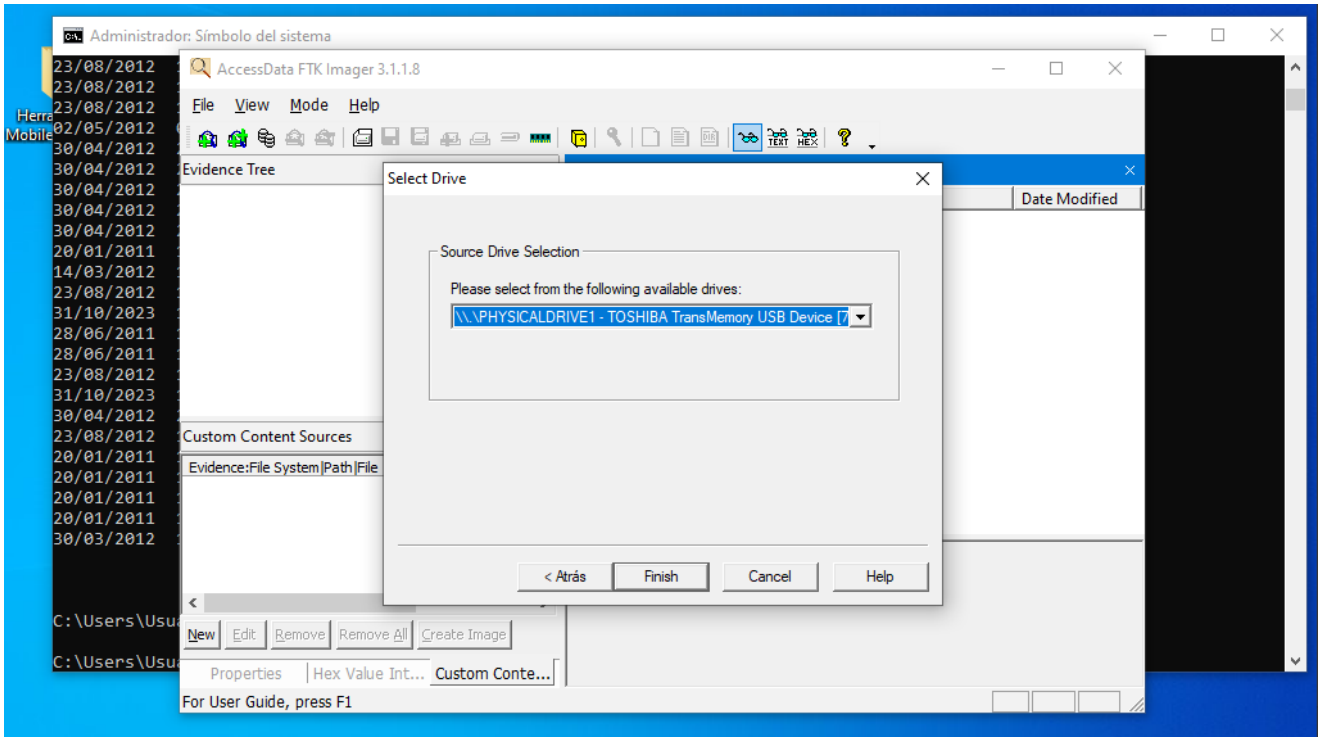
Práctica A05 AFI -- Adquisición Memoria USB

