

ERIC SERRANO MARIN



RETO AUTOPSY

ANÁLISIS FORENSE EN CIBERSEGURIDAD INFORMÁTICA

ERIC SERRANO MARÍN

ÍNDICE

Enunciado	2
Ejercicio 1	2
Ejercicio 2	3
Ejercicio 1	4
1. Creación de disco duro de 1GB.	4
2. Añadir fotografía y borrarla.....	7
3. Añadir al menos 20 carpetas y archivos.....	9
4. Añadir archivos que incluyan correos electrónicos y URLs.....	9
5. Insertar y esconder un Excel con datos “confidenciales” y modificar la extensión del Excel para que pase a ser .pdf.	10
6. Conseguir la imagen de la partición con FTK Imager.....	10
7. Mediante Autopsy conseguir ÚNICAMENTE los archivos borrados y los archivos sospechosos de haber sido modificada su extensión.....	15
8. Eliminar la partición de 1GB y vuelva a insertarla en su partición original.	21
9. Generar un informe con Autopsy donde se refleje el análisis forense de lo sucedido. Detallar paso a paso en un documento.	23
Ejercicio 2.....	25
1. Creación de imagen del disco duro de 5GB.....	25
2. Usar autopsy para encontrar la imagen.	28
3. Encontrar los hashes de las contraseñas del usuario ciber.....	31
4. Sacar la contraseña del hash con john the Ripper y extraer el .rar.	31
5. Usaremos autopsy para averiguar donde se realizó la imagen.	32
6. Guardar en todo momento la cadena de custodia del análisis forense a realizar.	35

Enunciado

Ejercicio 1

Desde una MV o desde un disco duro externo, reduzca el tamaño de su disco en 1GB y cree una nueva unidad de disco de 1GB. Realice con su móvil una fotografía a un objeto (añada en la configuración de su cámara que se almacenen los datos EXIF de la localización). Y siga los siguientes pasos:

- Pegue la imagen en la partición de 1GB
- Borre la imagen
- Añada una carpeta con al menos 20 archivos y carpetas.
- Entre estos archivos debe haber varios que incluyan correos electrónicos y URLs
- Inserte y "esconda" una Excel con datos "confidenciales" dentro de la carpeta anterior
- Modifique la extensión de la Excel para que pase a ser .pdf
- Mediante FTK Imager consiga una imagen forense de la partición
- Mediante Autopsy consiga ÚNICAMENTE los archivos borrados y los archivos sospechosos de haber sido modificada su extensión
- Elimine la partición de 1GB y vuelva a insertarla en su partición original
- Genere un informe con Autopsy donde se refleje el análisis forense de lo sucedido.
- Detalle paso a paso en un documento.

Genere un informe con Autopsy donde se refleje el análisis forense de lo sucedido.

Detalle paso a paso en un documento.

Ejercicio 2

Nos contratan para analizar un PC el cual dispone de 2 discos duros.

- Uno de gran tamaño con el sistema operativo y varios usuarios: Administrador, usuario, ciber e invitado
- Un disco duro de 5GB donde se encuentra diversa información

El empleado que usaba este PC ya no trabaja en la empresa y la empresa necesita averiguar en qué lugar de Sevilla se realizó una fotografía concreta.

La empresa nos informa que conoce que el extrabajador tenía guardada esa foto en su PC. Desconoce la ubicación, si la ha borrado o no, o lo que ha podido hacer con la fotografía. Quizás la haya podido encriptar, enmascarar, borrar o cualquier procedimiento informático para ocultar la fotografía.

El usuario del empleado es “ciber” y sus compañeros saben que el empleado normalmente utilizaba su contraseña de usuario de Windows para encriptar sus archivos.

La empresa solicita conseguir la fotografía que realizó y el lugar exacto donde realizó esta fotografía.

Documente paso a paso todos los procedimientos que ha realizado para averiguar dónde se realizó la fotografía.

Debe aplicar 2 métodos intermedios:

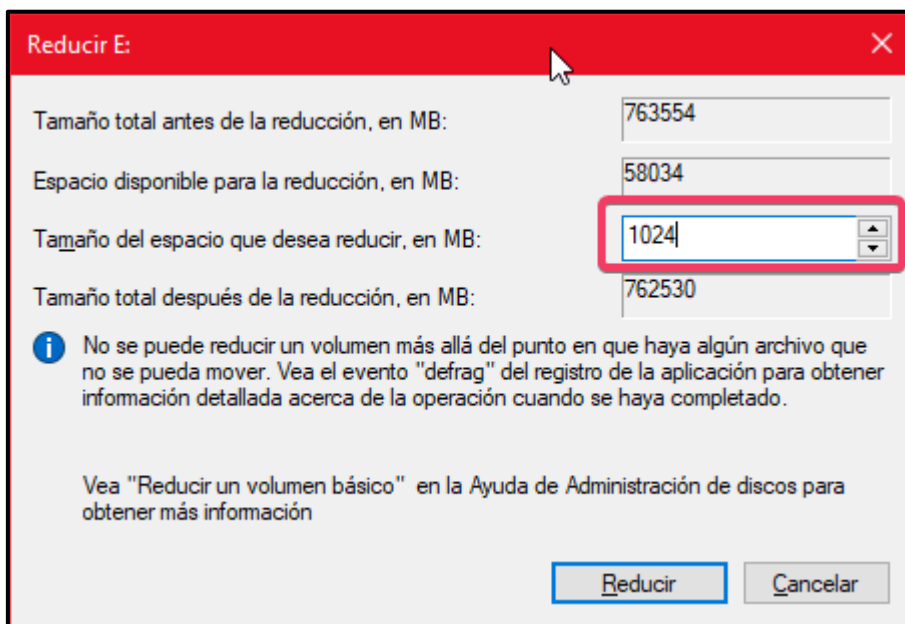
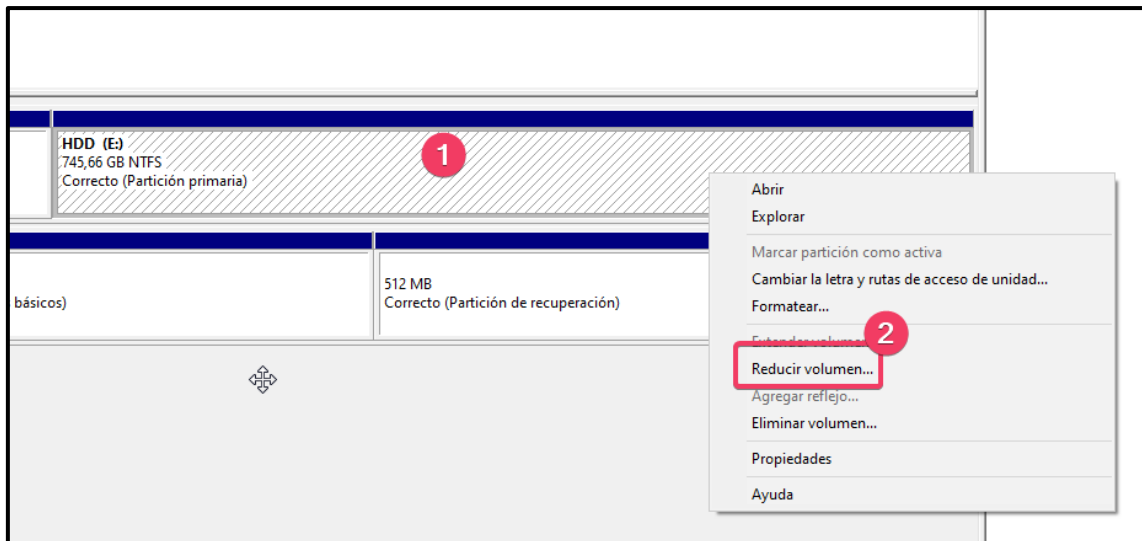
- Usando pwdump de Openwall en el mismo PC a analizar
- Usando otra herramienta informática para a través del SAM y del SYSTEM recopilados con FTK Imager consiga los códigos hash de los usuarios

