2. CLONACIÓN CON HARDWARE Y MONTAJE DE IMÁGENES

Hecho por:
Izan Navarro

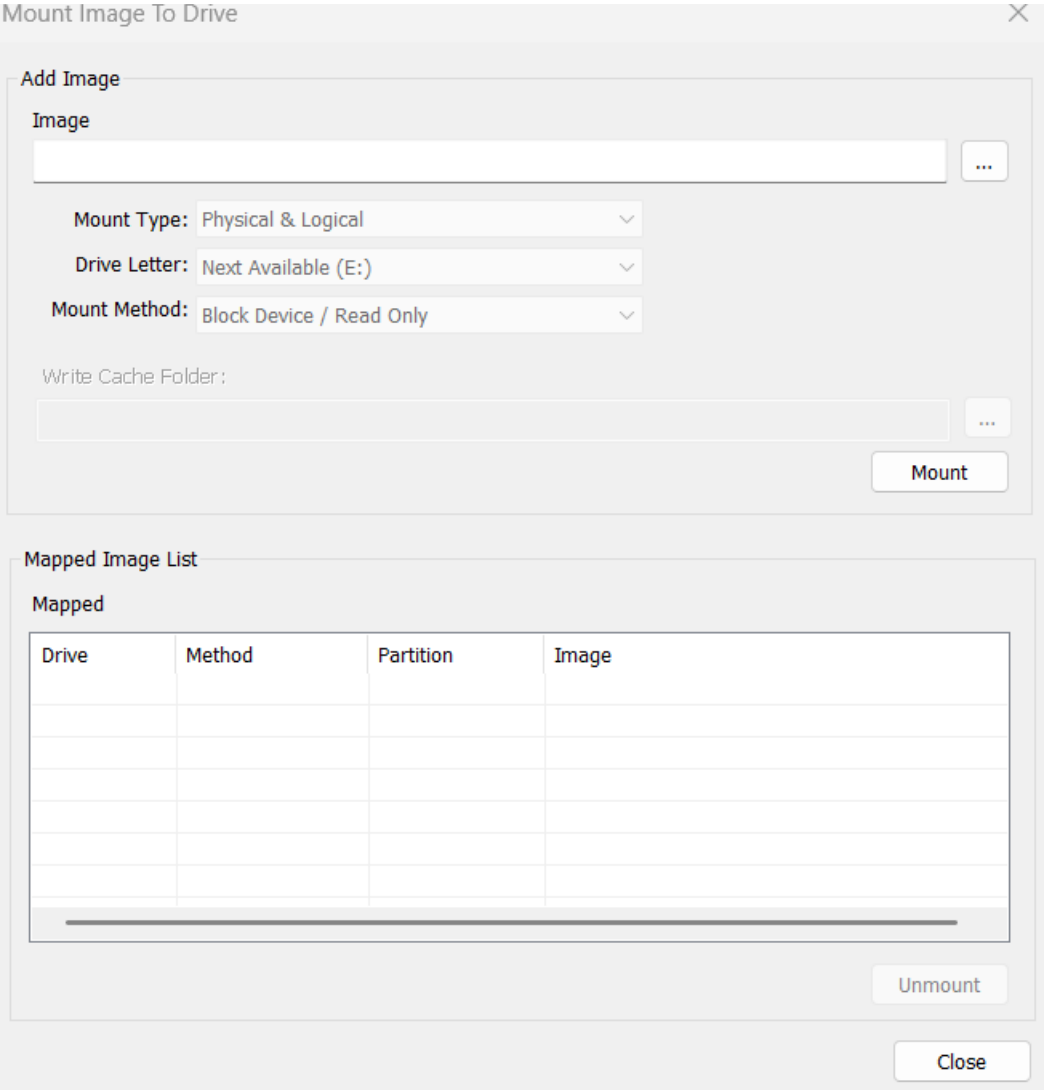
INDICE

1. MONTAJE DE IMAGEN

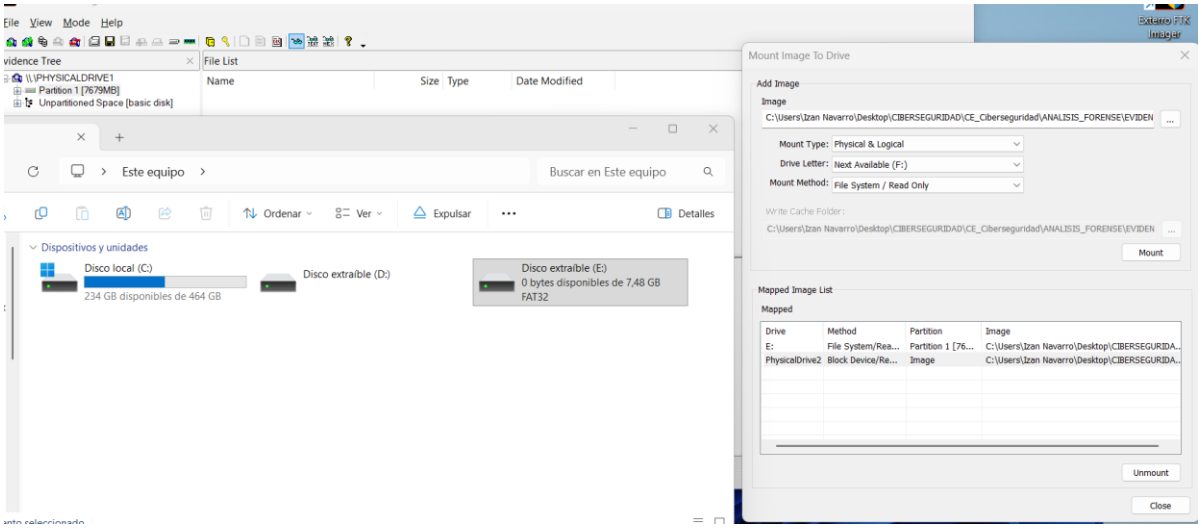
Elige cualquiera de las imágenes generadas en la práctica anterior y realiza