



Universidad
Francisco de
Vitoria

*Centro de
Documentación
Europea*

UFV Madrid

Informe taller FTK imager

Héctor Ramírez López

Índice

Identificación.....	3
Procedimiento	3

Identificación

Nombre del caso: Lab1

Numero de evidencia: 1

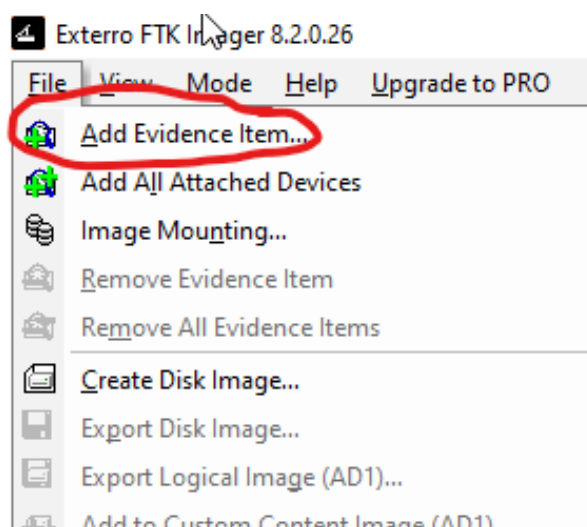
Fecha de adquisición: 23/10/2025

Nombre del perito: Héctor Ramírez López

Descripción del dispositivo: Carpeta de archivos

Procedimiento

Primero vamos a añadir las evidencias



En este caso sería el contenido de una carpeta, pero también puede ser de una imagen, de un disco lógico o un dispositivo físico.

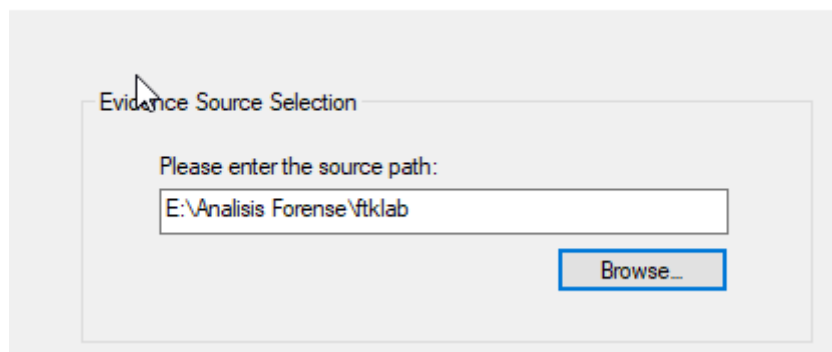
Select Source ×

Please Select the Source Evidence Type

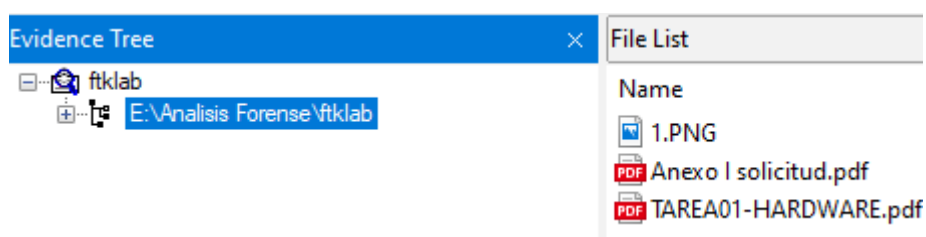
- ☐ Physical Drive
- ☐ Logical Drive
- ☐ Image File
- ☒ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

A continuación, seleccionaremos la ruta donde tenemos la carpeta.

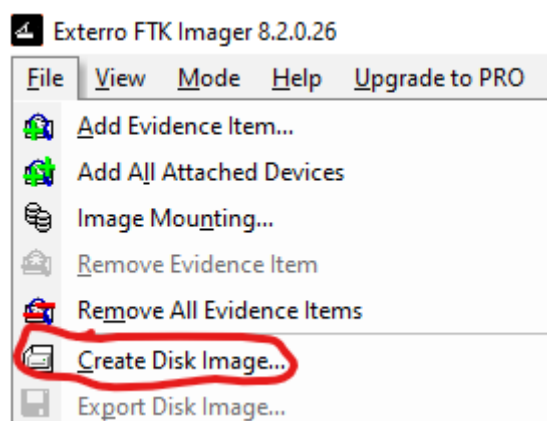
Select File



Después de esto en la pestaña evidence tree ya nos aparecerá nuestra carpeta con las evidencias.