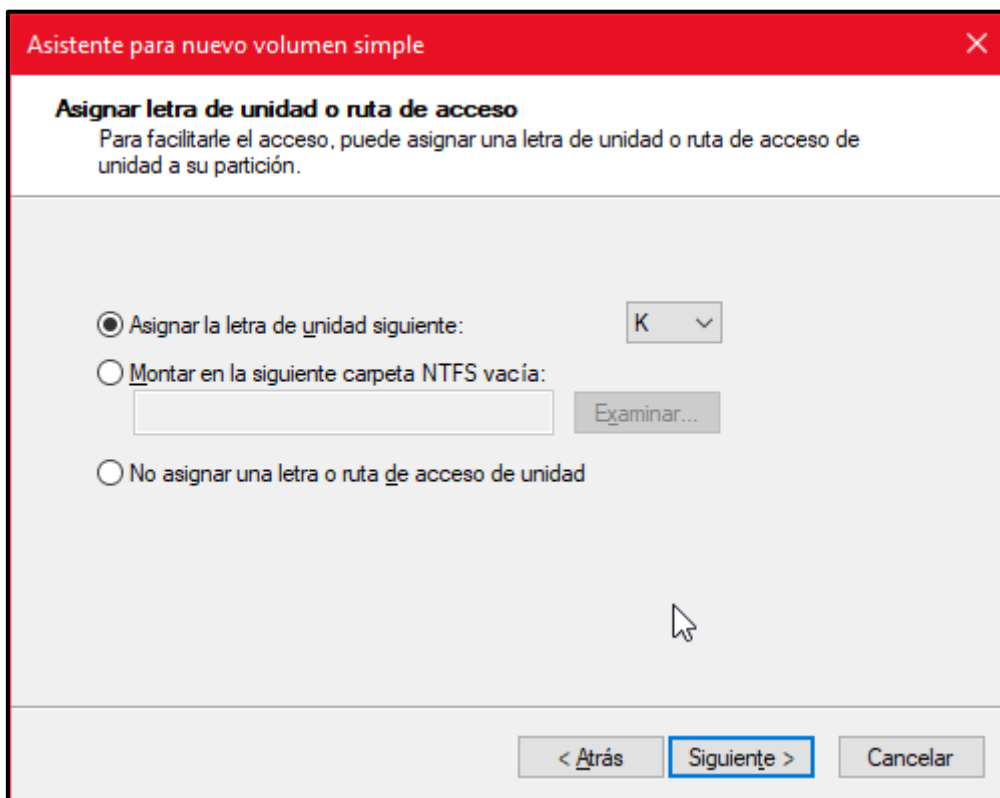
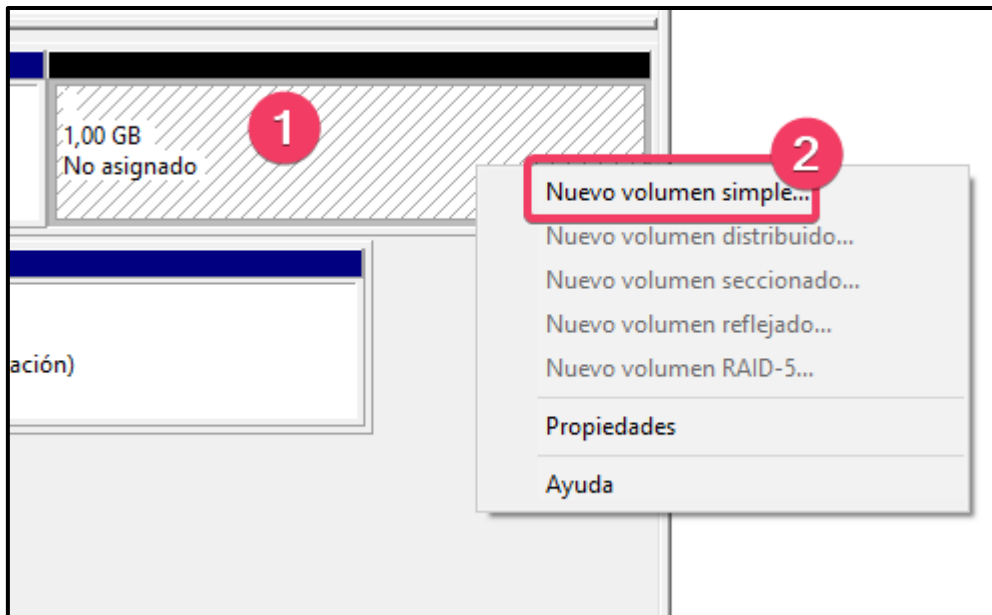
Recuerde guardar en todo momento la cadena de custodia del análisis forense a realizar.

