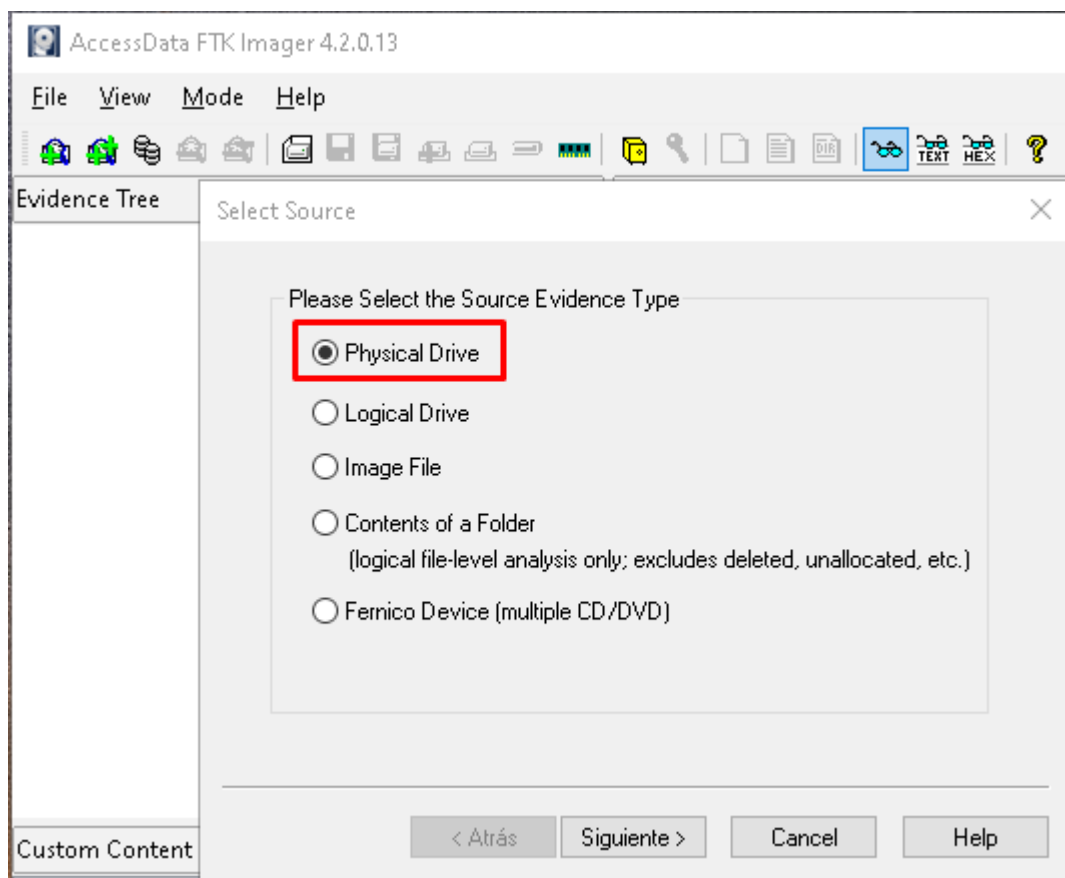


Actividad 05

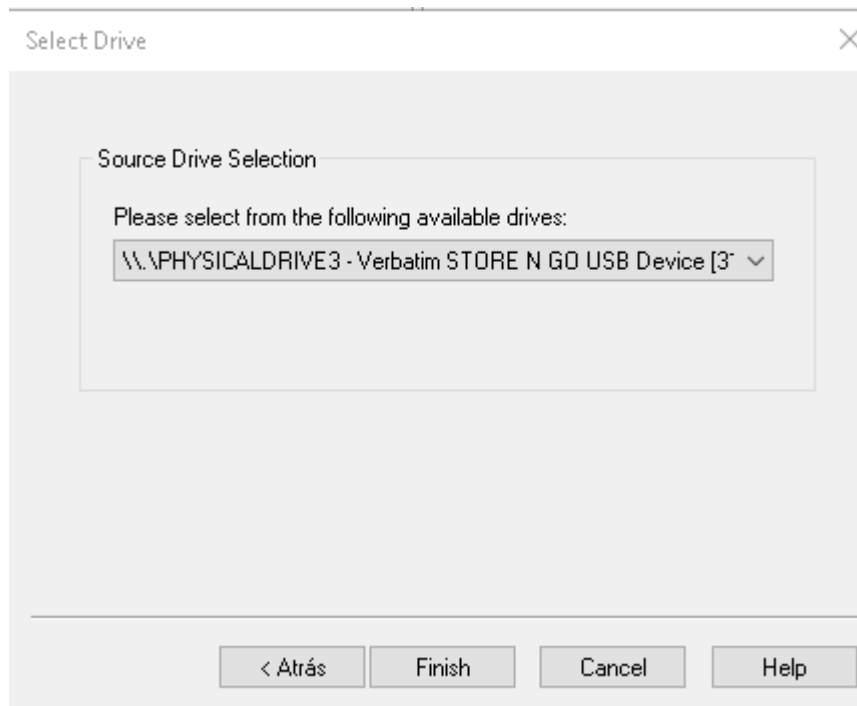
Adquisición forense de una memoria USB empleando las siguientes herramientas: FTK Imager, Guylmager y dd