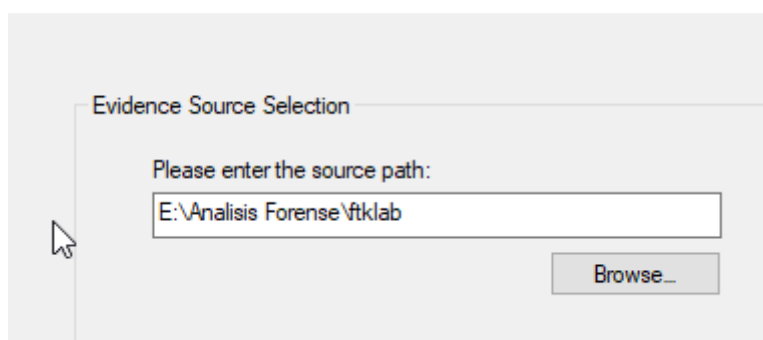


Procedemos a montar la imagen a partir de nuestra carpeta de evidencias



Seleccionamos de nuevo la carpeta donde están nuestras evidencias.

Select File



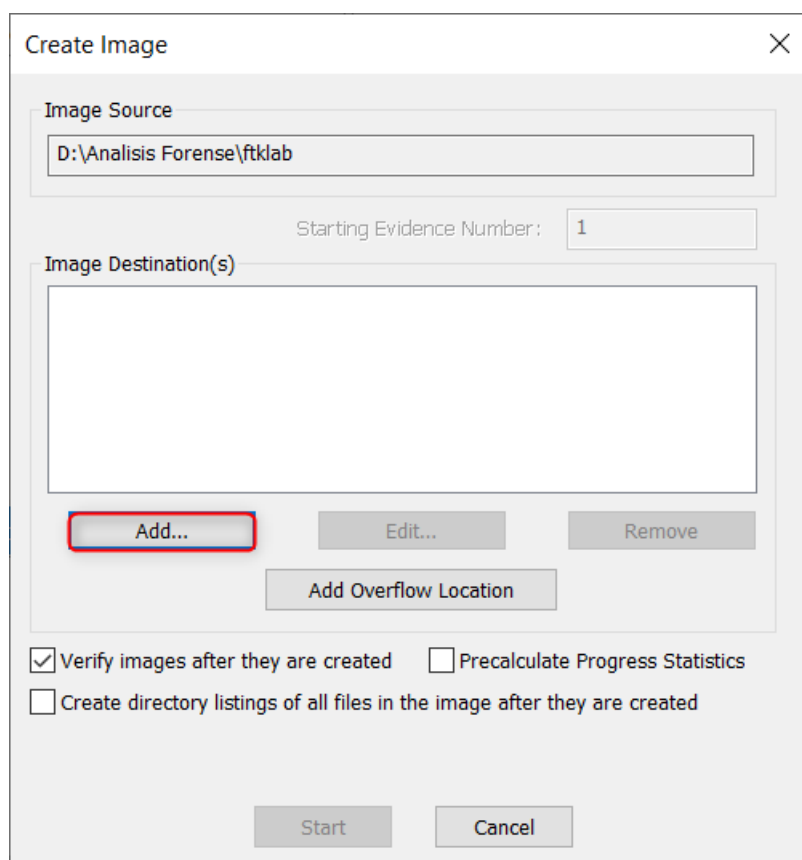
Evidence Source Selection

Please enter the source path:

E:\Análisis Forense\ftklab

Browse...

En la siguiente ventana hacemos click en add



Create Image

Image Source

D:\Análisis Forense\ftklab

Starting Evidence Number: 1

Image Destination(s)