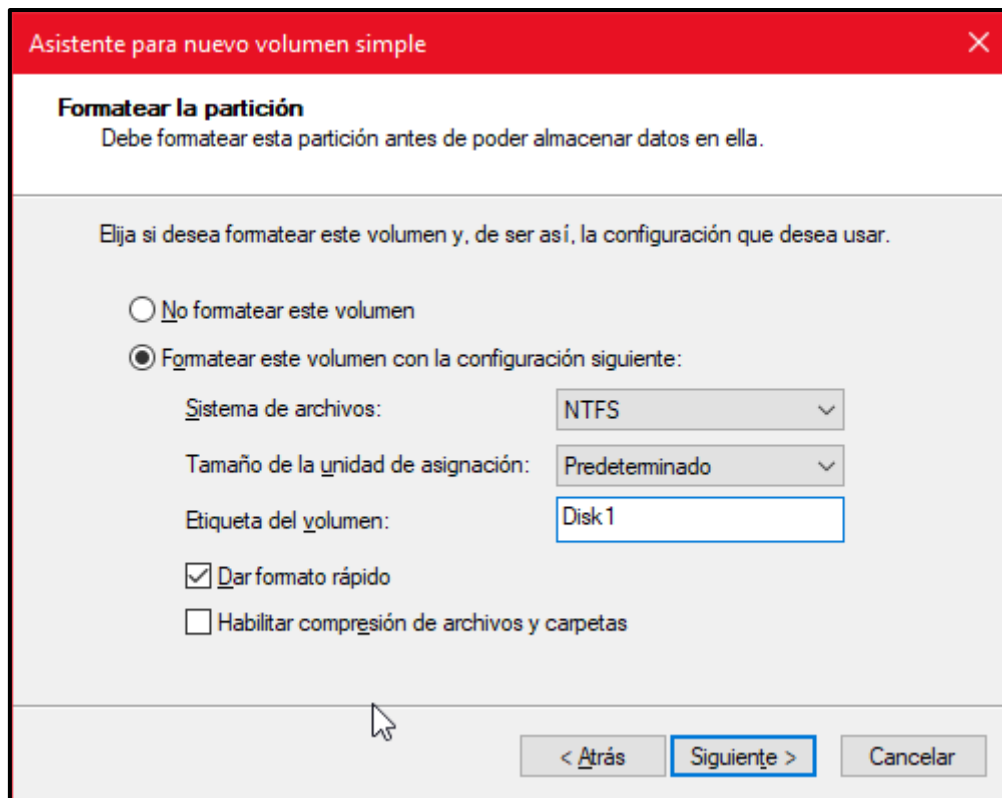
**** El siguiente índice y orden de pasos lo voy a realizarlo tal y como lo he hecho y he pensado que era mejor (ejercicio 2) ****

Ejercicio 1

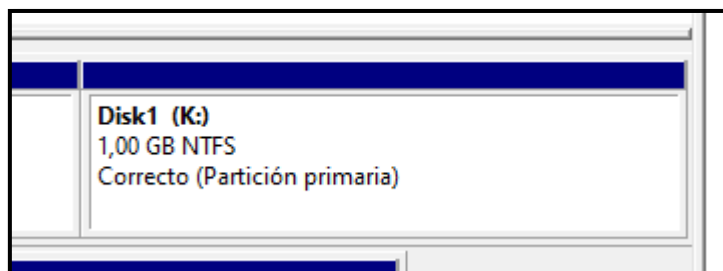
1. Creación de disco duro de 1GB.