FTK Imager

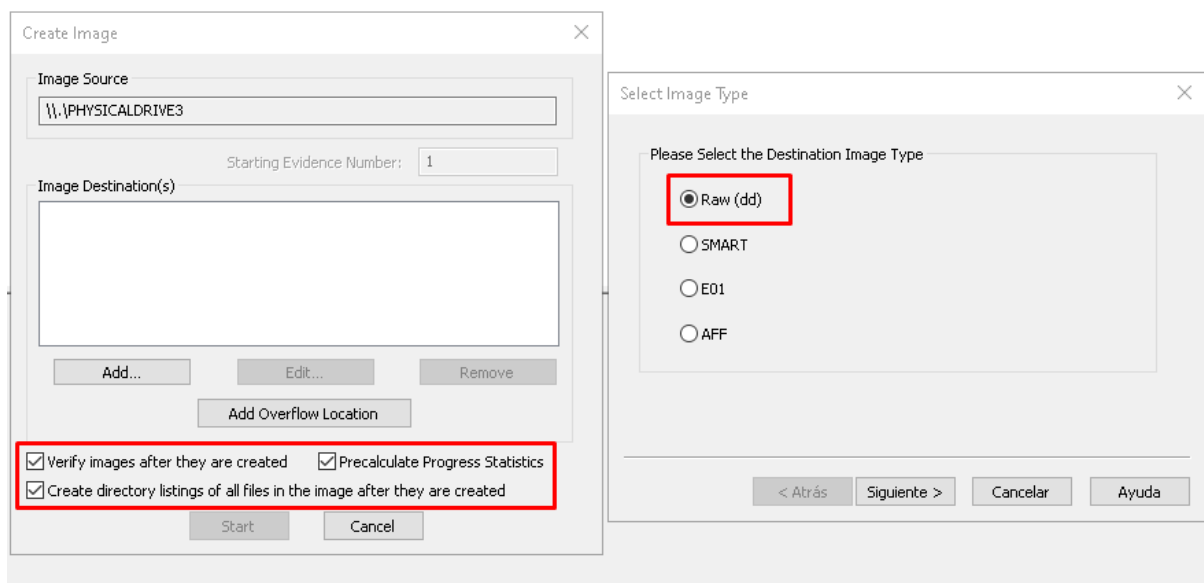
Empezamos añadiendo una fuente, en nuestro caso, al ser un USB vamos a seleccionar una unidad física.