las siguientes actividades con ella (puedes usar tanto FTK Imager como Arsenal image mounter)

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).

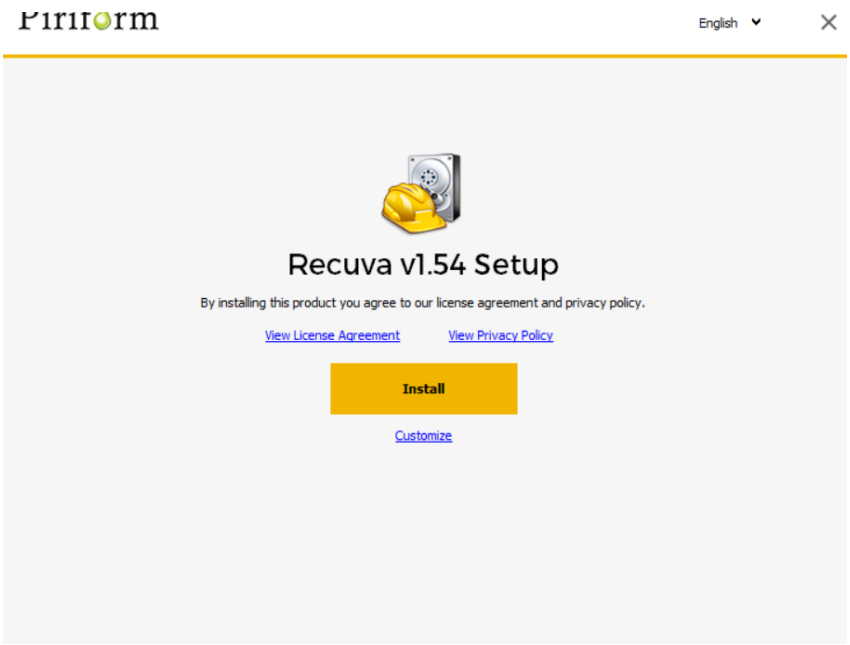


Nos aparecerá en nuevo disco duro con la imagen montada en read only:

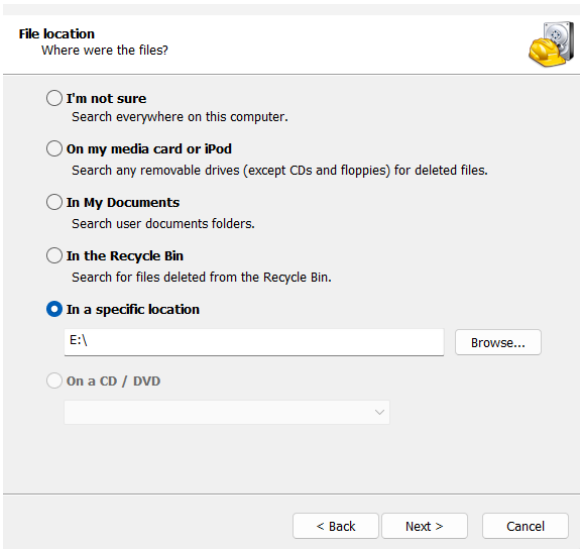


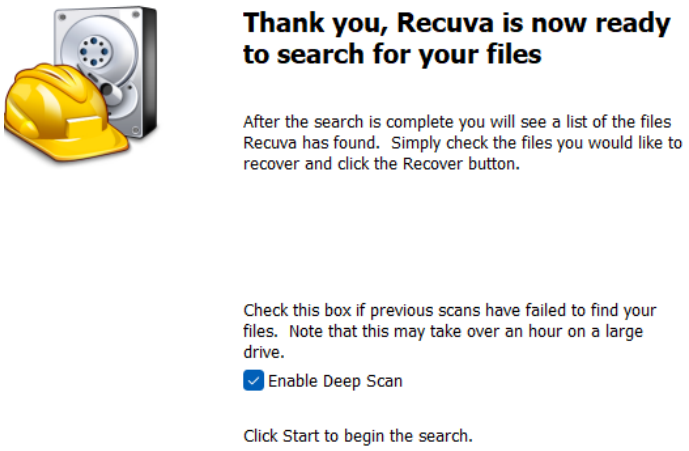
2. Utiliza cualquier herramienta Windows para recuperar archivos borrados (por ejemplo, Recuva https://www.ccleaner.com/recuva). ¿Has descubierto archivos eliminados?

1) Instalamos Recuva:

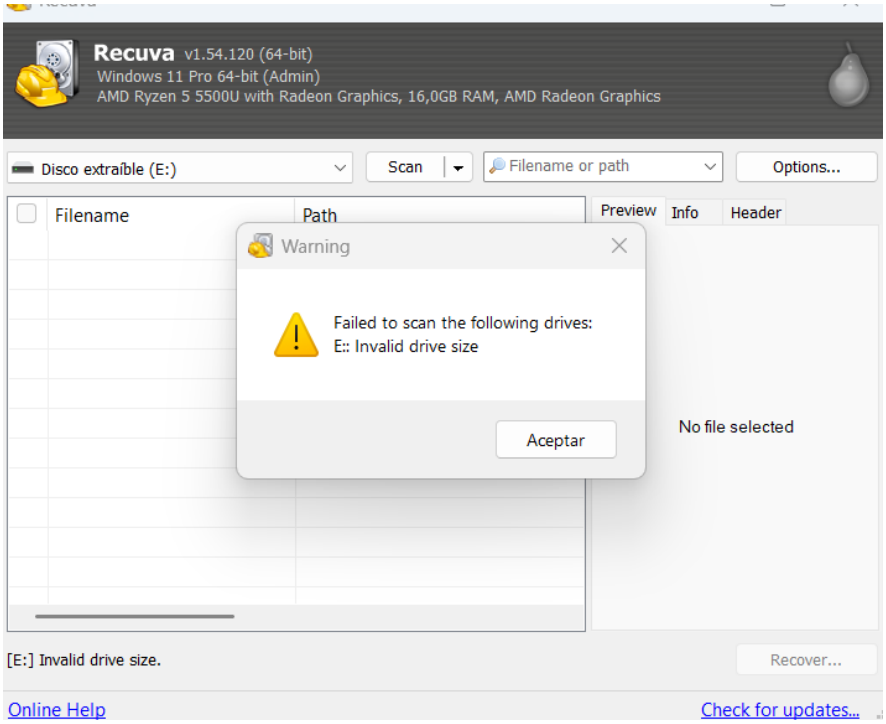


2) Elegimos el disco a recuperar archivos, en mi caso el E: y seleccionamos “all Files” y activamos la opción de Deep Scan:

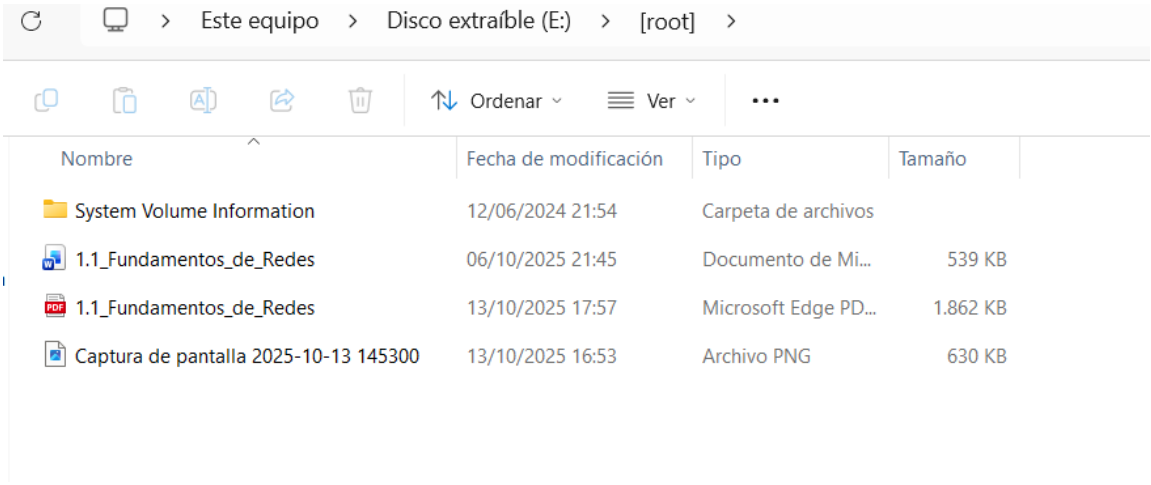




3) Intento Scanear la imagen en Recuva y siempre me salta este Mensaje:

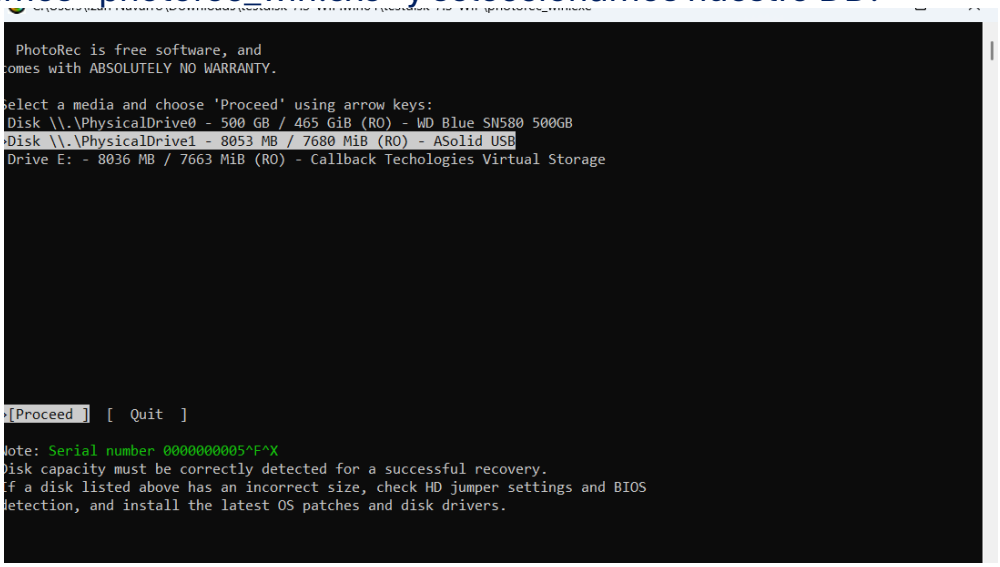


Pero en cambio sí que puedo entrar dentro de la imagen y ver los archivos dentro de la carpeta “root”:

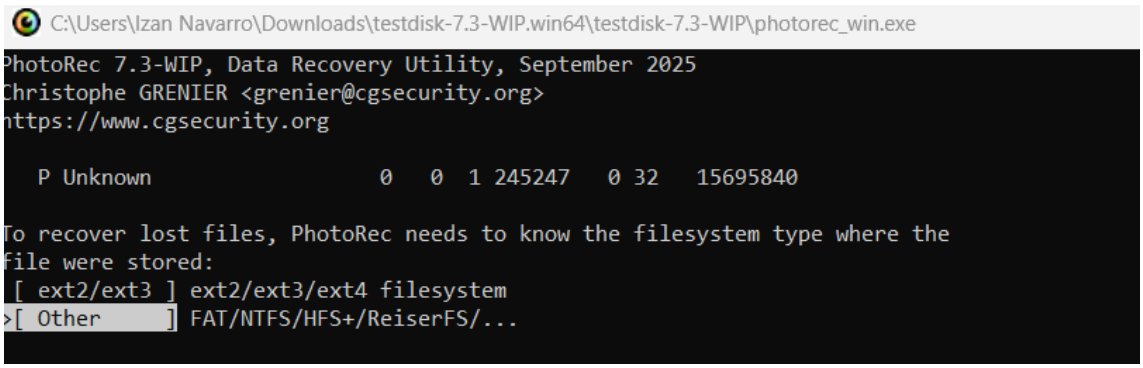


3. Utiliza ahora PhotoRec para hacer carving sobre la imagen y observa el resultado, ¿Has descubierto más archivos o los mismos que en el punto anterior? Explica el motivo del resultado de esta comparación.