Add... Edit... Remove

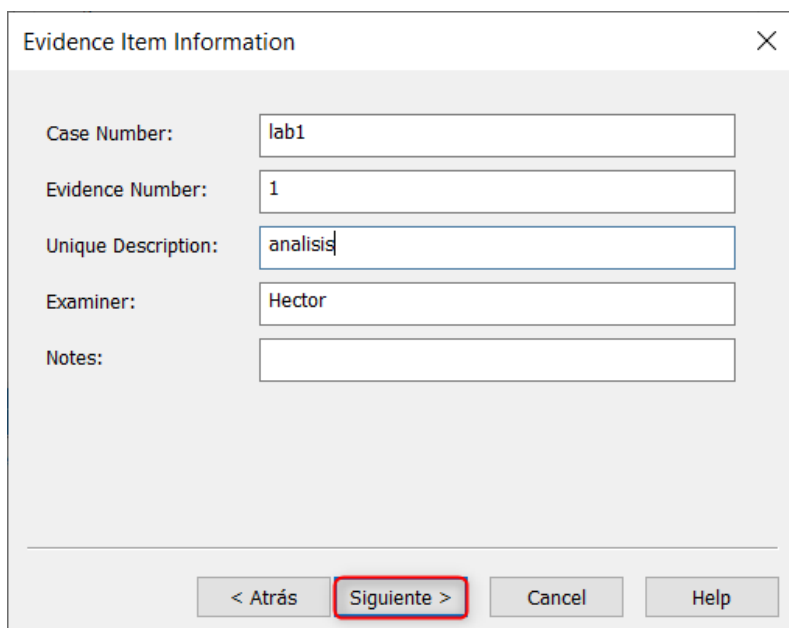
Add Overflow Location

☒ Verify images after they are created ☐ Precalculate Progress Statistics

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

Start Cancel

Rellenamos los campos y damos a siguiente



Evidence Item Information

Case Number: lab1

Evidence Number: 1

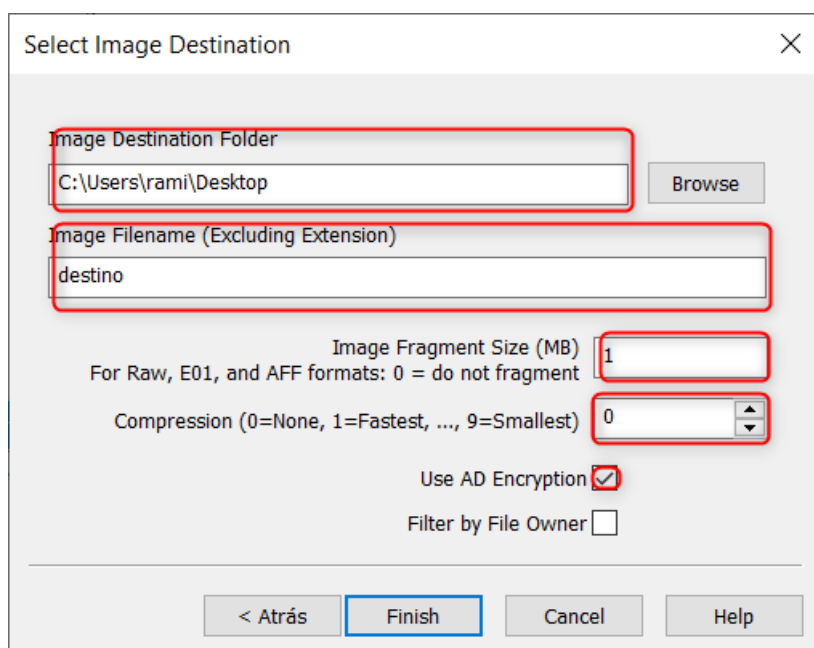
Unique Description: analisis

Examiner: Hector

Notes:

< Atrás **Siguiente >** Cancel Help

Ahora tendremos que indicar en que carpeta queremos que se nos guarde y el nombre de la imagen. En tamaño de la imagen seleccionaremos 1mb y en compresión lo pondremos a 0 por último marcamos la casilla Use AD encryption.



Select Image Destination

Image Destination Folder
 C:\Users\rami\Desktop Browse

Image Filename (Excluding Extension)
 destino

Image Fragment Size (MB) 1
 For Raw, E01, and AFF formats: 0 = do not fragment

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

Use AD Encryption ☒

Filter by File Owner ☐

< Atrás **Finish** Cancel Help

Nos pedirá una contraseña para encriptar introducimos la que queramos.

AD Encryption Credentials

Enter Credentials To Encrypt

☒ Password:
Re-enter: ☐ Show password

☐ Certificate (.pfx, .p12, .pem)

Browse

OK Cancel

Después le daríamos a start.

Create Image

Image Source

Starting Evidence Number:

Image Destination(s)