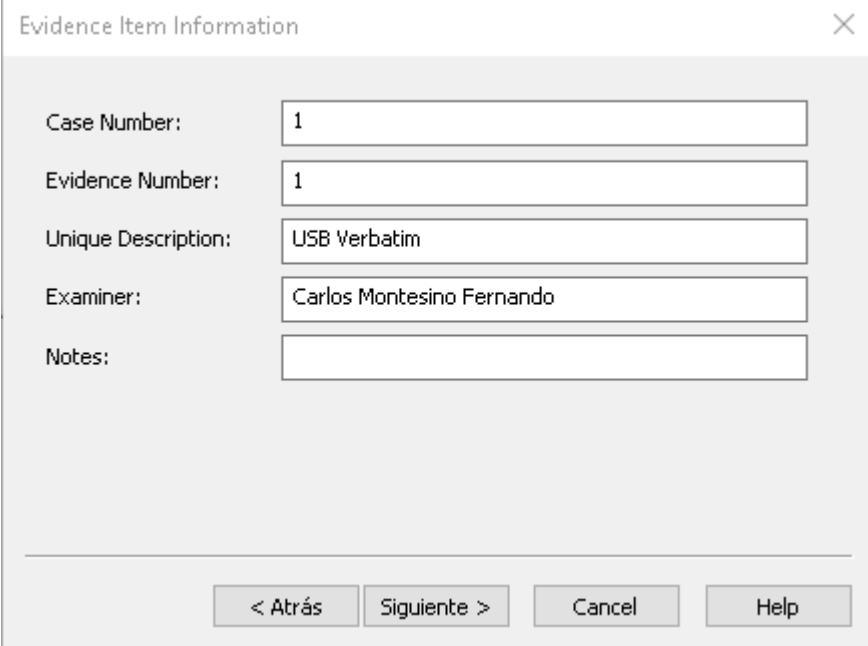
Tras esto seleccionamos cual de todas vamos a elegir, en nuestro caso elegimos el USB.



Ahora establecemos las opciones de como se van a hacer la copia, en mi caso utiliza el formato de salida **Raw** y especifico que se hagan comprobaciones tras la creación de la imagen.



Ahora nos pide que rellenemos información sobre la evidencia y el caso que estamos tratando.



Evidence Item Information

Case Number: 1

Evidence Number: 1

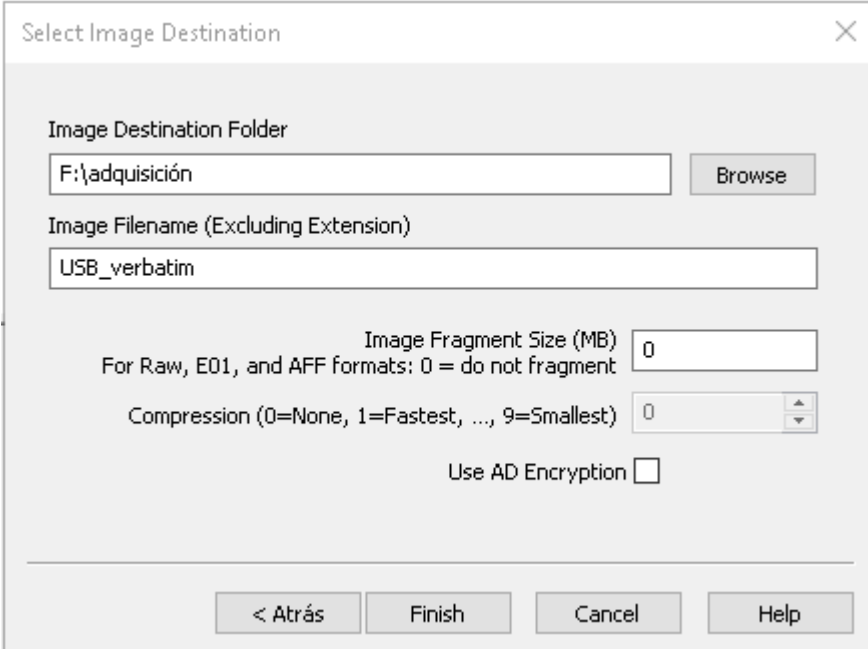
Unique Description: USB Verbatim

Examiner: Carlos Montesino Fernando

Notes:

< Atrás Siguiete > Cancel Help

Establecemos una ruta para la salida, un nombre para el archivo y la fragmentación de la imagen, en mi caso uso 0 para que se cree en solo una imagen.



