

Práctica 4

Adquisición de Evidencias en Máquina Encendida

Índice

Índice.....	2
Pasos Previos:.....	3
1. Creación de Máquinas Virtuales (VM):.....	3
a. Windows 10:.....	3
2. Configuración del Pendrive:.....	4
3. Enlaces a las Herramientas:.....	5
a. dd (windows):.....	5
b. FTK imager (windows):.....	5
dd (Disco no cifrado):.....	6
FTK Imager Lite (Disco no cifrado):.....	14
¿Cómo cifrar un disco con BitLocker?:.....	28
dd (Disco cifrado):.....	47
FTK Imager Lite (Disco cifrado):.....	50
Evidencias Obtenidas:.....	62

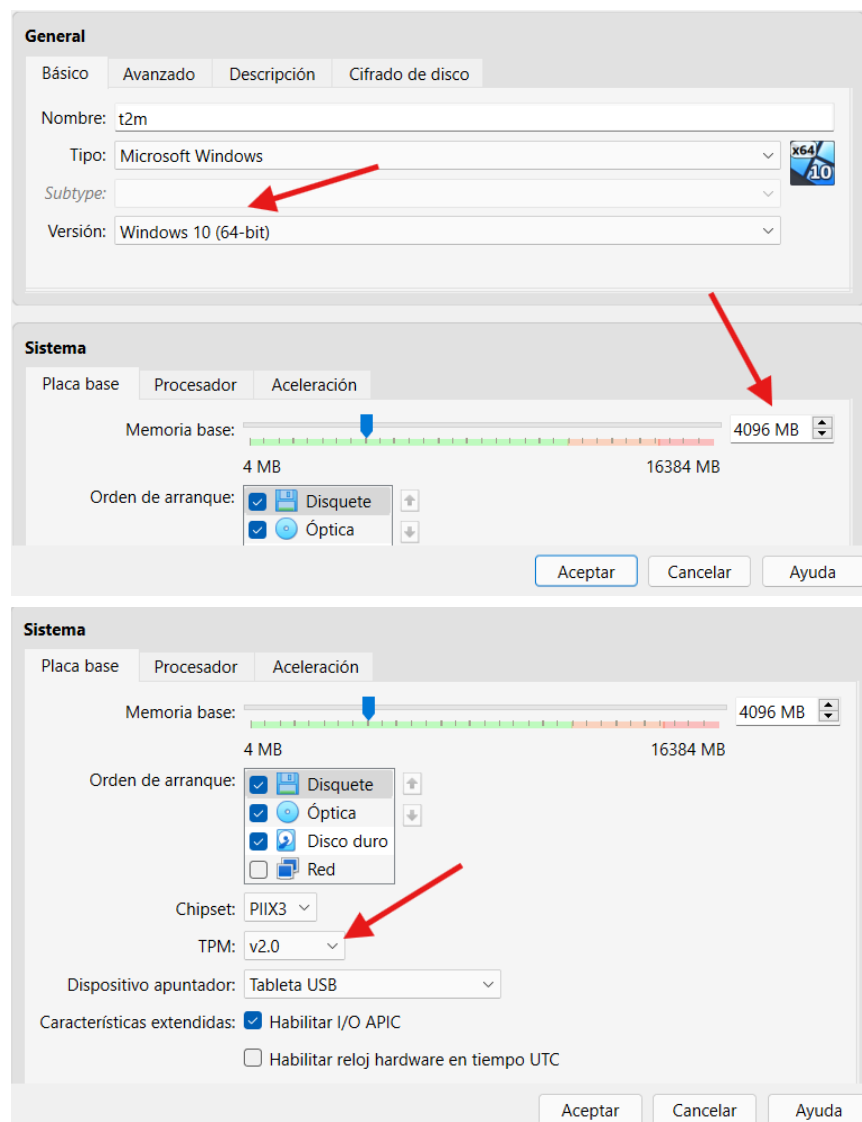
Pasos Previos:

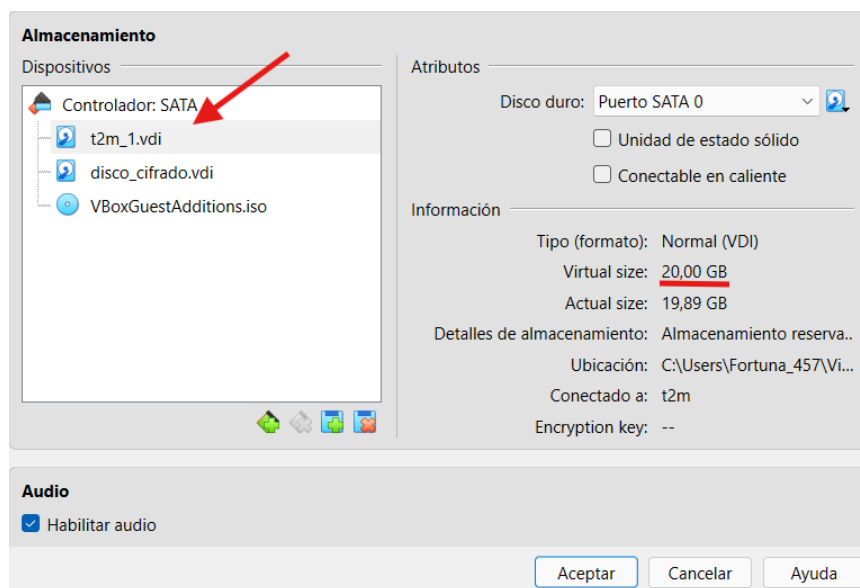
1. Creación de Máquinas Virtuales (VM):

a. Windows 10:

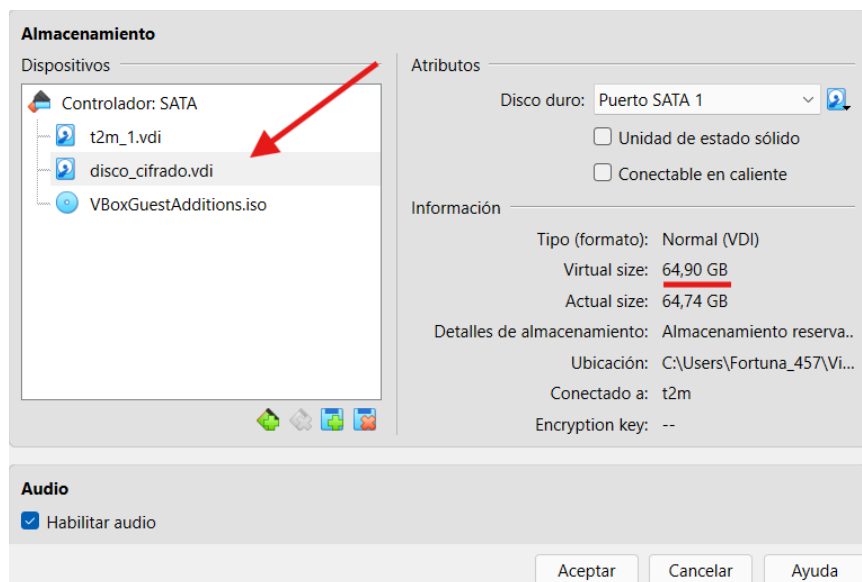
Configuramos la máquina virtual para que tenga 4GB de memoria Ram, 20 GB de disco duro y el TPM con versión 2.0.

Usamos una ISO de Windows 10 Pro x64.





2. Configuración del Pendrive:



3. Enlaces a las Herramientas:

a. dd (windows):

Enlace a la web original: [Descargar desde la web oficial.](#)

Downloads for dd family					
Program	Version	Content	Format	Platform	Download
dd	0.6beta3	Binary	.zip	Windows	dd-0.6beta3.zip
dd	0.6beta3	Source	.zip	Delphi	dd-0.6beta3.src.zip
dd	0.6beta1	Source	.zip	Delphi	dd-0.6beta1.src.zip
dd	0.5	Binary	.zip	Windows	dd-0.5.zip
dd	0.4beta4	Binary	.zip	Windows	dd-0.4beta4.zip
dd	0.4beta4	Source	.zip	Delphi	dd-0.4beta4.src.zip
Installation Instructions					

b. FTK imager (windows):

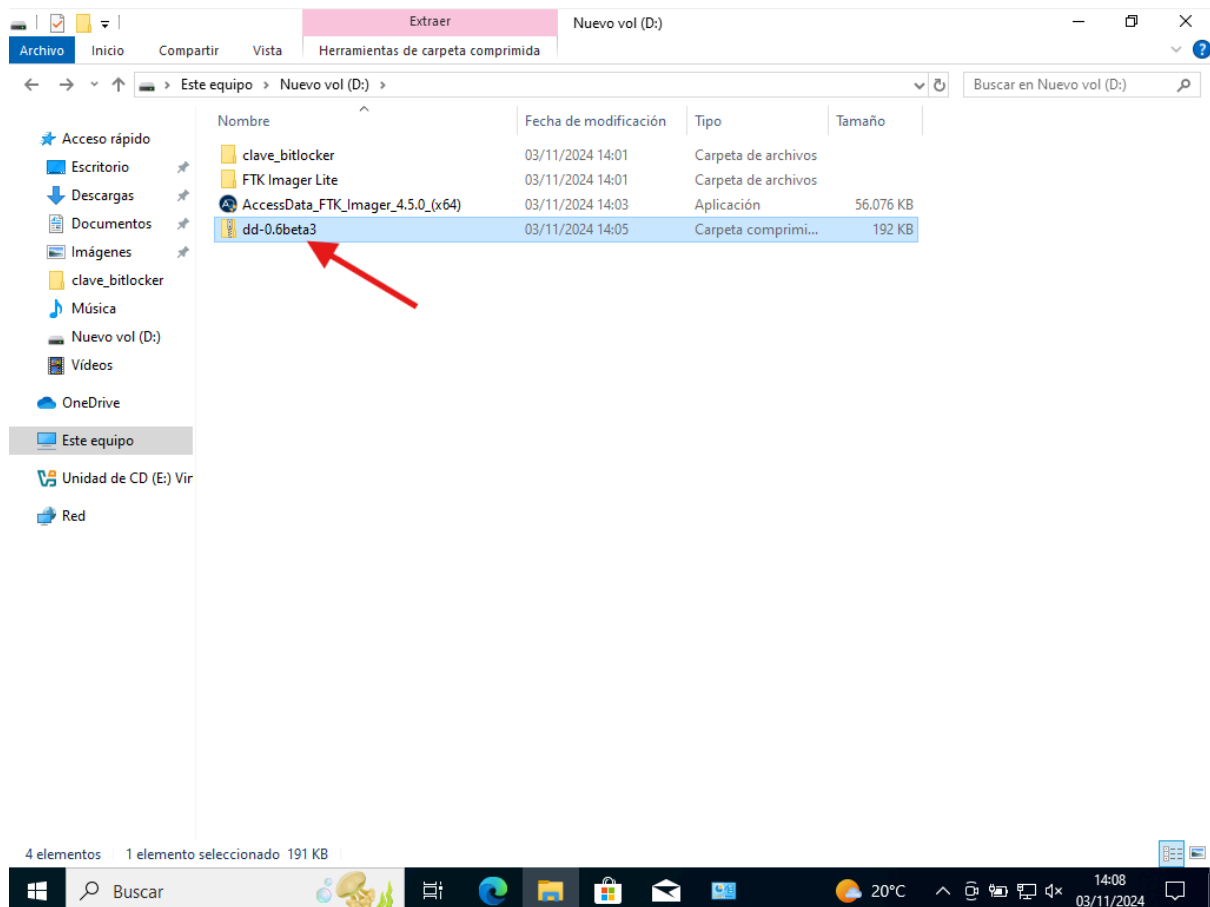
Enlace a la web original: [Descargar desde Drive.](#)

ftk Imager Lite_3.1.1 portable.zip 28 elementos

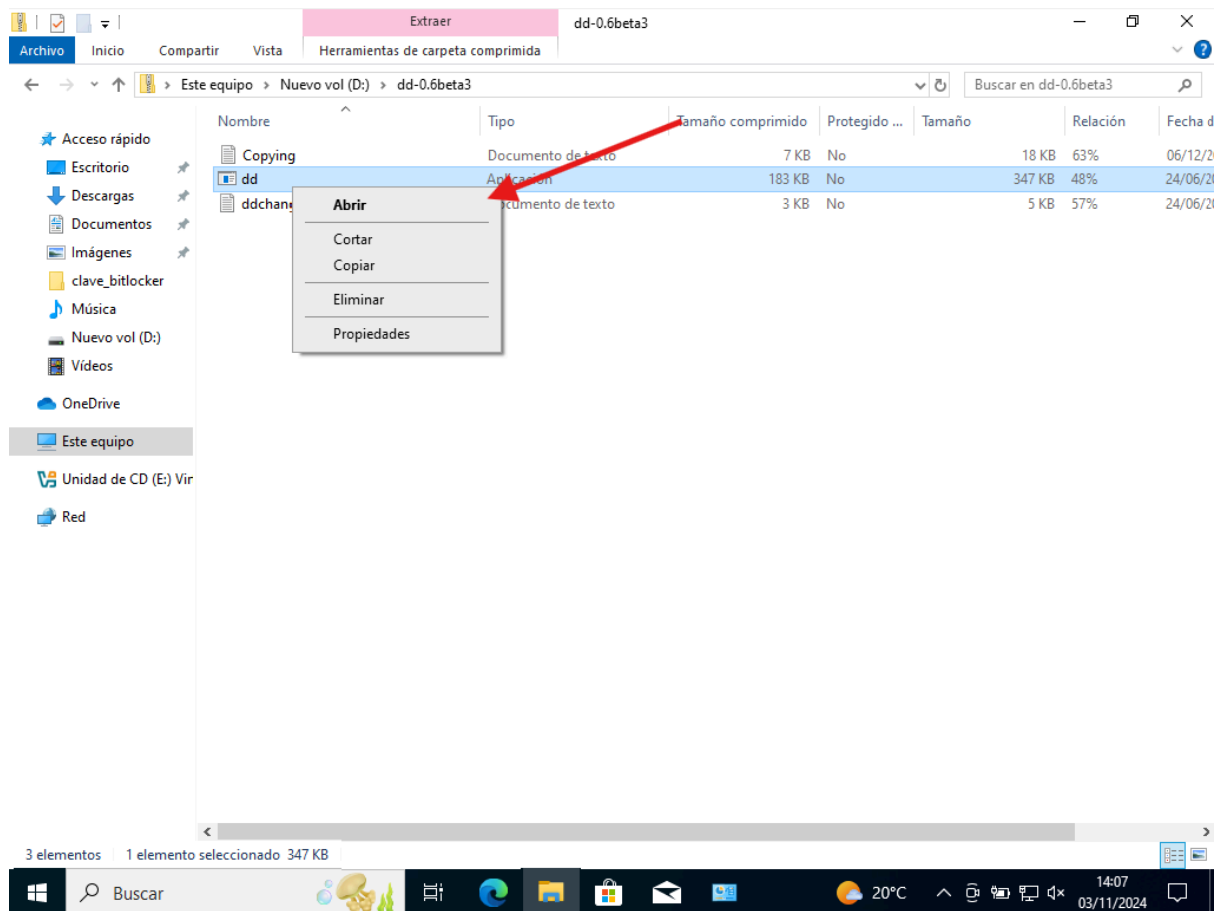
Nombre	Ultima modificación	Tamaño del arc...
help	-	632 KB
langs	-	15 MB
ad_globals.dll	23 ago 2012	147 KB
ad_log.dll	2 may 2012	311 KB
adefs.dll	23 ago 2012	1 MB
adencrypt.dll	23 ago 2012	279 KB
adencrypt_gui.exe	23 ago 2012	227 KB
adfs_globals.dll	23 ago 2012	8 KB
ADisoDLL.dll	23 ago 2012	69 KB
adshattrdefs.dll	23 ago 2012	369 KB
boost_date_time-vc100-mt-1_49.dll	1 may 2012	52 KB
boost_filesystem-vc100-mt-1_49.dll	1 may 2012	163 KB

dd (Disco no cifrado):

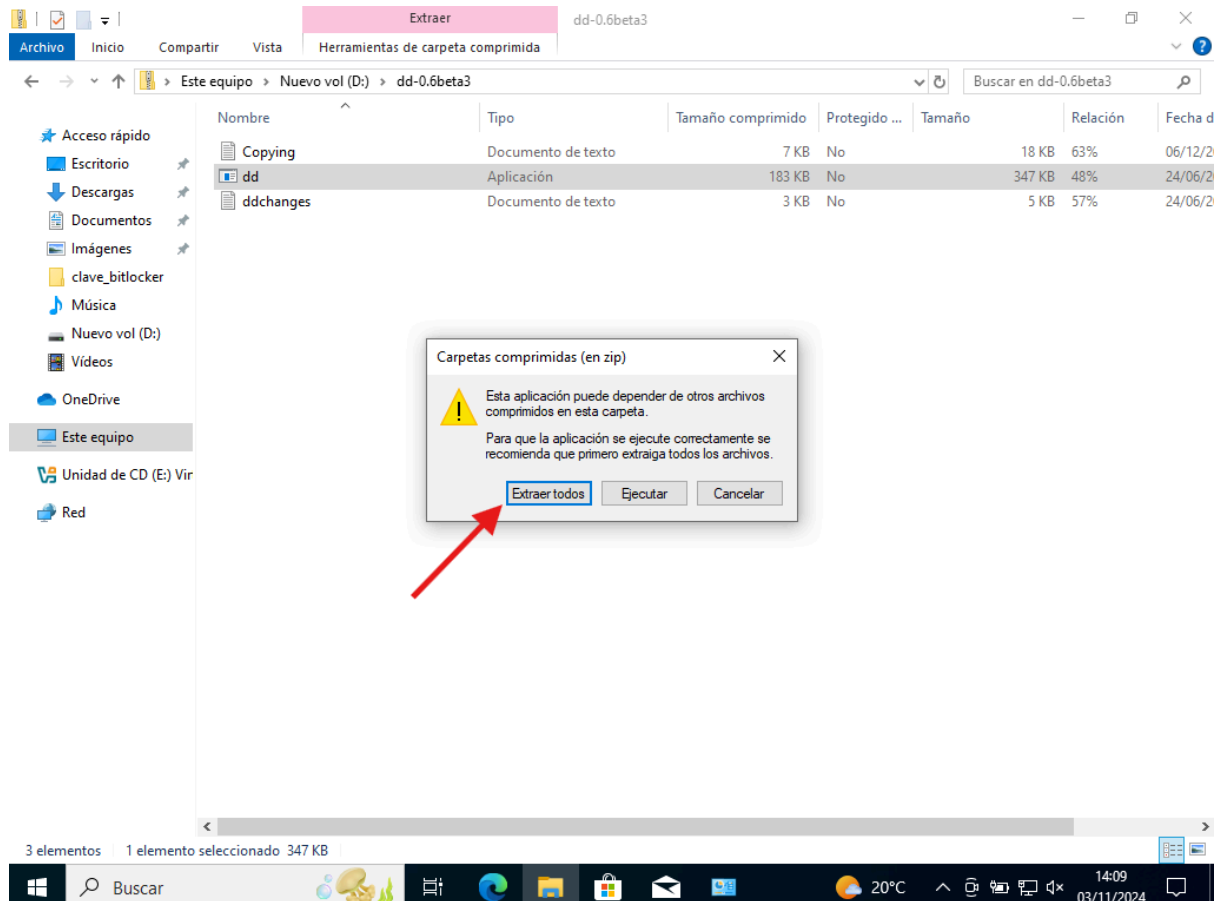
Instalamos la herramienta desde la [web oficial](#).



Extraemos los archivos del fichero.



ANÁLISIS FORENSE



← Extraer carpeta comprimida (en zip)

Seleccionar un destino y extraer archivos

Los archivos se extraerán a esta carpeta:

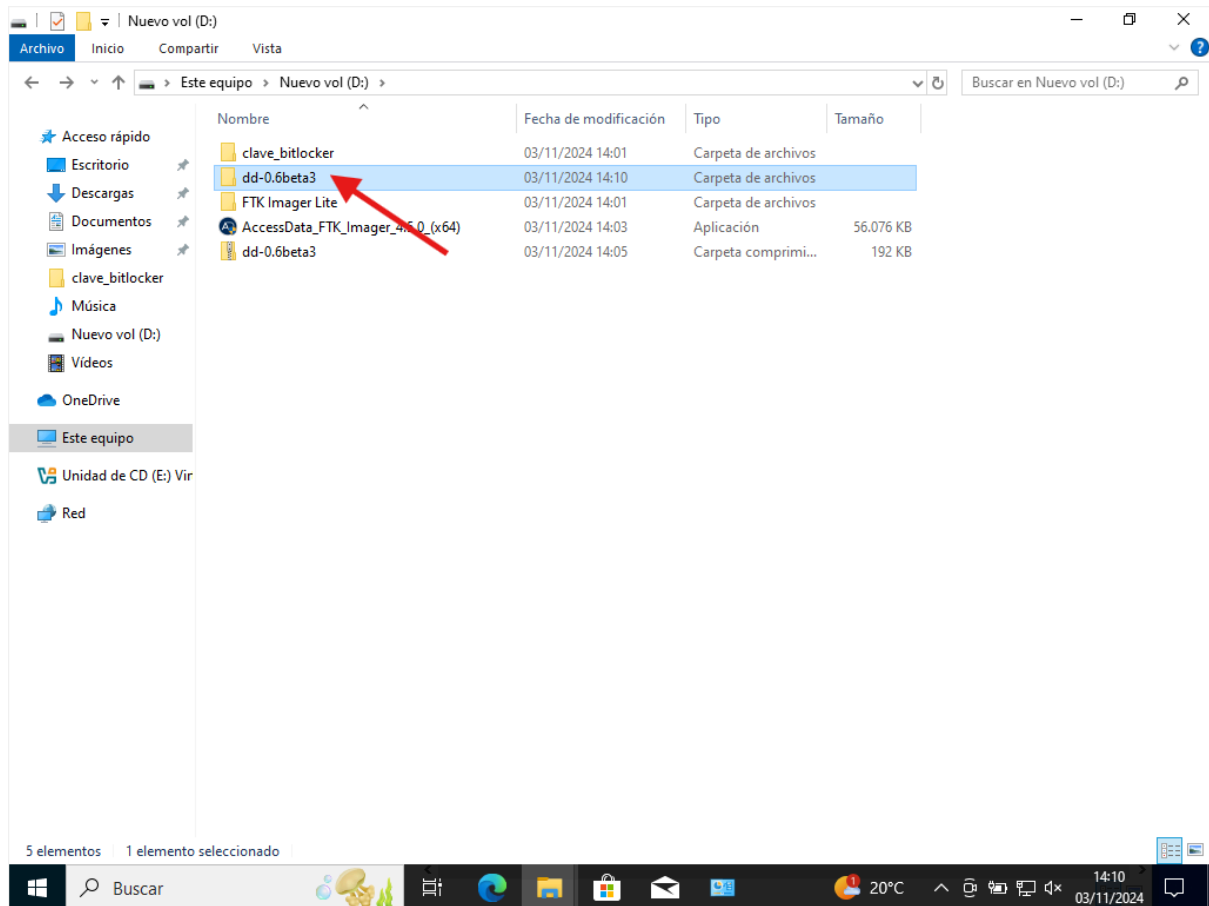
D:\dd-0.6beta3

Examinar...

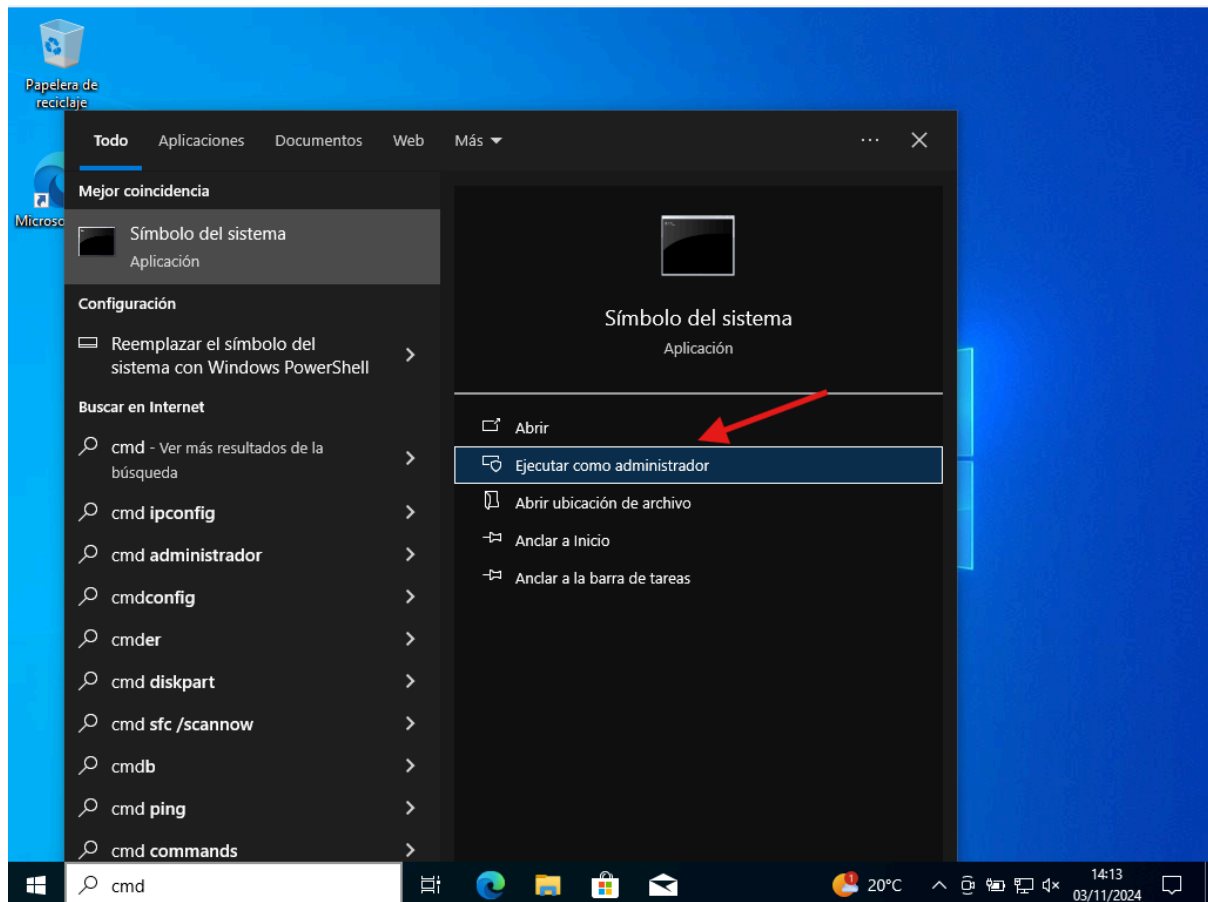
☒ Mostrar los archivos extraídos al completar



ANÁLISIS FORENSE



Una vez hemos extraído todo, abrimos el cmd de Windows como Administradores.