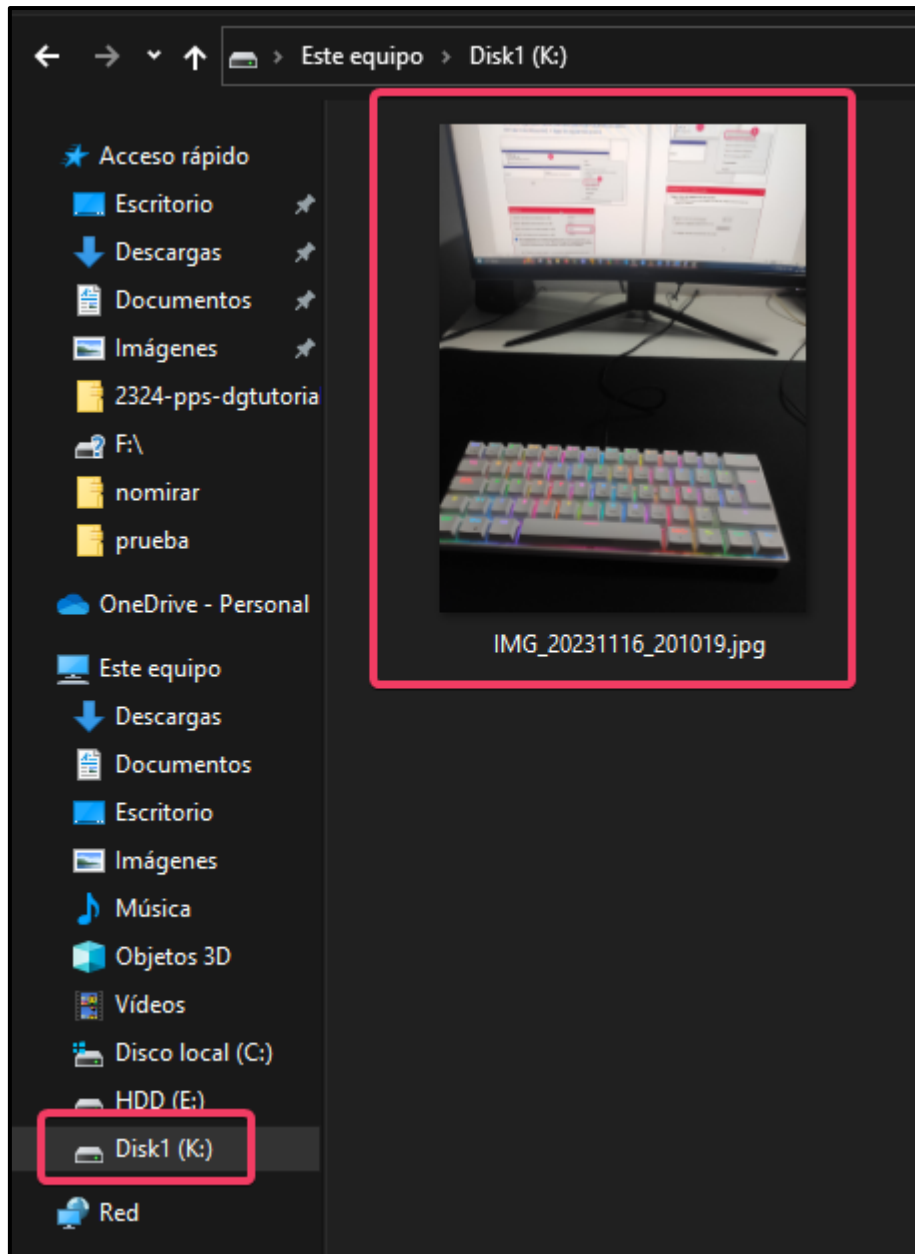


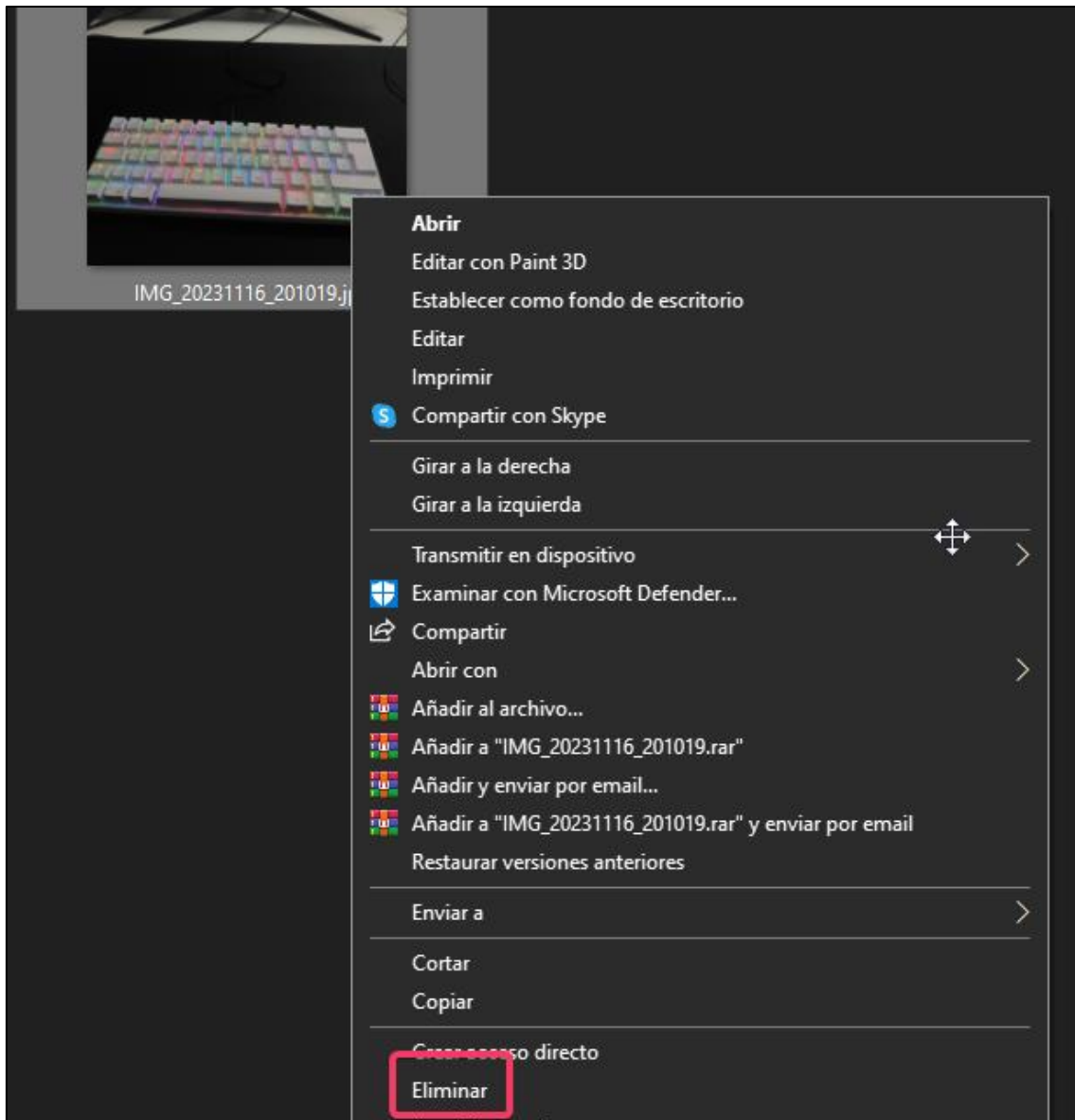


Ya tenemos nuestra partición de 1GB.