Select Image Destination

Image Destination Folder
F:\adquisición Browse

Image Filename (Excluding Extension)
USB_verbatim

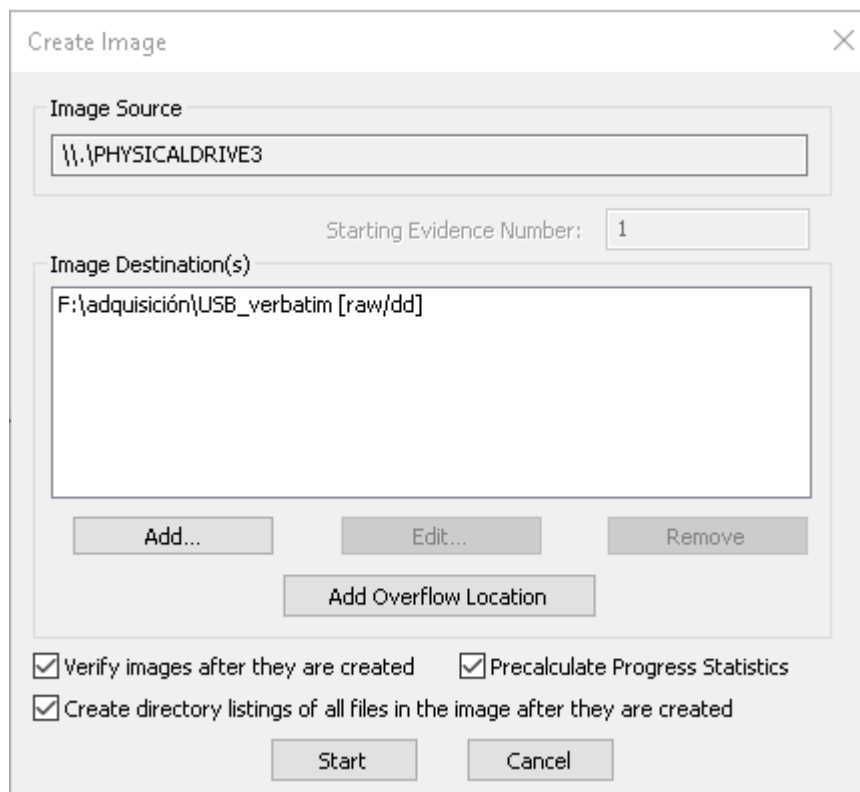
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment 0