Adquisición con FTK Imager

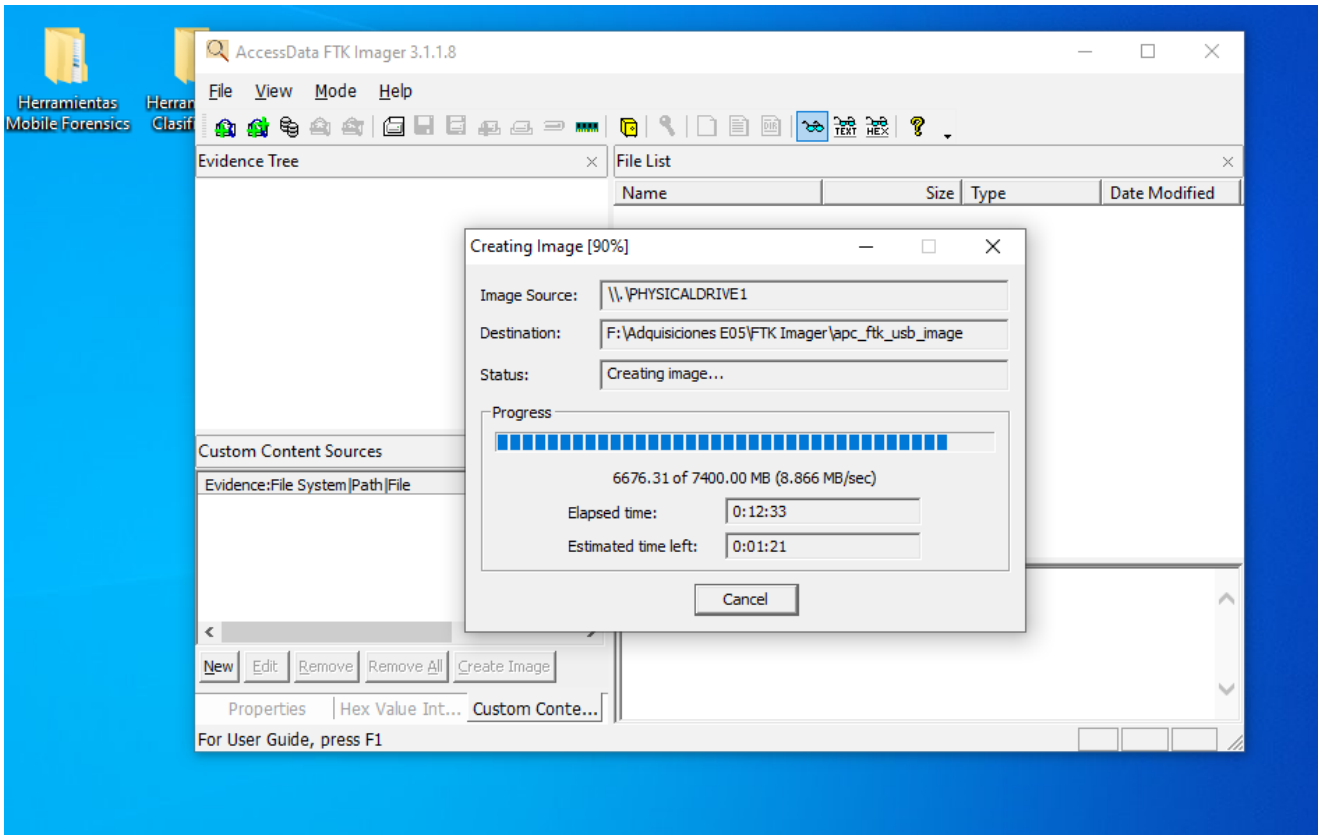
A la hora de realizar una adquisición con este programa, hay que tener en cuenta los siguientes aspectos:

- Contar con un medio USB para poder sacar el vestigio.
- A la hora de configurar el programa, asegurarnos de que elegimos la opción "Physical".
- Elegir como tipo de imagen destino, la opción E01.
- Marcar las opciones de:
  - Creación de directorio para los ficheros generados.
  - Verificado de las imágenes después de que estas sean creadas.
  - Mostrar las estadísticas.
- Elegir el tamaño de bytes en el que queramos fragmentar el vestigio.
- Dejar el valor de compresión en 6.

