

Práctica A06 AFI -- Adquisición Forense Máquina Windows (En vivo)

Según el apartado 2.1 de la metodología forense: APINA G4, el orden de volatilidad que debemos de seguir a la hora de adquirir vestigios forenses, es el siguiente:


- Registros y contenido de la caché.
- Tabla de enrutamiento, caché ARP, tabla de procesos, estadísticas del kernel y memoria.
- Información temporal del sistema.
- Disco.
- Logs del sistema.
- Configuración física y topología de la red.
- Documentos.

En este caso, vamos a realizar adquisiciones de la memoria RAM del sistema y del disco físico del equipo.

Adquisición de Memoria

Para la adquisición de memoria, he usado uno de los programas vistos en clase: DumpIt

En la siguiente imagen, muestro el programa construyendo y completando el vestigio, también muestro la ruta en la que se va a almacenar este:

 F:\Dumpit\DumpIt.exe

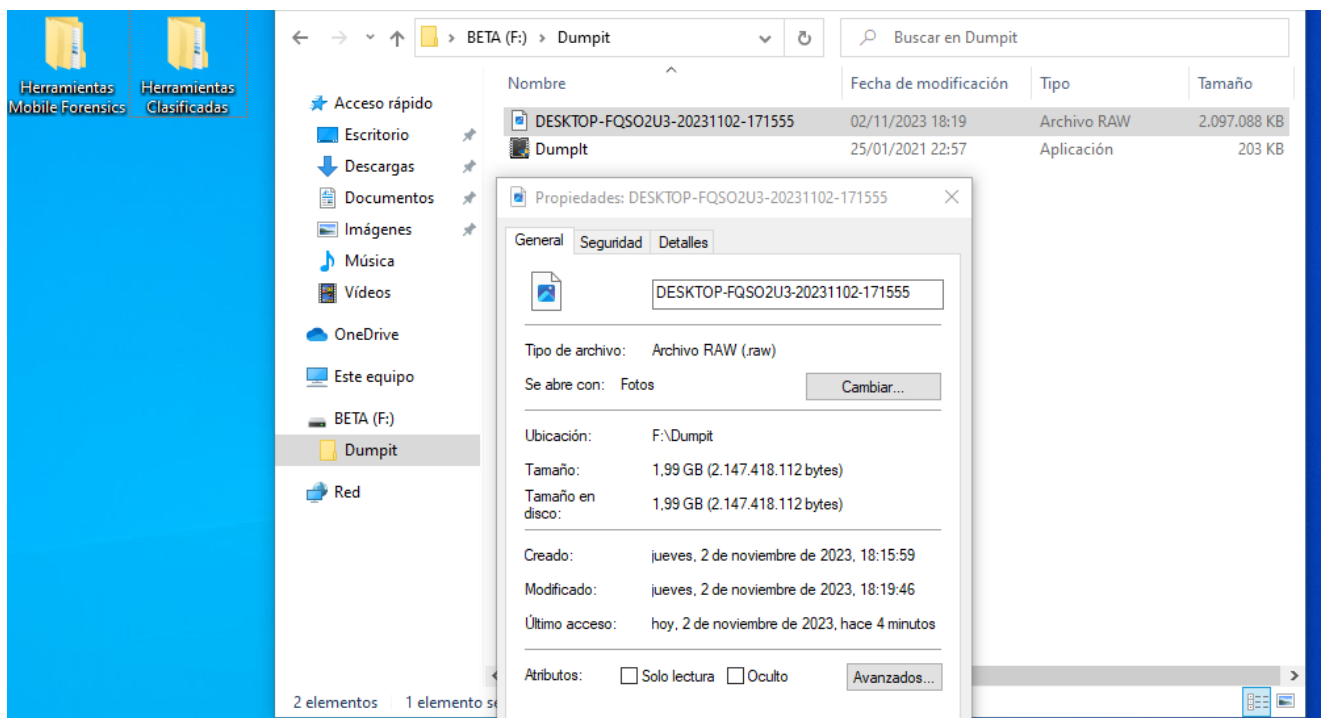
```
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>
```

```
Address space size:      2147418112 bytes (   2047 Mb)
Free space size:        30923927552 bytes (  29491 Mb)
```

```
* Destination = \\?\F:\Dumpit\DESKTOP-FQS02U3-20231102-171555.raw
```

```
--> Are you sure you want to continue? [y/n] y
+ Processing... Success.
```