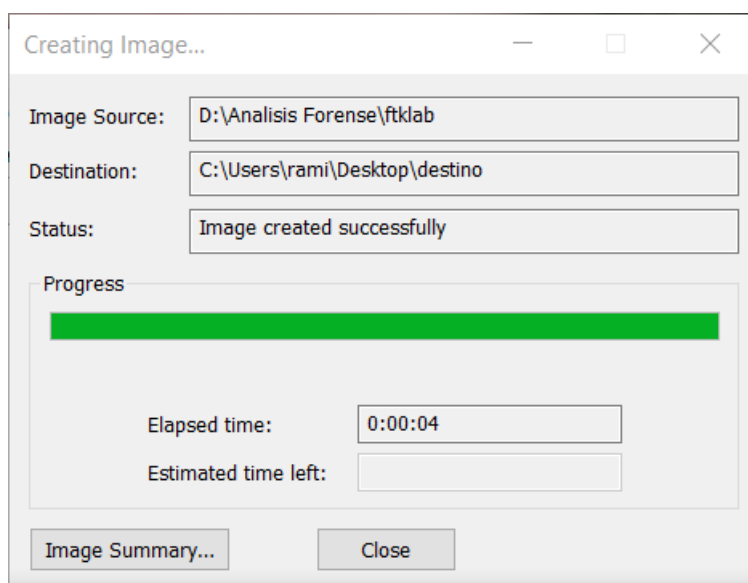
Add... Edit... Remove

Add Overflow Location

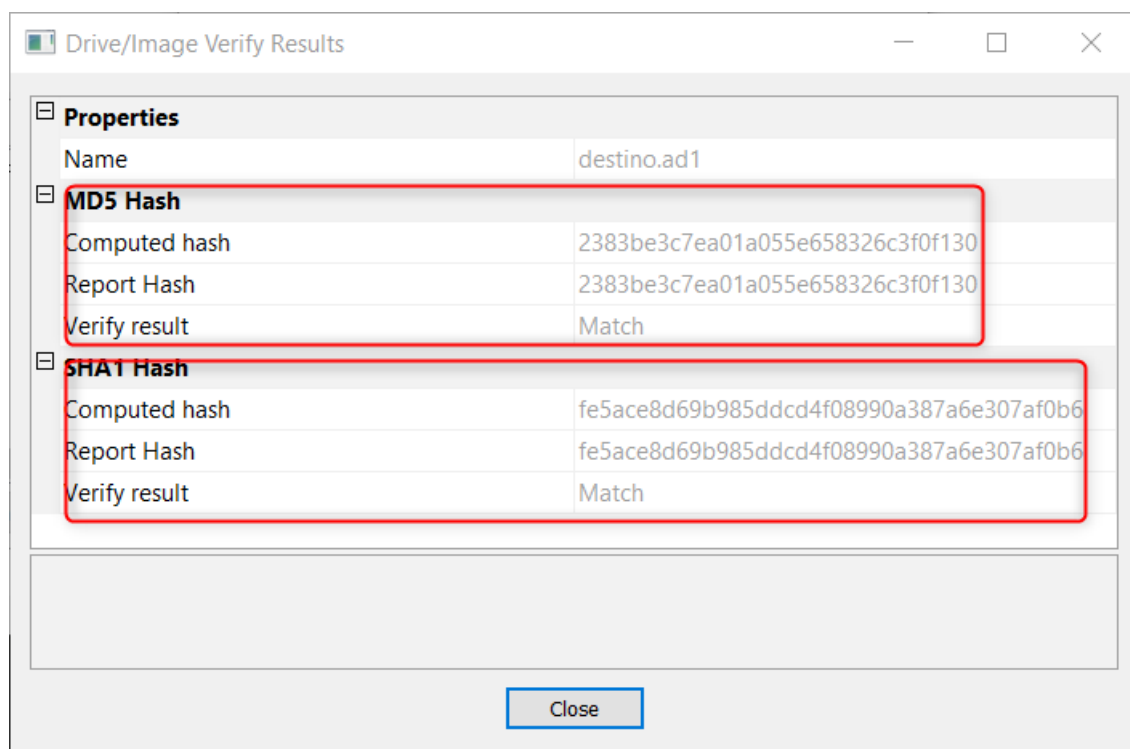
☒ Verify images after they are created ☐ Precalculate Progress Statistics
☐ Create directory listings of all files in the image after they are created

Start Cancel

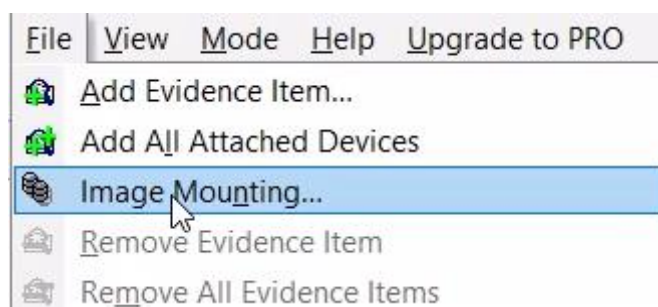
Empezara el proceso de encriptación.