Y en la ruta de la carpeta que acabamos de crear, ejecutamos el comando **dir** para comprobar que todo está correcto.

```

CA: Administrador: Símbolo del sistema

C:\Windows\System32>D:

D:\>cd dd-0.6beta3

D:\dd-0.6beta3>dir
El volumen de la unidad D es Nuevo vol
El número de serie del volumen es: 062C-ACF4

Directorio de D:\dd-0.6beta3

03/11/2024  14:10    <DIR>          .
03/11/2024  14:10    <DIR>          ..
06/12/2003  14:50                18.325 Copying.txt
24/06/2009  22:03             355.328 dd.exe
24/06/2009  21:53                5.026 ddchanges.txt
               3 archivos             378.679 bytes
               2 dirs  69.340.622.848 bytes libres

D:\dd-0.6beta3>_

```

Y comprobamos el funcionamiento de la herramienta.

```

CA: Administrador: Símbolo del sistema

D:\dd-0.6beta3>dd.exe --help
rawwrite dd for windows version 0.6beta3.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by terms of the GPL Version 2.

dd [bs=SIZE] [count=BLOCKS] [if=FILE] [of=FILE] [seek=BLOCKS] [skip=BLOCKS] [--size] [--list] [--progress]
SIZE and BLOCKS may have one of the following suffix:
 k = 1024
 M = 1048576
 G = 1073741824
default block size (bs) is 512 bytes
skip specifies the starting offset of the input file (if)
seek specifies the starting offset of the output file (of)

D:\dd-0.6beta3>

```

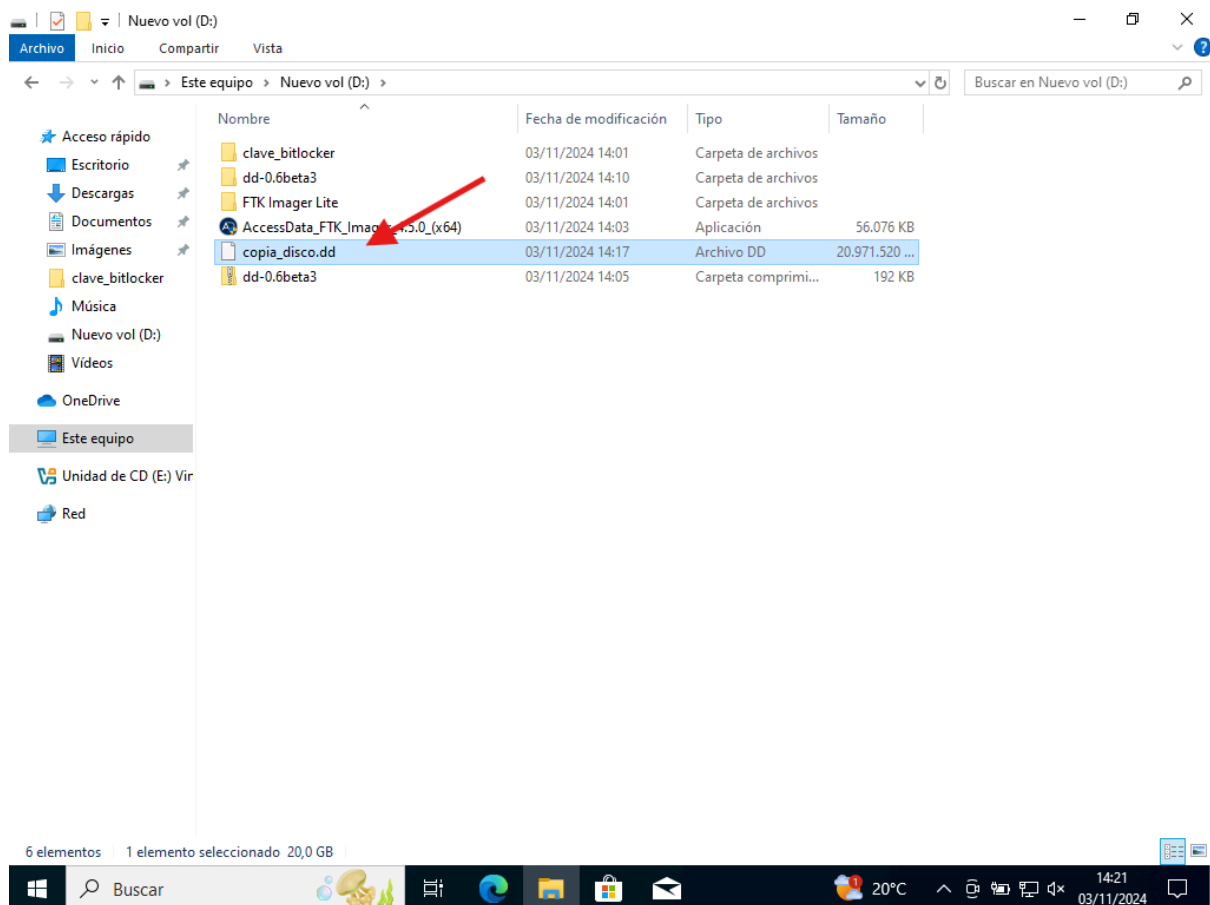
Una vez vemos que todo funciona correctamente, ejecutamos el siguiente comando:

dd.exe if=\\.\PHYSICALDRIVE0 of=E:\copia_disco.dd bs=4M --progress

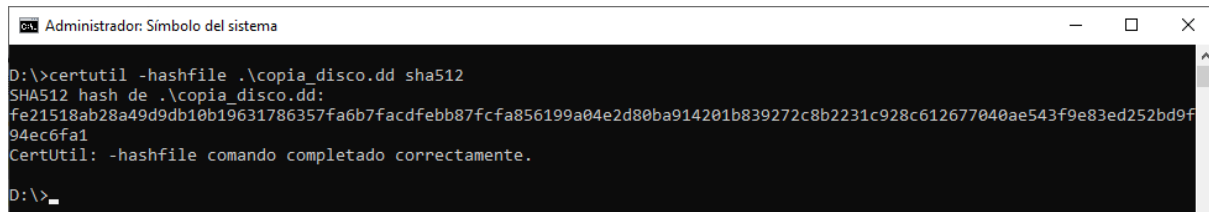
```
D:\dd-0.6beta3>dd.exe if=\\.\PHYSICALDRIVE0 of=D:\copia_disco.dd bs=4M --progress
rawwrite dd for windows version 0.6beta3.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by terms of the GPL Version 2.

844M _
```

Una vez se termina, comprobamos que se ha creado un archivo .dd en el disco duro externo.



Y calculamos el hash de la evidencia obtenida.



```
D:\>certutil -hashfile .\copia_disco.dd sha512
SHA512 hash de .\copia_disco.dd:
fe21518ab28a49d9db10b19631786357fa6b7facdfebb87fcfa856199a04e2d80ba914201b839272c8b2231c928c612677040ae543f9e83ed252bd9f94ec6fa1
CertUtil: -hashfile comando completado correctamente.
D:\>_
```

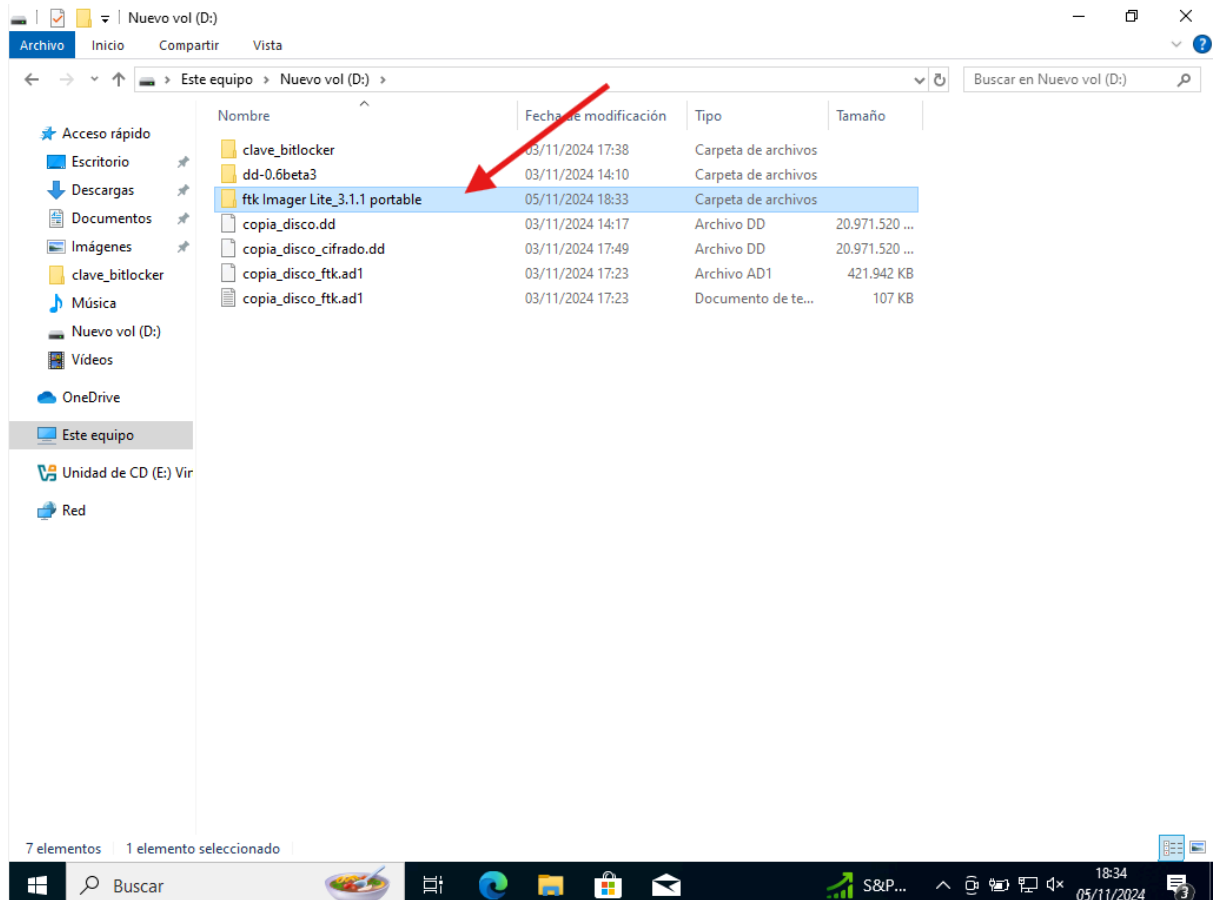
SHA512 hash de .\copia_disco.dd:

**fe21518ab28a49d9db10b19631786357fa6b7facdfebb87fcfa856199a04e2d80ba914
201b839272c8b2231c928c612677040ae543f9e83ed252bd9f94ec6fa1**

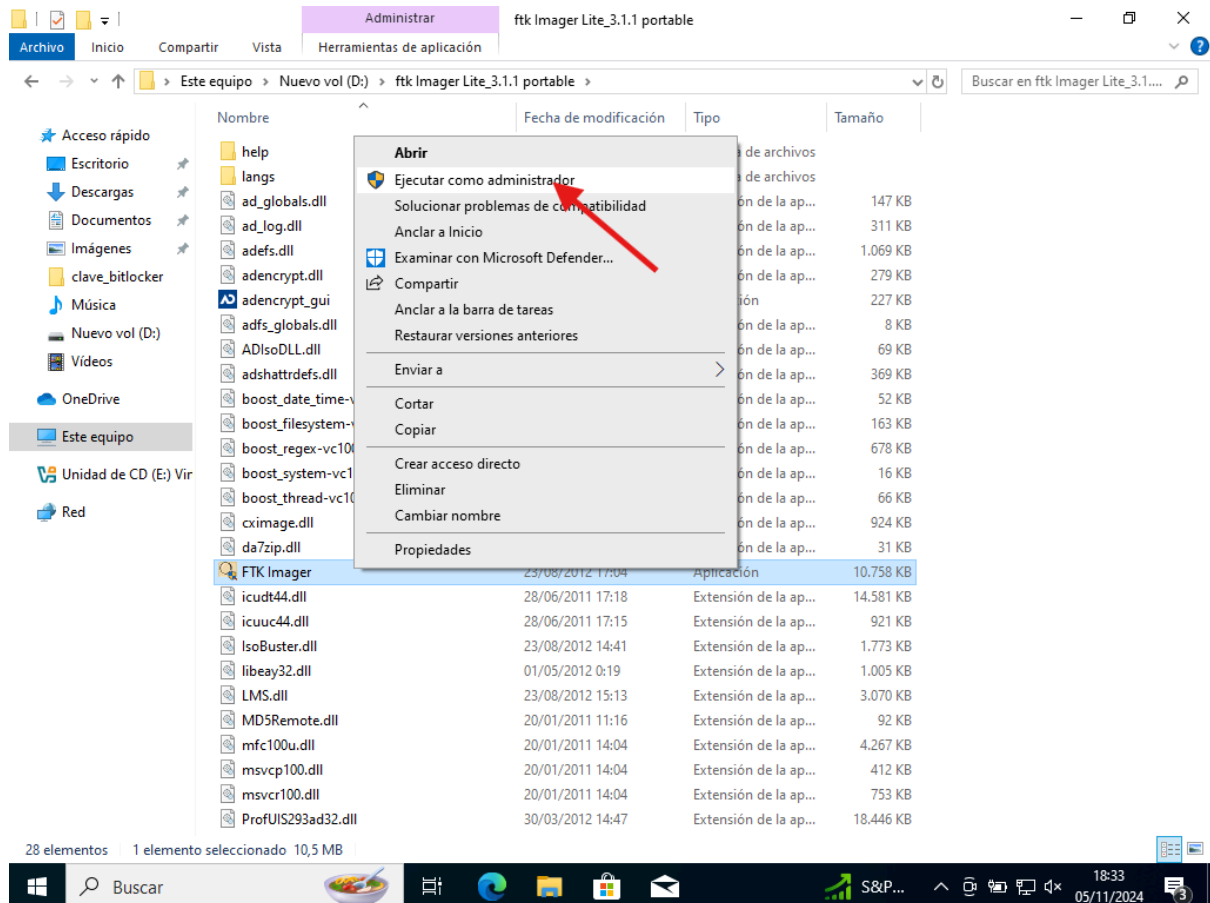
CertUtil: -hashfile comando completado correctamente.

FTK Imager Lite (Disco no cifrado):

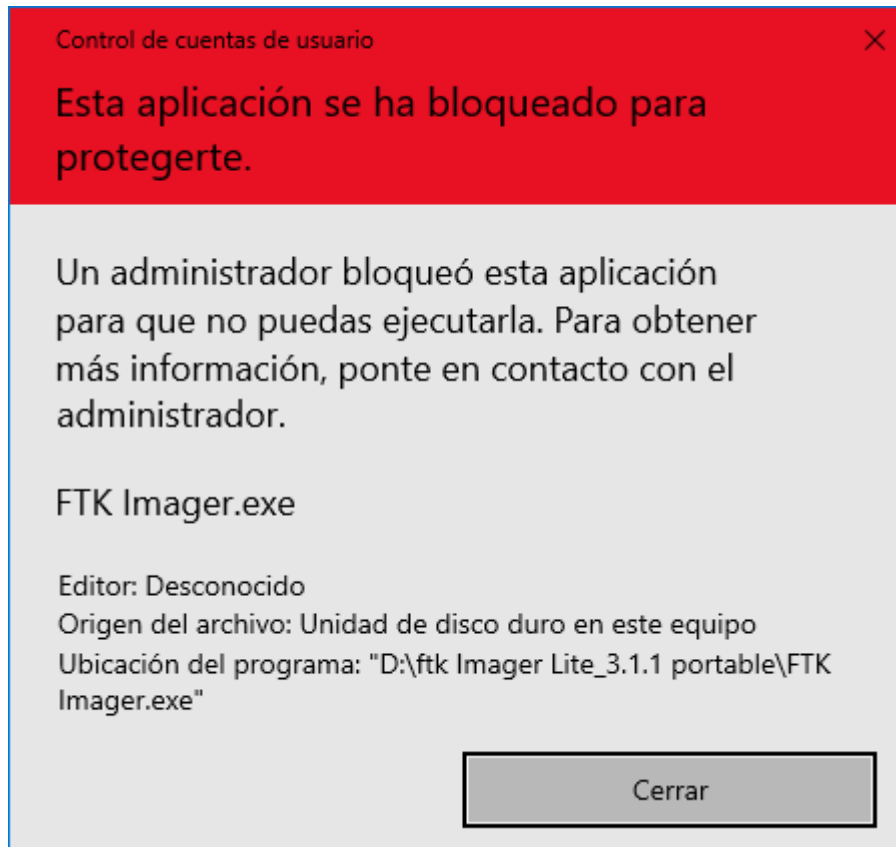
Ejecutamos FTK Imager como Administradores.



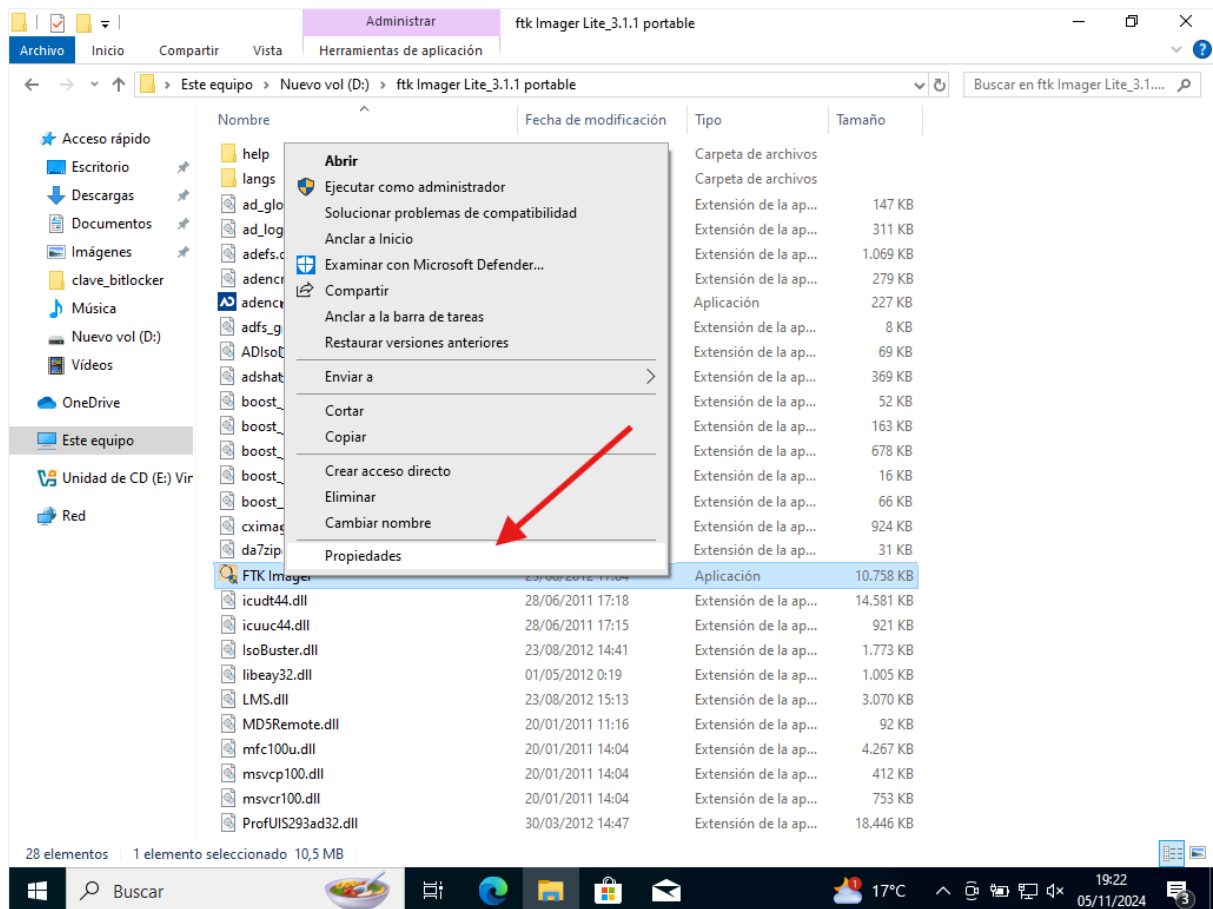
ANÁLISIS FORENSE



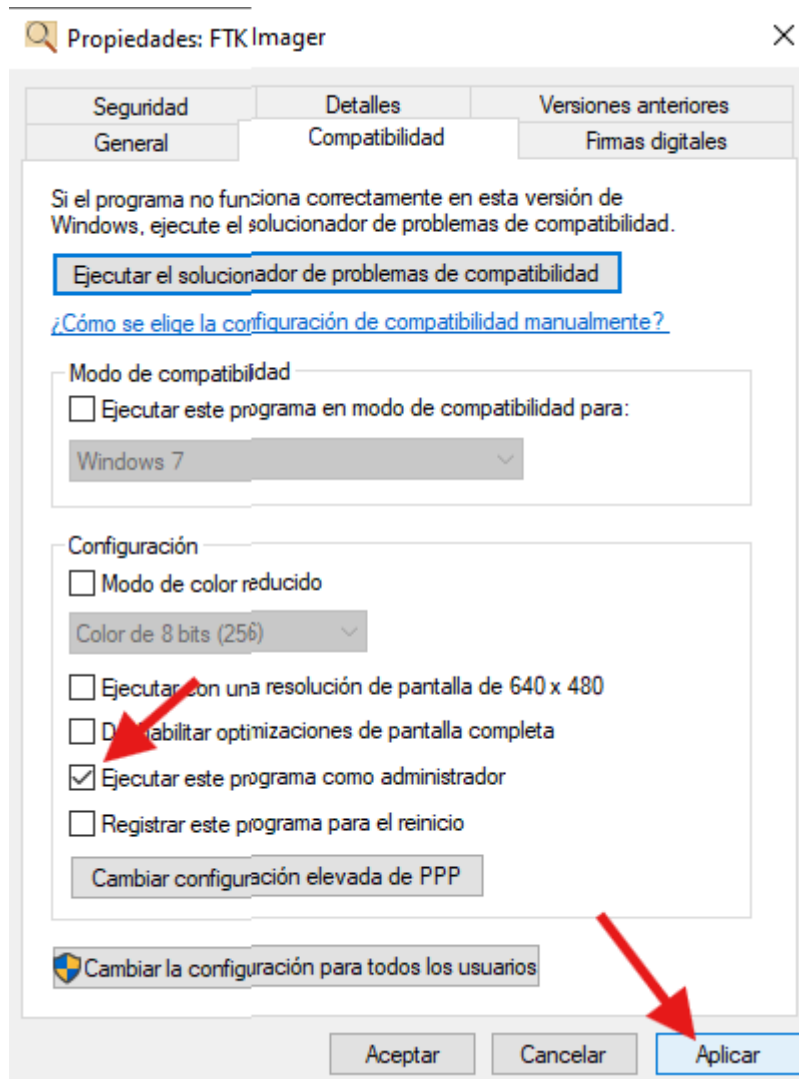
Al hacerlo nos dirá lo siguiente.