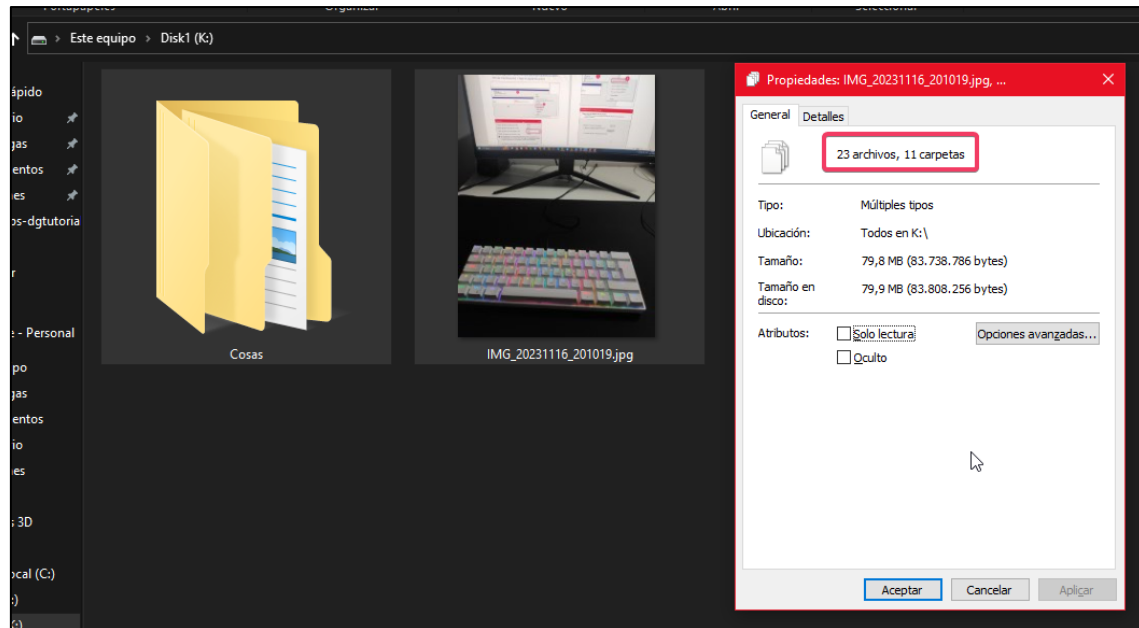


2. Añadir fotografía y borrarla.

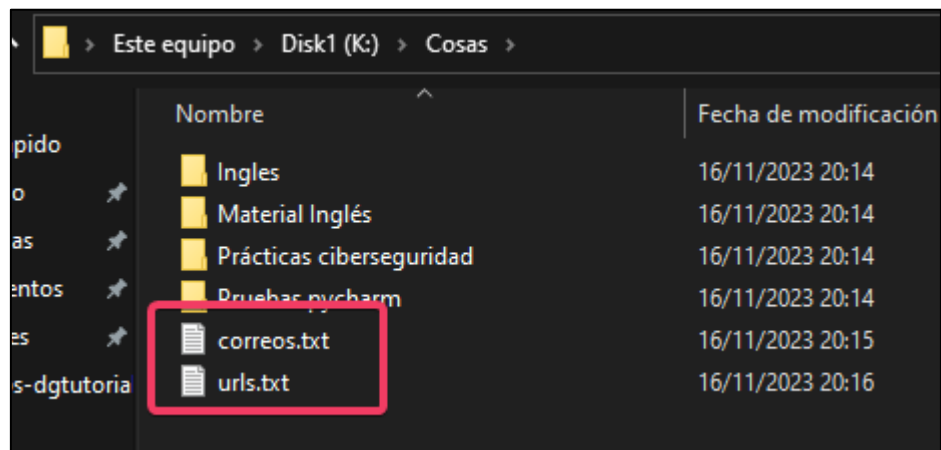




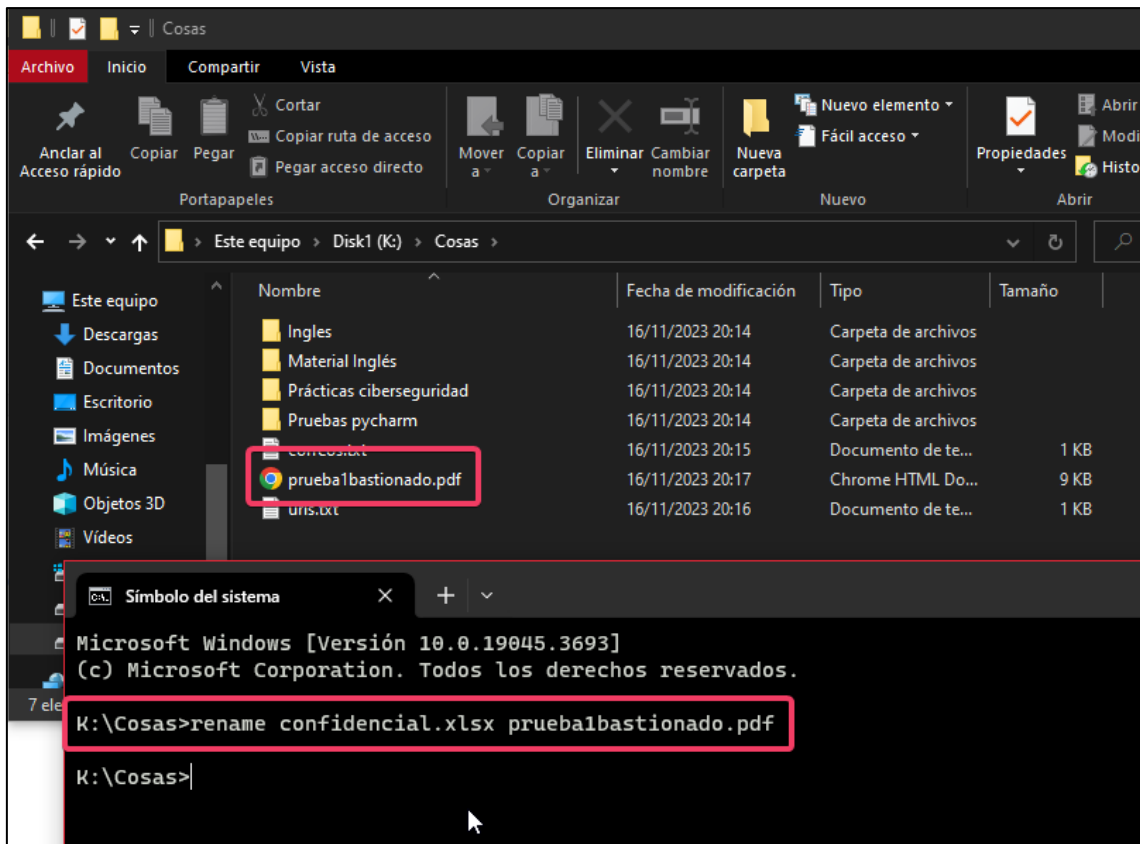
3. Añadir al menos 20 carpetas y archivos.