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



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



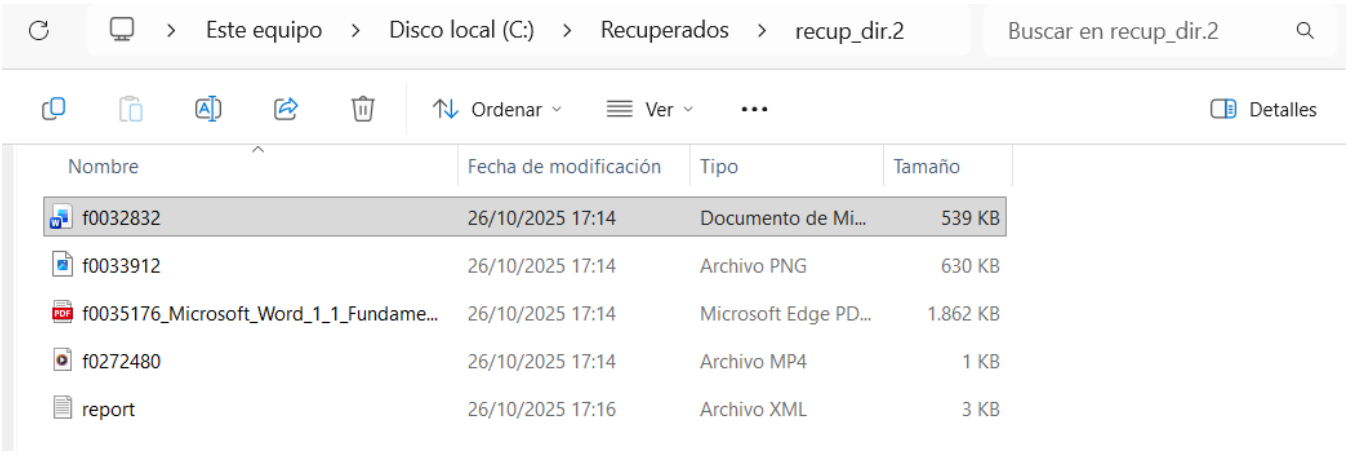
3) Seleccionamos un espacio del equipo donde recuperar los datos borrados y no borrados de la imagen creada, en mi caso “C:/Recuperados”:

```
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:

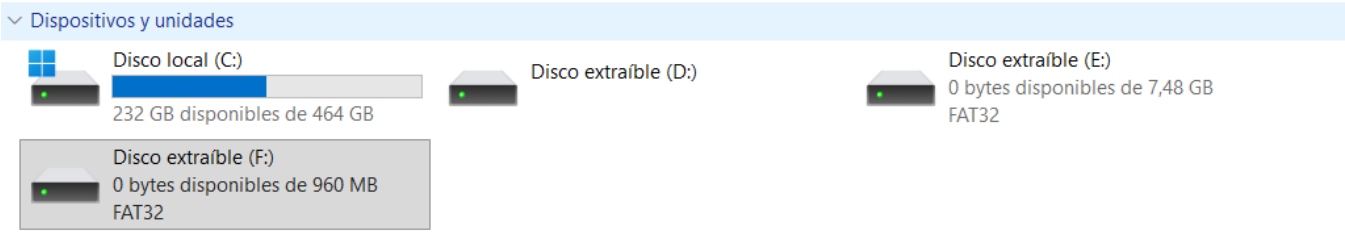


2. MONTAJE DE IMAGEN LINUX

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:

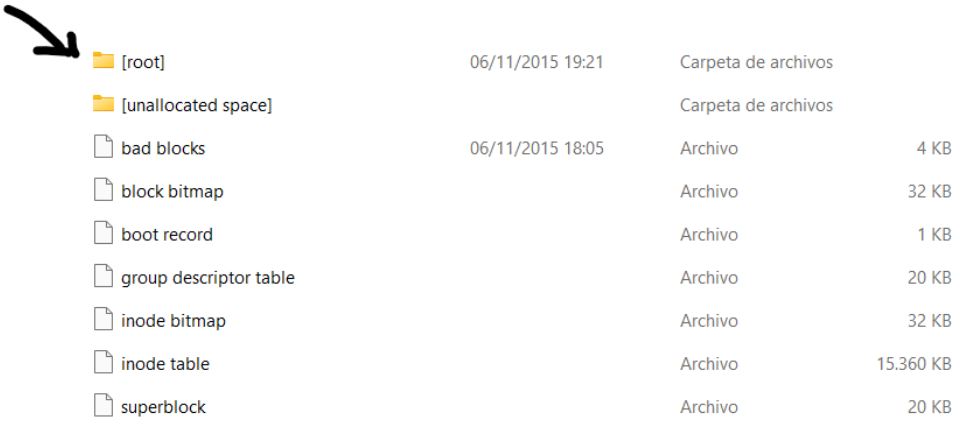