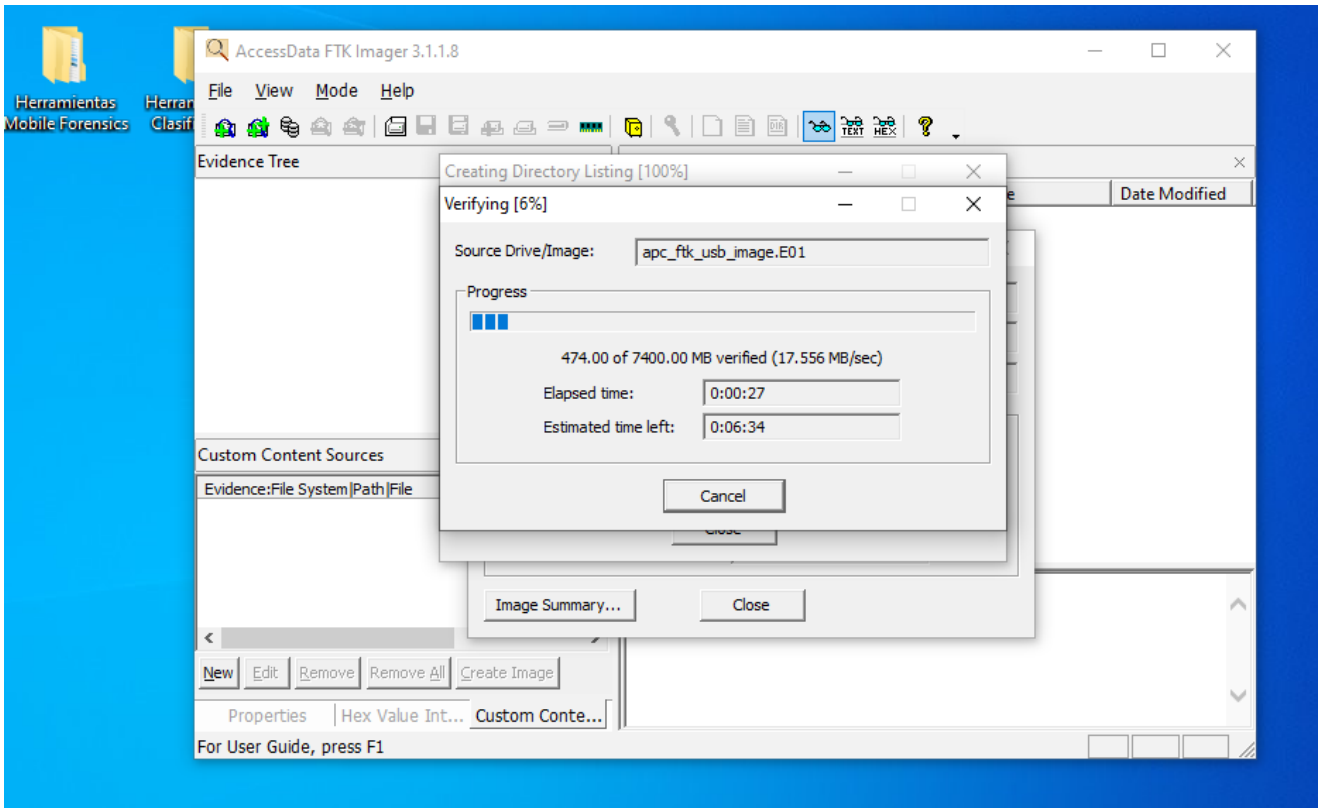
A continuación, muestro el momento en el que selecciono el dispositivo del cual voy a realizar la adquisición:



Ahora muestro el programa construyendo el vestigio:



Ahora muestro el programa verificando el vestigio:



Por último, muestro la ficha generada por el programa. En la cual se muestran datos interesantes como:

- Información sobre el caso.
- Información sobre los hashes generados por el programa, tanto en SHA1SUM, como en MD5.

apc_ftk_usb_image.E01: Bloc de notas

Archivo Edición Formato Ver Ayuda

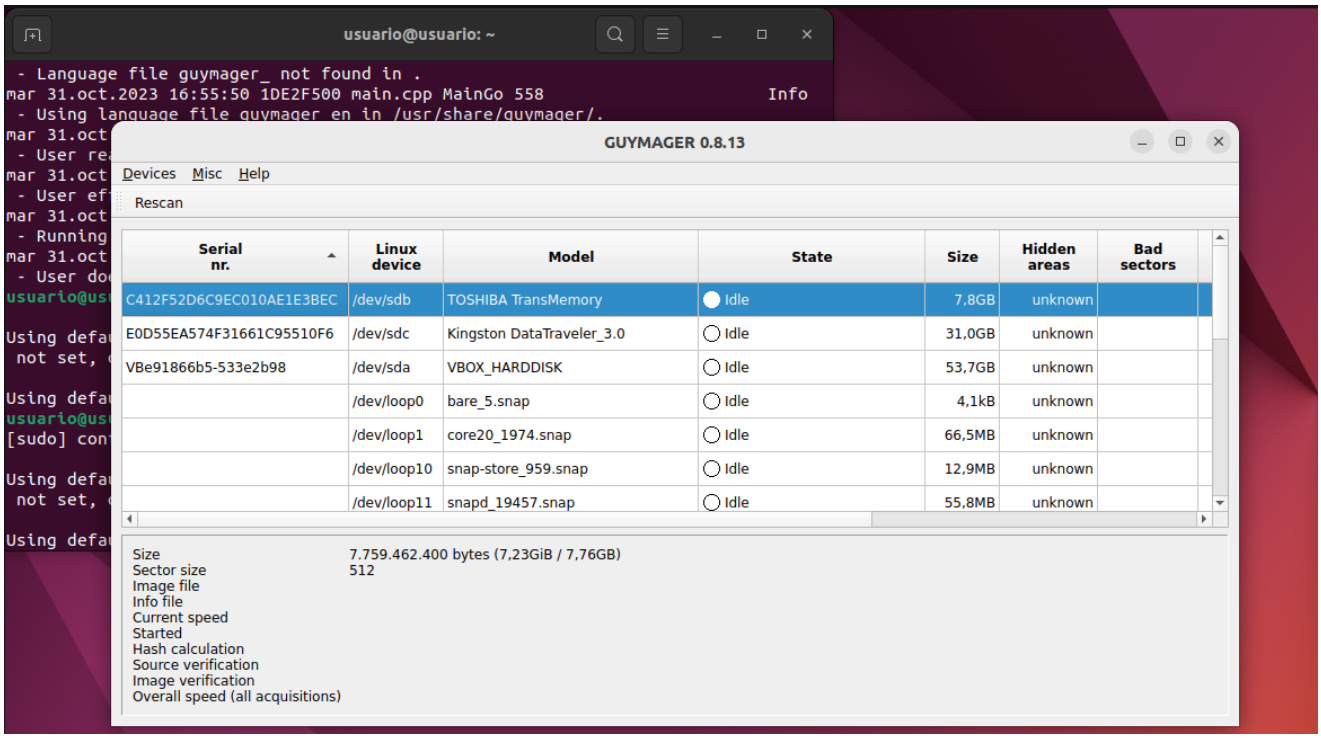
```
Created By AccessData® FTK® Imager 3.1.1.8

Case Information:
Acquired using: ADI3.1.1.8
Case Number: 01
Evidence Number: 01
Unique description: Adquisición Memoria USB
Examiner: Antonio Peñalver Caro
Notes:

---------------------------------------------------------------

Information for F:\Adquisiciones E05\FTK Imager\apc_ftk_usb_image:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 943
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 15.155.200
[Physical Drive Information]
 Drive Model: TOSHIBA TransMemory USB Device
 Drive Serial Number: C
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 7400 MB
 Sector count:    15155200
[Computed Hashes]
 MD5 checksum:    caf25f83e61a413fbd8941247aebf944
 SHA1 checksum:   139143efd54a3932f271057a6c97ed27ab0ffebd
```