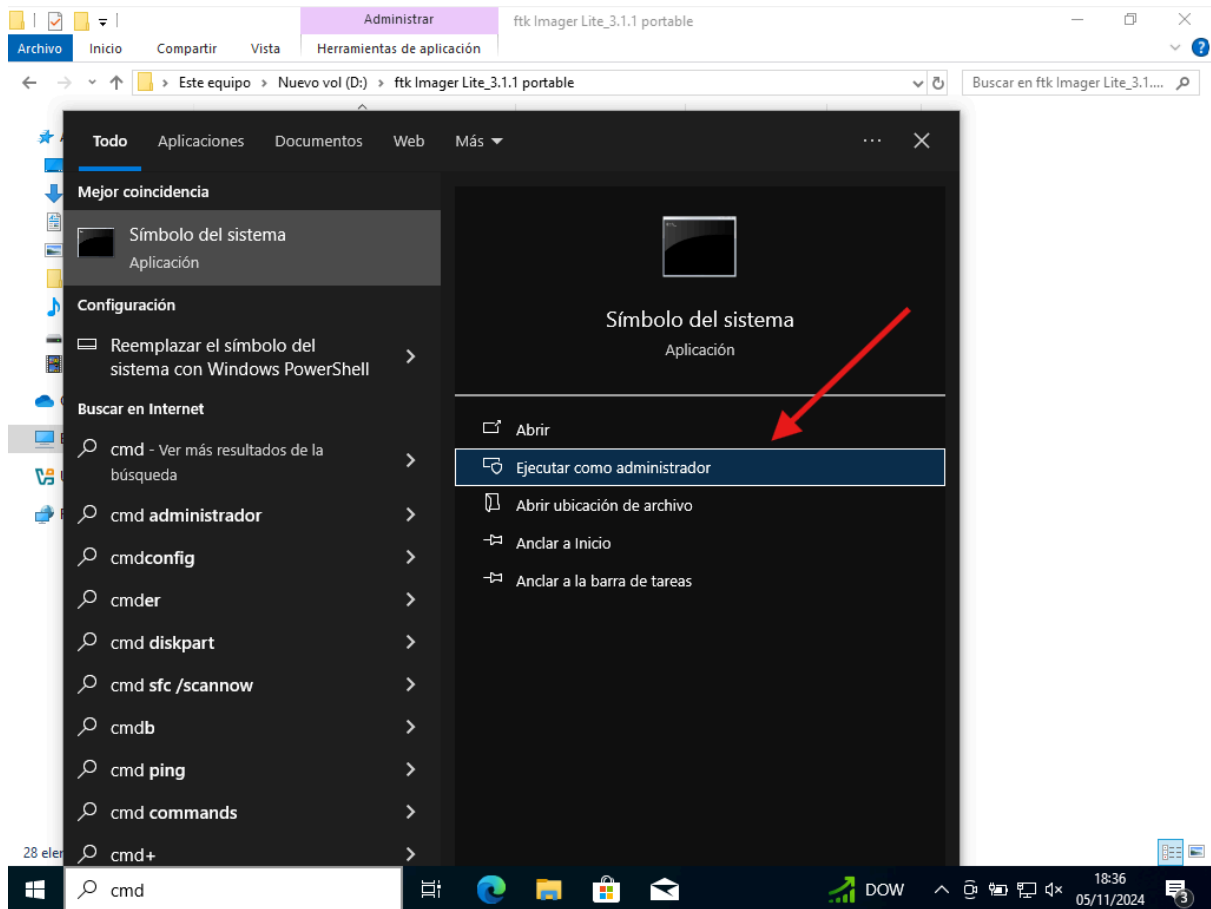
Por ello, nos iremos a la opción **Propiedades** del .exe.



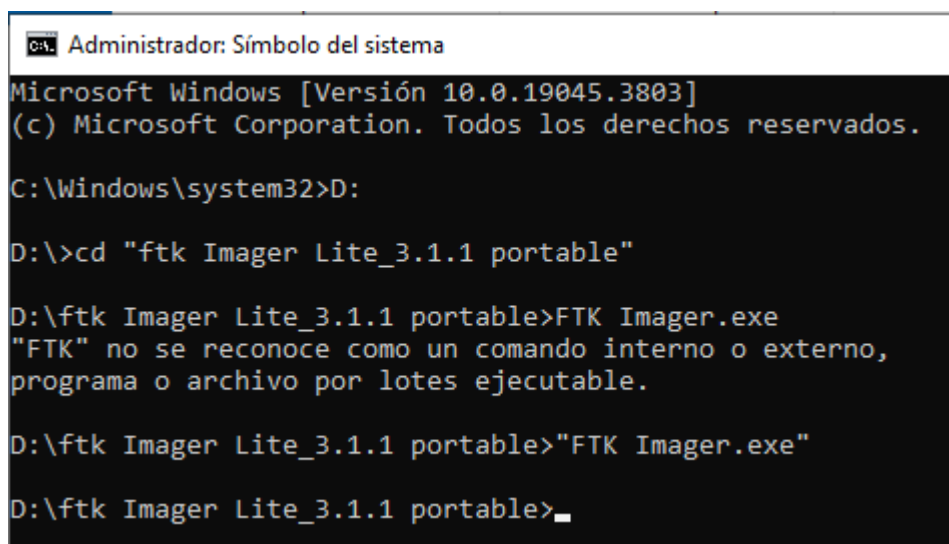
Y en el apartado **Compatibilidad**, seleccionaremos la opción **Ejecutar este programa como administrador**. Al terminar clicamos en **Aplicar**.



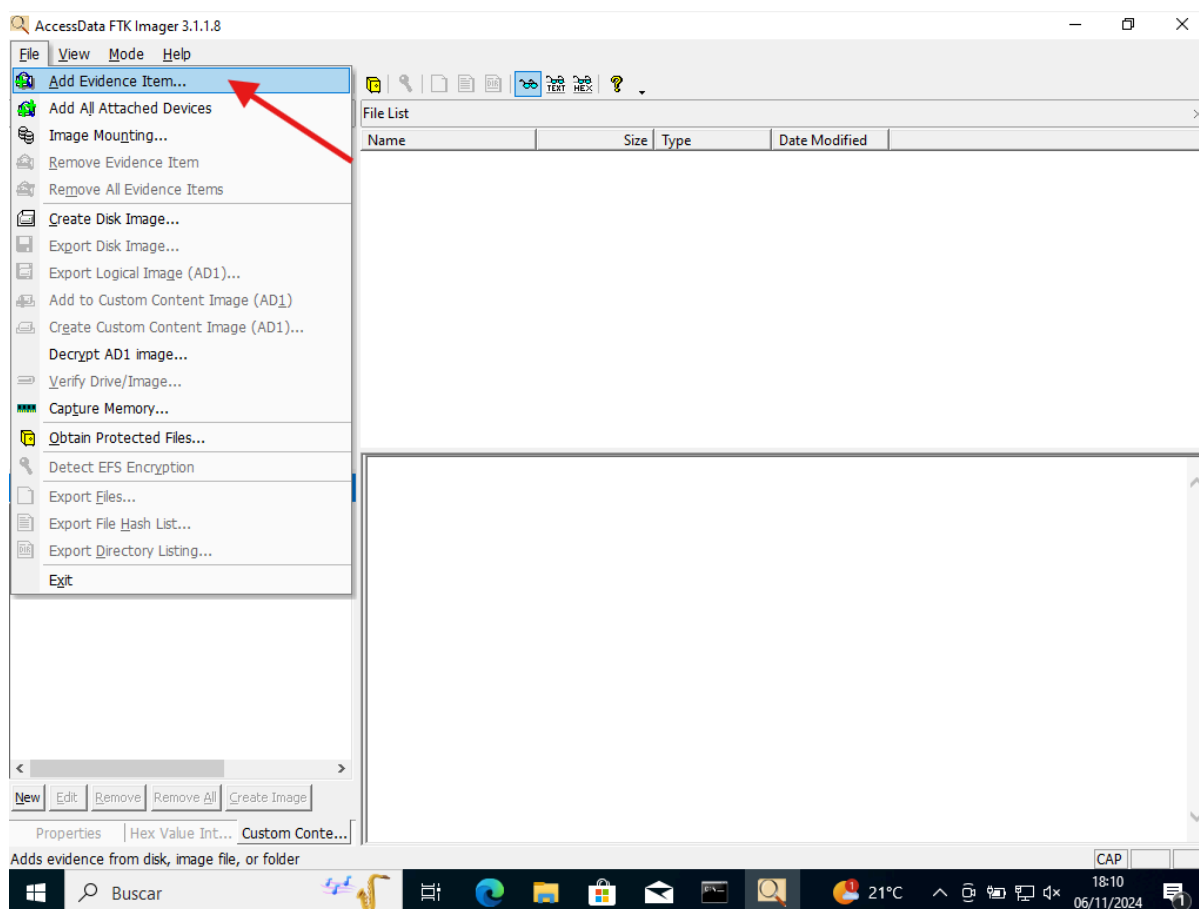
Una vez hecho los pasos previos, abrimos el cmd como Administrador.



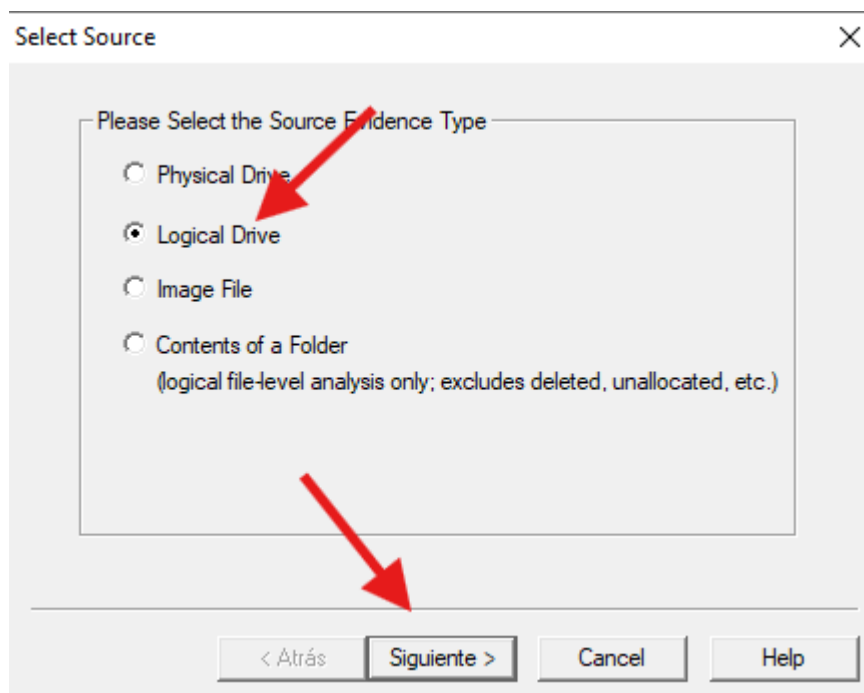
Y ejecutamos el programa.



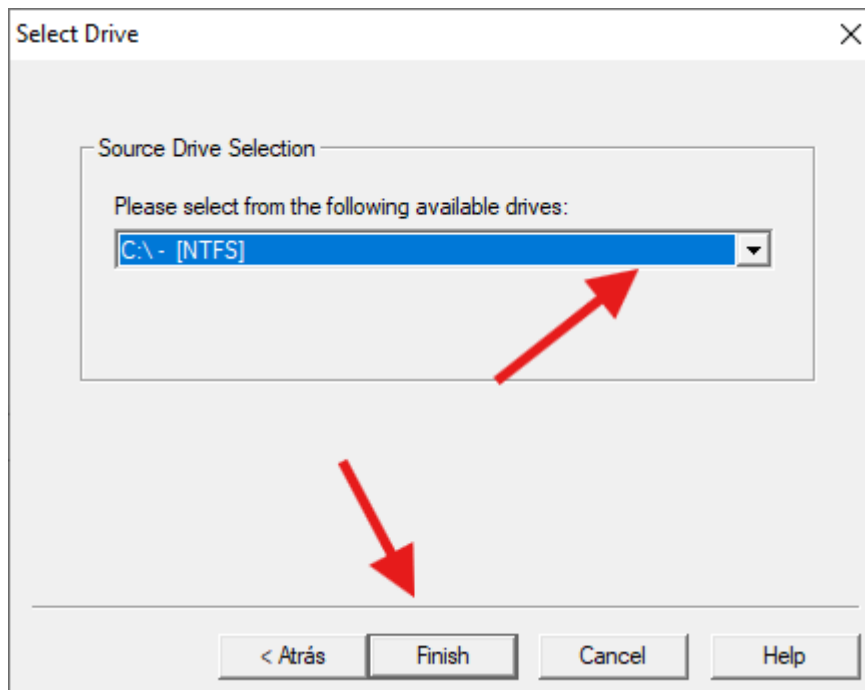
Con la herramienta inicializada, clicamos en **File** y seleccionamos **Add Evidence Item**.



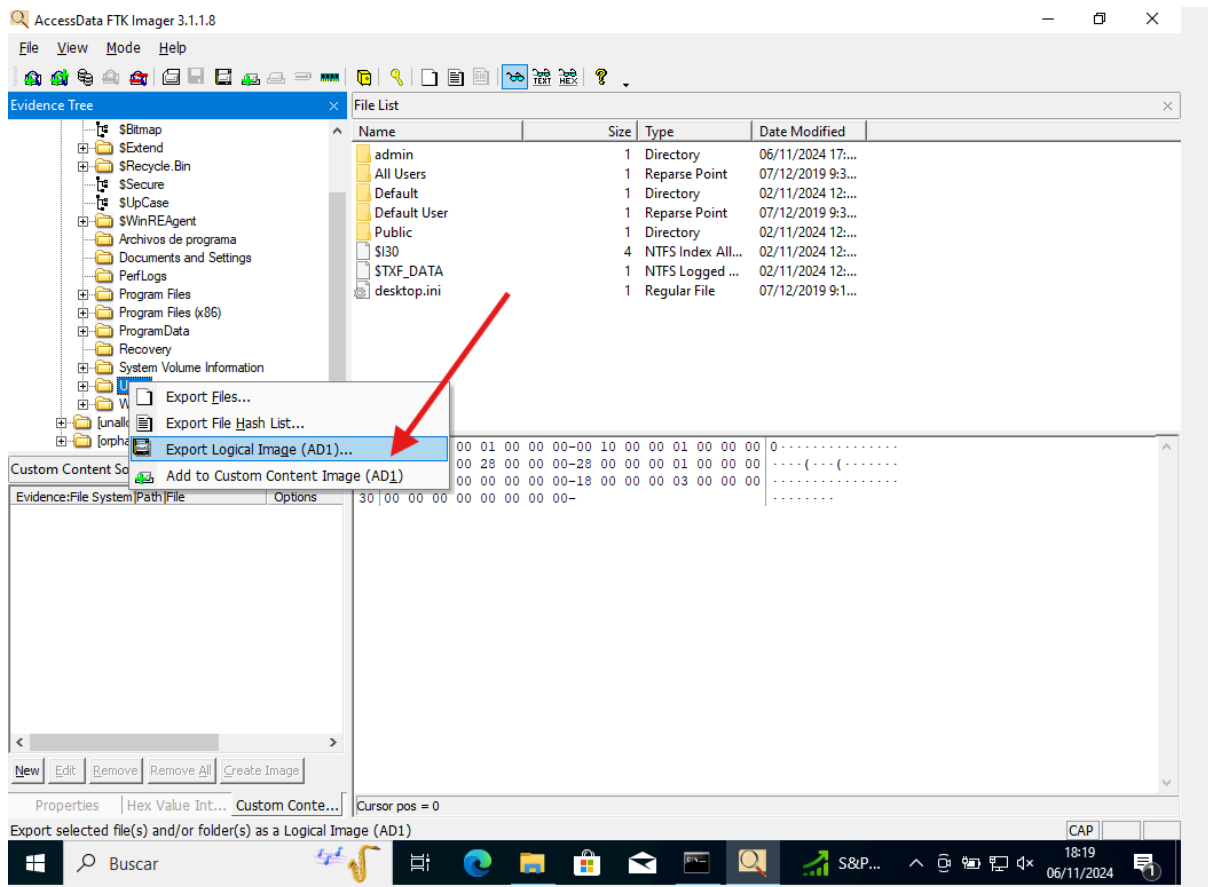
Seleccionamos **Logical Drive**.



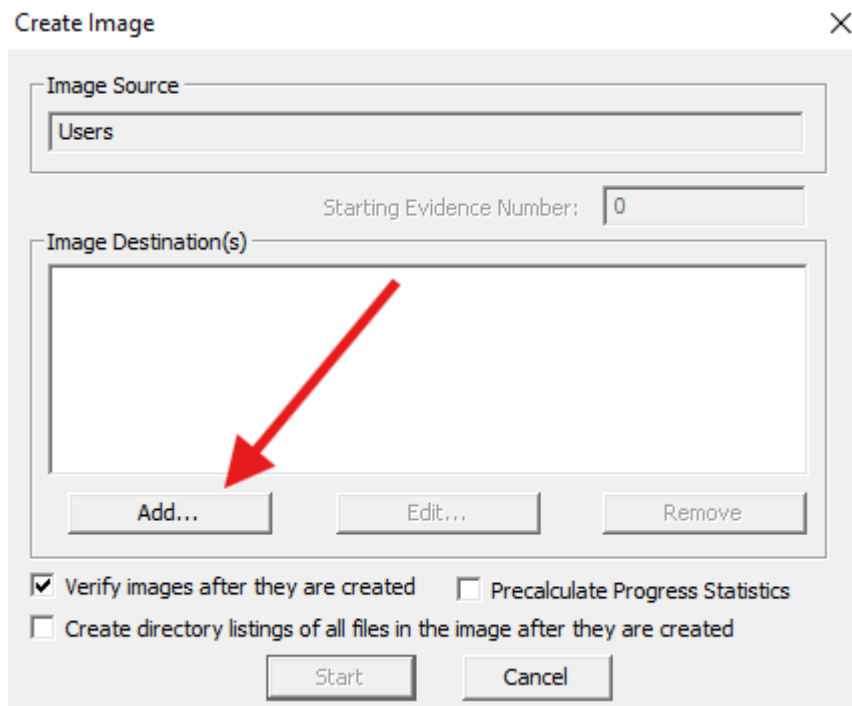
Escogemos el disco que contenga la evidencia.



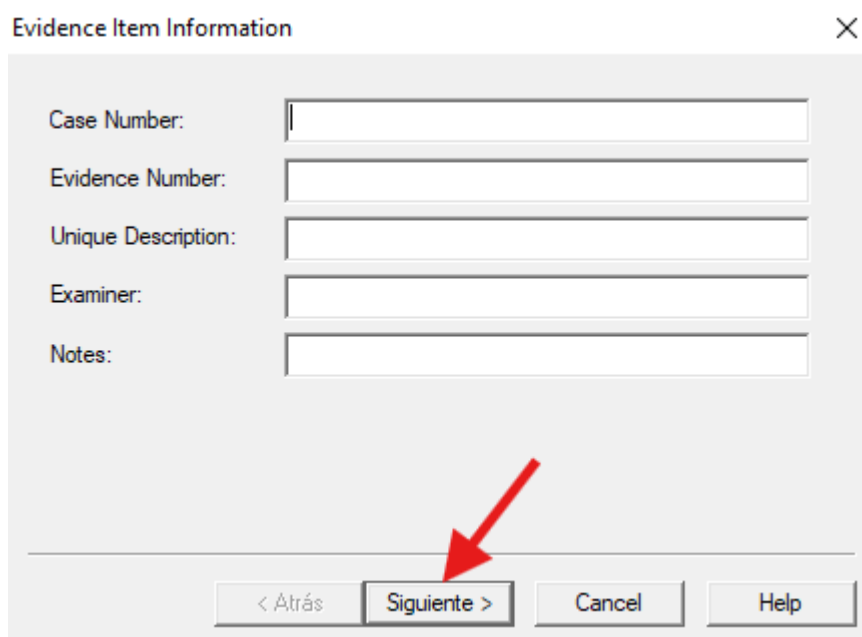
Una vez se ha cargado toda la estructura de carpetas del disco seleccionado, hacemos click derecho sobre la evidencia a obtener, en este caso la carpeta **Users**, y clicamos en **Export Logical Image (AD1)**.



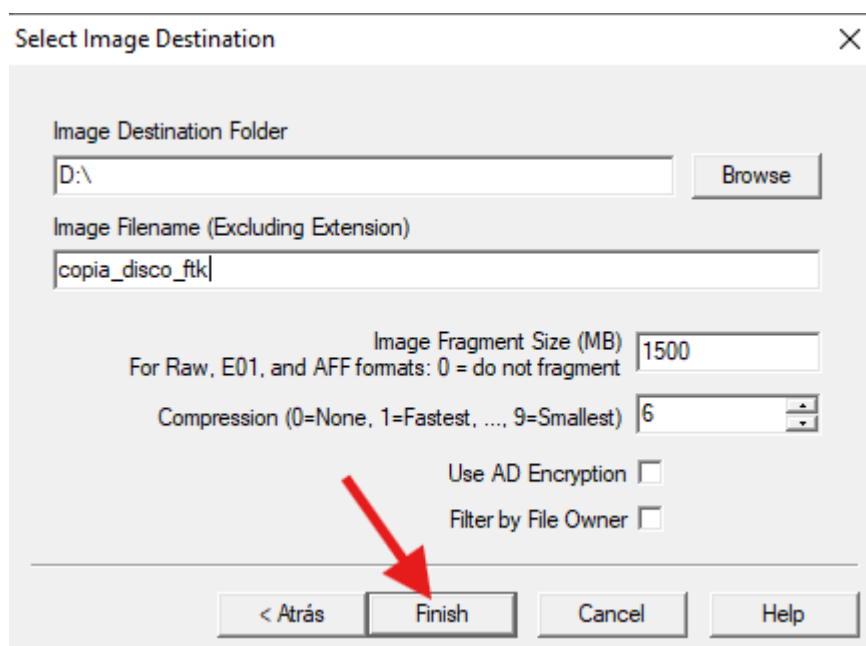
Clicamos en **Add**.



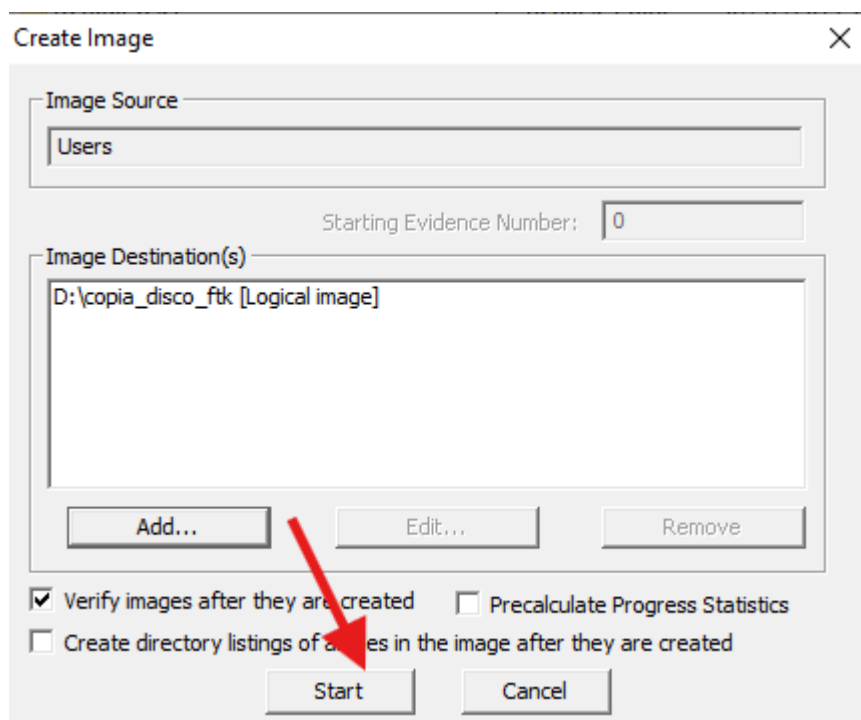
Ponemos la información sobre la evidencia.

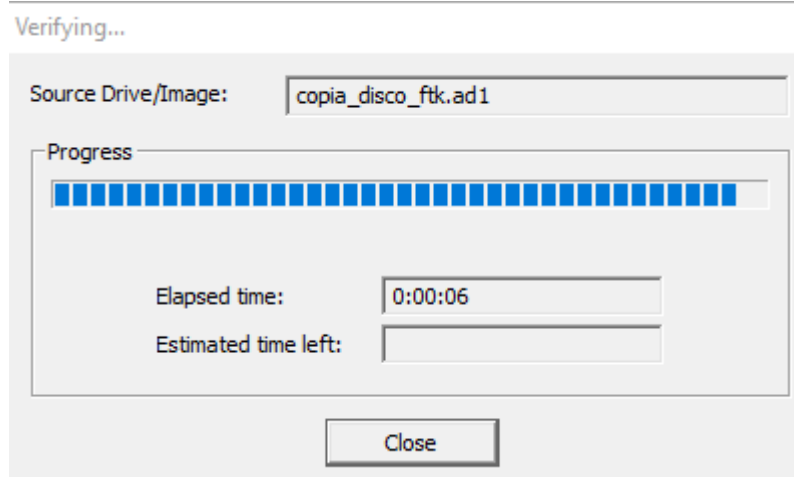
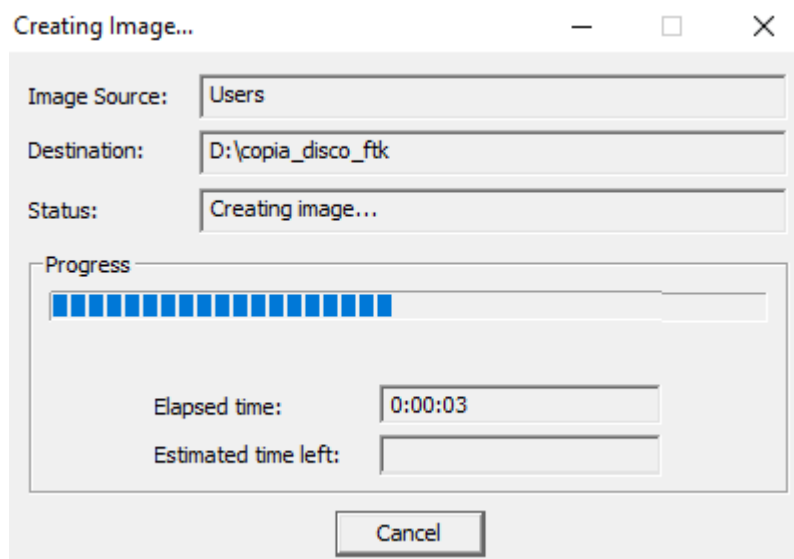


Y especificamos donde se va a guardar la evidencia y con qué nombre.