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

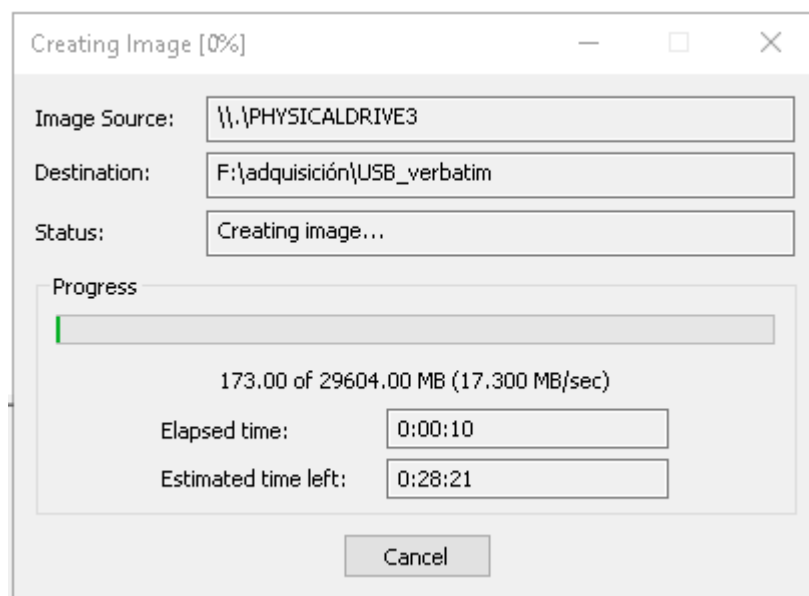
Use AD Encryption ☐

< Atrás Finish Cancel Help

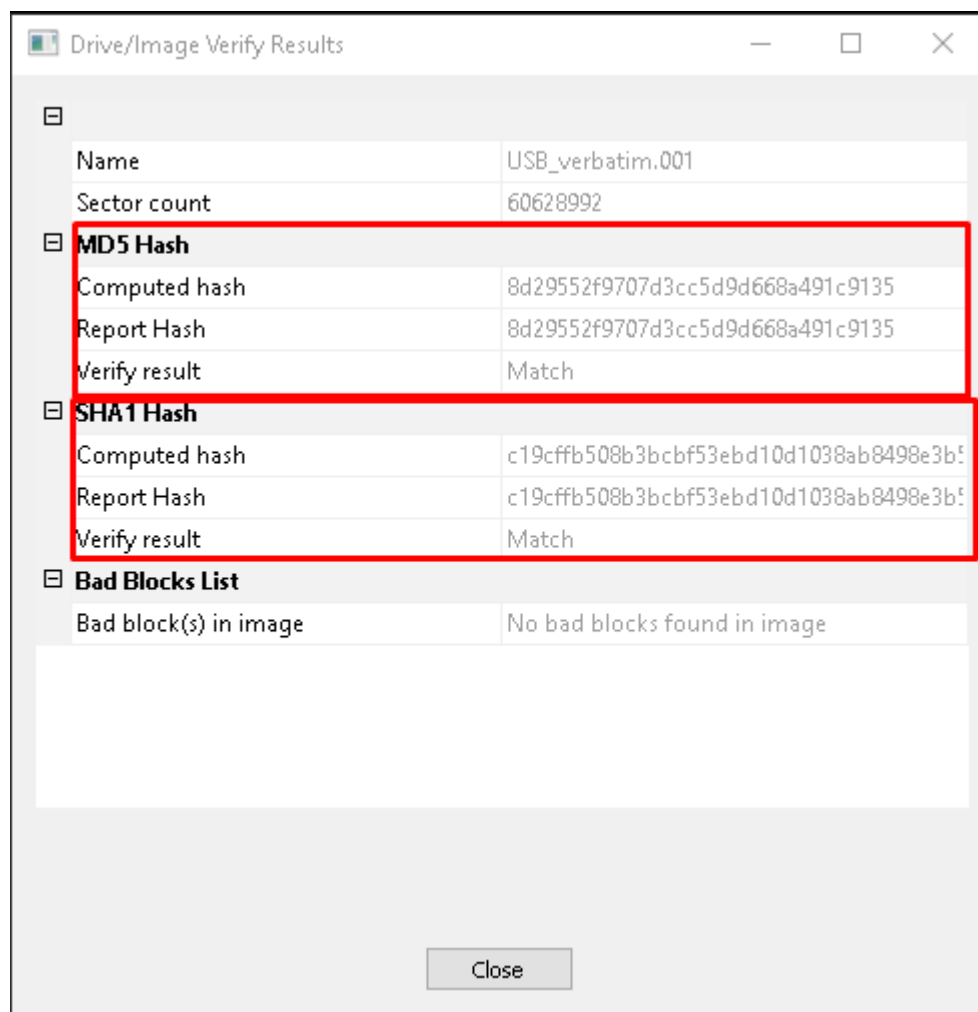
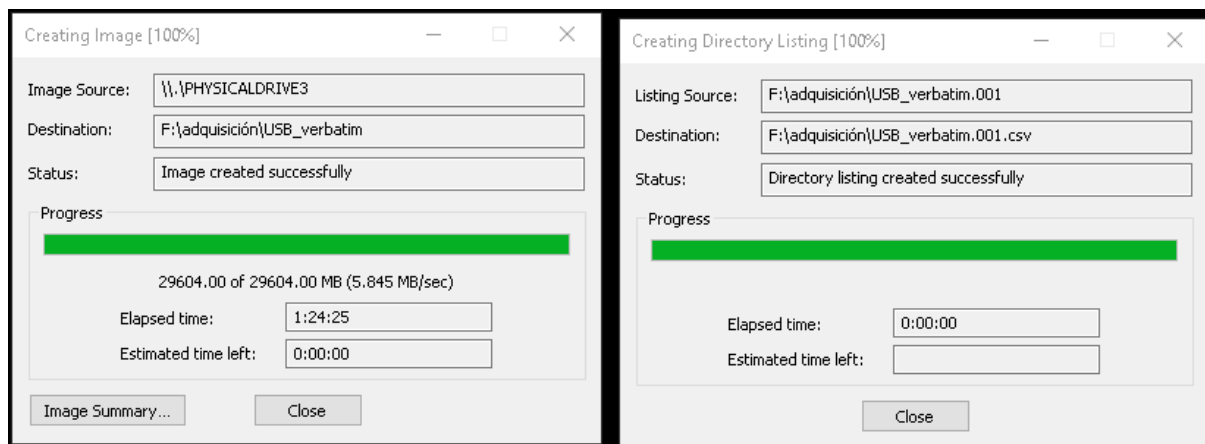
La página de creación de imagen queda así y le damos a iniciar.