1. Monta la imagen en un sistema Windows con la misma herramienta que el punto anterior (FTK Imager o Arsenal image mounter)

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

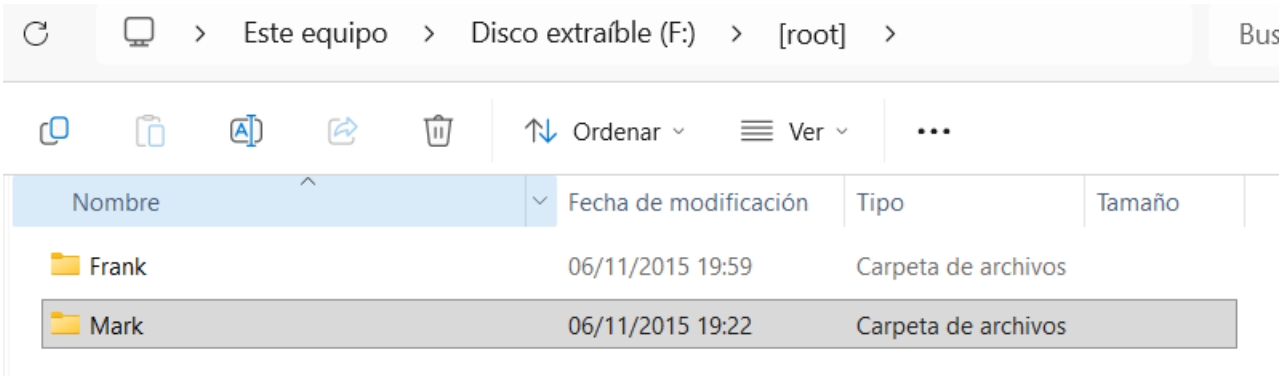


2. Después de montarla, ¿puedes acceder al sistema de archivos? En caso afirmativo pasa directamente al punto 5. En caso negativo, ¿Por qué crees que no puedes acceder al sistema de archivos?

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