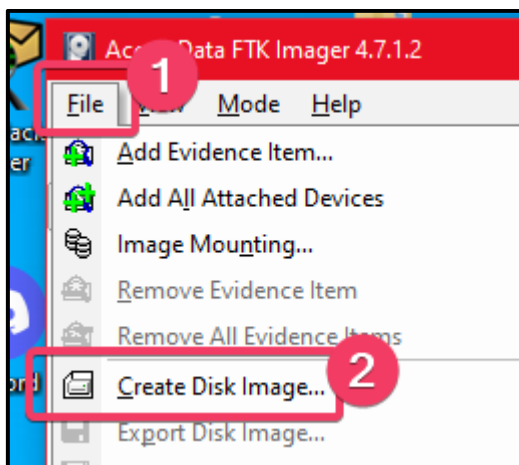
4. Añadir archivos que incluyan correos electrónicos y URLs.

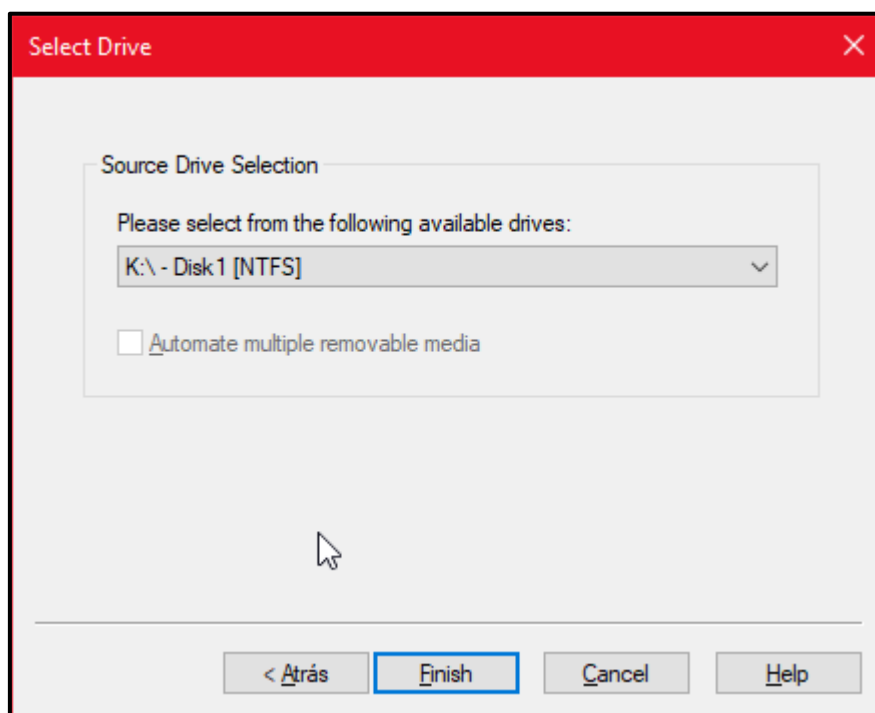
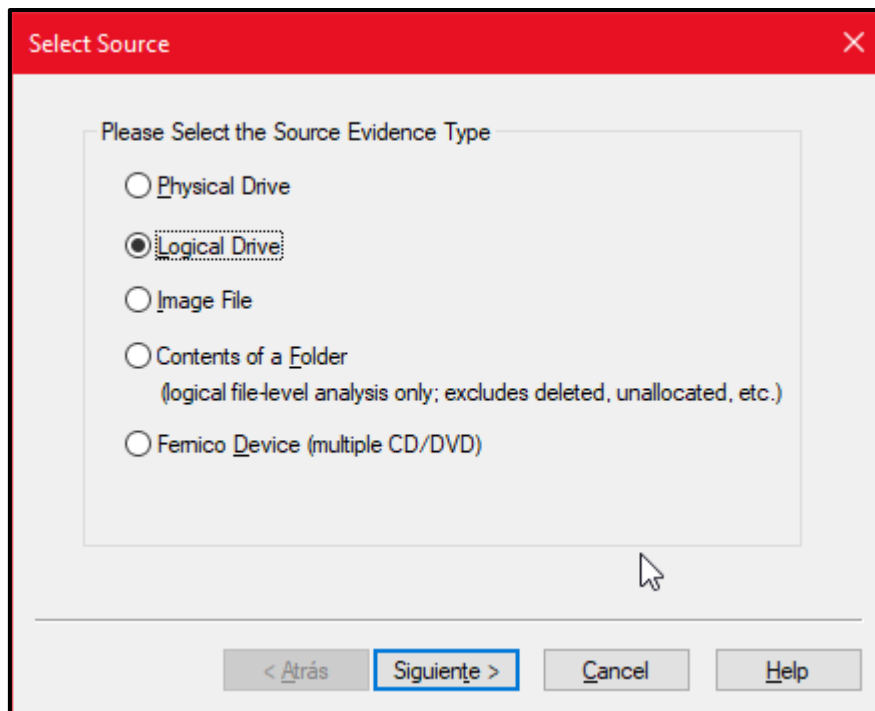


5. Insertar y esconder un Excel con datos “confidenciales” y modificar la extensión del Excel para que pase a ser .pdf.



6. Conseguir la imagen de la partición con FTK Imager.





Create Image [X]

Image Source
K:\

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]

Select Image Type [X]

Please Select the Destination Image Type

☒ Raw (dd)
☐ SMART
☐ E01
☐ AFF

[< Atrás] [Siguiete >] [Cancelar] [Ayuda]

Evidence Item Information [X]

Case Number:

Evidence Number:

Unique Description:

Examiner:

Notes:

< Atrás **Siguiente >** Cancel Help

Select Image Destination [X]