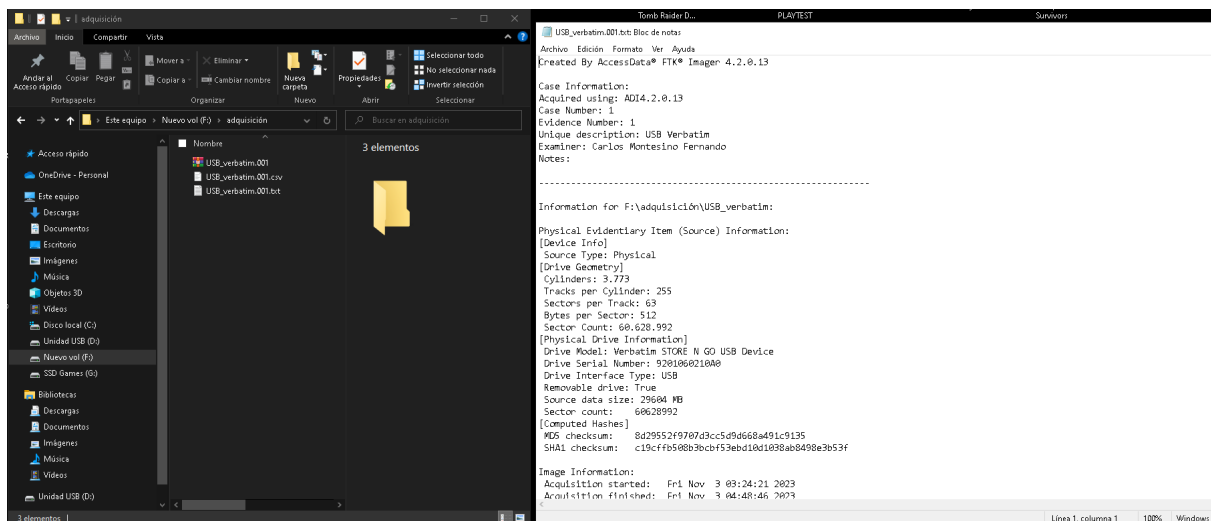
Inicia la adquisición.



Al terminar la adquisición obtenemos la siguiente pestaña, en la que se nos indica que los hash de la imagen y el original coinciden.