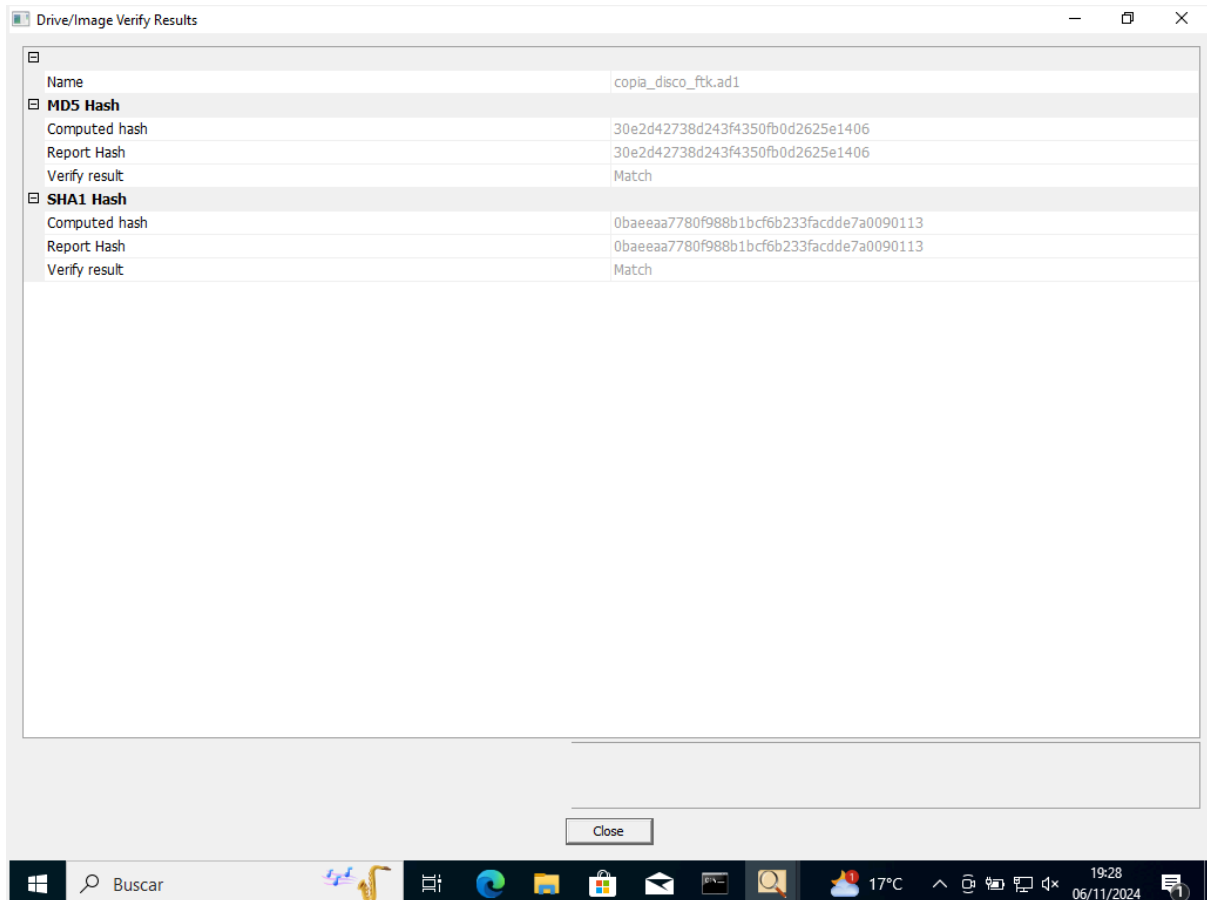


Una vez terminado, empezamos el clonado de la carpeta **Users**.

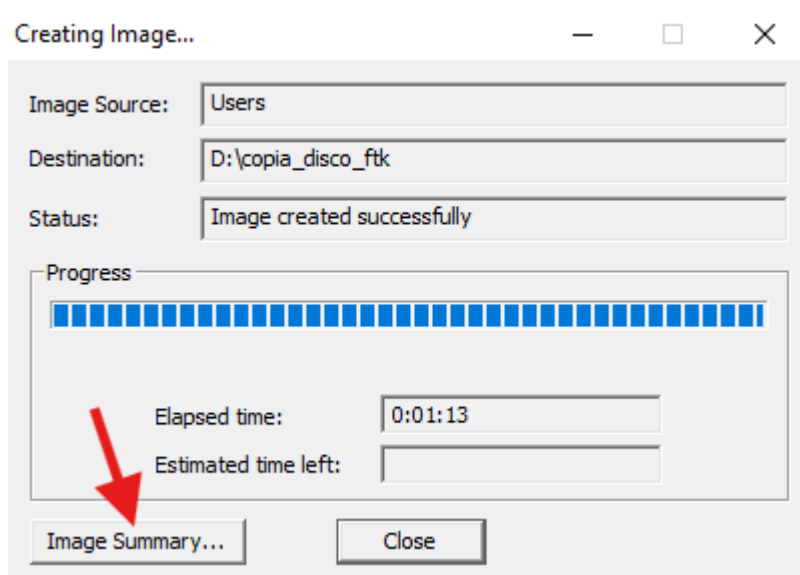


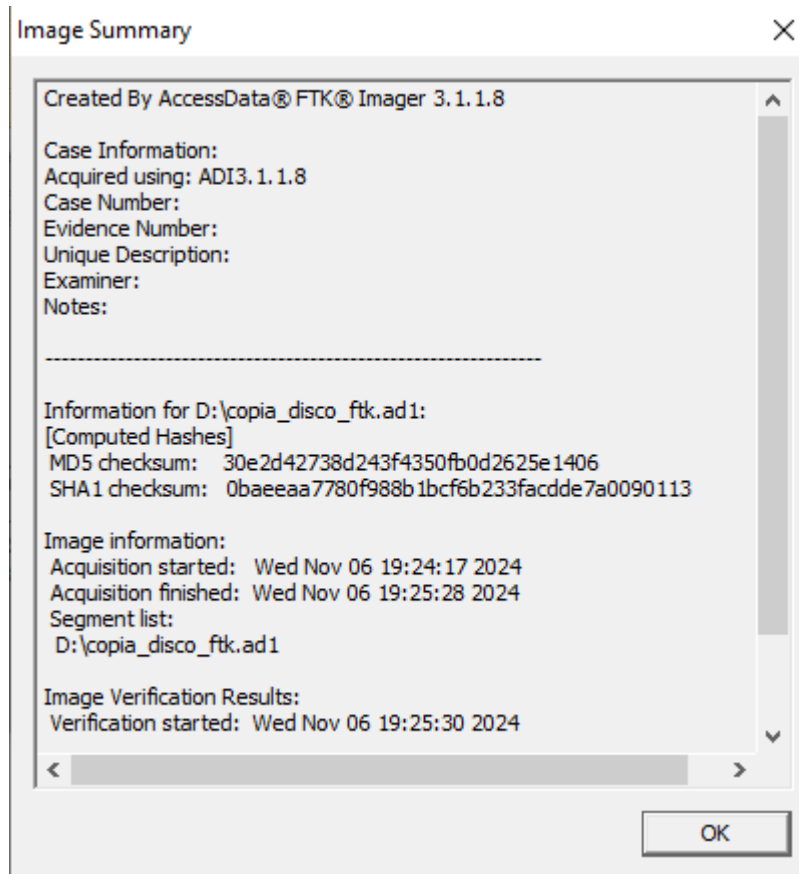


Nos generará unos hashes que nos indicarán que la evidencia obtenida, corresponde con la evidencia original.

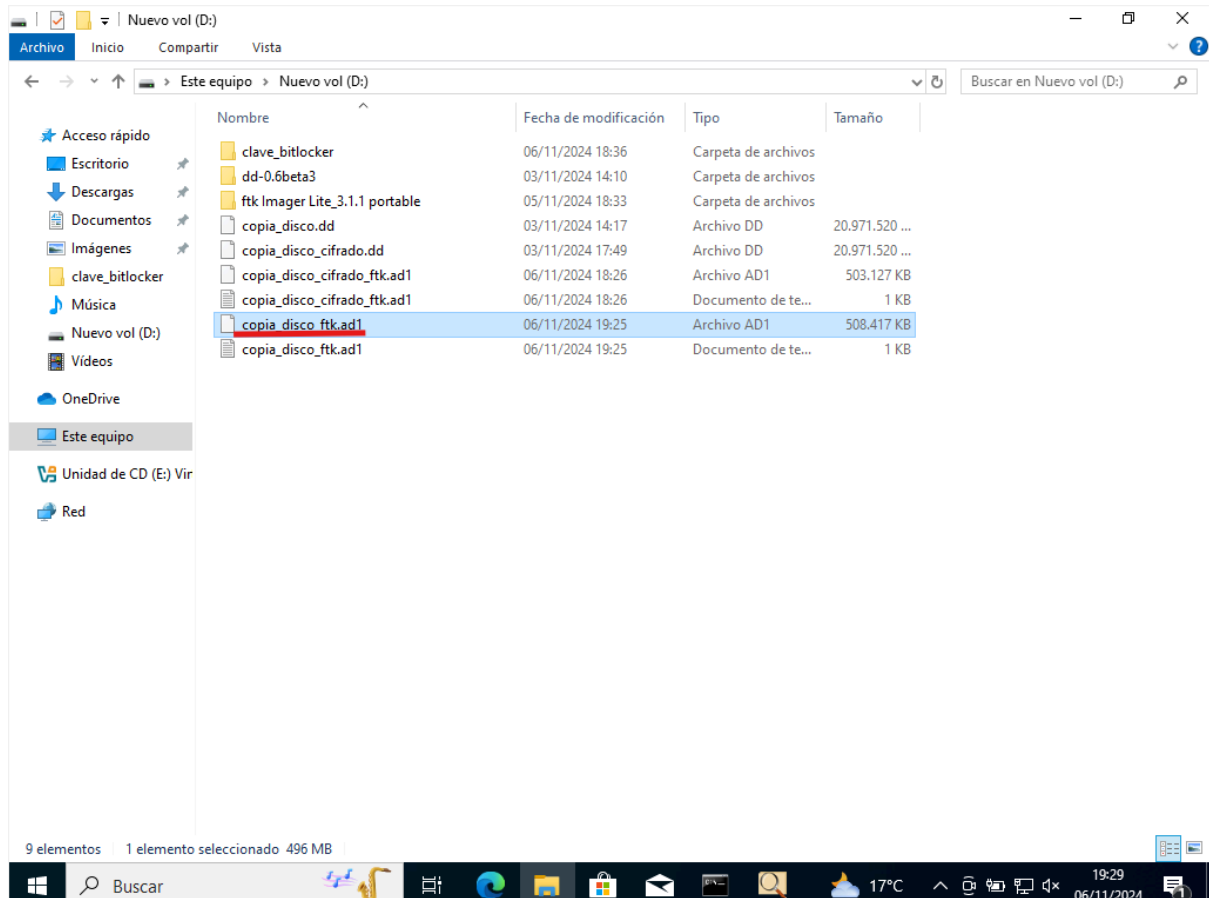


También podemos visualizar el sumario de la imagen.





Y por último comprobamos que se nos ha generado una imagen lógica en el disco duro externo.



También podemos generar nuestro propio hash para identificar la evidencia obtenida.

```
D:\>certutil -hashfile copia_disco_ftk.ad1 sha512
SHA512 hash de copia_disco_ftk.ad1:
2d401e5a96b824e32b06272cec44186845953dd81ff5112391083060be64b0ee5fce03aef51aab80af80c37a179c2fbcd895a4c8508b5cbc0fc9b3dc
cb7f176e
CertUtil: -hashfile comando completado correctamente.
D:\>
```

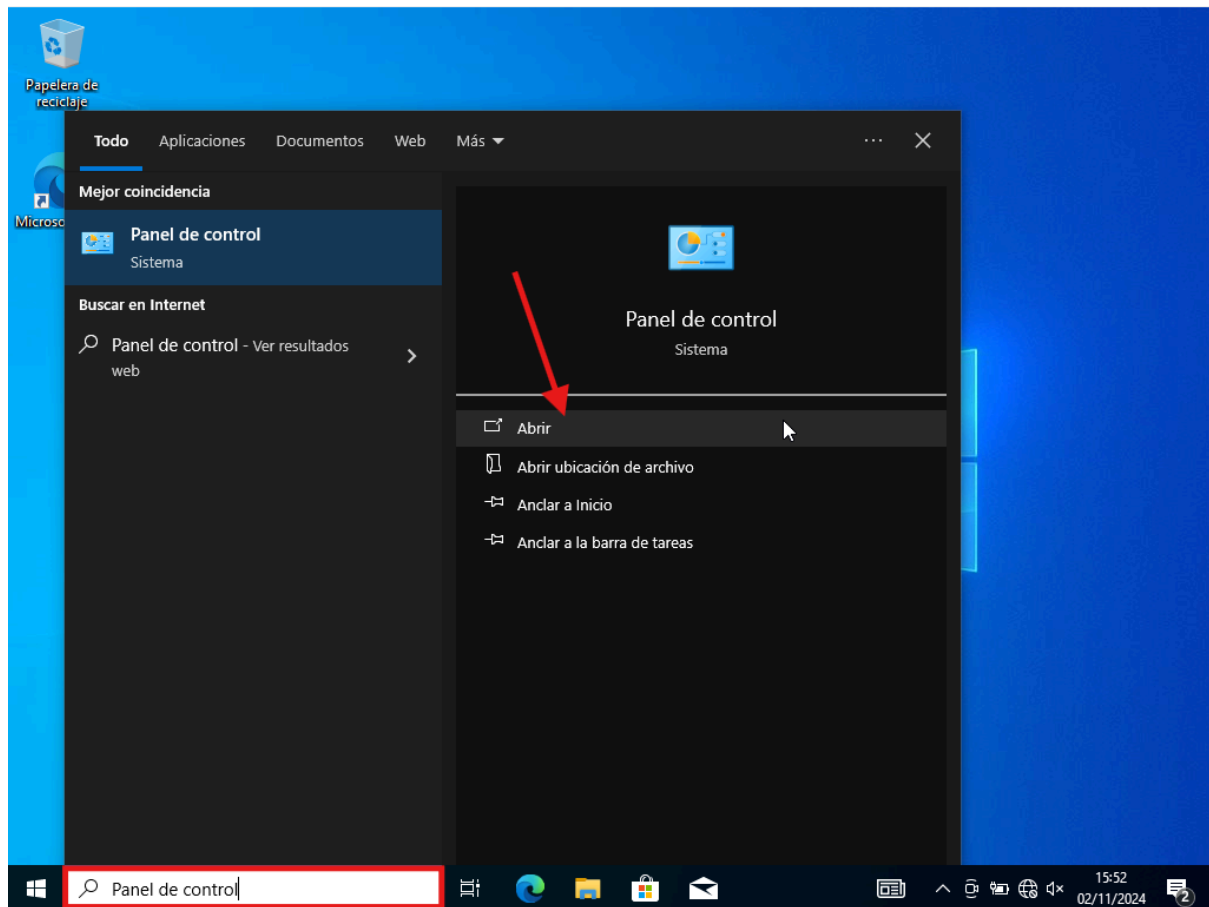
SHA512 hash de copia_disco_ftk.ad1:

2d401e5a96b824e32b06272cec44186845953dd81ff5112391083060be64b0ee5fce03aef51aab80af80c37a179c2fbcd895a4c8508b5cbc0fc9b3dccb7f176e

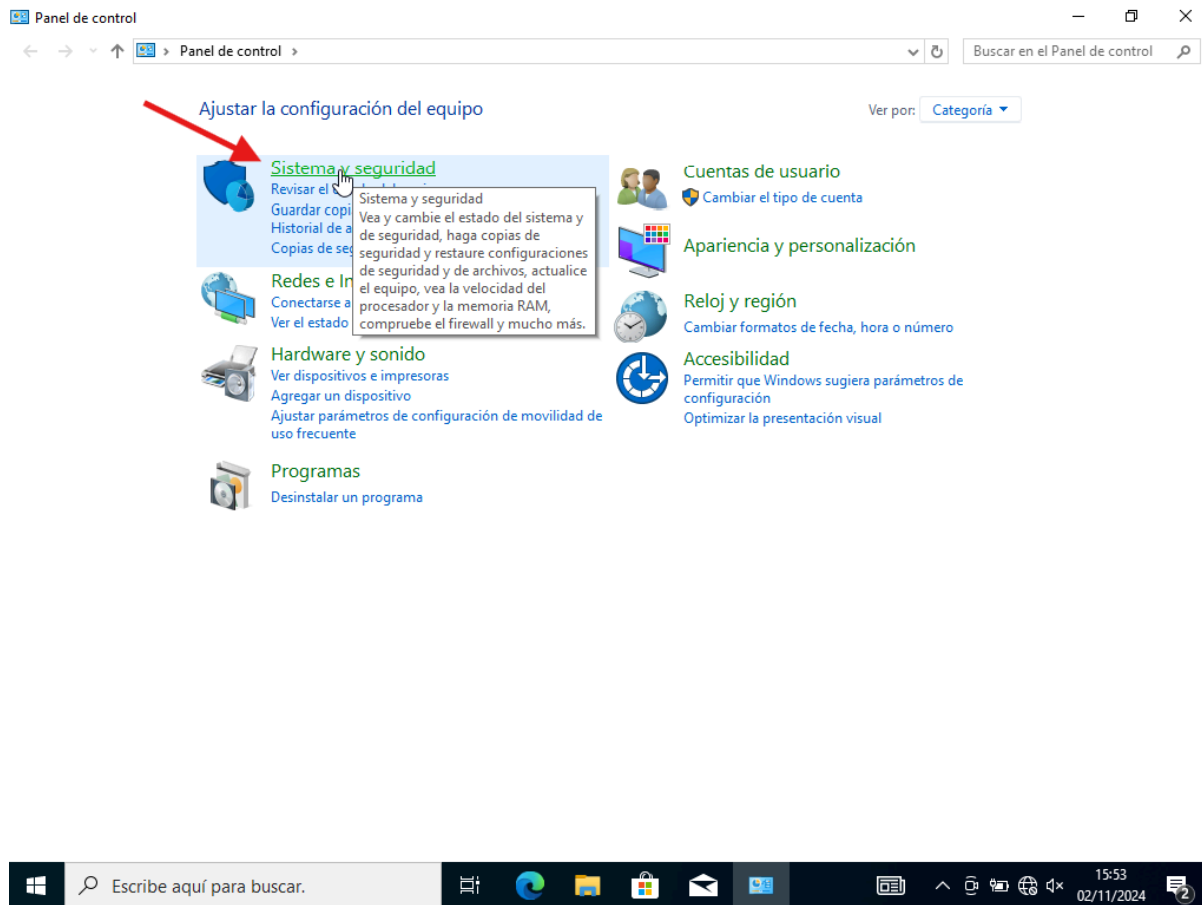
CertUtil: -hashfile comando completado correctamente.

¿Cómo cifrar un disco con BitLocker?:

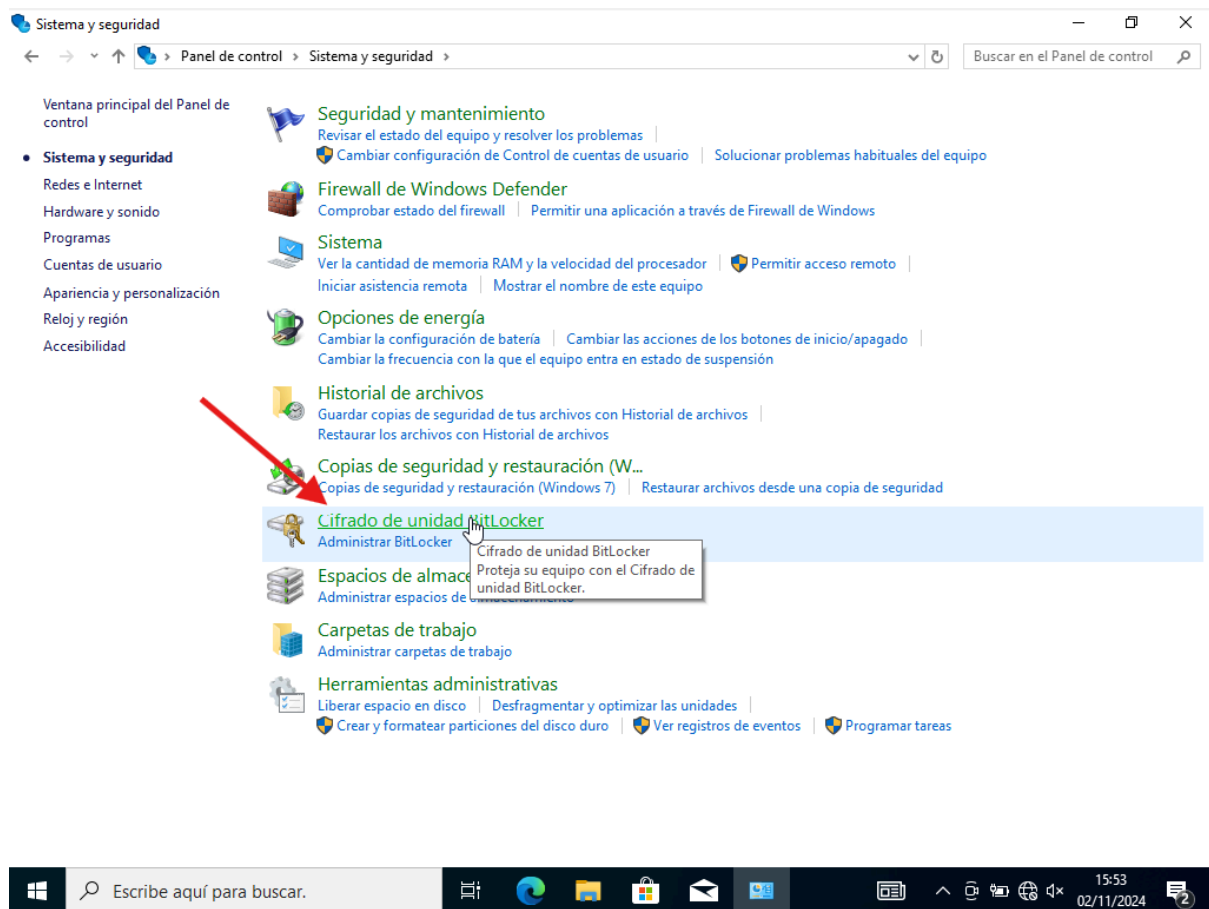
Abrimos el Panel de Control.



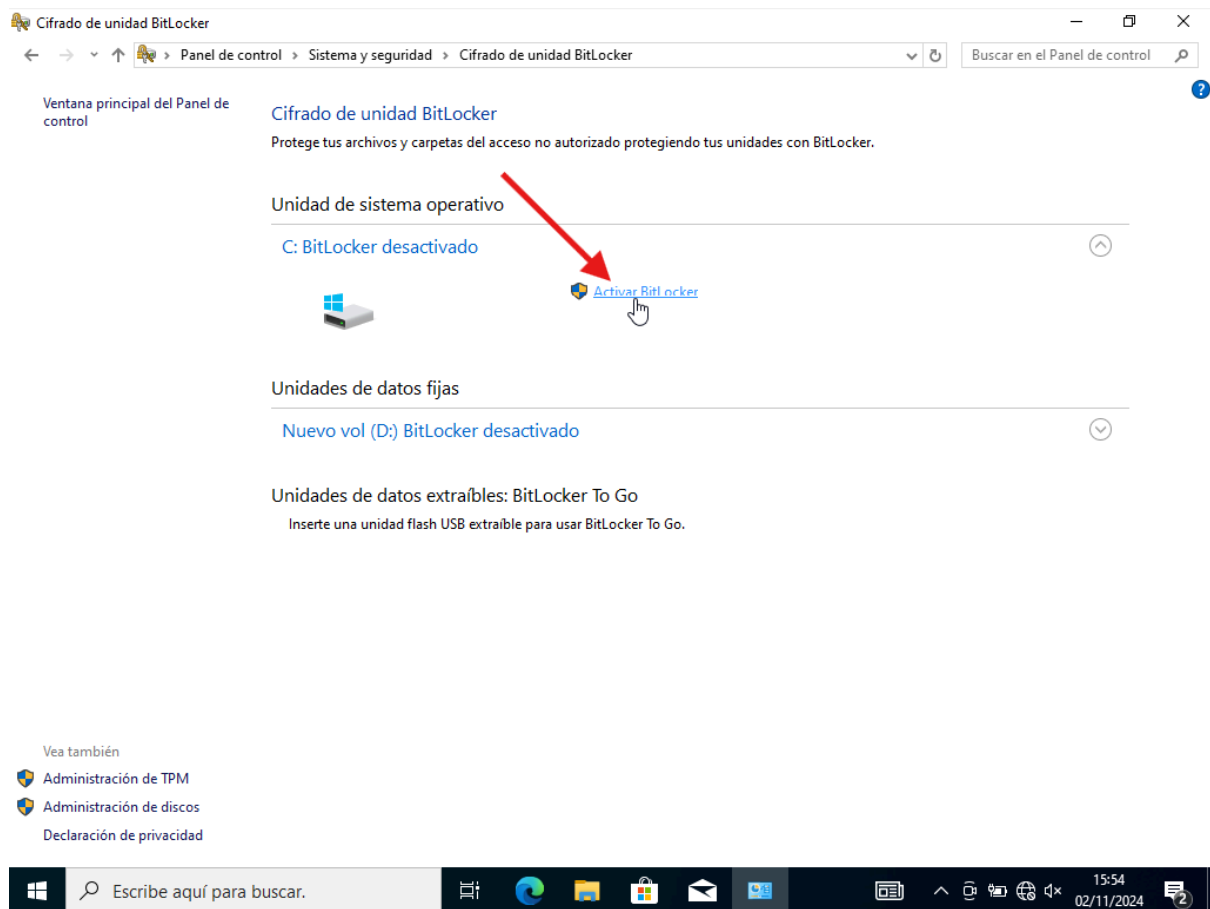
Entramos en **Sistema y seguridad**.