Por último, muestro el tamaño y el tipo de archivo que se genera. El contenido de dicho archivo habría que consultarlo con algún editor de código, como por ejemplo, Visual Studio Code:



Adquisición de Disco

Triage

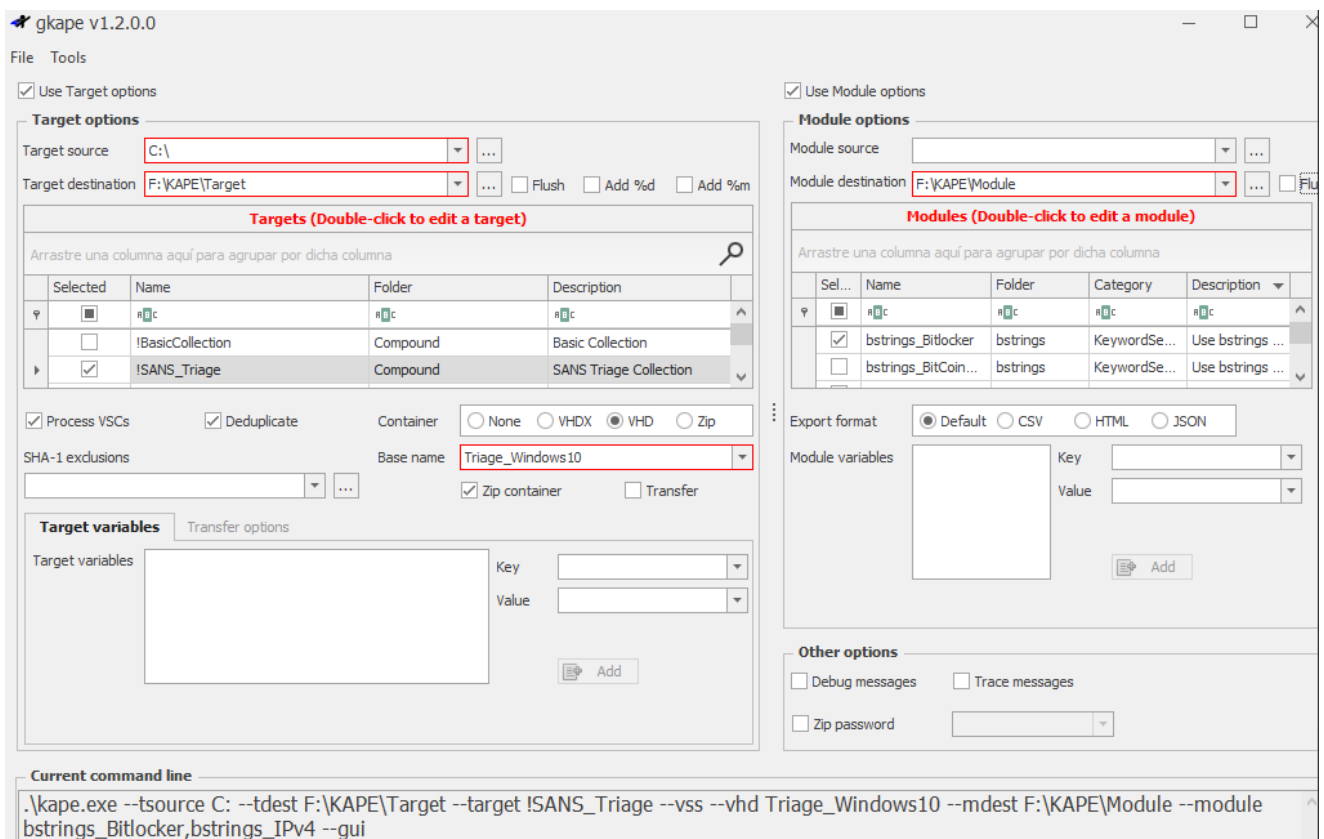
A continuación, usaré Kape para poder sacar información concreta del equipo antes de sacar la imagen del disco completo.