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)

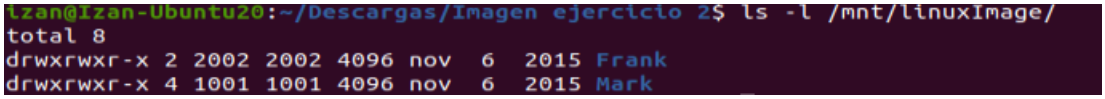
```
izan@Izan-Ubuntu20:~/Descargas/Imagen ejercicio 2$ sudo kpartx -av Linux\ Financ
ial\ Case.001
add map loop7p1 (253:0): 0 1966080 linear 7:7 2048
izan@Izan-Ubuntu20:~/Descargas/Imagen ejercicio 2$
```

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

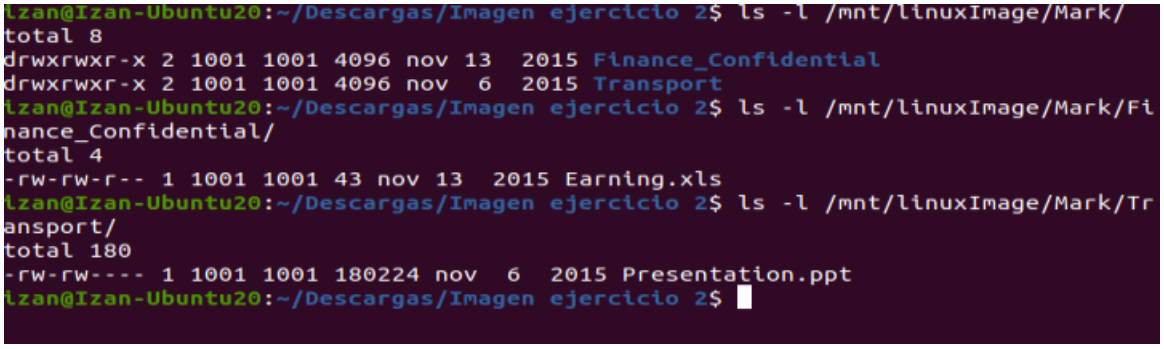


5. ¿Cuántas carpetas encuentras y cuáles son sus nombres?

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”.