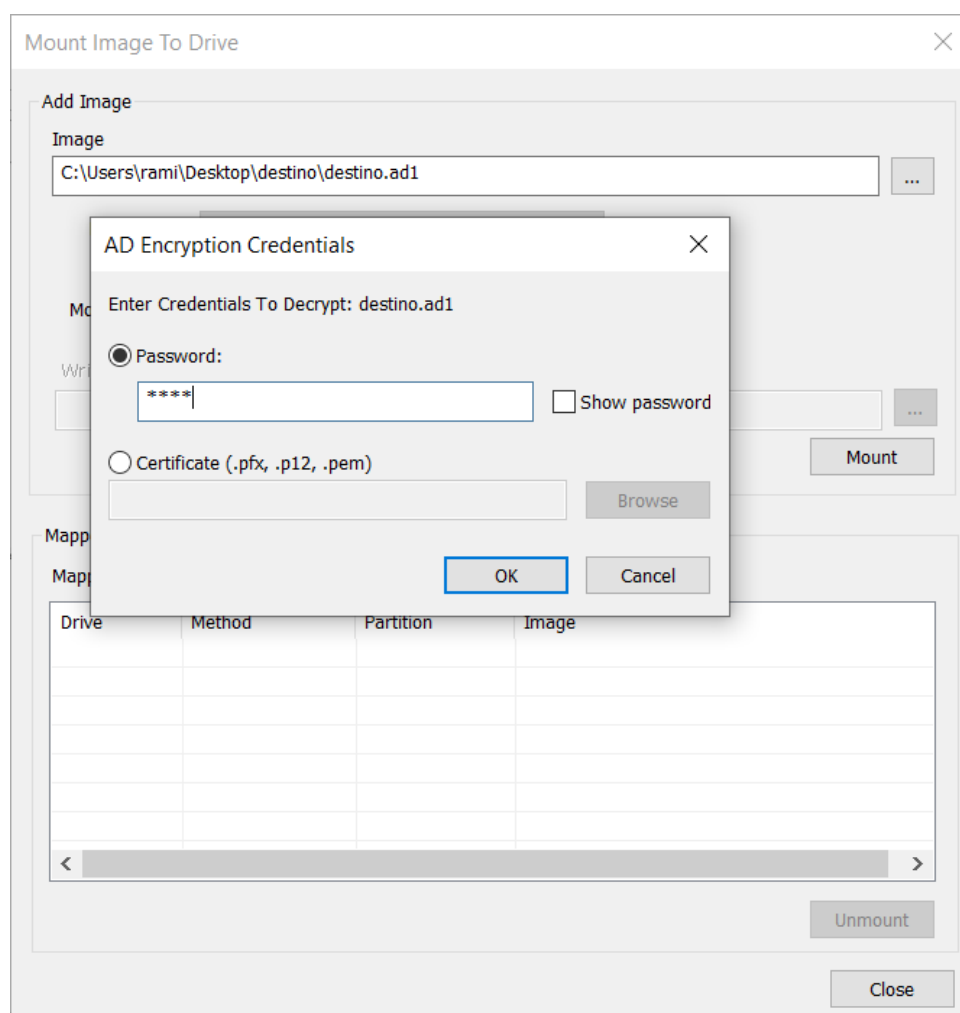
Una vez terminado se nos abrirá una ventana con los hashes que nos ha creado md5 y sha1.



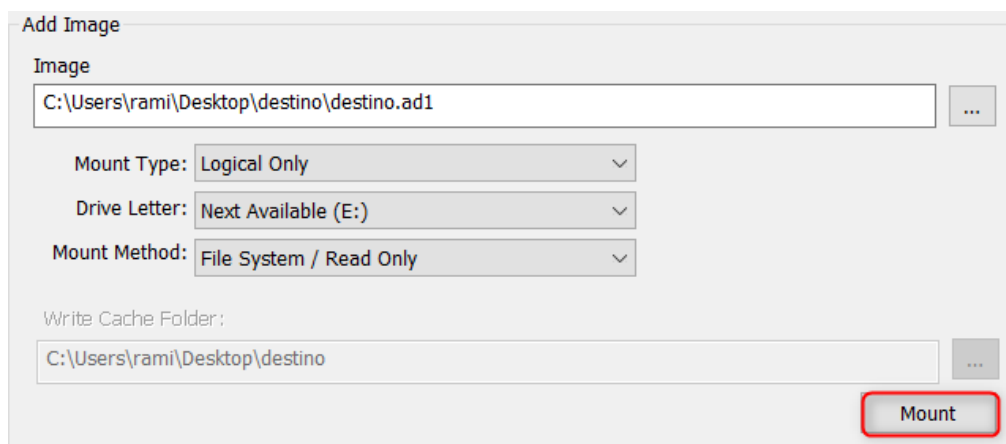
A continuación, procederemos a montar la imagen le damos a file image mounting.