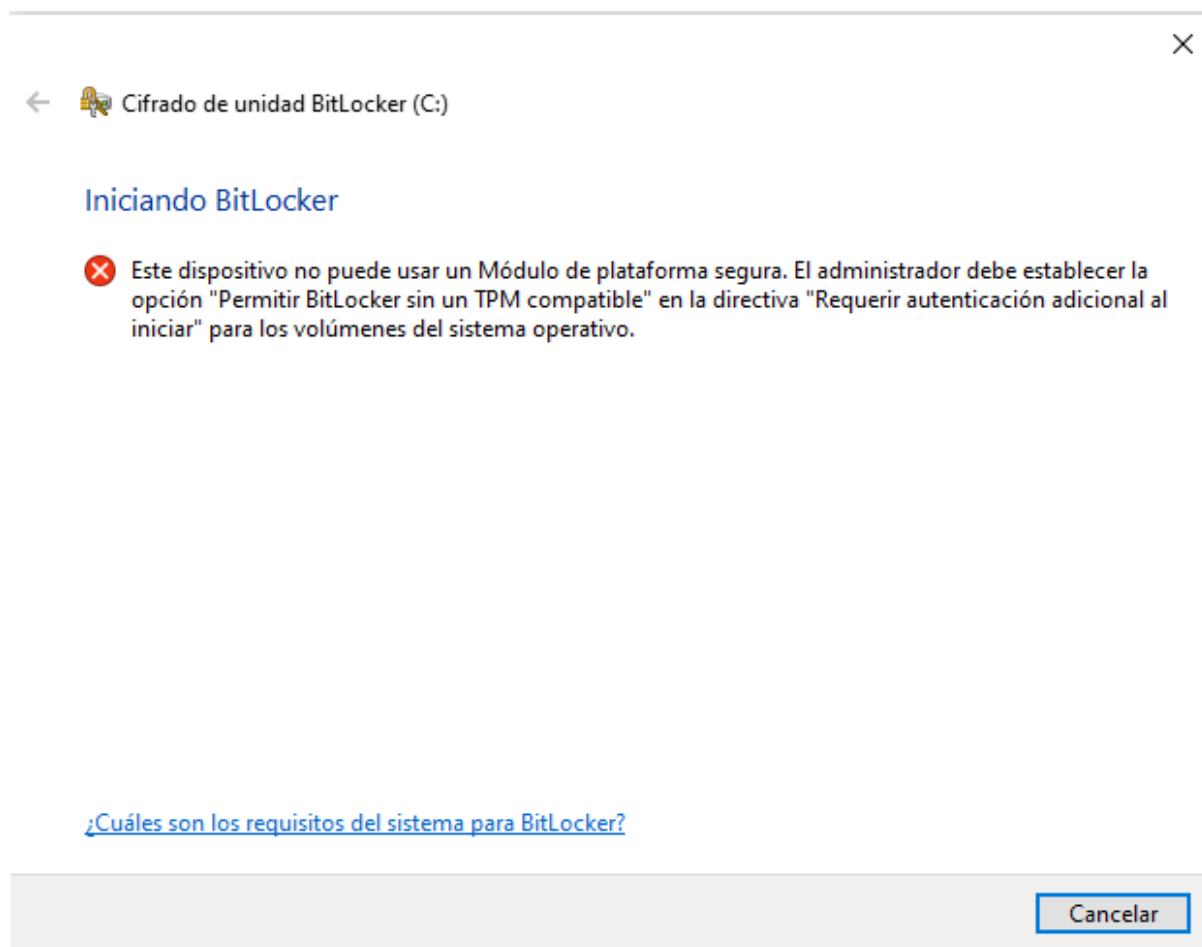
Clicamos en **Cifrado de unidad BitLocker**.



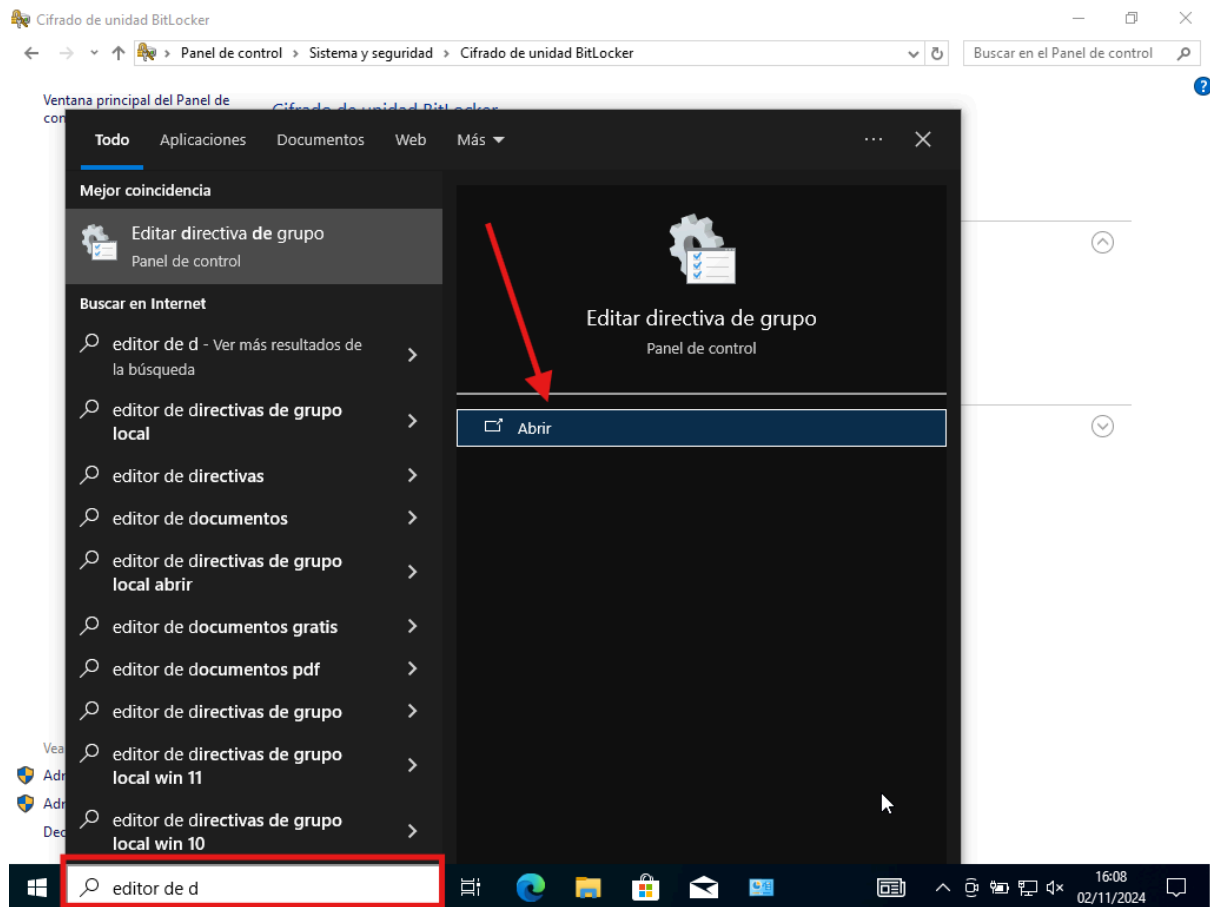
Clicamos en **Activar BitLocker**.



Y nos dirá lo siguiente.



Así que nos iremos a **Editar directiva de grupo**.



Y buscaremos la directiva **Requerir autenticación adicional al iniciar**.

La cual se encuentra en esta ruta: **Configuración del equipo \ Plantillas administrativas \ Componentes de Windows \ Cifrado de unidad BitLocker \ Unidades del sistema operativo**.

The screenshot shows the 'Editor de directivas de grupo local' (Local Group Policy Editor) window. The left sidebar shows the navigation tree with 'Unidades del sistema operativo' (Operating System Drives) selected under 'Componentes de Windows' (Windows Components). The main pane displays the 'Requerir autenticación adicional al iniciar' (Require additional authentication at startup) policy. A red arrow points to this policy in the list. The policy is currently set to 'No configurada' (Not configured).

Configuración	Estado	Comentari
Permitir desbloqueo de la red al iniciar	No configurada	No
Permitir Arranque seguro para comprobación de integridad	No configurada	No
Requerir autenticación adicional al iniciar	No configurada	No
Requerir autenticación adicional al iniciar (Windows Server 2...	No configurada	No
No permitir que usuarios estándar cambien el PIN o la contr...	No configurada	No
Permite que los dispositivos compatibles con InstantGo o H...	No configurada	No
Habilitar el uso de autenticación BitLocker que requiera entr...	No configurada	No
Permitir los PIN mejorados para el inicio	No configurada	No
Configurar longitud mínima de PIN para el inicio	No configurada	No
Configurar el uso de cifrado basado en hardware para unida...	No configurada	No
Aplicar tipo de cifrado de unidad en unidades de sistema op...	No configurada	No
Configurar el uso de contraseñas para unidades de sistema ...	No configurada	No
Elegir cómo se pueden recuperar unidades del sistema oper...	No configurada	No
Configurar el perfil de validación de plataforma del TPM par...	No configurada	No
Configurar el perfil de validación de plataforma de TPM (Wi...	No configurada	No
Configurar el perfil de validación de plataforma del TPM par...	No configurada	No
Configurar la dirección URL y el mensaje de recuperación pr...	No configurada	No
Restablecer datos de validación de plataforma después de la...	No configurada	No
Usar perfil de comprobación de datos de configuración de a...	No configurada	No

Una vez dentro, habilitaremos la directiva, y en caso de no estar seleccionada, seleccionaremos la opción **Permitir BitLocker sin un TPM compatible**.

Requerir autenticación adicional al iniciar

Valor anterior Valor siguiente

☐ No configurada Comentario:

☒ **Habilitada**

☐ Deshabilitada

Compatible con: Al menos Windows Server 2008 R2 o Windows 7

Opciones:

☒ **Permitir BitLocker sin un TPM compatible**
(requiere contraseña o clave de inicio en una unidad flash USB)

Opciones para equipos con un TPM:

Configurar inicio del TPM:
Permitir TPM

Configurar PIN de inicio del TPM:
Permitir PIN de inicio con TPM

Configurar clave de inicio del TPM:
Permitir clave de inicio con TPM

Configurar la clave de inicio y el PIN del TPM:
Permitir clave y PIN de inicio con TPM

Ayuda:

Esta configuración de directiva te permite configurar si BitLocker requiere autenticación adicional cada vez que se inicia el equipo y si se usa BitLocker con un Módulo de plataforma segura (TPM). Esta configuración de directiva se aplica al activar BitLocker.

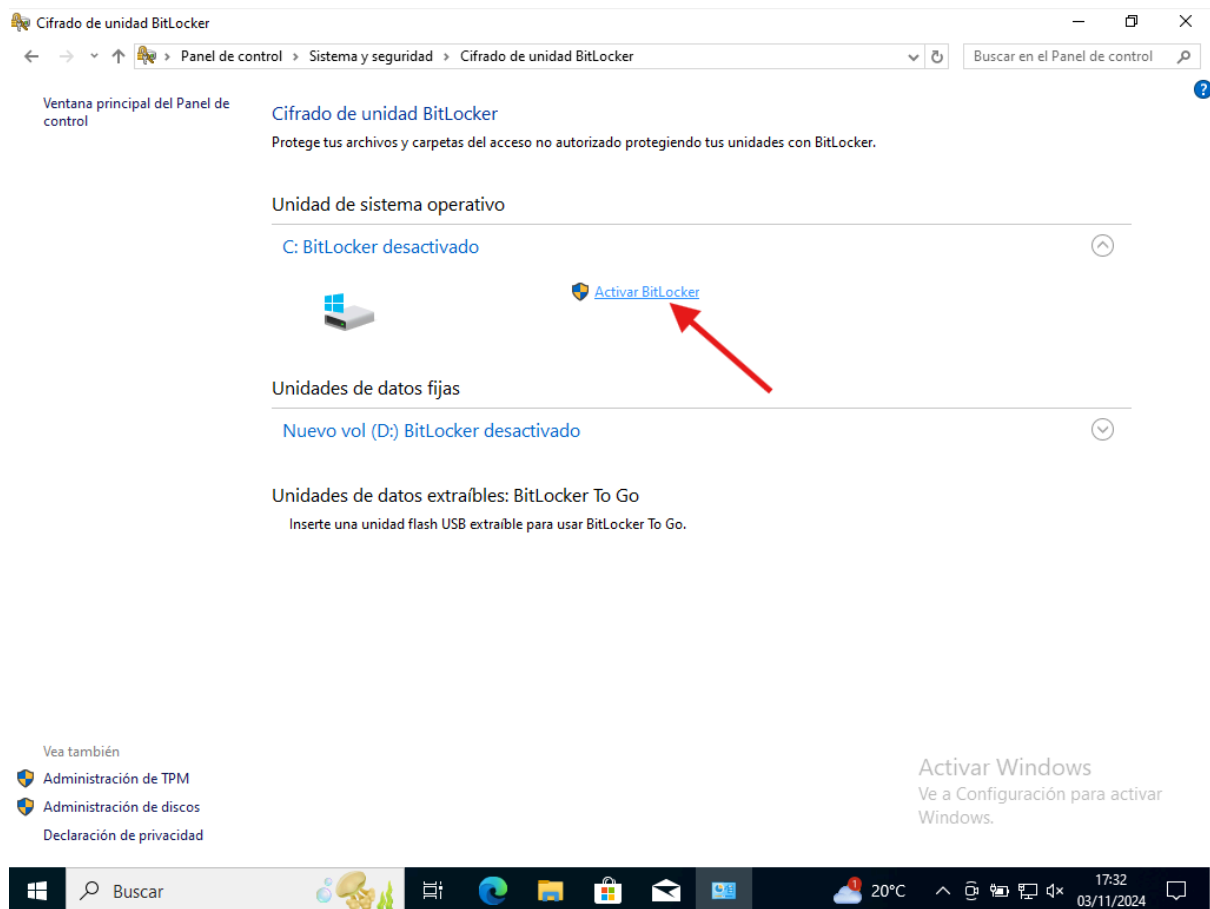
Nota: al iniciar, solo se puede solicitar una de las opciones de autenticación adicional; de lo contrario, se produce un error de directiva.

Si deseas usar BitLocker en un equipo sin un TPM, activa la casilla "Permitir BitLocker sin un TPM compatible". En este modo, se requiere o bien contraseña o una unidad USB para iniciar. Cuando se usa una clave de inicio, la información de clave usada para cifrar la unidad se almacena en la unidad USB, creando una clave USB. Cuando se inserta la clave USB se autentica el acceso a la unidad, que queda accesible. Si la clave USB no está accesible o se pierde, o si olvidas la contraseña, será necesario usar una de las opciones de recuperación de BitLocker para tener acceso a la unidad.

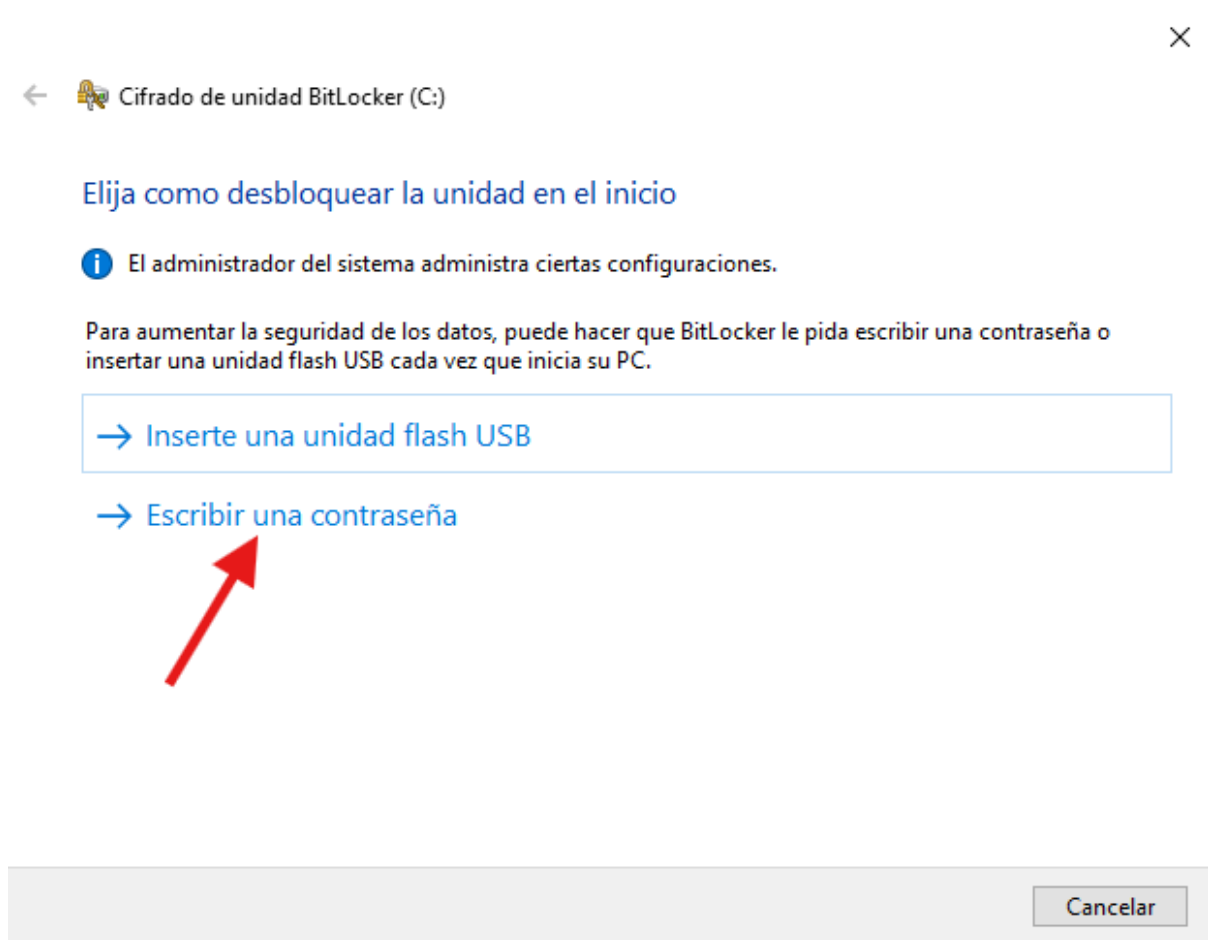
En un equipo con un TPM compatible, se pueden usar cualquier

Aceptar Cancelar Aplicar

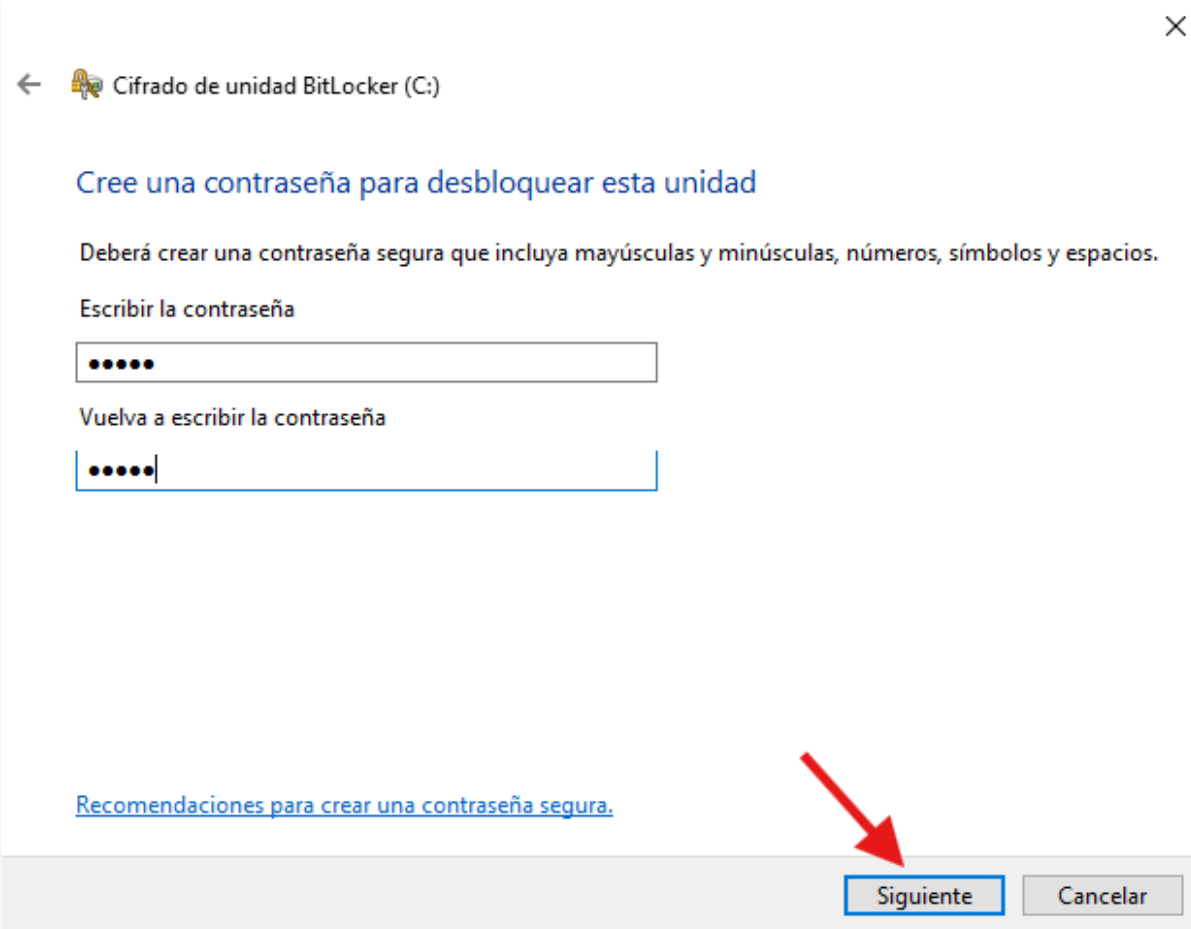
Ya esta vez sí, clicamos en **Activar BitLocker**.




Apareciendo la siguiente ventana, donde seleccionaremos la opción **Escribir una contraseña**.



Escribimos la contraseña.



←  Cifrado de unidad BitLocker (C:)

×

Cree una contraseña para desbloquear esta unidad

Deberá crear una contraseña segura que incluya mayúsculas y minúsculas, números, símbolos y espacios.