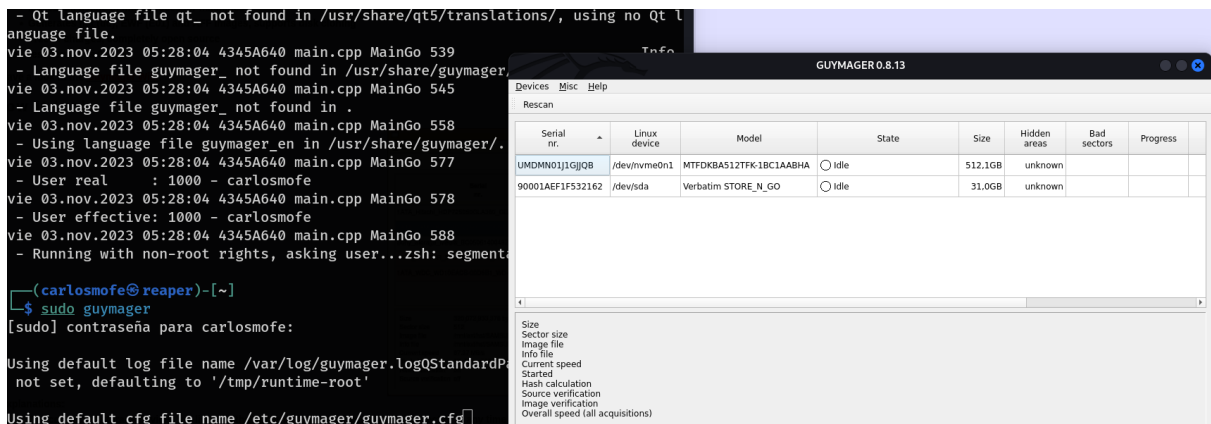


En la ruta de salida obtenemos la imagen y un par de archivos con información sobre la adquisición.



GuyImager

Utilizaremos la herramienta instalada en Kali Linux, la iniciaremos desde la consola con sudo ya que necesita permisos de administrador.



Hacemos click derecho sobre el dispositivo, en este caso **/dev/sda** es nuestro USB. Ahora nos aparecerá la siguiente pestaña para iniciar la adquisición:

Acquire image of /dev/sda

File format

☐ Linux dd raw image (file extension .dd or .xxx)
 ☒ Split image files

☒ Expert Witness Format, sub-format Guymager (file extension .Exx)
 Split size MiB

Case number

Evidence number

Examiner

Description

Notes

Destination

Image directory

Image filename (without extension)

Info filename (without extension)

Hash calculation / verification

☒ Calculate MD5
 ☒ Calculate SHA-1
 ☐ Calculate SHA-256

☐ Re-read source after acquisition for verification (takes twice as long)

☒ Verify image after acquisition (takes twice as long)

Elegimos calcular tanto el **MD5** como el **SHA-1** y la verificación de la imagen. Esta vez hemos elegido otro formato de salida para la imagen y hemos dividido la imagen en grupos de 2047 MiB. Tras esto comienza la adquisición.