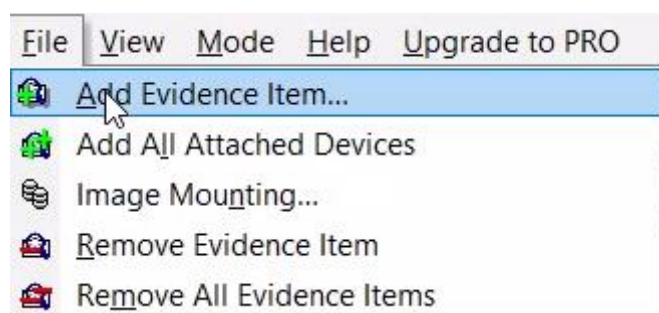
Tendremos que seleccionar la carpeta donde hemos creado la imagen y nos pedirá la contraseña.



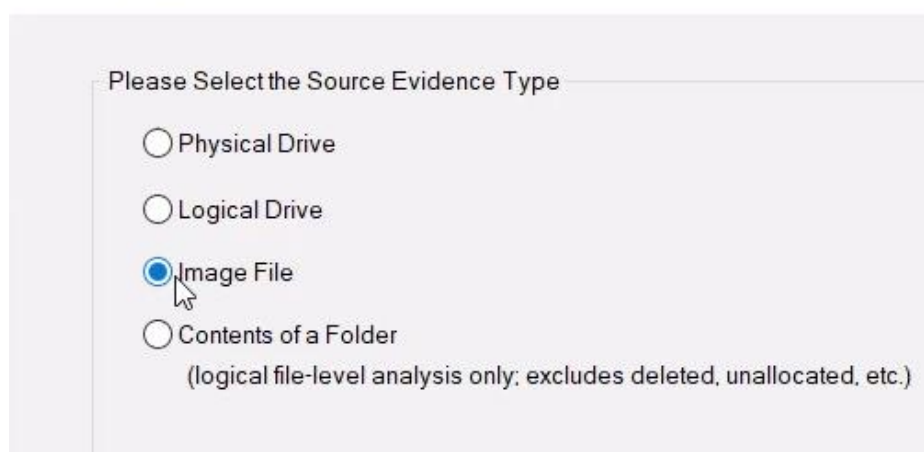
Le daremos a mount para que nos monte la imagen.



Añadiremos la imagen montada a las evidencias para ello vamos a file add evidence ítem, seleccionamos image file y damos a siguiente.



Select Source



Nos pedirá seleccionar la ruta donde tenemos nuestra imagen montada, ahora le damos a finish y nos pedirá la contraseña que hemos usado para encriptar.

Evidence Source Selection

Please enter the source path:

C:\Users\rami\Desktop\destino\destino.ad1

Browse_

Evidence Source Selection

Please enter the source path:

C:\Users\rami\Desktop\destino\destino.ad1

Browse_

AD Encryption Credentials

Enter Credentials To Decrypt: destino.ad1

☒ Password:

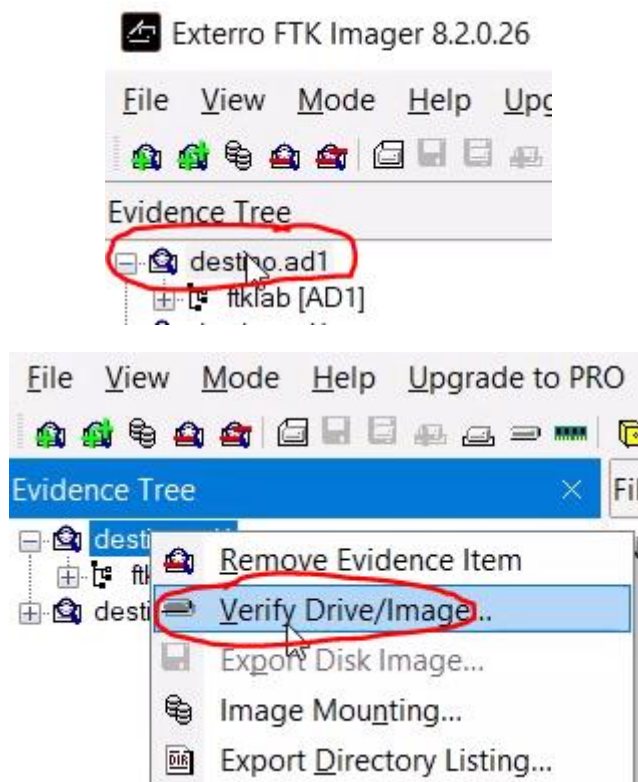
☐ Show password

☐ Certificate (.pfx, .p12, .pem)