Escribir la contraseña

•••••

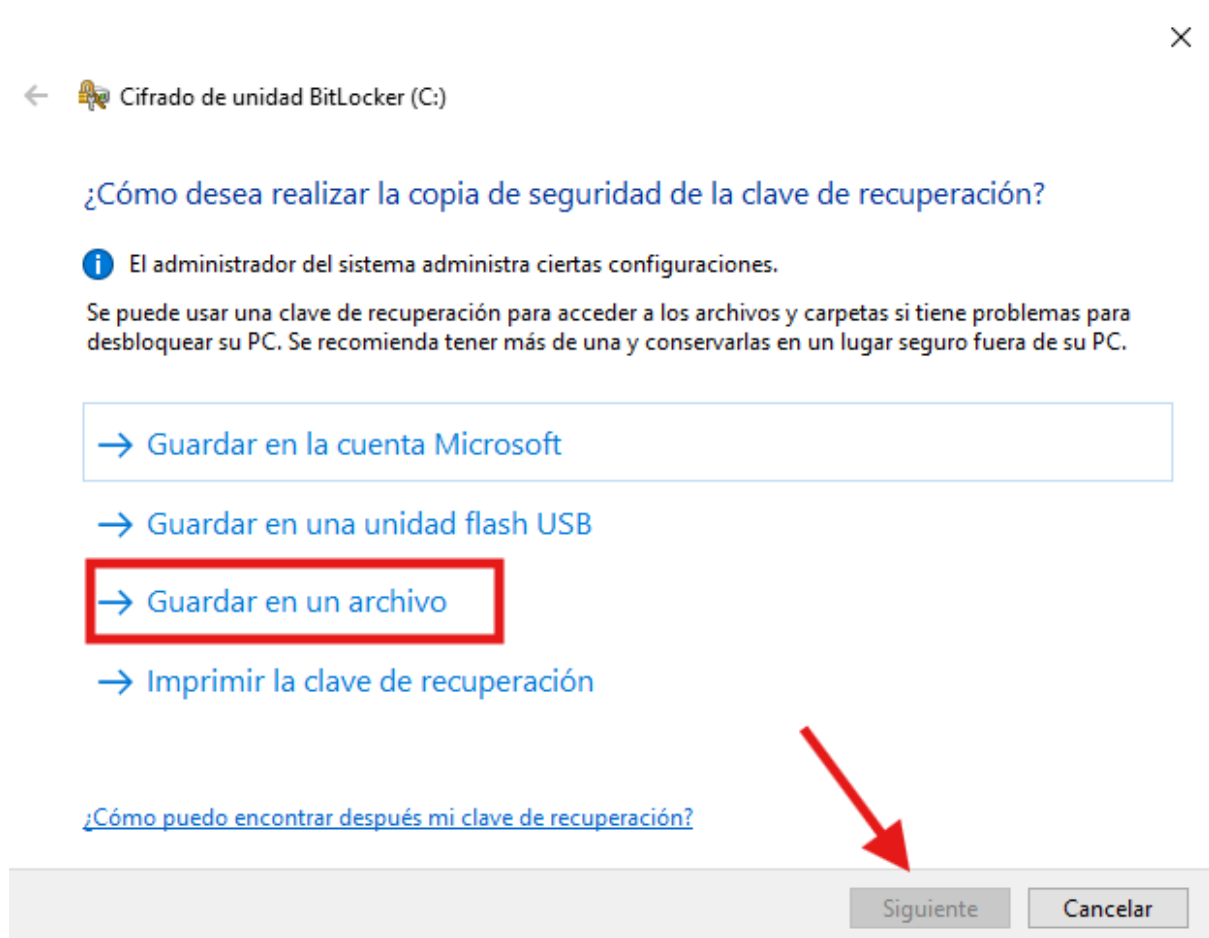
Vuelva a escribir la contraseña

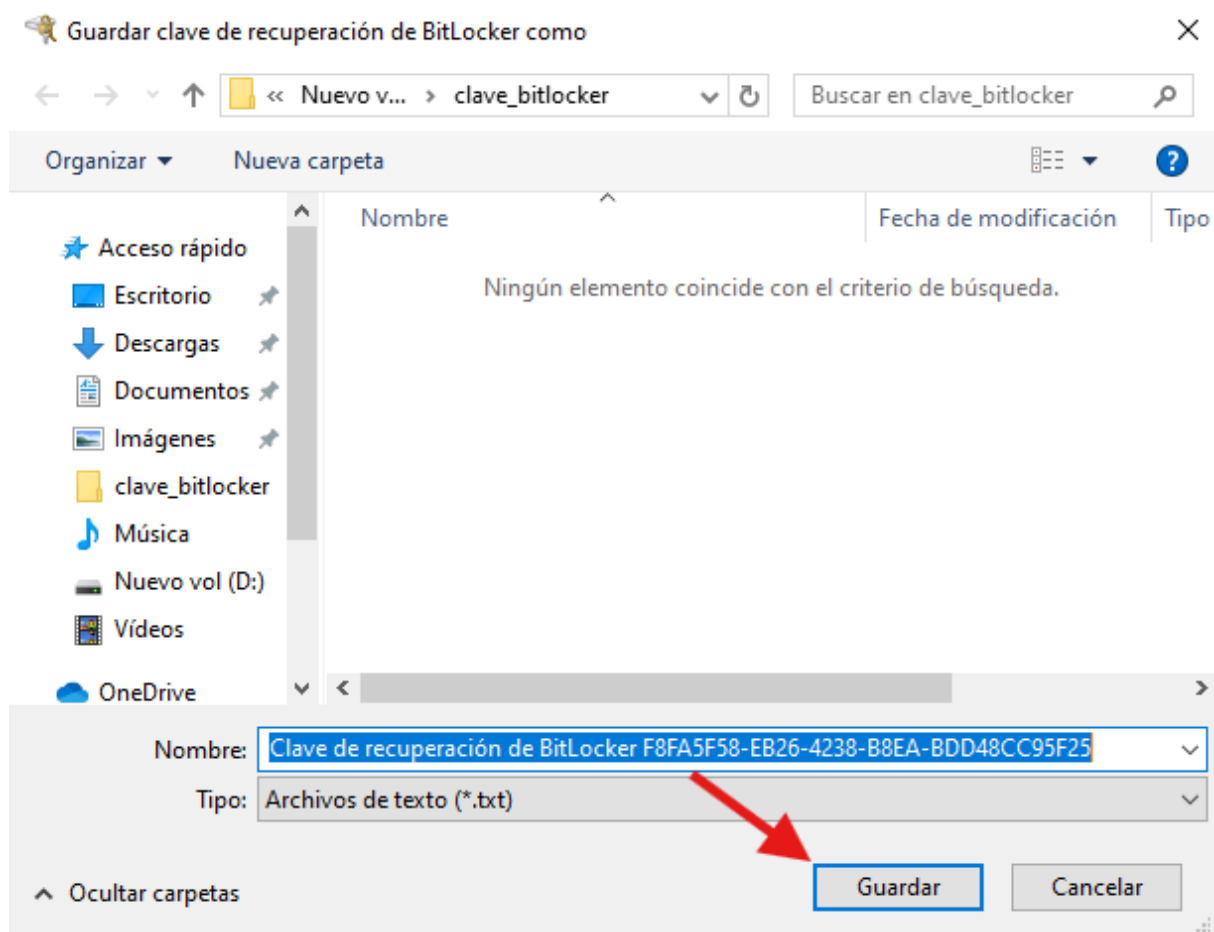
•••••

[Recomendaciones para crear una contraseña segura.](#)

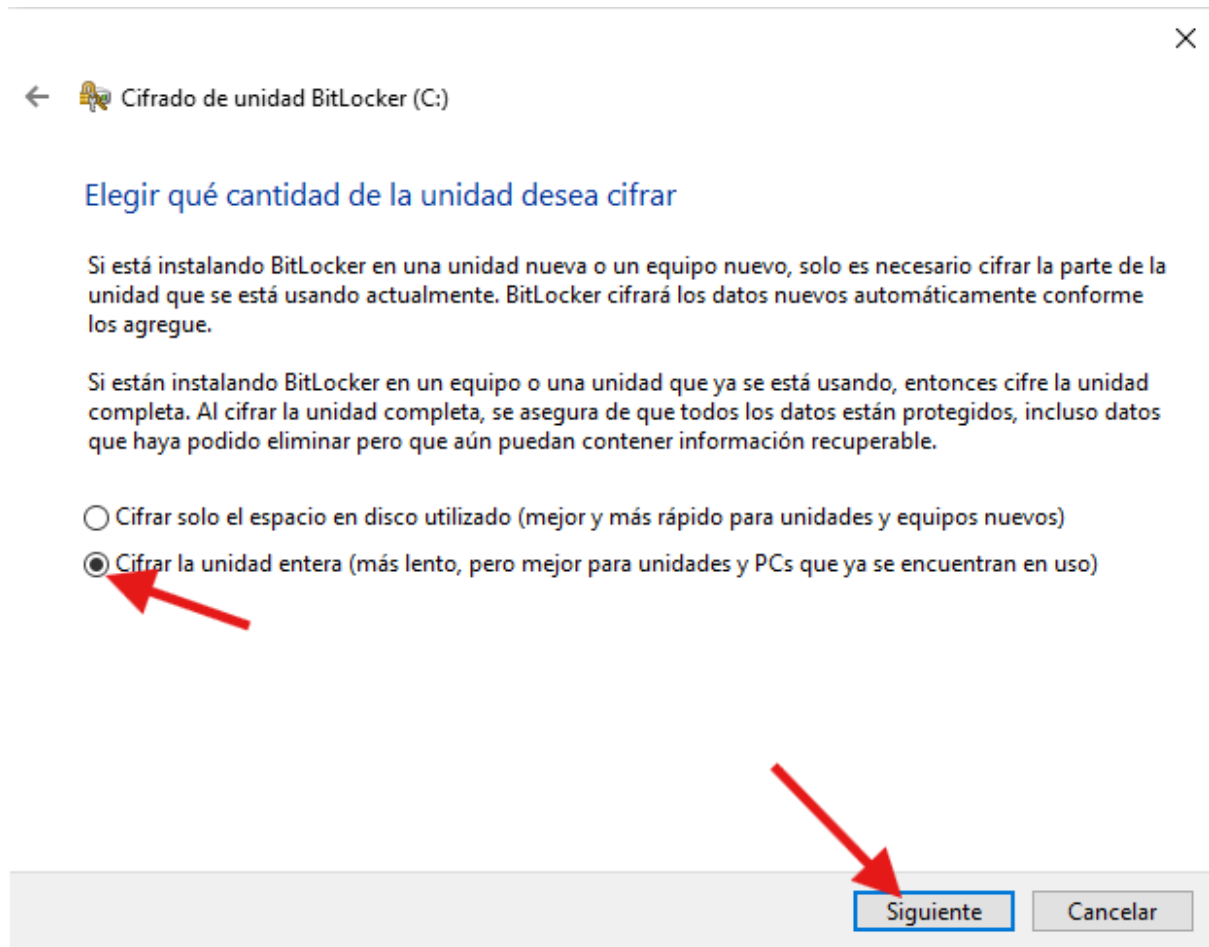
Siguiete Cancelar

Y la guardamos en un archivo donde podamos visualizarla en caso de que se nos olvide.

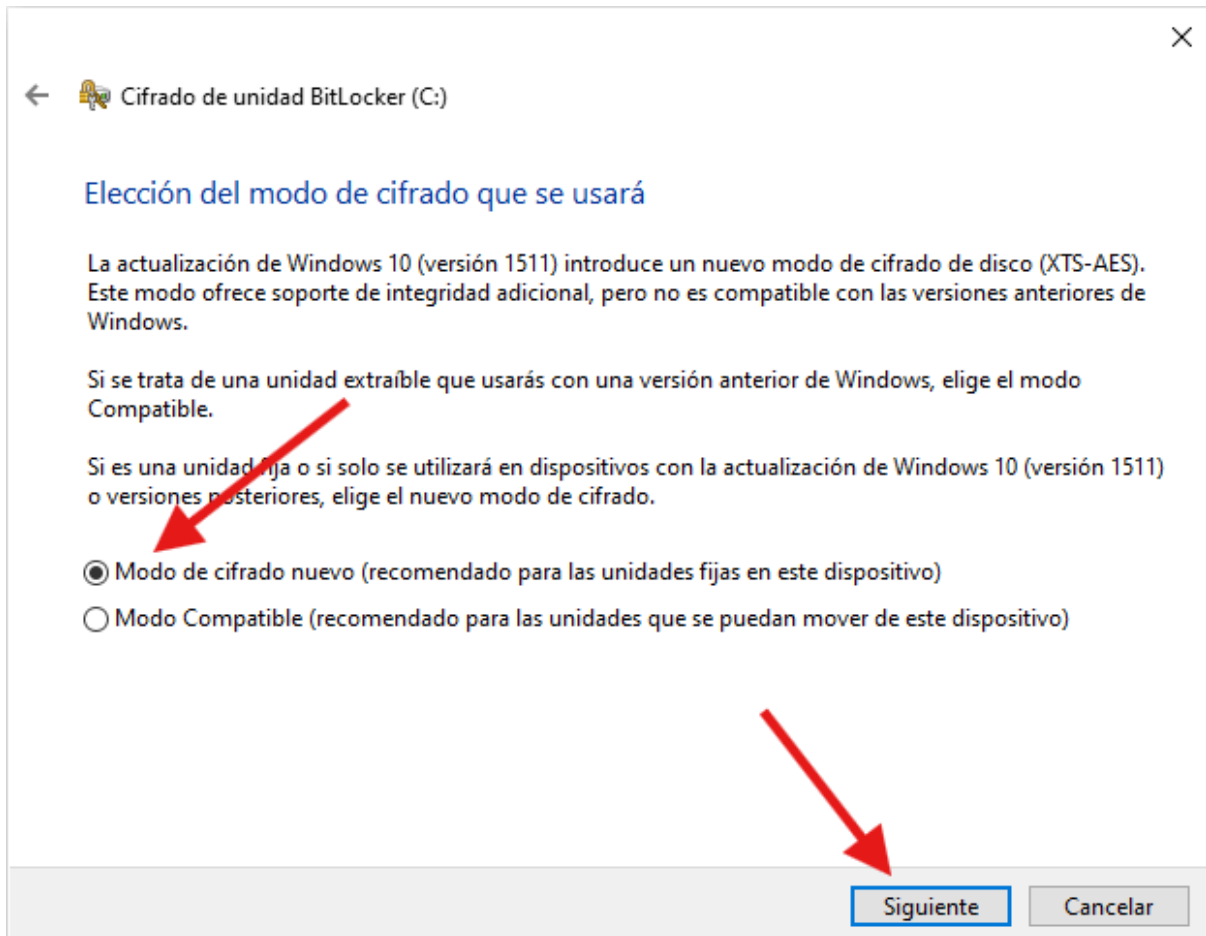





Luego escogemos si queremos cifrar la unidad entera, o solo el espacio ocupado. En mi caso he seleccionado **Cifrar la unidad entera**.



A continuación se nos pregunta, si queremos el **Modo de cifrado nuevo** o el **Modo Compatible**. Y ya que el disco que vamos a cifrar es una unidad fija en el dispositivo, seleccionamos el **Modo de cifrado nuevo**.



Y por último, clicamos en **Continuar**.

←  Cifrado de unidad BitLocker (C:)

¿Está listo para cifrar esta unidad?

El cifrado podría tardar varios minutos, según el tamaño de la unidad.


Puede continuar trabajando mientras se cifra la unidad, aunque es posible que se ralentice el funcionamiento del equipo.

☒ Ejecutar la comprobación del sistema de BitLocker

La comprobación del sistema confirmará que BitLocker pueda leer correctamente las claves de recuperación y de cifrado antes de que se cifre la unidad.


BitLocker reiniciará el equipo antes de iniciar el cifrado.

Nota: esta comprobación puede tardar un tiempo, pero se recomienda asegurarse de que el método de desbloqueo seleccionado funciona sin que sea necesario usar la clave de recuperación.

 Continuar

Cancelar


Y nos dirá que es necesario reiniciar el equipo.

 Cifrado de unidad BitLocker

×

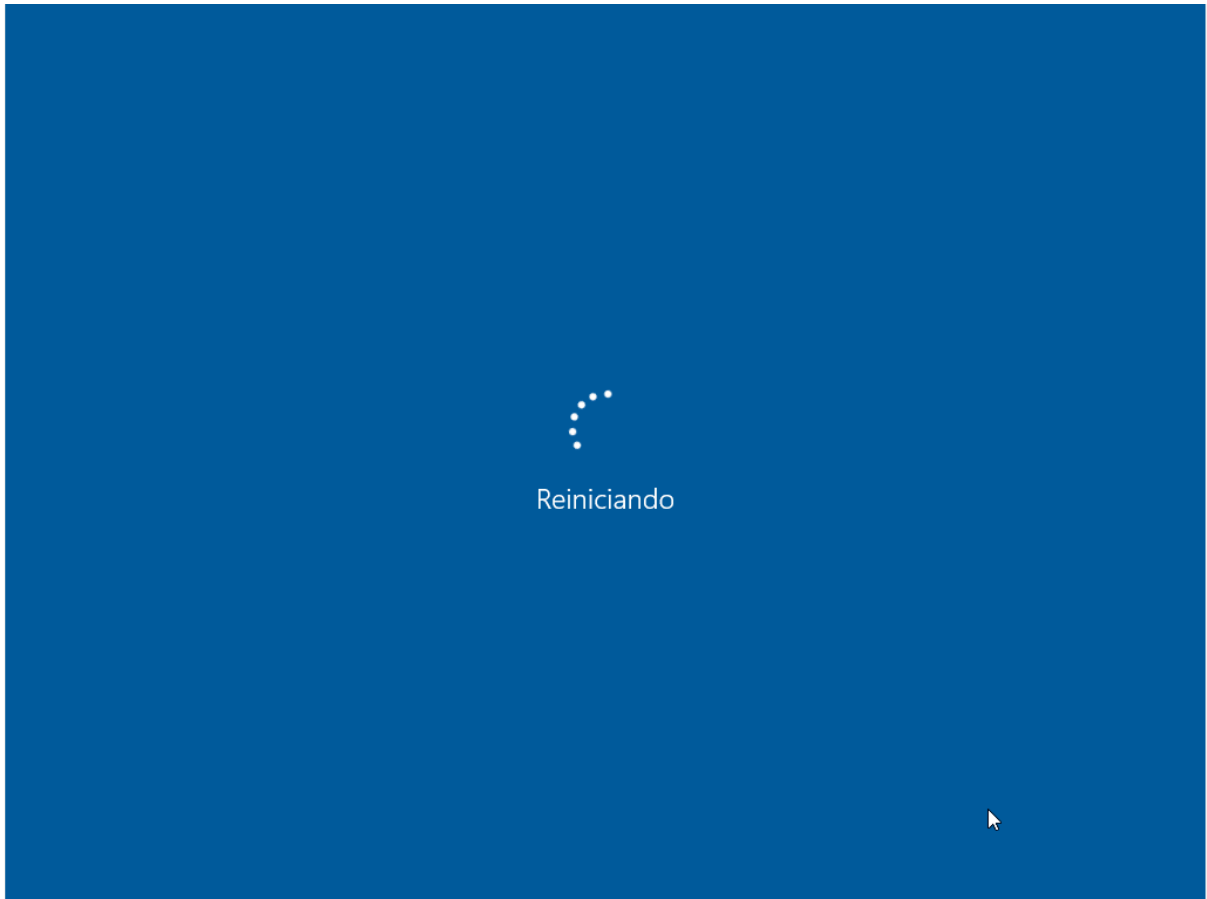


Debe reiniciarse el equipo

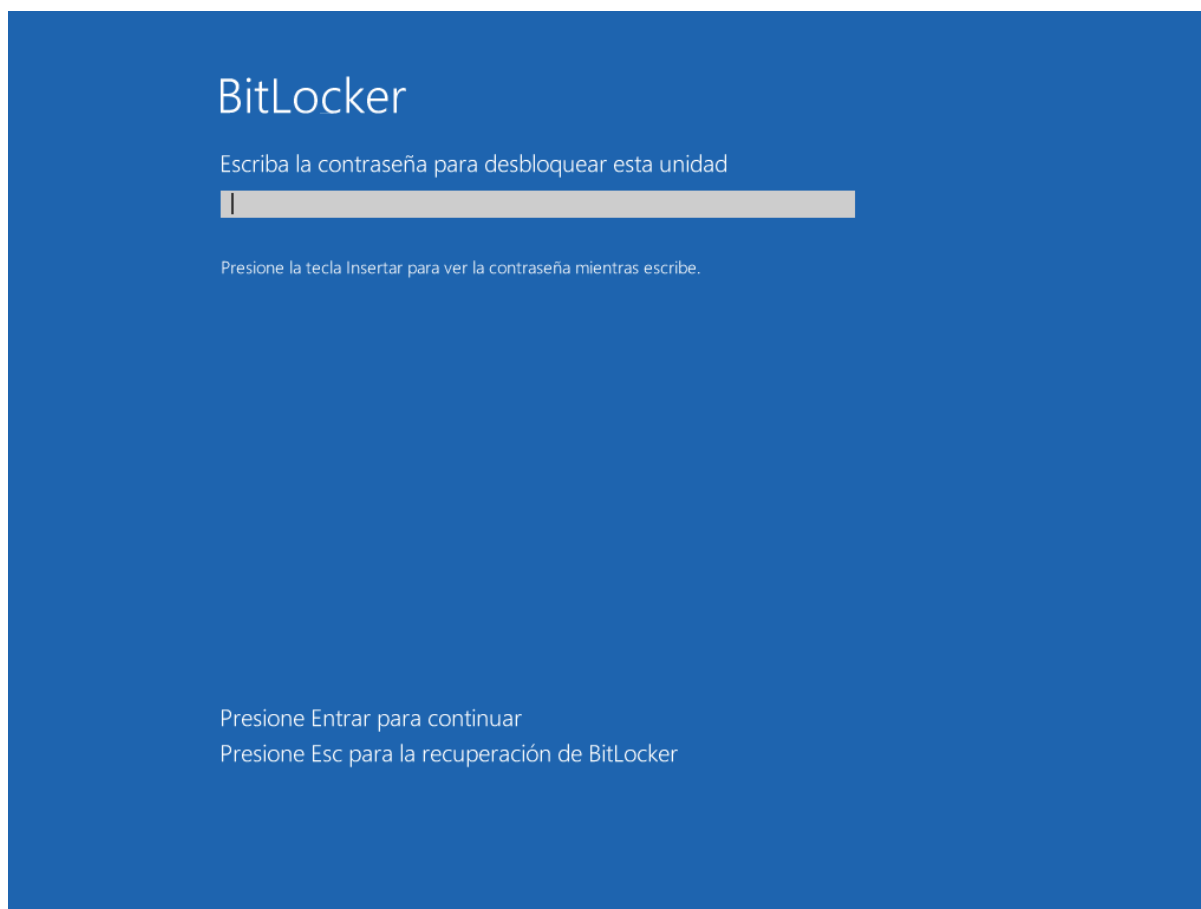
 Reiniciar ahora

Reiniciar más tarde

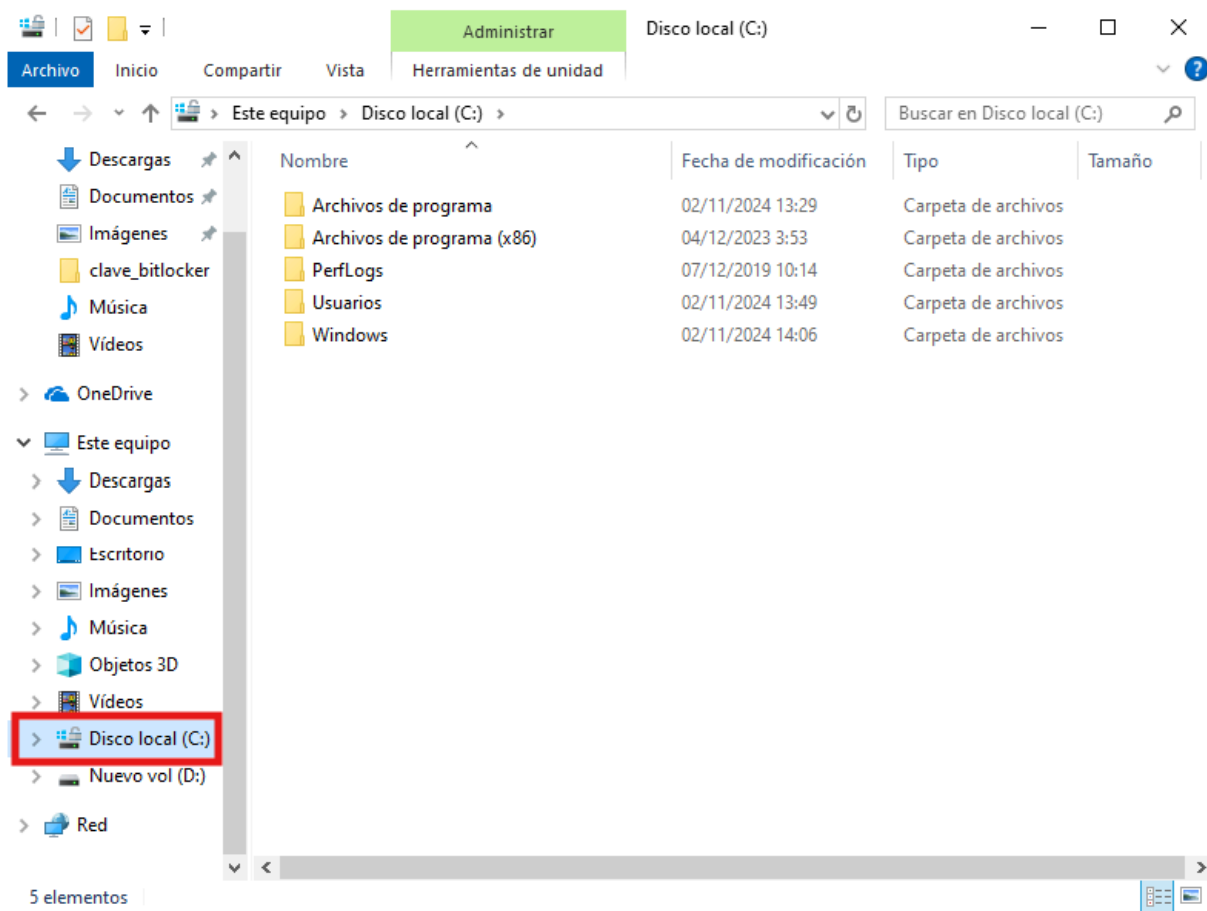
[Administrar BitLocker](#)



Una vez finalice el reinicio, se nos pedirá la contraseña recién creada.

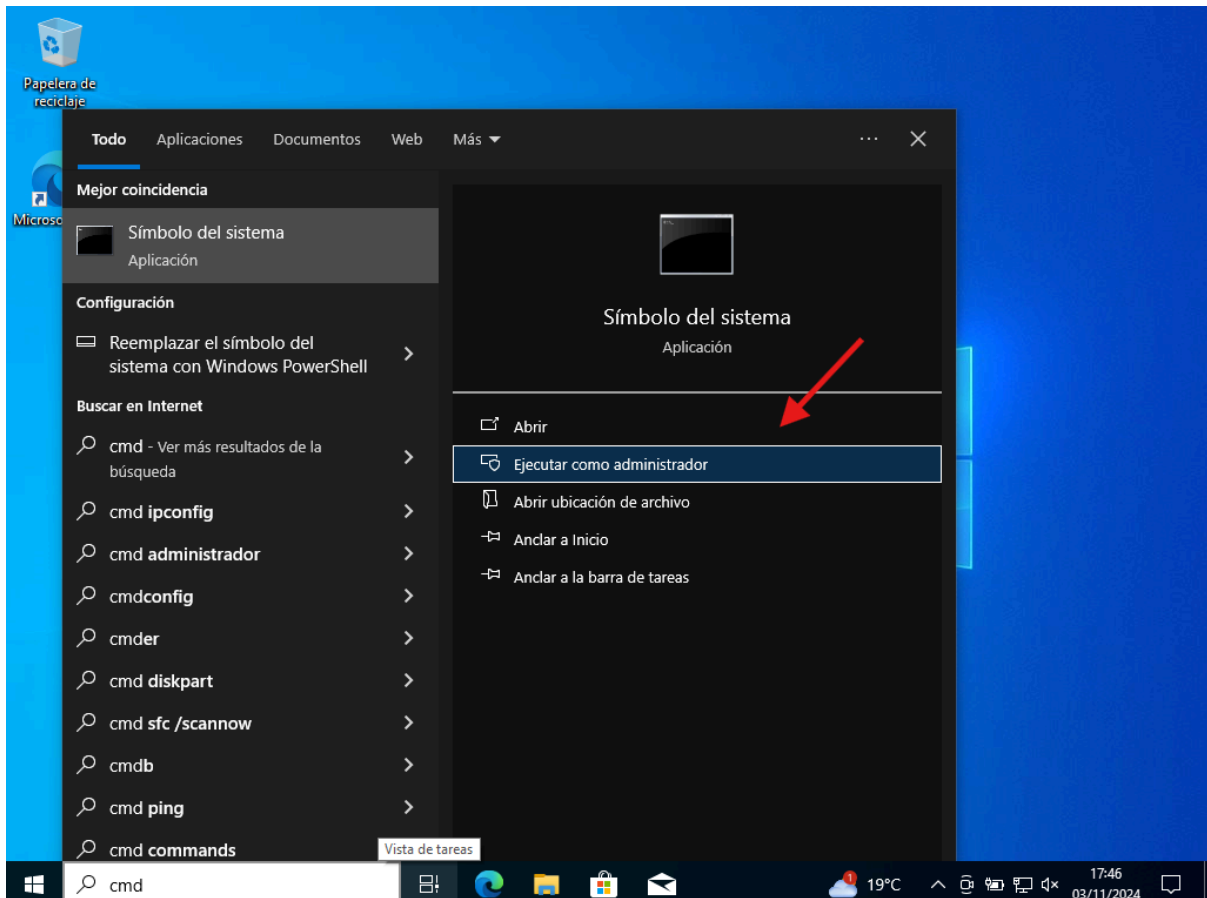


También nos aparecerá un candado en el disco cifrado, en este caso en el disco C:\.



dd (Disco cifrado):

Abrimos nuevamente el cmd como Administradores.