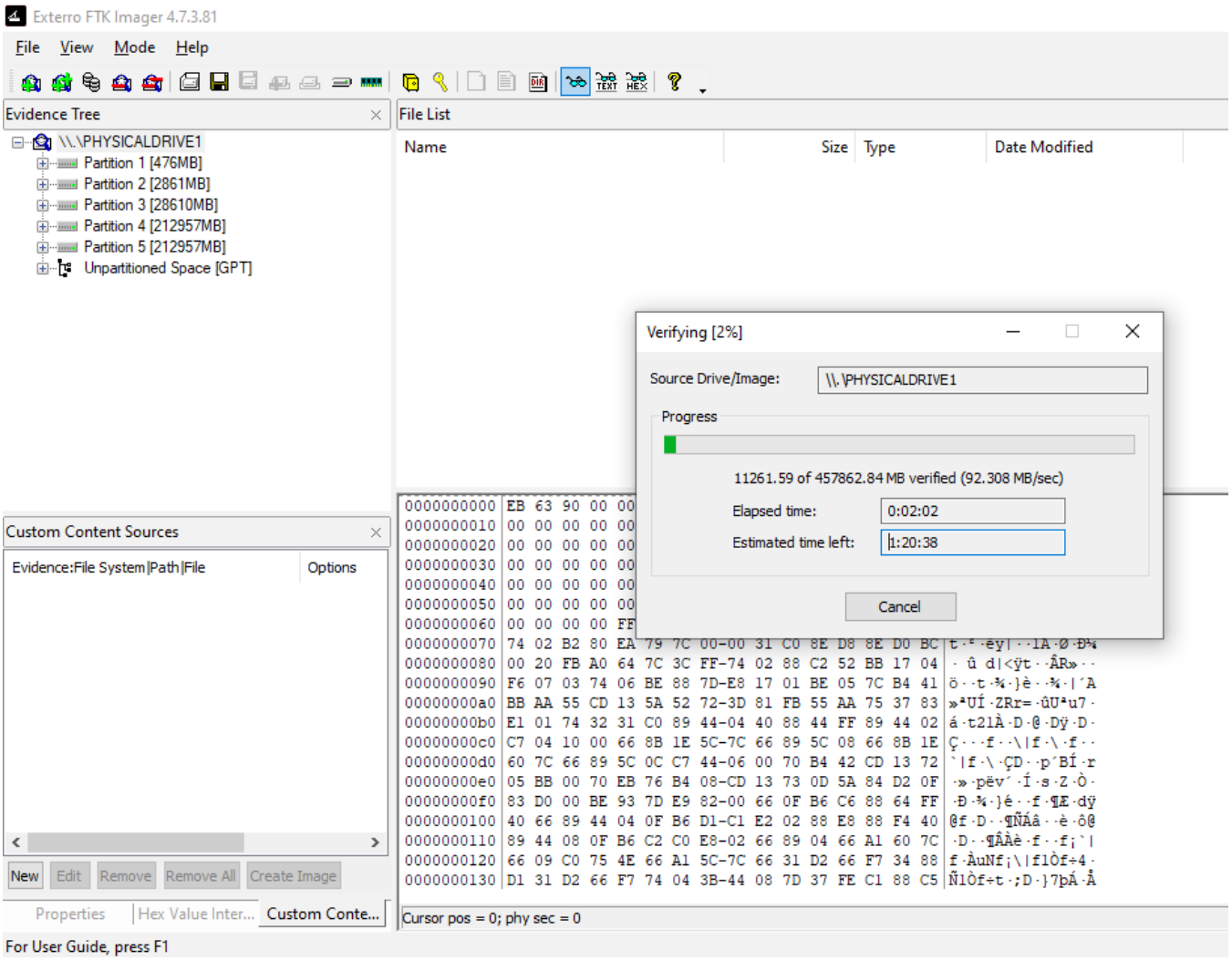
Dentro de la Carpeta “Frank” encontraremos un archivo .xls llamado “Appointments.xls”

3. ADQUISICIÓN DE EVIDENCIA MEDIANTE HARDWARE

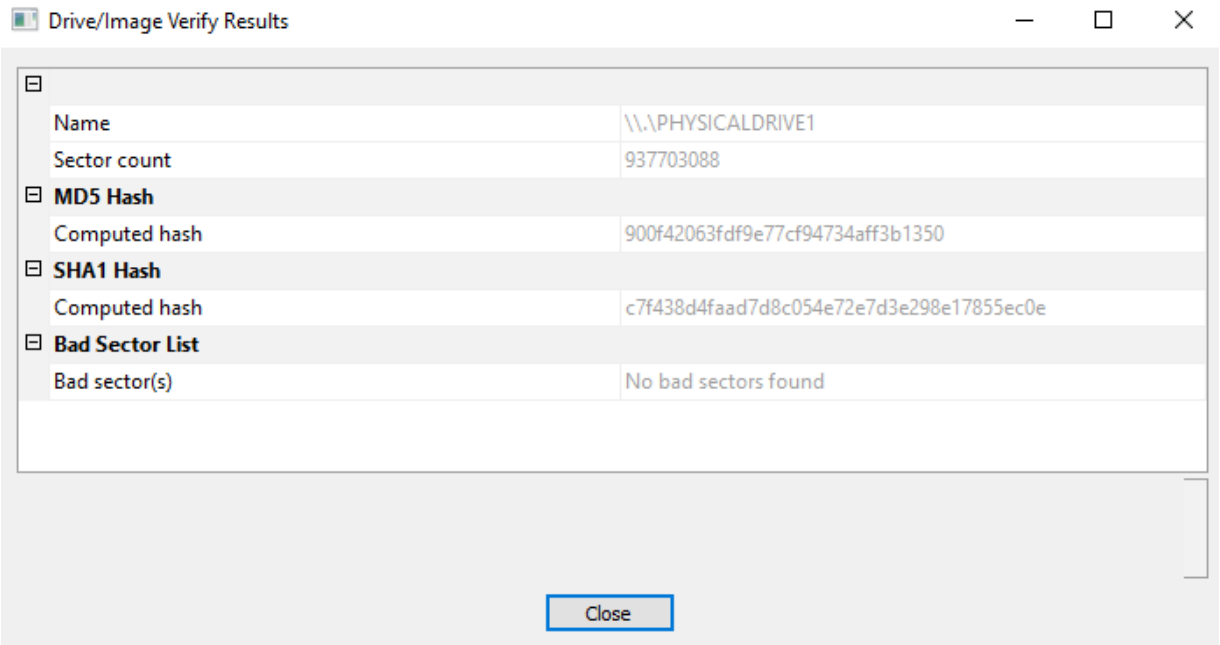
DISCO ORIGEN – INF 23

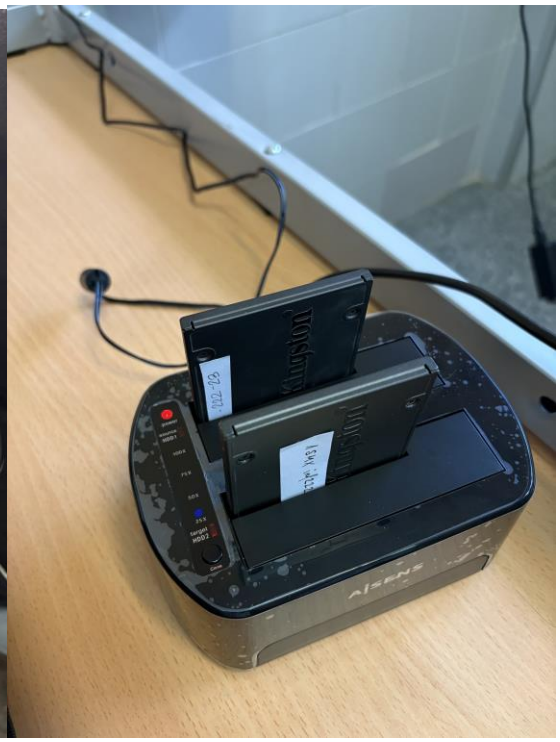
DISCO DESTINO – INF 28

1) Verificar la Imagen para hallar el hash

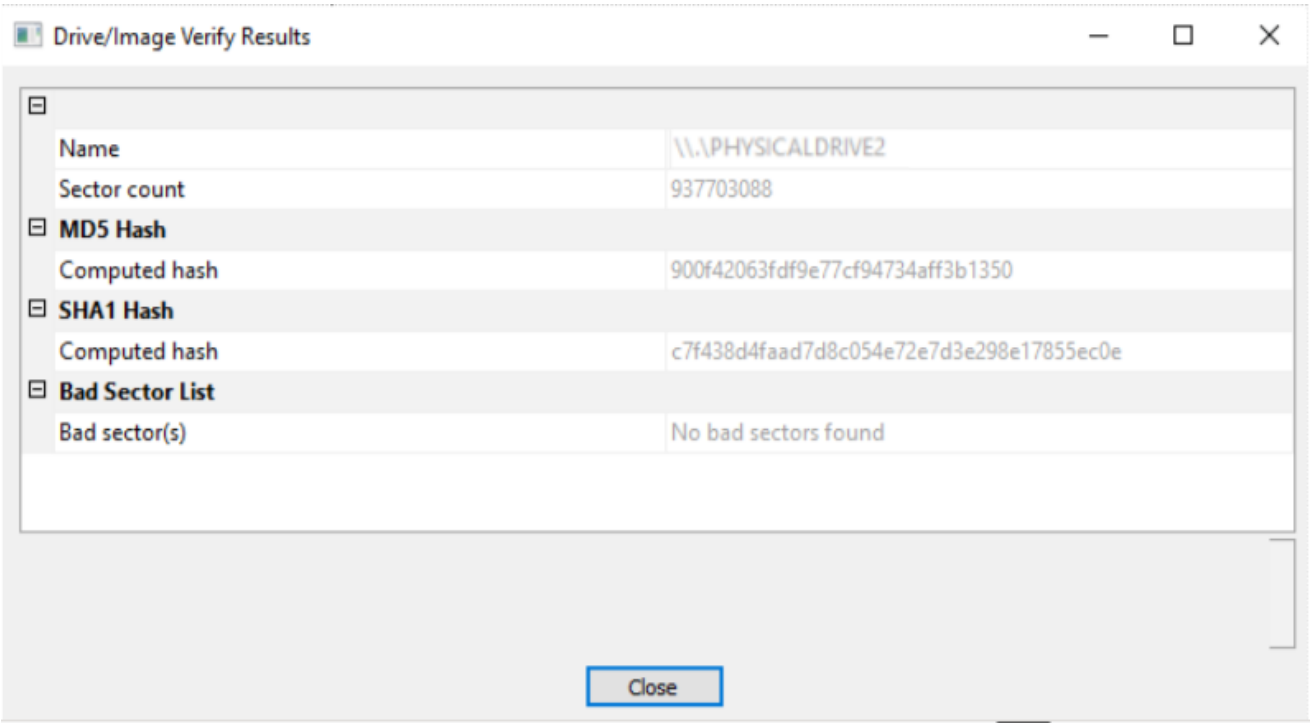


2) HASH DEL DISCO ORIGEN





3) Clonación hecha!



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