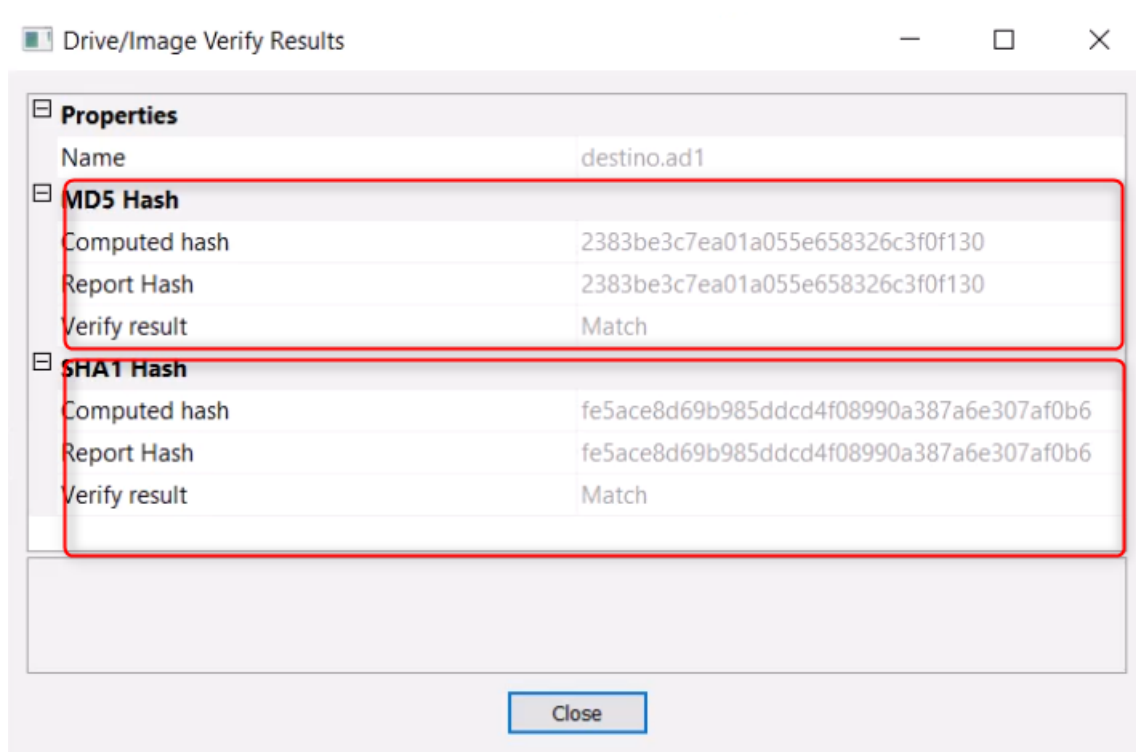
Browse

OK Cancel

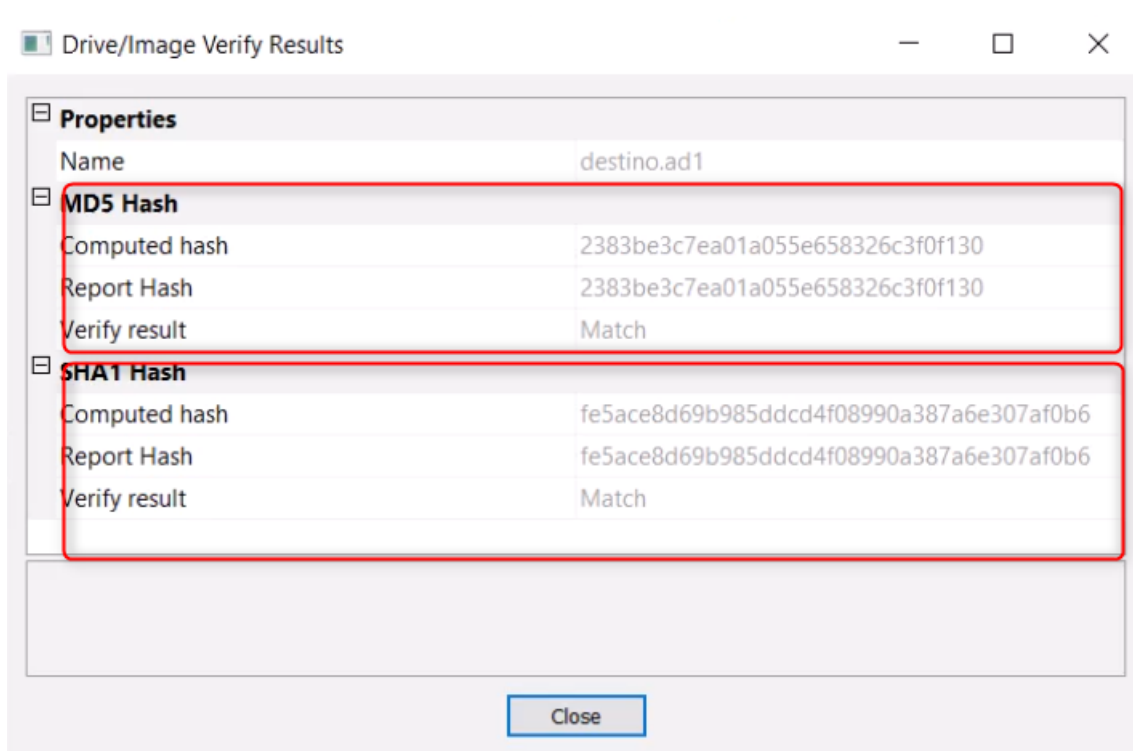
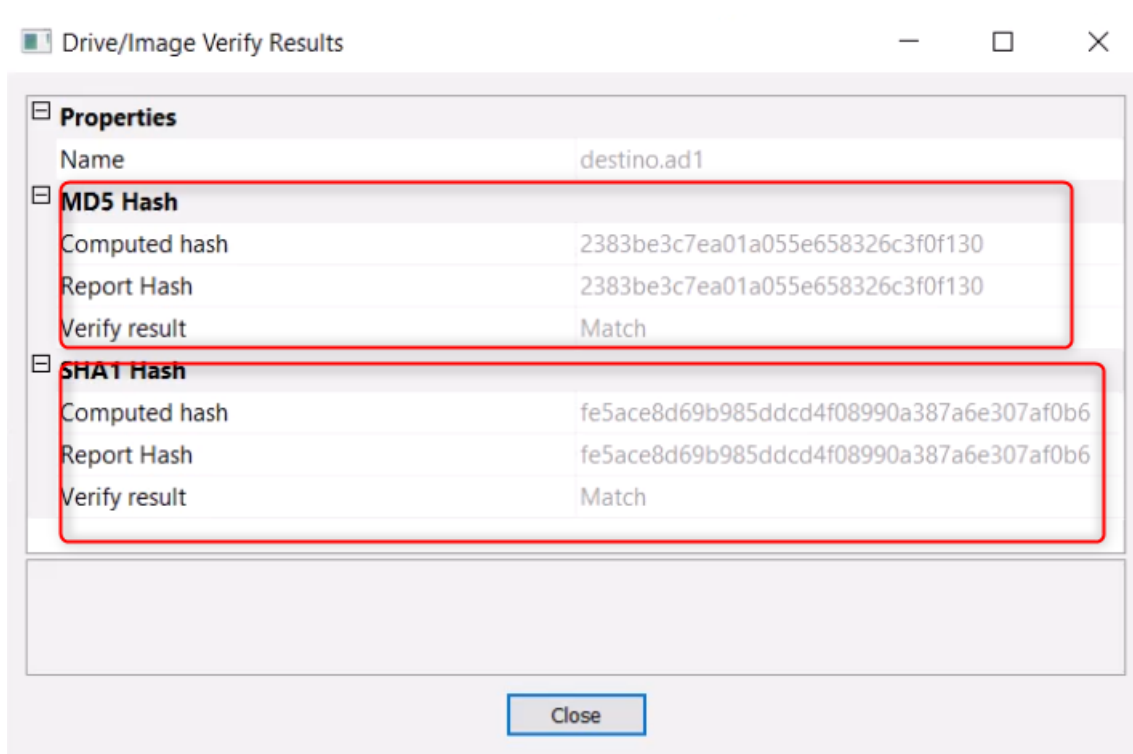
Una vez ya tengamos nuestra imagen importada a nuestras evidencias le daremos click derecho verify image.



Cuando le demos a verify image nos abrirá una ventana con los hashes md5 y sha1.



Por último, procederemos a comprobar que la carpeta que exportamos como la que importamos tienen los mismos hashes, esto por lo tanto significaría que no se ha modificado el archivo.





Universidad
Francisco de
Vitoria

*Centro de
Documentación
Europea*

UFV Madrid