Y escribimos el siguiente comando:

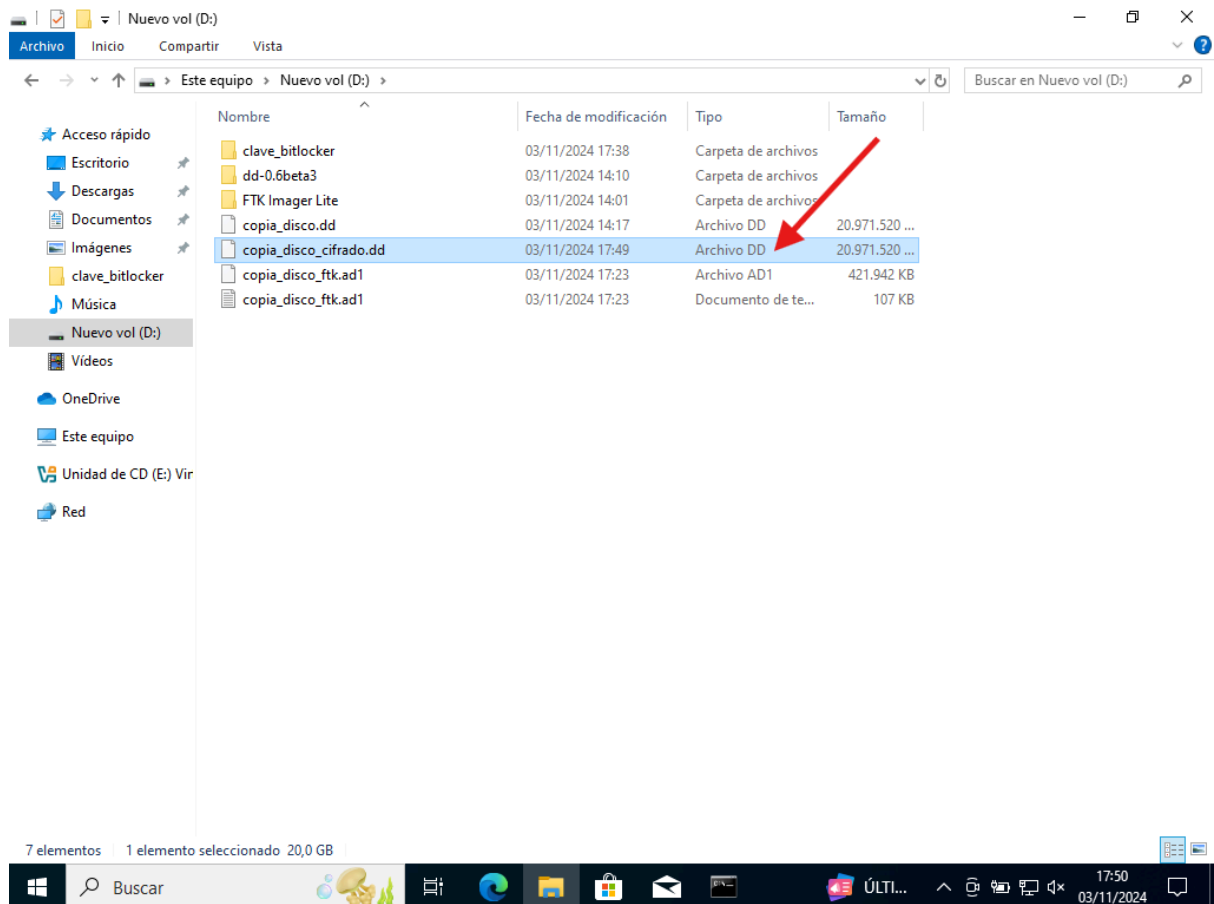
dd.exe if=\\.\PHYSICALDRIVE0 of=D:\copia_disco_cifrado.dd bs=4M --progress

C:\> Administrador: Símbolo del sistema - dd.exe if=\\.\PHYSICALDRIVE0 of=D:\copia_disco_cifrado.dd bs=4M --progress

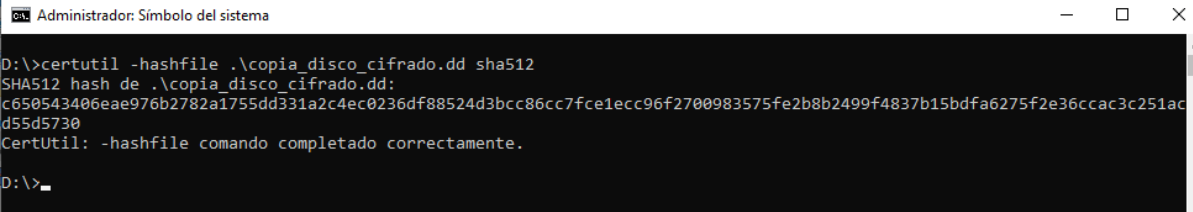
```
D:\dd-0.6beta3>dd.exe if=\\.\PHYSICALDRIVE0 of=D:\copia_disco_cifrado.dd bs=4M --progress
rawwrite dd for windows version 0.6beta3.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by terms of the GPL Version 2.

564M
```

Y comprobamos que se ha generado la imagen correctamente.



Calculamos el hash de la evidencia.



```
D:\>certutil -hashfile .\copia_disco_cifrado.dd sha512
SHA512 hash de .\copia_disco_cifrado.dd:
c650543406eae976b2782a1755dd331a2c4ec0236df88524d3bcc86cc7fce1ecc96f2700983575fe2b8b2499f4837b15bdfa6275f2e36ccac3c251acd55d5730
CertUtil: -hashfile comando completado correctamente.

D:\>_
```

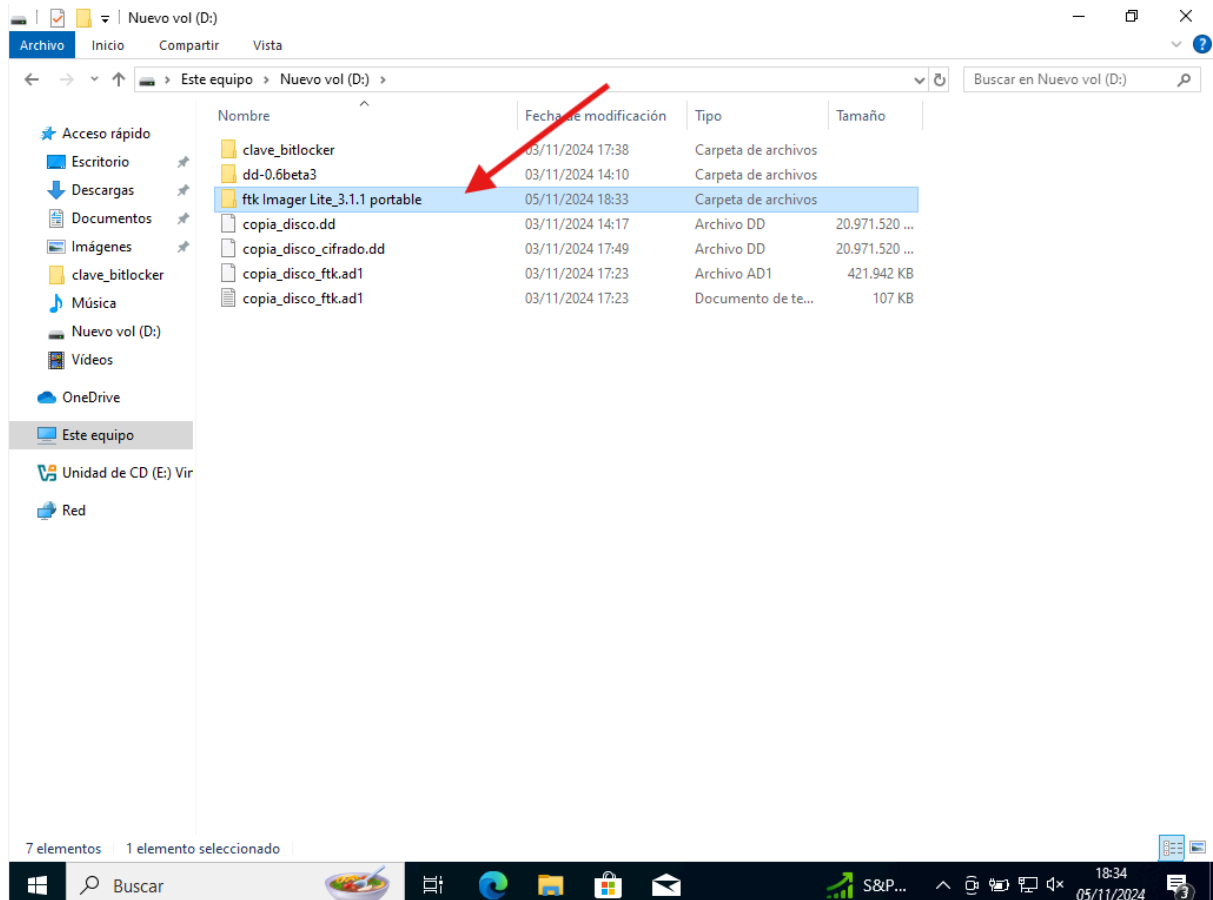
SHA512 hash de .\copia_disco_cifrado.dd:

c650543406eae976b2782a1755dd331a2c4ec0236df88524d3bcc86cc7fce1ecc96f2700983575fe2b8b2499f4837b15bdfa6275f2e36ccac3c251acd55d5730

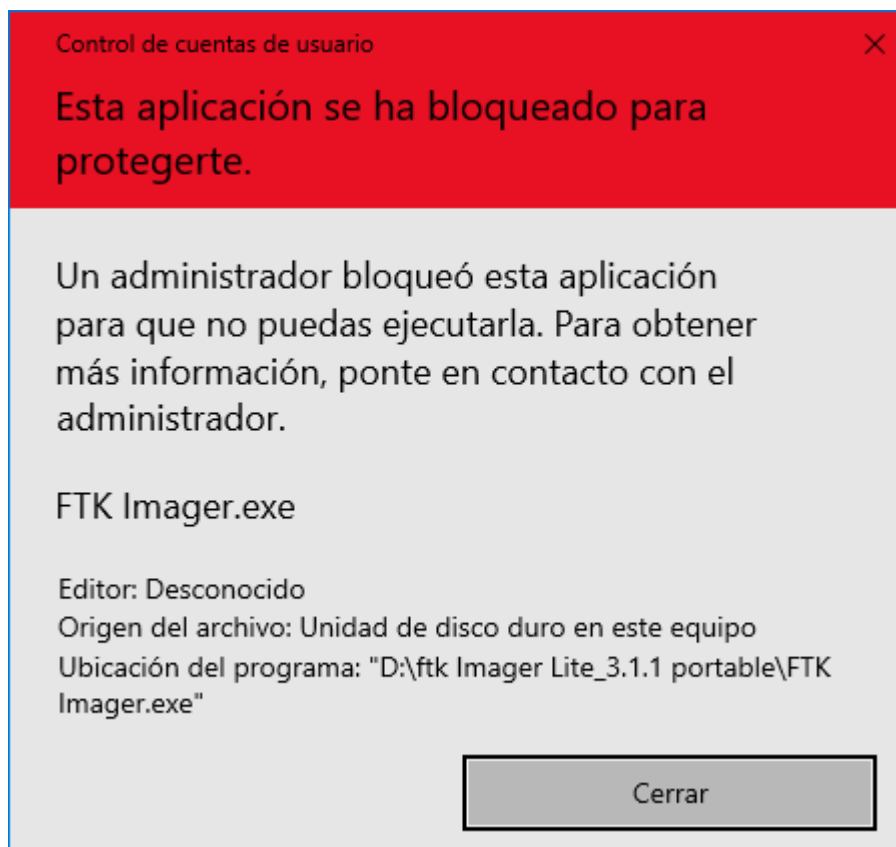
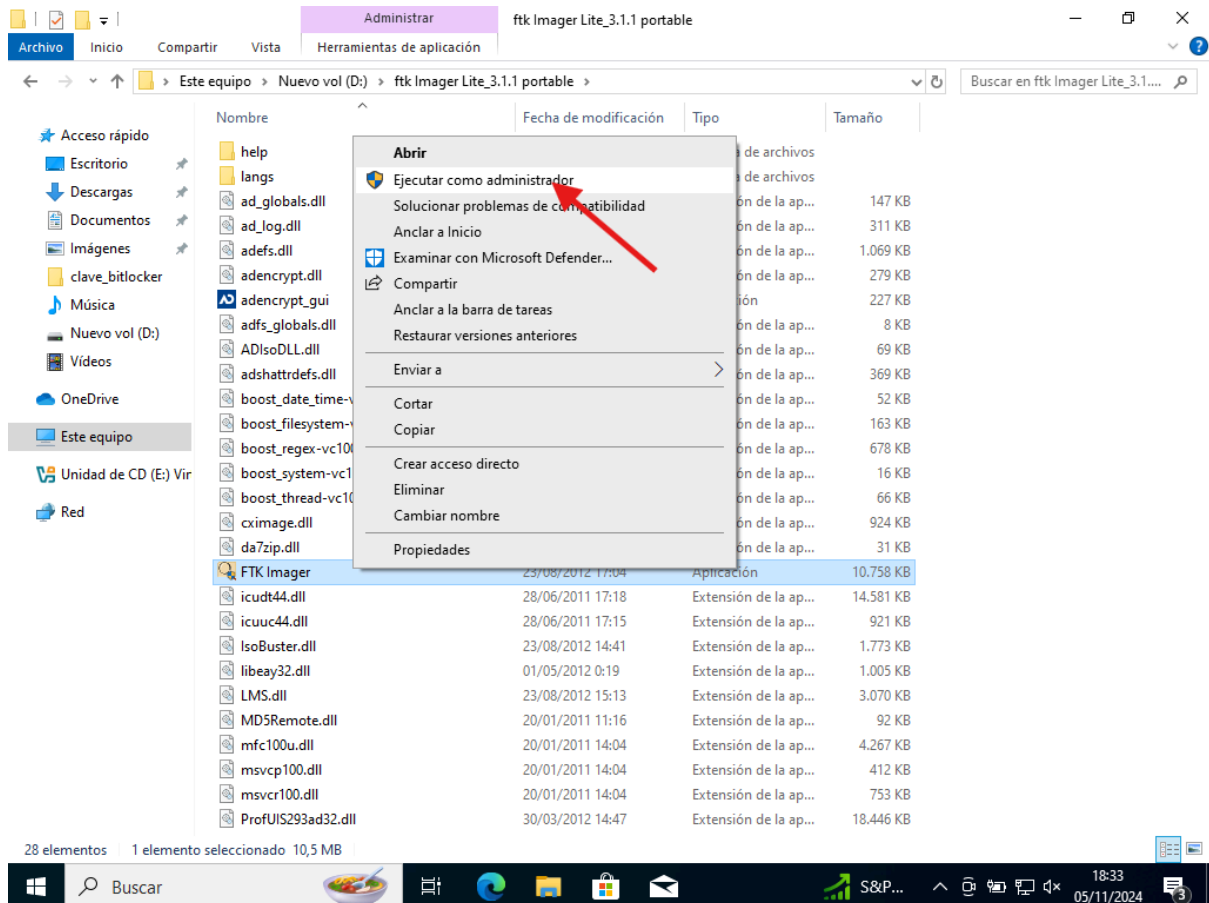
CertUtil: -hashfile comando completado correctamente.

FTK Imager Lite (Disco cifrado):

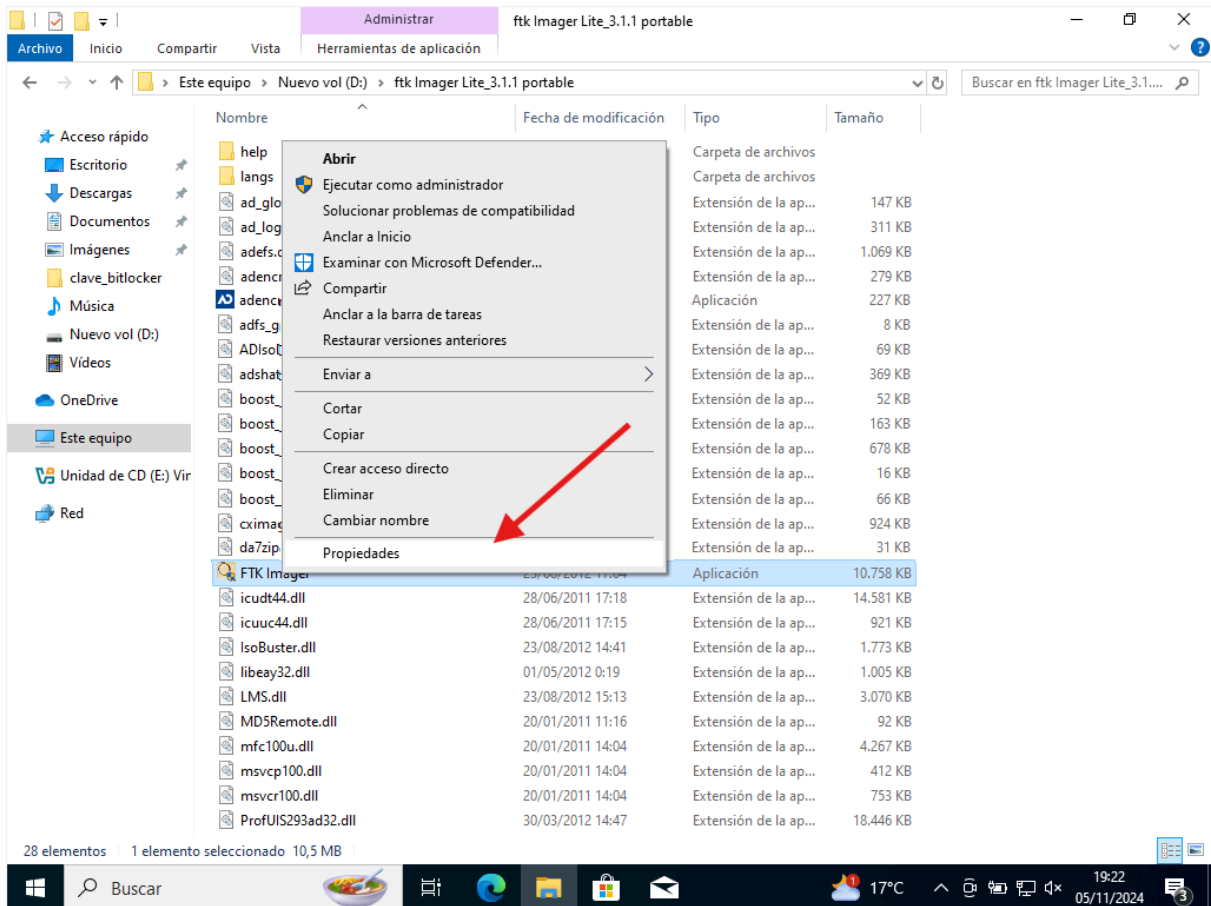
Ejecutamos FTK Imager como Administradores.