Aplicaciones Lugares guymager (root) 3 de nov 06:19
GUYMAGER 0.8.13

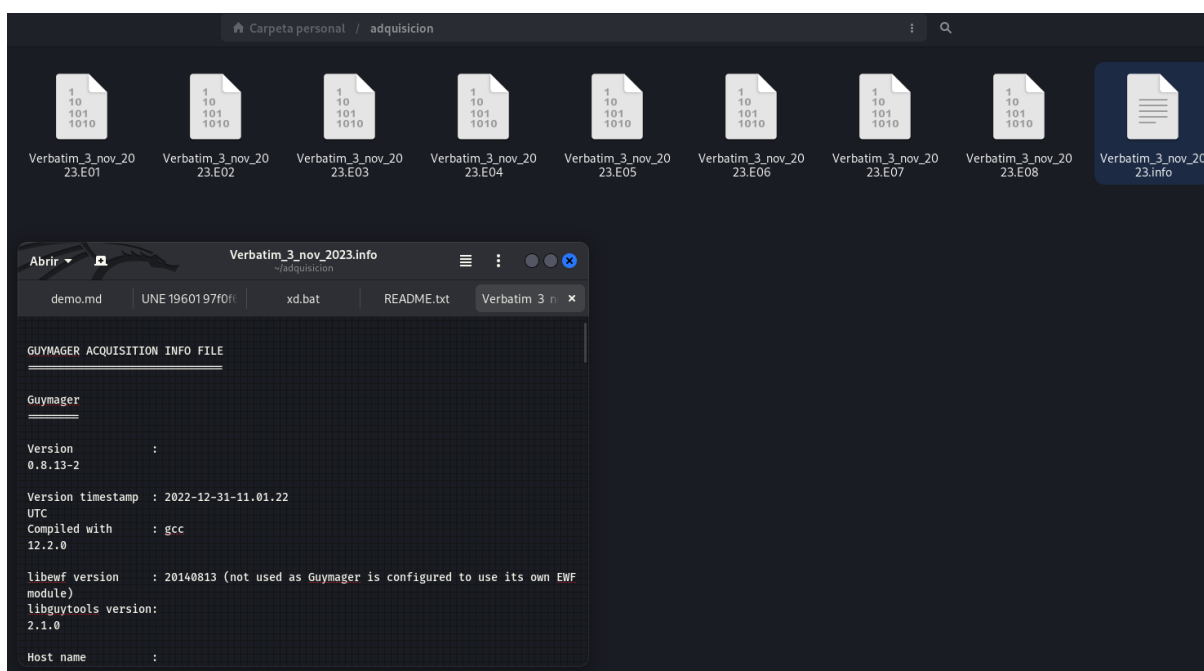
Devices Misc Help

Rescan

Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Average speed [MB/s]	Time remaining	FIFO queues usage [%]
UMDMN011GjJB	/dev/nvme0n1	MTFDKBA512TFK1BC1AABHA	Idle	512.1GB	unknown					
90001AEF1F532162	/dev/sda	Verbatim STORE_N_GO	Running	31.0GB	unknown	0	14%	2.96	04:46:04	r 0 h 0 c 0 w

GUYMAGER 0.8.13										
Devices Misc Help										
Rescan										
Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Average speed [MB/s]	Time remaining	FIFO queues usage [%]
UMDMN011GjJB	/dev/nvme0n1	MTFDKBA512TFK-1BC1AABHA	Idle	512.1GB	unknown					
90001AEF1F532162	/dev/sda	Verbatim STORE_N_GO	Finished - Verified & ok	31.0GB	unknown	0	100%	2.48		

Como vemos en la captura anterior, termina correctamente y ahora nos dirigimos a la carpeta de output para confirmar la salida, donde vemos los diferentes bloques y un archivo con información sobre la adquisición.



dd

Esta herramienta viene instalada por defecto en sistemas Linux, se usa a través de CLI, para realizar la adquisición usaremos el siguiente comando:


```
(carlosmofe@reaper)-[~]
$ df
S.ficheros      bloques de 1K    Usados Disponibles  Uso% Montado en
udev            5732580         0      5732580    0% /dev
tmpfs           1154708         1788    1152920    1% /run
/dev/nvme0n1p4  215234824 131708476  72520244   65% /
tmpfs           5773536         0      5773536    0% /dev/shm
tmpfs           5120           0        5120    0% /run/lock
/dev/nvme0n1p1  265700        48228    217472   19% /boot/efi
tmpfs           1154704        120     1154584    1% /run/user/1000
/dev/sda        30298112        80     30298032    1% /media/carlosmofe/202E-1CCE

(carlosmofe@reaper)-[~]
$ sudo dd if=/dev/sda of=/home/carlosmofe/adquisicion/USB_Verbatim.dd bs=4k conv=noerror,sync status=progress
[sudo] contraseña para carlosmofe: █
```

Entre las opciones tenemos:

- **if** - Define el dispositivo de input.
- **of** - La ruta donde queremos el output.
- **bs** - Tamaño de los bloques
- **conv** - Esta opción es vital si ejecutamos el comando **dd** en un disco que se sospecha que tiene bloques/sectores "malos" o "defectuosos". Normalmente, la herramienta **dd** finalizará abruptamente el comando si se encuentra un error de lectura en la unidad de origen, lo que evita el parámetro **noerror**.

Tras ingresar el comando se inicia la adquisición.

```
(carlosmofe@reaper)-[~]
$ sudo dd if=/dev/sda of=/home/carlosmofe/adquisicion/USB_Verbatim.dd bs=4k conv=noerror,sync status=progress
[sudo] contraseña para carlosmofe:
33177600 bytes (33 MB, 32 MiB) copied, 3 s, 11,0 MB/s █
```

```
(carlosmofe@reaper)-[~]
$ sudo dd if=/dev/sda of=/home/carlosmofe/adquisicion/USB_Verbatim.dd bs=4k conv=noerror,sync status=progress
[sudo] contraseña para carlosmofe:
31039569920 bytes (31 GB, 29 GiB) copied, 5879 s, 5,3 MB/s
7578624+0 records in
7578624+0 records out
31042043904 bytes (31 GB, 29 GiB) copied, 5879,7 s, 5,3 MB/s

(carlosmofe@reaper)-[~]
$ █
```

Al terminar vamos a la ruta y vemos que se ha creado la imagen.



USB_Verbatim.dd