Image Destination Folder
 Browse

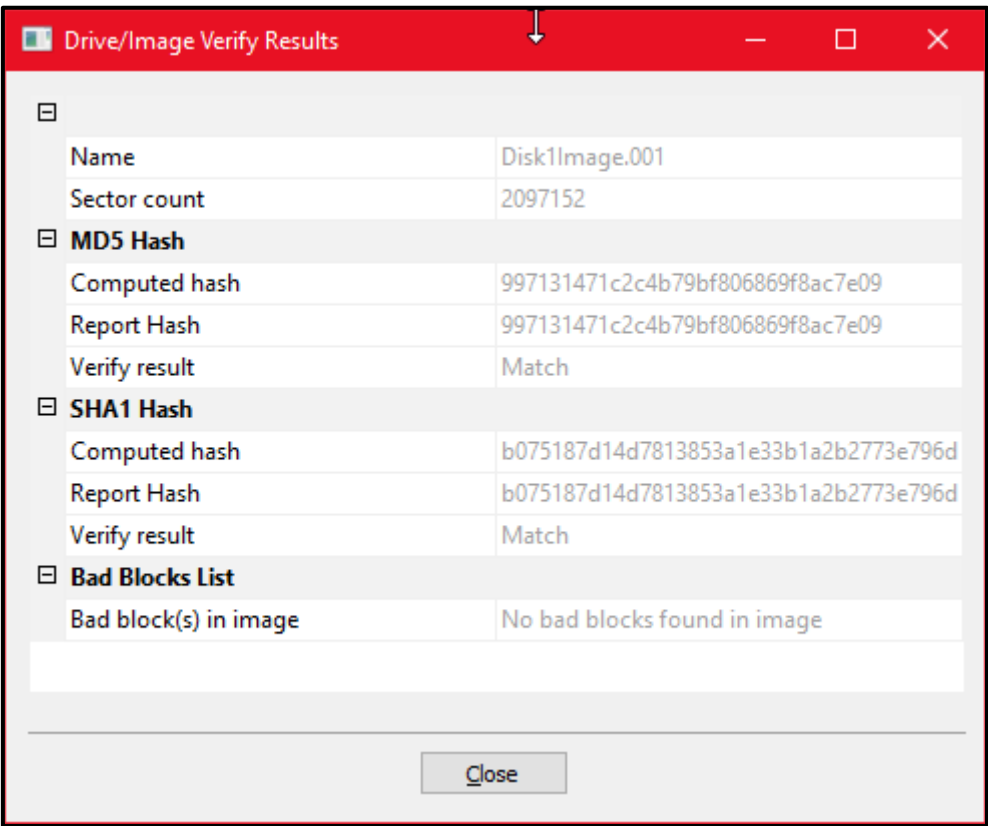
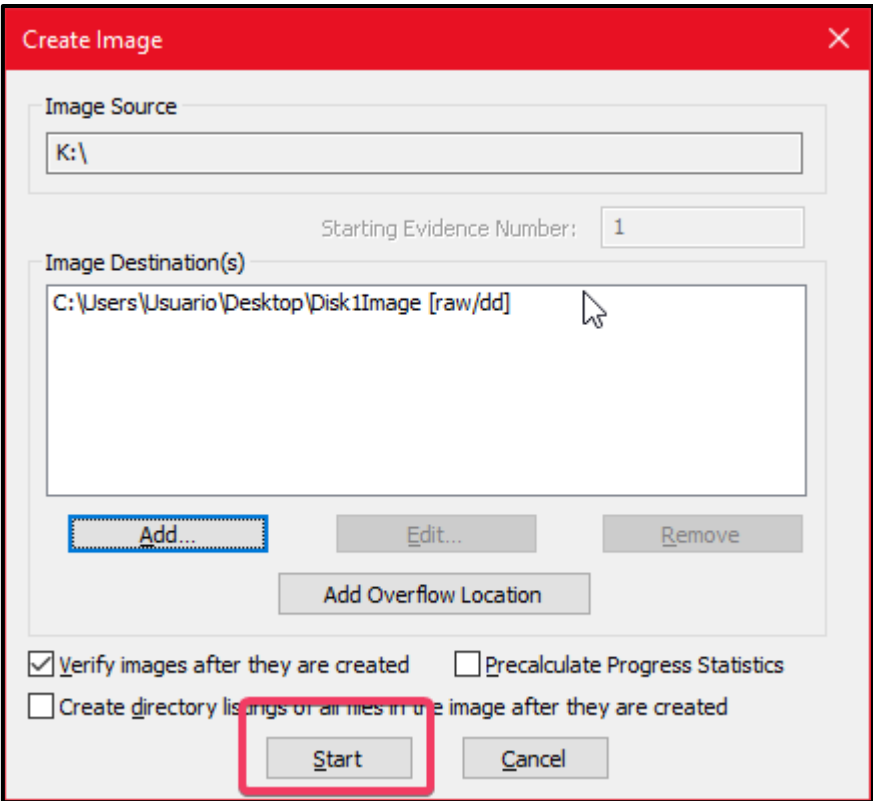
Image Filename (Excluding Extension)

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

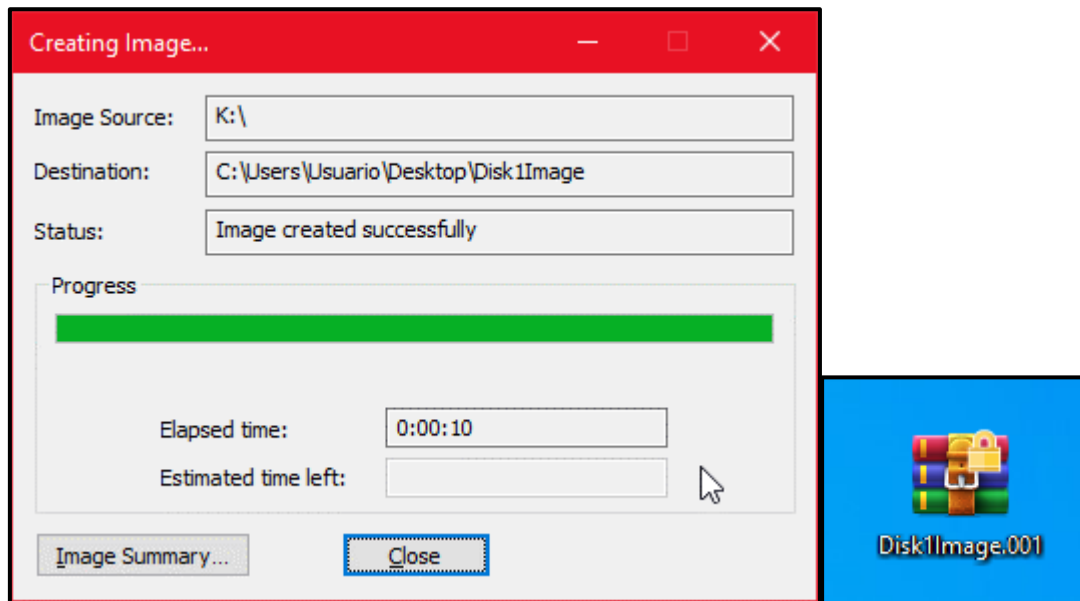
Compression (0=None, 1=Fastest, ..., 9=Smallest)