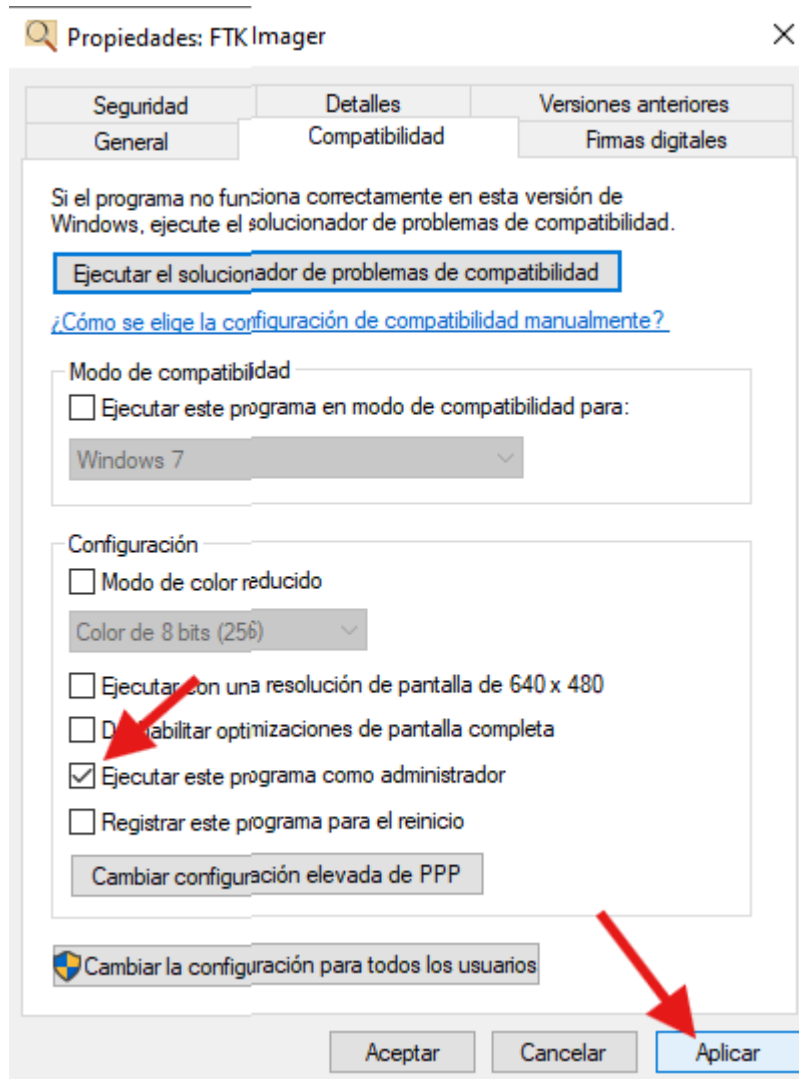


ANÁLISIS FORENSE

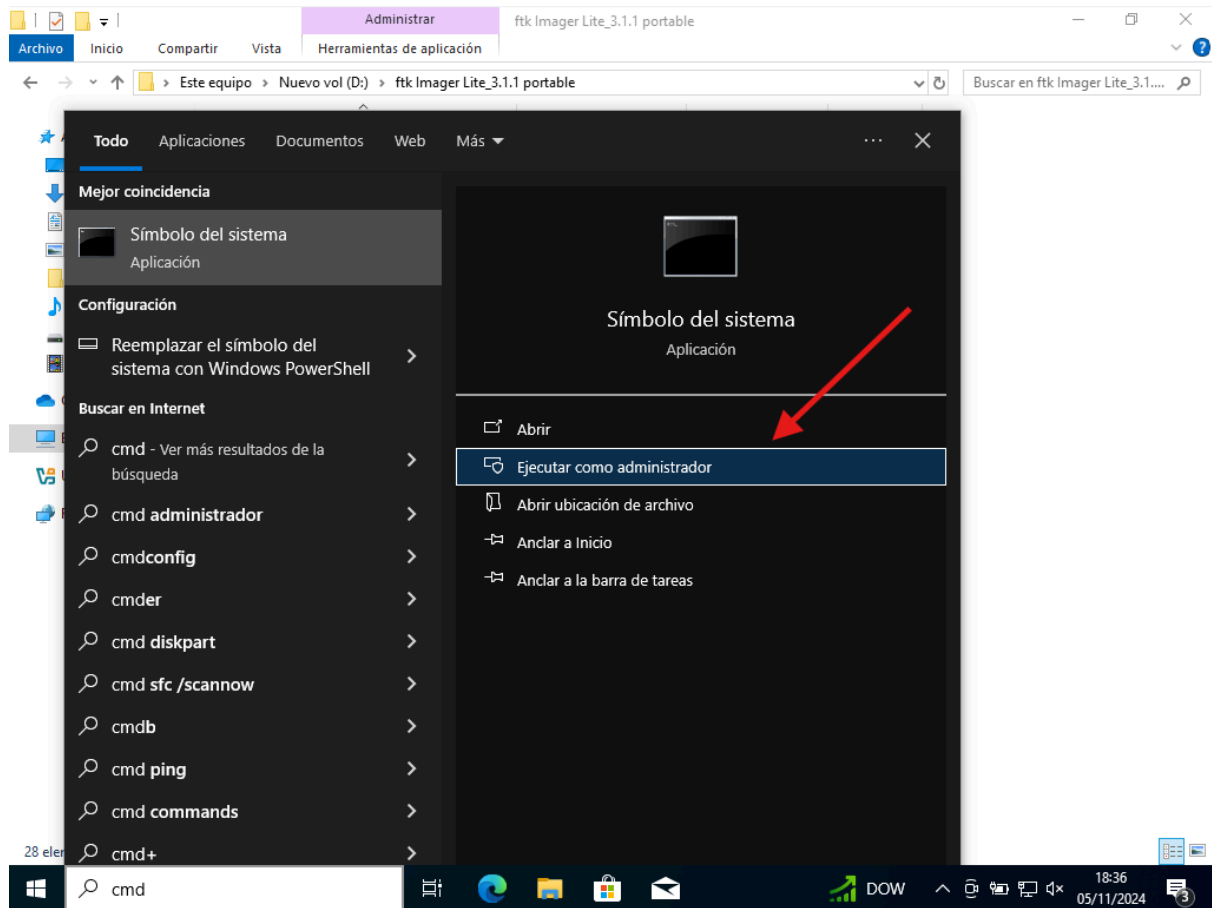


ANÁLISIS FORENSE





ANÁLISIS FORENSE



```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.3803]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>D:

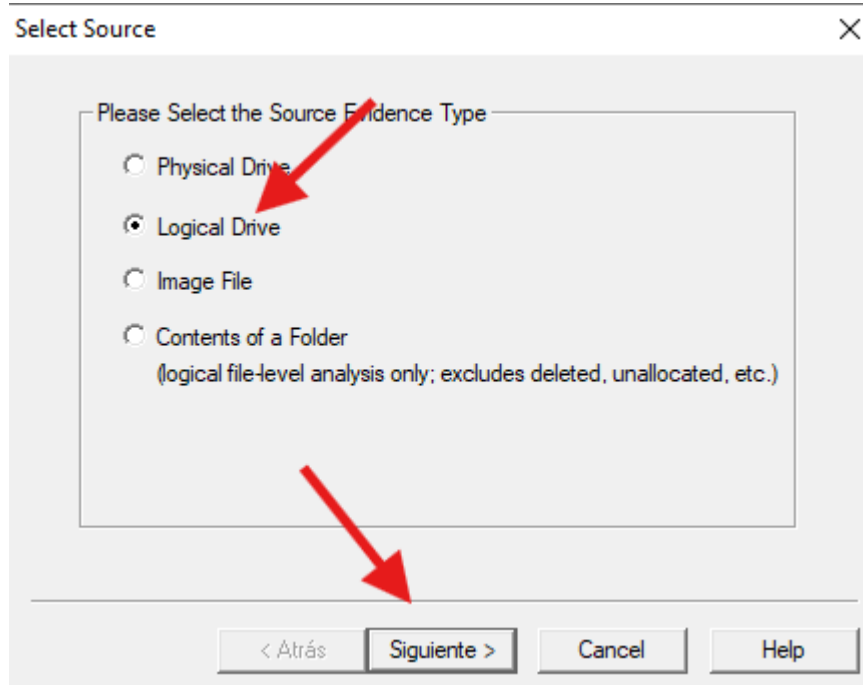
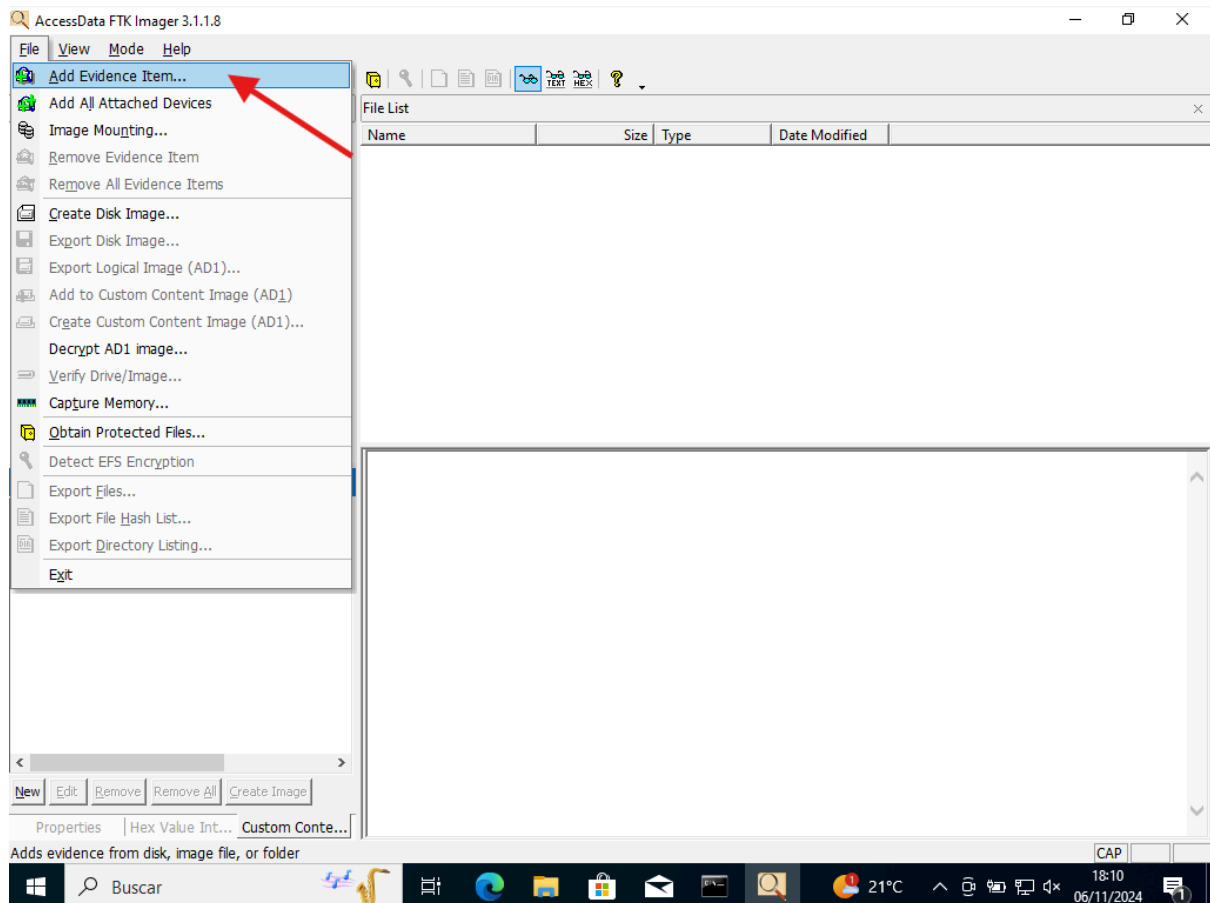
D:\>cd "ftk Imager Lite_3.1.1 portable"

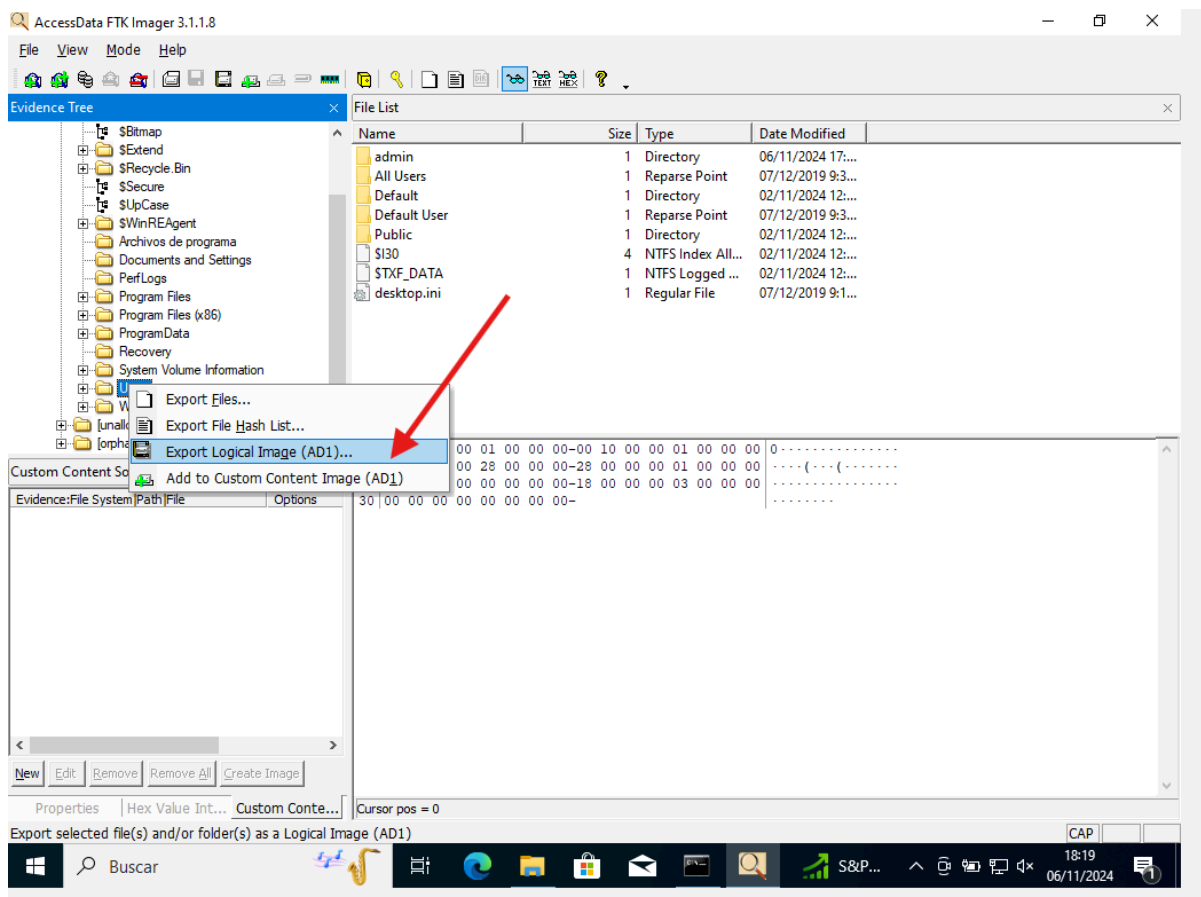
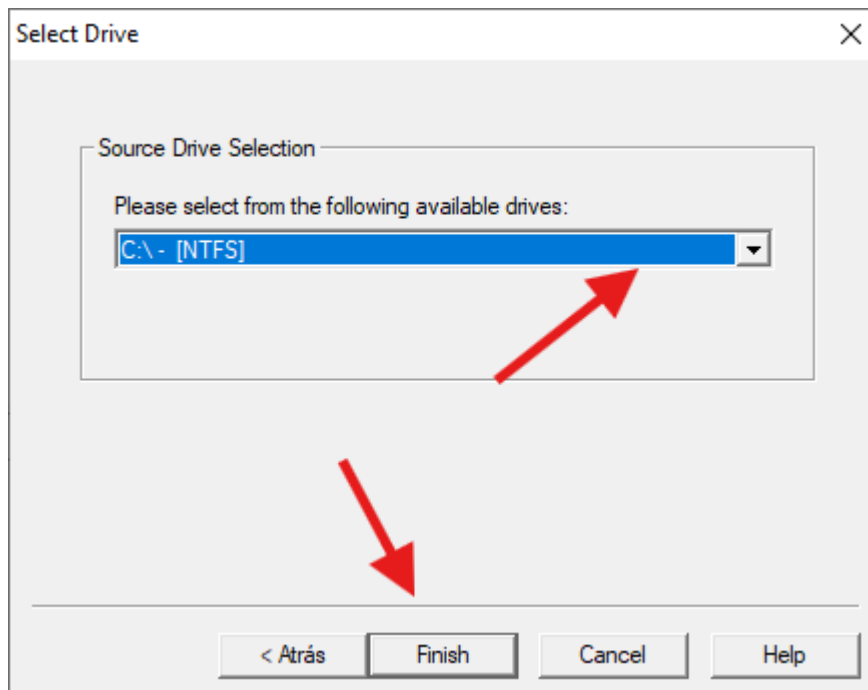
D:\ftk Imager Lite_3.1.1 portable>FTK Imager.exe
"FTK" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

D:\ftk Imager Lite_3.1.1 portable>"FTK Imager.exe"

D:\ftk Imager Lite_3.1.1 portable>_
```

ANÁLISIS FORENSE






Create Image ✕


Image Source:

Starting Evidence Number:

Image Destination(s):



☒ Verify images after they are created ☐ Precalculate Progress Statistics
☐ Create directory listings of all files in the image after they are created



Evidence Item Information ✕


Case Number:

Evidence Number:

Unique Description:

Examiner:

Notes:



Select Image Destination



Image Destination Folder
D:\ Browse

Image Filename (Excluding Extension)
copia_disco_cifrado_ftk

Image Fragment Size (MB) 1500
For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest) 6

Use AD Encryption ☐

Filter by File Owner ☐

< Atrás Finish Cancel Help

Create Image



Image Source
Users

Starting Evidence Number: 0

Image Destination(s)
D:\copia_disco_cifrado_ftk [Logical image]

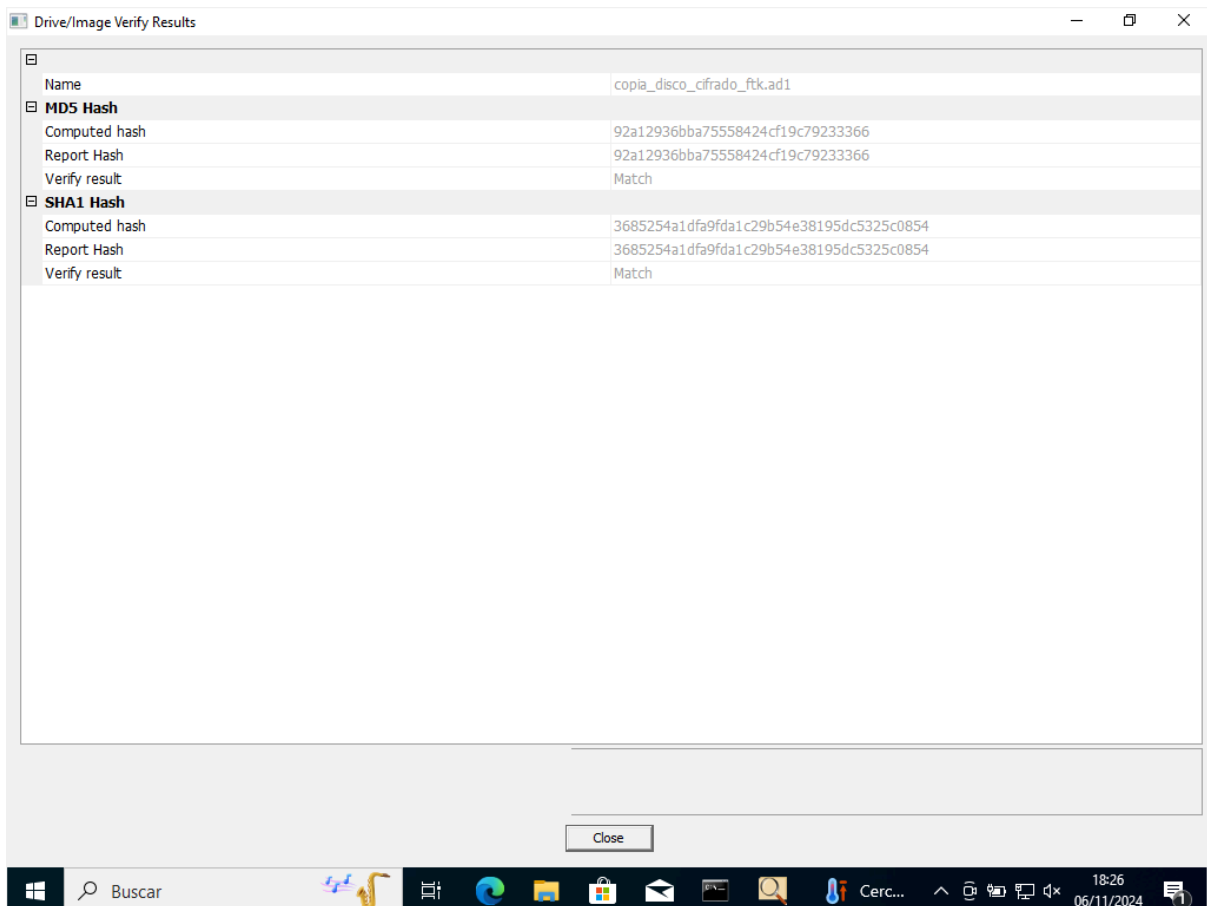
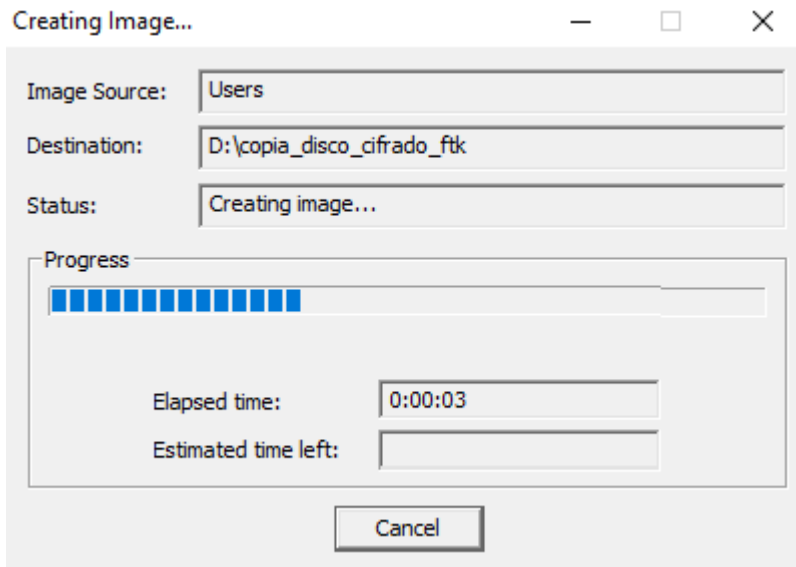
Add... Edit... Remove

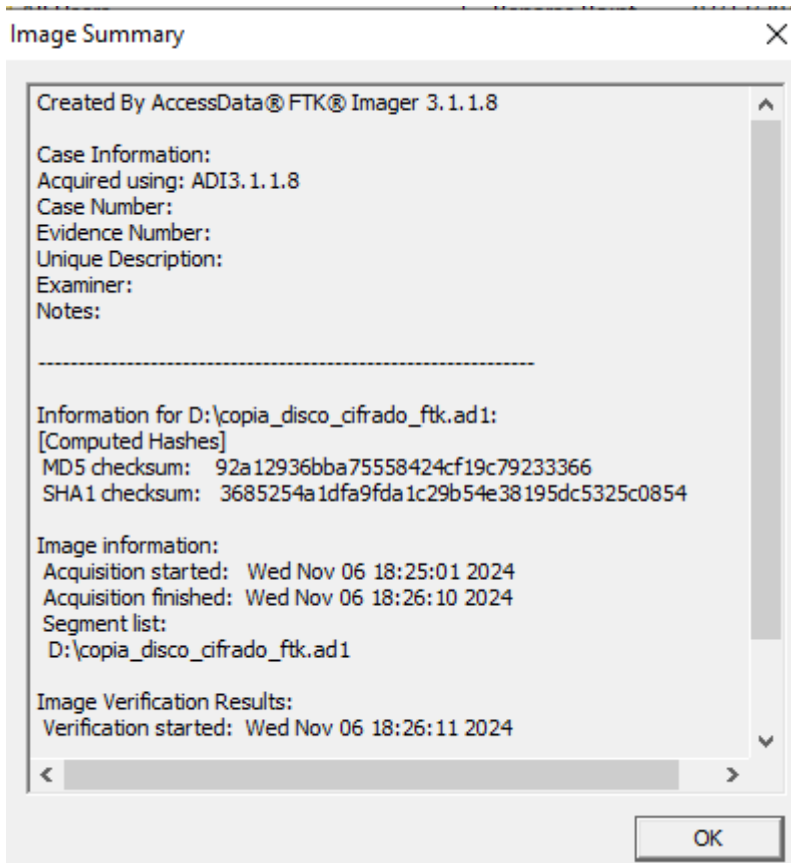
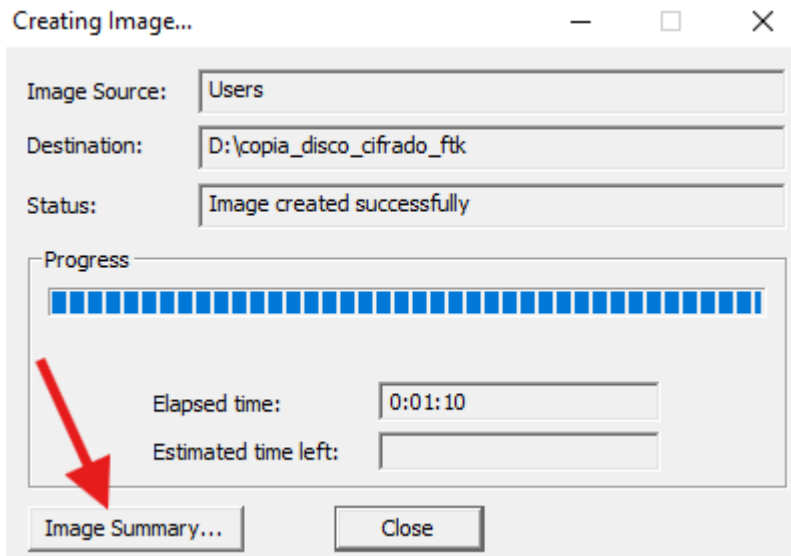
☒ Verify images after they are created ☐ Precalculate Progress Statistics

☐ Create directory listings of files in the image after they are created

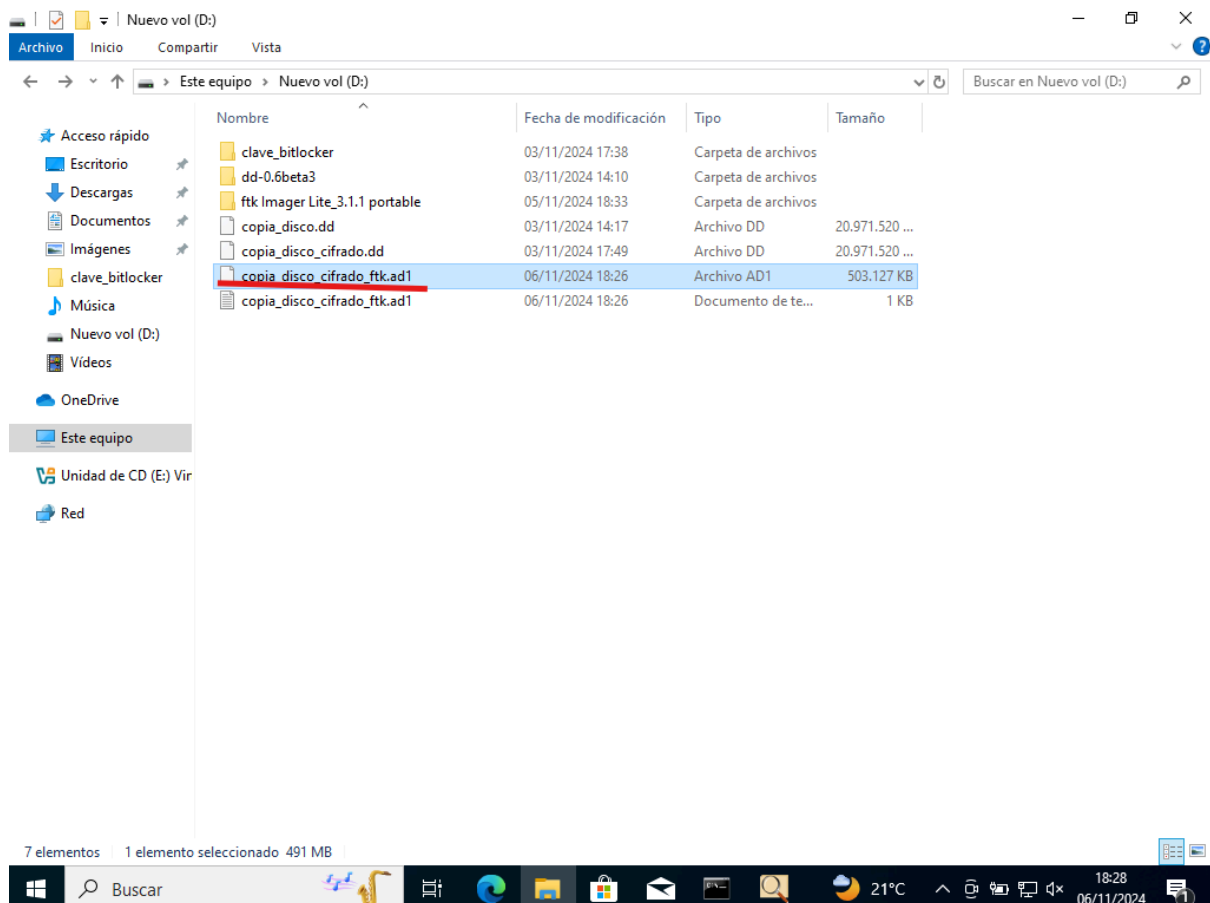
Start Cancel

ANÁLISIS FORENSE





ANÁLISIS FORENSE



```
D:\>certutil -hashfile copia_disco_cifrado_ftk.ad1 sha512
SHA512 hash de copia_disco_cifrado_ftk.ad1:
ff756e253bd17857e6683717ff342d401261a9ba01634b5f05ceea186f81296f8699f7166b1de98296ce8502e326991f8ae3bcb6d868a6ff5295bb79628f6
cee
CertUtil: -hashfile comando completado correctamente.
D:\>
```

SHA512 hash de copia_disco_cifrado_ftk.ad1:

**ff756e253bd17857e6683717ff342d401261a9ba01634b5f05ceea186f81296f8699f71
66b1de98296ce8502e326991f8ae3bcb6d868a6ff5295bb79628f6cee**

CertUtil: -hashfile comando completado correctamente.

Evidencias Obtenidas:

Resultado final del disco duro externo.

