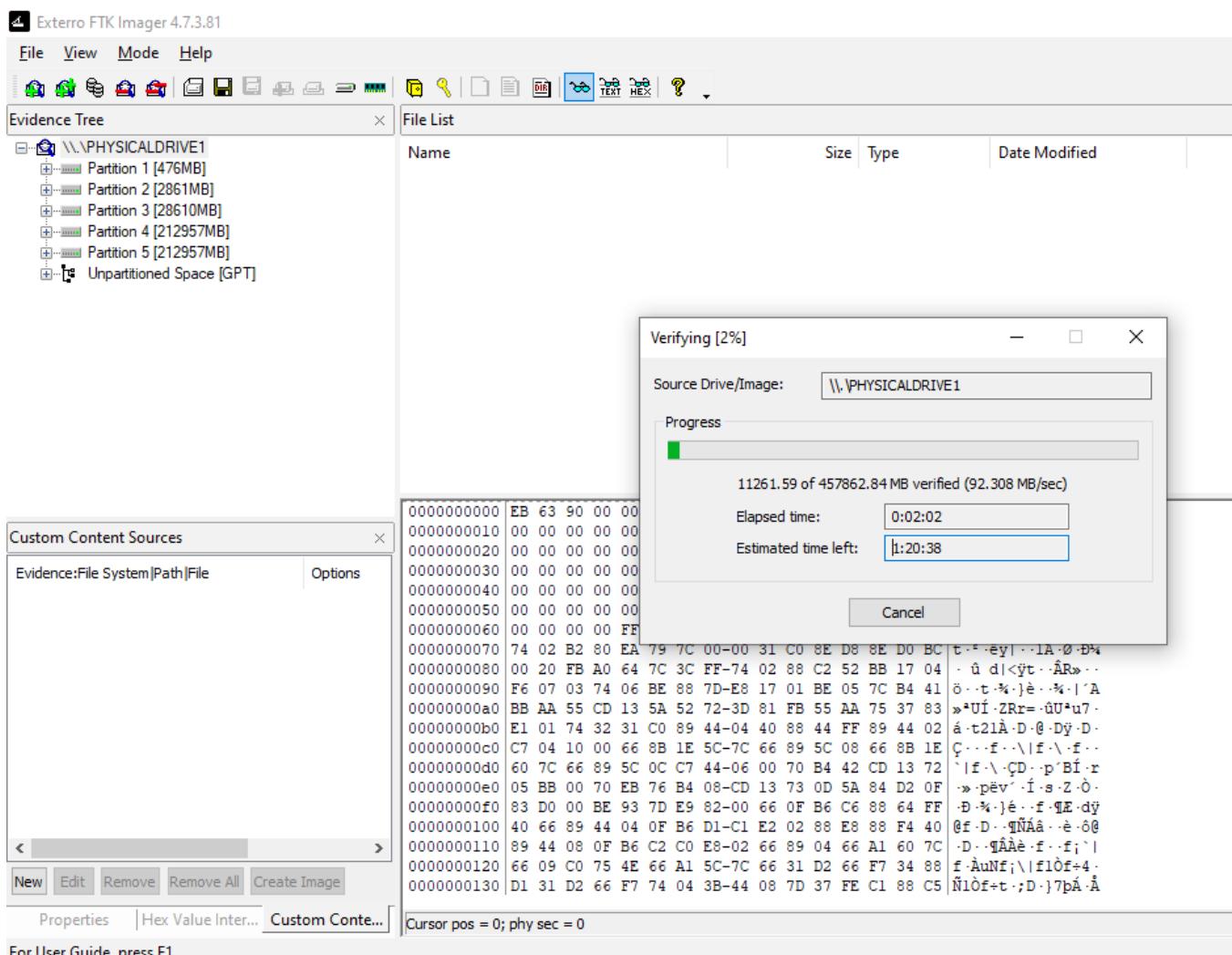
Dentro de la Carpeta “Frank” encontraremos un archivo .xls llamado “Appointments.xls”

3. ADQUISICIÓN DE EVIDENCIA MEDIANTE HARDWARE

DISCO ORIGEN – INF 23

DISCO DESTINO – INF 28

1) Verificar la Imagen para hallar el hash



2) HASH DEL DISCO ORIGEN

Drive/Image Verify Results

Name	\.\.\PHYSICALDRIVE1
Sector count	937703088
MD5 Hash	
Computed hash	900f42063fdf9e77cf94734aff3b1350
SHA1 Hash	
Computed hash	c7f438d4faad7d8c054e72e7d3e298e17855ec0e
Bad Sector List	
Bad sector(s)	No bad sectors found

Close



3) Clonación hecha!

Drive/Image Verify Results	
<input type="checkbox"/>	
Name	\.\.\PHYSICALDRIVE2
Sector count	937703088
<input type="checkbox"/> MD5 Hash	
Computed hash	900f42063fdf9e77cf94734aff3b1350
<input type="checkbox"/> SHA1 Hash	
Computed hash	c7f438d4faad7d8c054e72e7d3e298e17855ec0e
<input type="checkbox"/> Bad Sector List	
Bad sector(s)	No bad sectors found
<input type="button" value="Close"/>	

- 4) Sí, son iguales los hashes del disco origen “PHYSICALDRIVE1” que el hash del disco destino “PHYSICALDRIVE2”.