Adquisición con Guymager

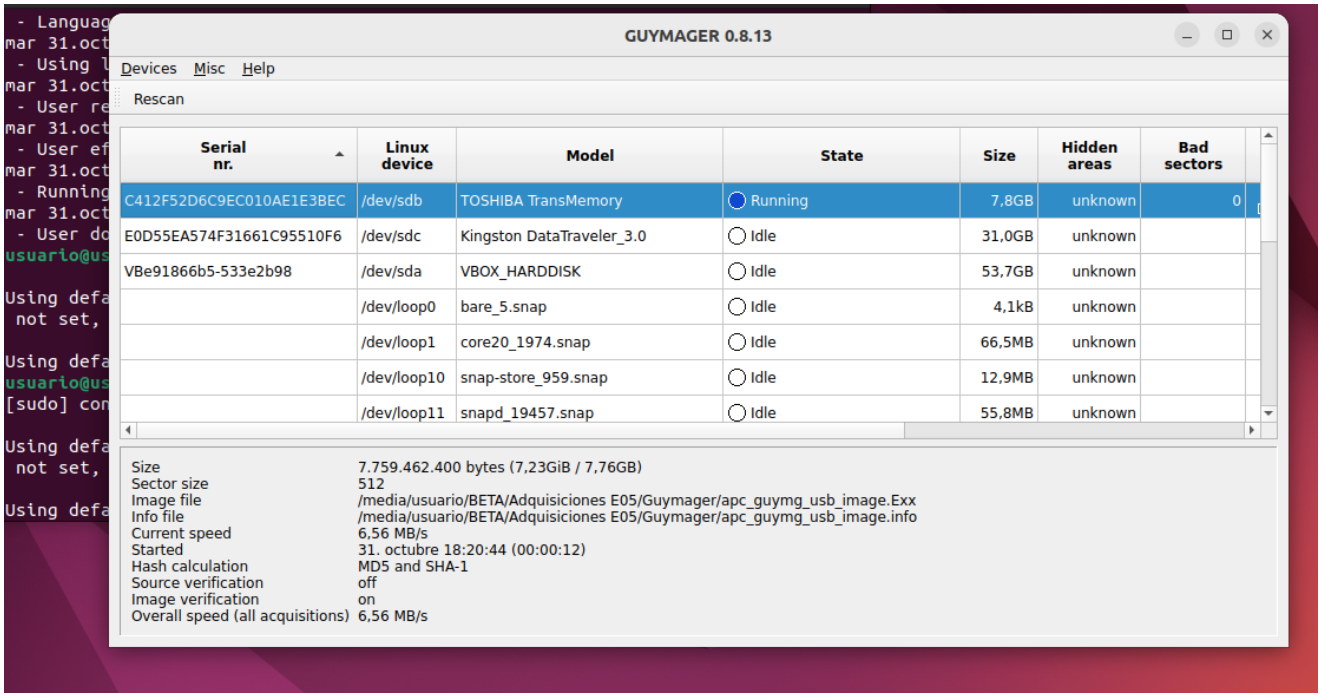
A la hora de realizar una adquisición con este programa, hay que tener en cuenta los siguientes aspectos:

- Contar con un medio USB para poder sacar el vestigio.
- Seleccionar el dispositivo USB y darle a "Acquire Image".
- Cumplimentar el formulario con los datos del caso y las opciones de adquisición.

A continuación, muestro el momento en el que selecciono el dispositivo del cual voy a realizar la adquisición:



Ahora muestro el programa construyendo el vestigio:



Ahora muestro el proceso de creación del vestigio finalizado:

Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress
C412F52D6C9EC010AE1E3BEC	/dev/sdb	TOSHIBA TransMemory	Finished - Verified & ok	7,8GB	unknown	0	100%
E0D55EA574F31661C95510F6	/dev/sdc	Kingston DataTraveler_3.0	Idle	31,0GB	unknown		
VBe91866b5-533e2b98	/dev/sda	VBOX_HARDDISK	Idle	53,7GB	unknown		
	/dev/loop0	bare_5.snap	Idle	4,1kB	unknown		
	/dev/loop1	core20_1974.snap	Idle	66,5MB	unknown		
	/dev/loop10	snap-store_959.snap	Idle	12,9MB	unknown		
	/dev/loop11	snapd_19457.snap	Idle	55,8MB	unknown		

Por último, muestro la verificación de los hashes realizados tanto en SHA1, como en MD5. En el mismo documento viene también el resumen de la adquisición:

```
77 Acquisition
78 ===========
79
80 Linux device            : /dev/sdb
81 Device size             : 7759462400 (7,8GB)
82 Format                  : Expert Witness Format, sub-format Guymager - file extension is .Exx
83 Image meta data
84    Case number          : 01
85    Evidence number      : 02
86    Examiner             : Antonio Peñalver Caro
87    Description          :
88    Notes                : C412F52D6C9EC010AE1E3BEC
89 Image path and file name: /media/usuario/BETA/Adquisiciones E05/Guymager/apc_guymg_usb_image.Exx
90 Info  path and file name: /media/usuario/BETA/Adquisiciones E05/Guymager/apc_guymg_usb_image.info
91 Hash calculation        : MD5 and SHA-1
92 Source verification     : off
93 Image verification      : on
94
95 No bad sectors encountered during acquisition.
96 State: Finished successfully
```

Adquisición con DD

A la hora de realizar una adquisición con este programa, hay que tener en cuenta los siguientes aspectos:

- Contar con un medio USB para poder sacar el vestigio.
- Asegurarse de que el comando que se utiliza para crear el vestigio, está escrito de manera correcta.

Ahora muestro el comando que he utilizado para la creación del vestigio:

```
usuario@usuario:~/Escritorio$ sudo dd if=/dev/sdb1 of=/media/usuario/BETA/Adquis
iciones\ E05/DD/apc_dd_usb_image.dd bs=512
```

Ahora muestro el proceso de creación del vestigio finalizado:

```
usuario@usuario:~/Escritorio$ sudo dd if=/dev/sdb1 of=/media/usuario/BETA/Adquis
iciones\ E05/DD/apc_dd_usb_image.dd bs=512
15150996+0 registros leídos
15150996+0 registros escritos
7757309952 bytes (7,8 GB, 7,2 GiB) copied, 1821,72 s, 4,3 MB/s
```

Por último, genero el SHA1 y el MD5 del vestigio adquirido, para ello he utilizado los siguientes comandos:

- sha1sum apc_dd_usb_image.dd
  ```
  usuario@usuario:~/Escritorio/Adquisiciones E05/DD$ sha1sum apc_dd_usb_image.dd
  875487618fe0c85a843b18d11d0e43f2ed48d9ad  apc_dd_usb_image.dd
  ```
- md5sum apc_dd_usb_image.dd
  ```
  usuario@usuario:~/Escritorio/Adquisiciones E05/DD$ md5sum apc_dd_usb_image.dd
  75b5ee50bbaa6df6fe3356196c9b1acc  apc_dd_usb_image.dd
  ```