En el apartado "Target", he realizado la siguiente configuración:

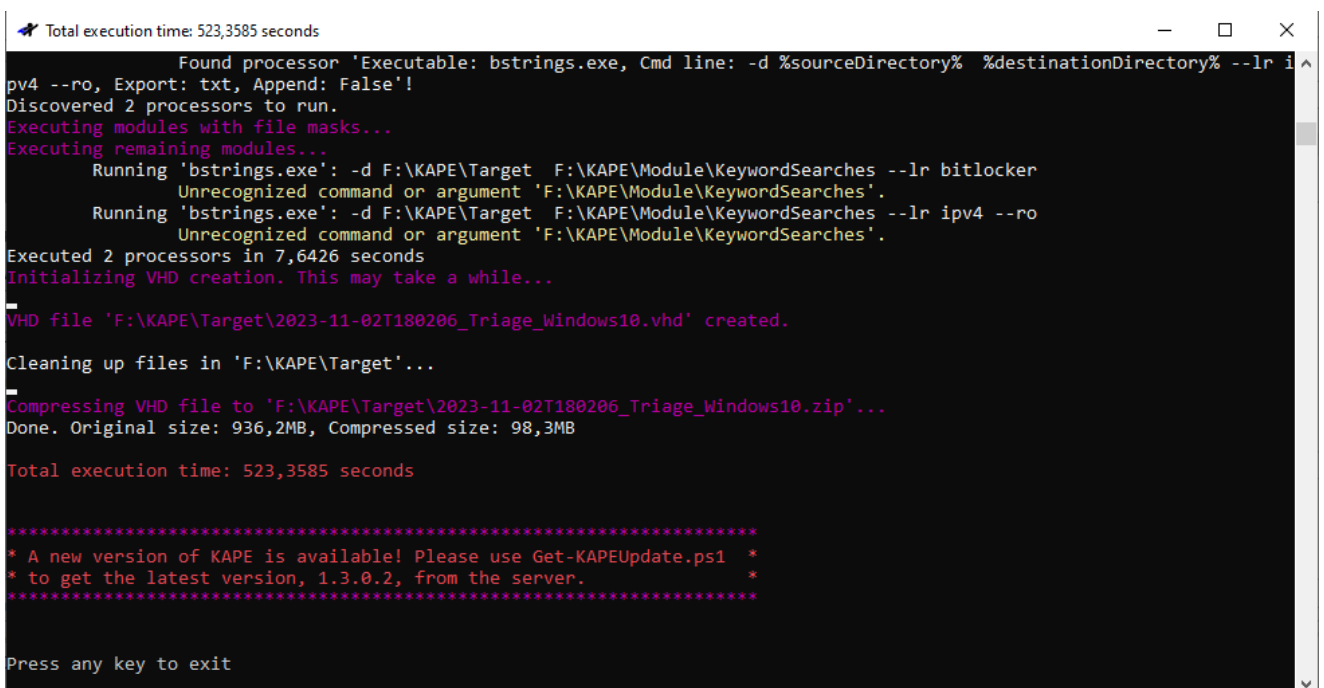
- Carpeta objetivo
- Carpeta sobre la que se volcarán los resultados del "Target".
- Check a las opciones de: Mostrar fecha y hora de la adquisición.
- Selección del set de herramientas de triage (¡SANS_Triage).
- Check "Process VSCs"
- Tipo de contenedor: VHD
- Nombre de evidencia
- Desmarcar la opción "Flush"

En el apartado "Module", he realizado la siguiente configuración:

- Carpeta sobre las que se volcarán los resultados del "Module".
- Check herramientas que se aplicarán a lo sacado en el "Target":
 - bstrings_IPv4: Usa "bstrings" para filtrar por direcciones IPv4.
 - bstrings_Bitlocker: Usa "bstrings" para filtrar por claves de recuperación de Bitlocker.
- Desmarcar la opción "Flush"

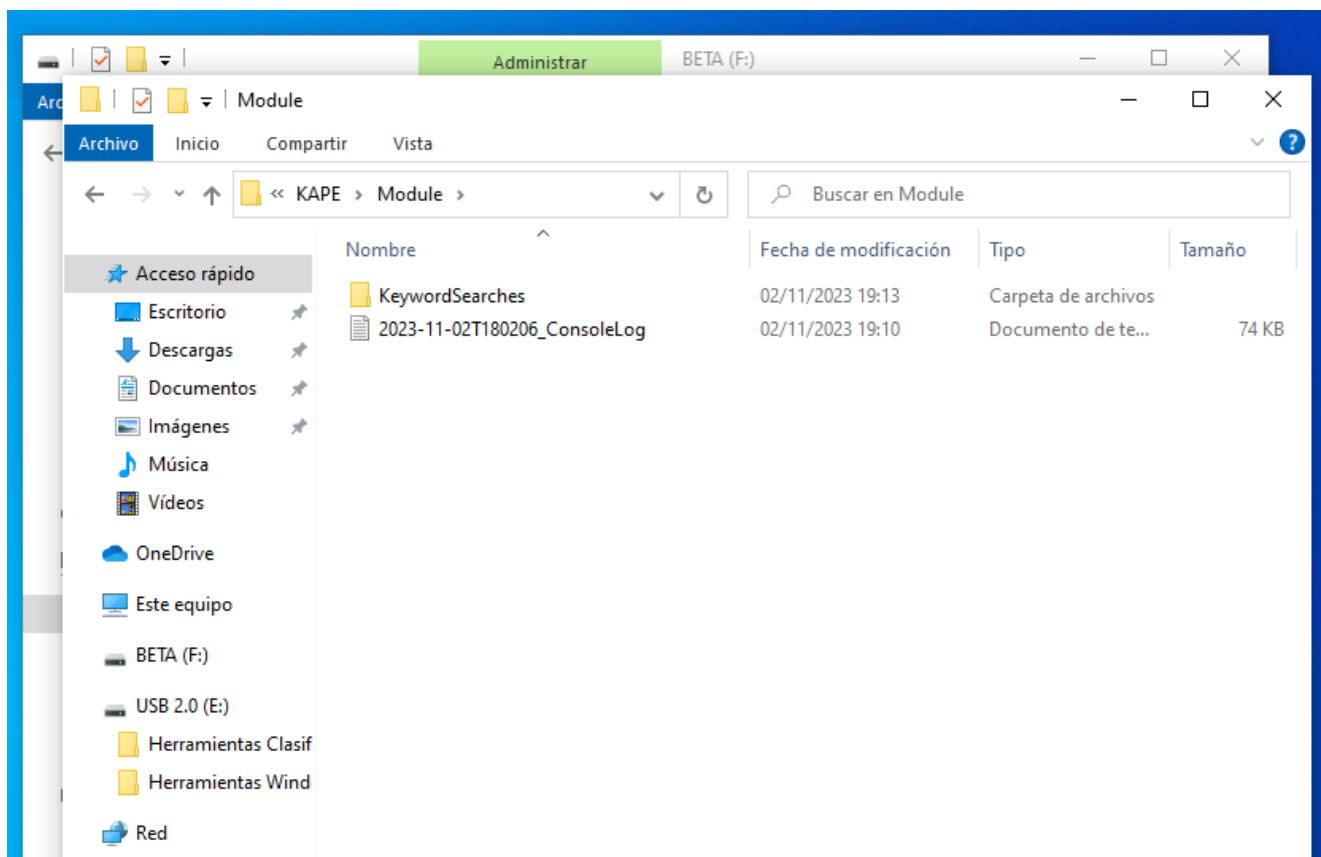


Ahora en la siguiente imagen, muestro el resultado final de la creación de los vestigios por parte de Kape:

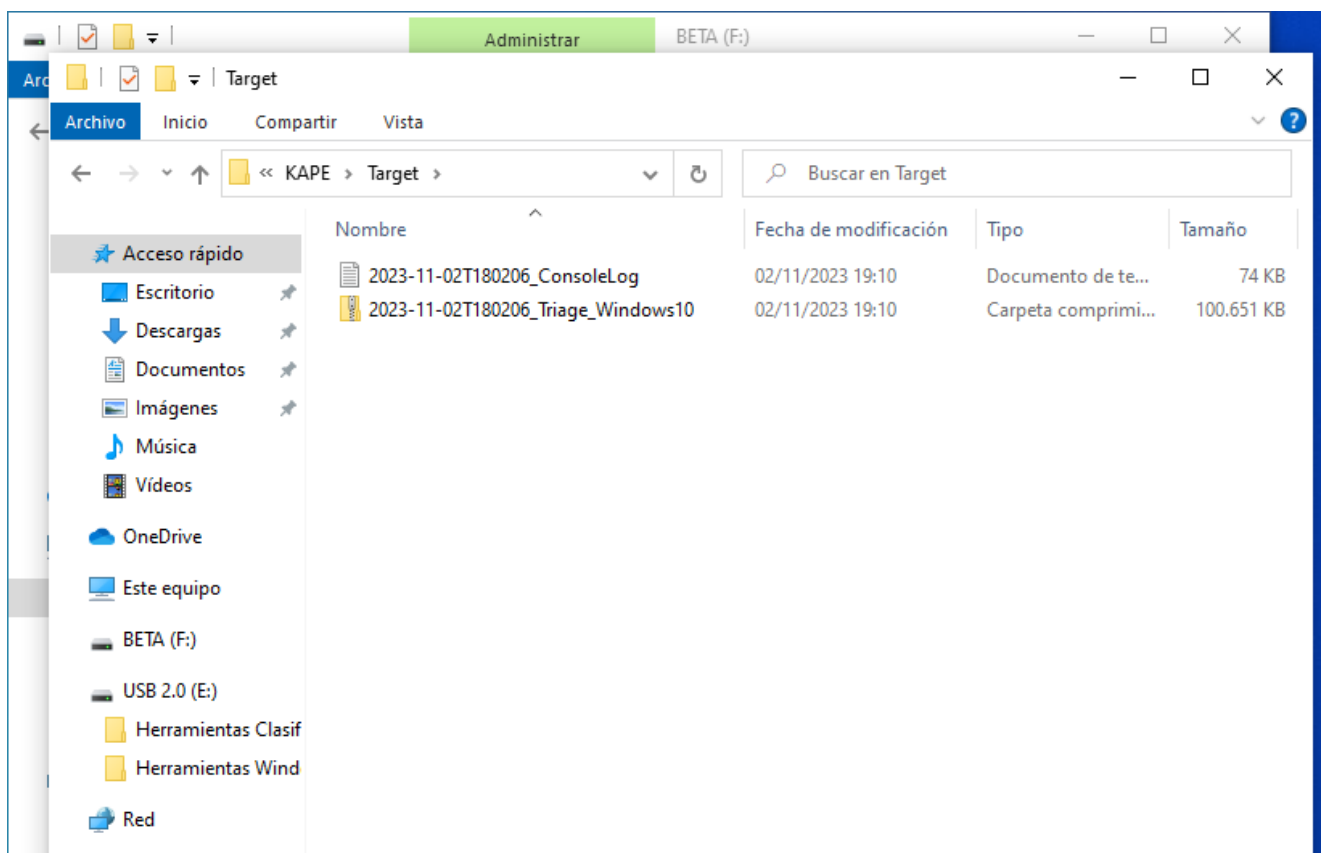


Por último, muestro el contenido de las carpetas resultantes:

Carpeta Module

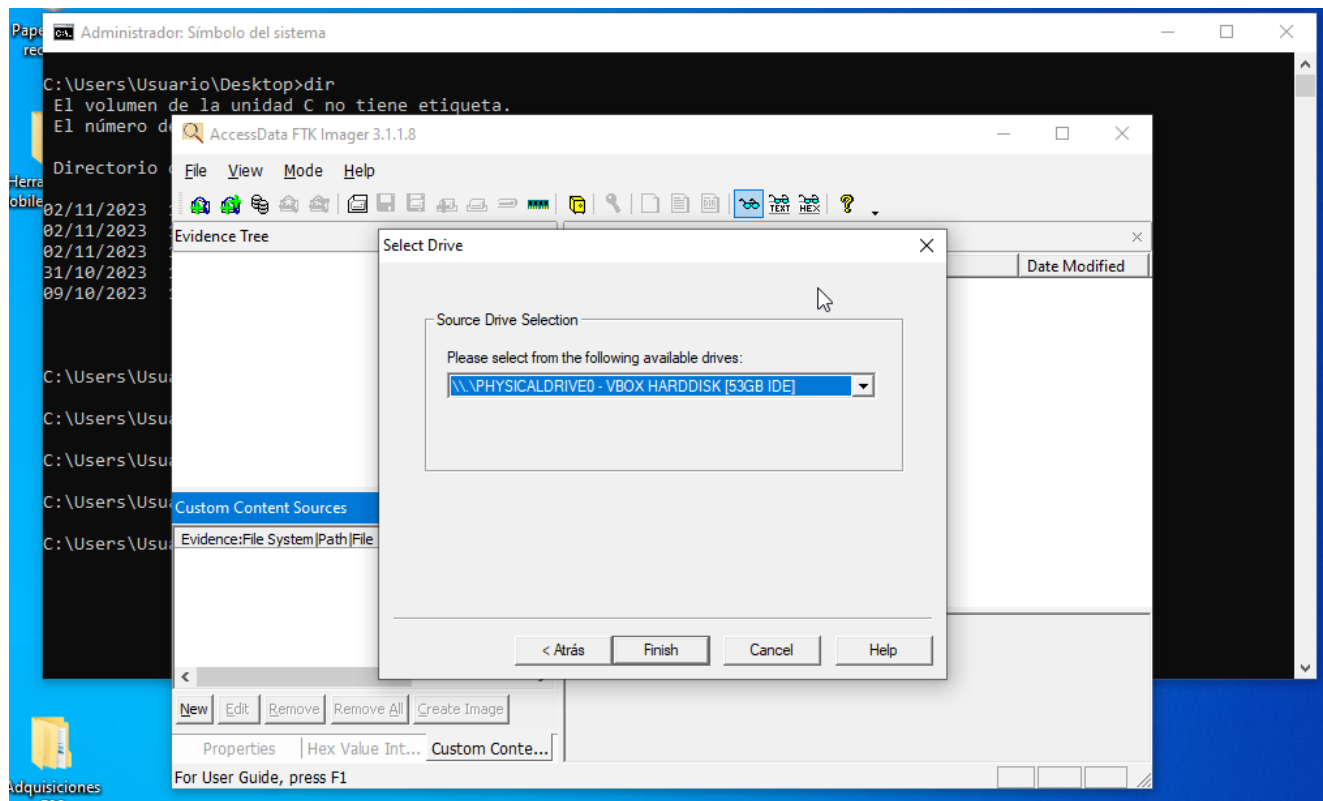


Carpeta Target

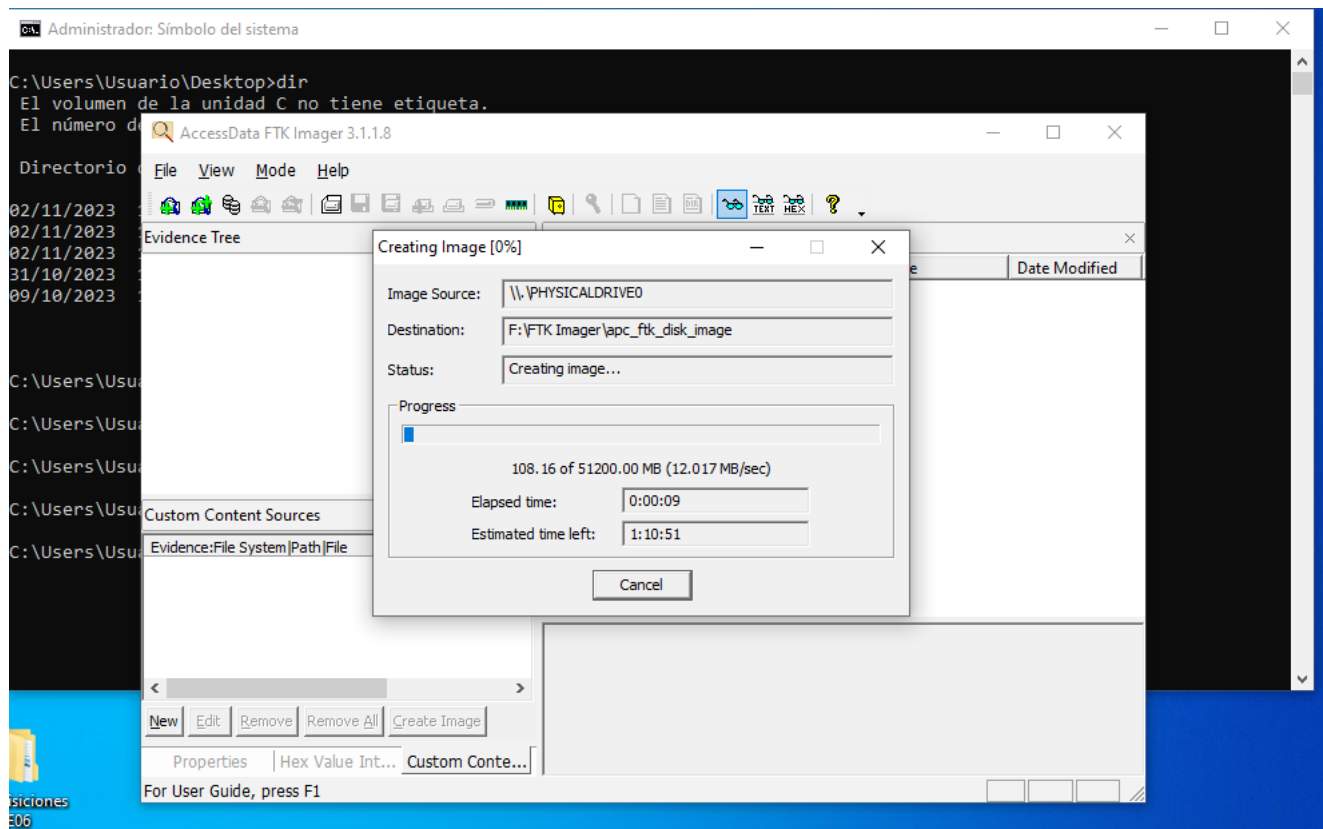


Por último, como indiqué anteriormente, realizaré una imagen completa de mi máquina virtual usando FTK Imager.

A continuación, muestro el momento en el que selecciono el disco de la máquina virtual del cual voy a realizar la imagen:



Ahora muestro el programa construyendo 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_disk_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: 02

Evidence Number: 01

Unique description: Adquisición Disco

Examiner: Antonio Peñalver Caro

Notes:

Information for F:\FTK Imager\apc_ftk_disk_image:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 6.527

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 104.857.600

[Physical Drive Information]

Drive Model: VBOX HARDDISK

Drive Serial Number: VBa81251d3-b19e747b

Drive Interface Type: IDE

Removable drive: False

Source data size: 51200 MB

Sector count: 104857600

[Computed Hashes]

MD5 checksum: 220cbd38489f9d878129bfff6a125e842

SHA1 checksum: 18991124893730b59f8c210aa65412e2d45dc4ac