Use AD Encryption ☐

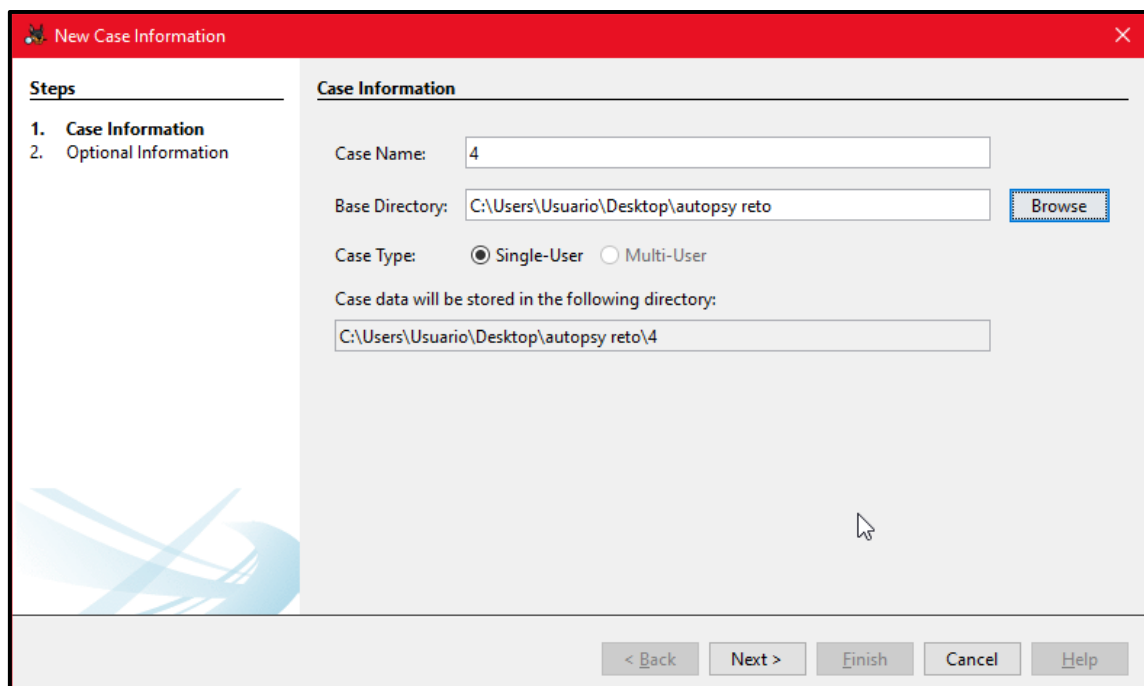
< Atrás **Finish** Cancel Help

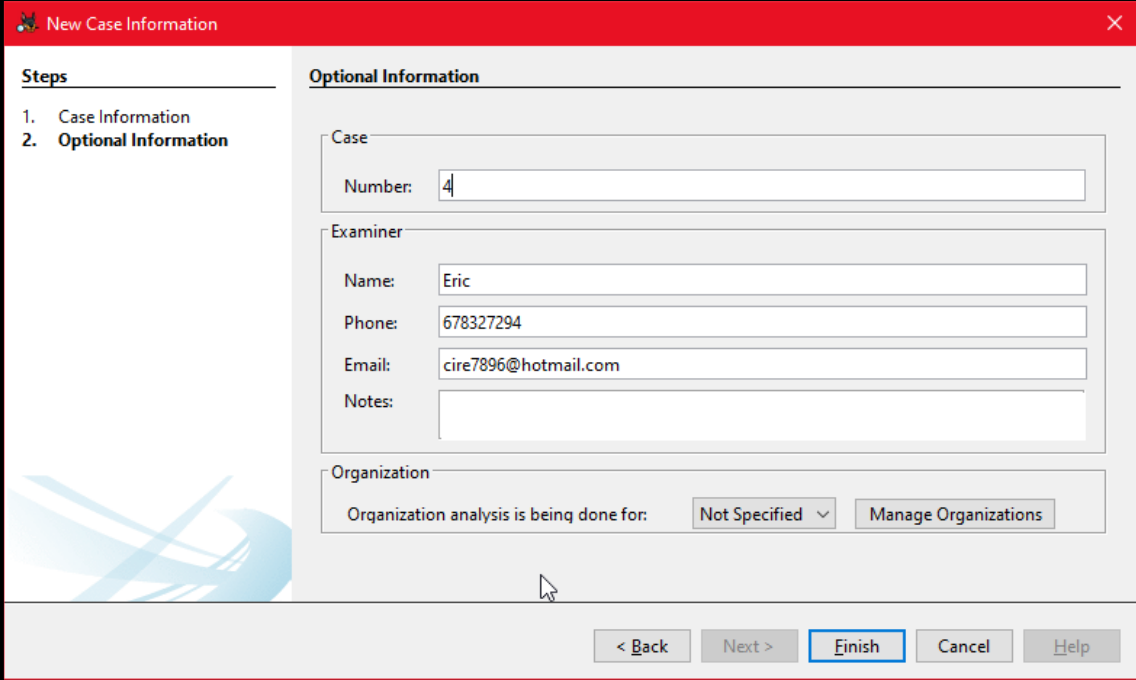


Ya tendríamos nuestra imagen.



7. Mediante Autopsy conseguir ÚNICAMENTE los archivos borrados y los archivos sospechosos de haber sido modificada su extensión.





New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number:

Examiner

Name:

Phone:

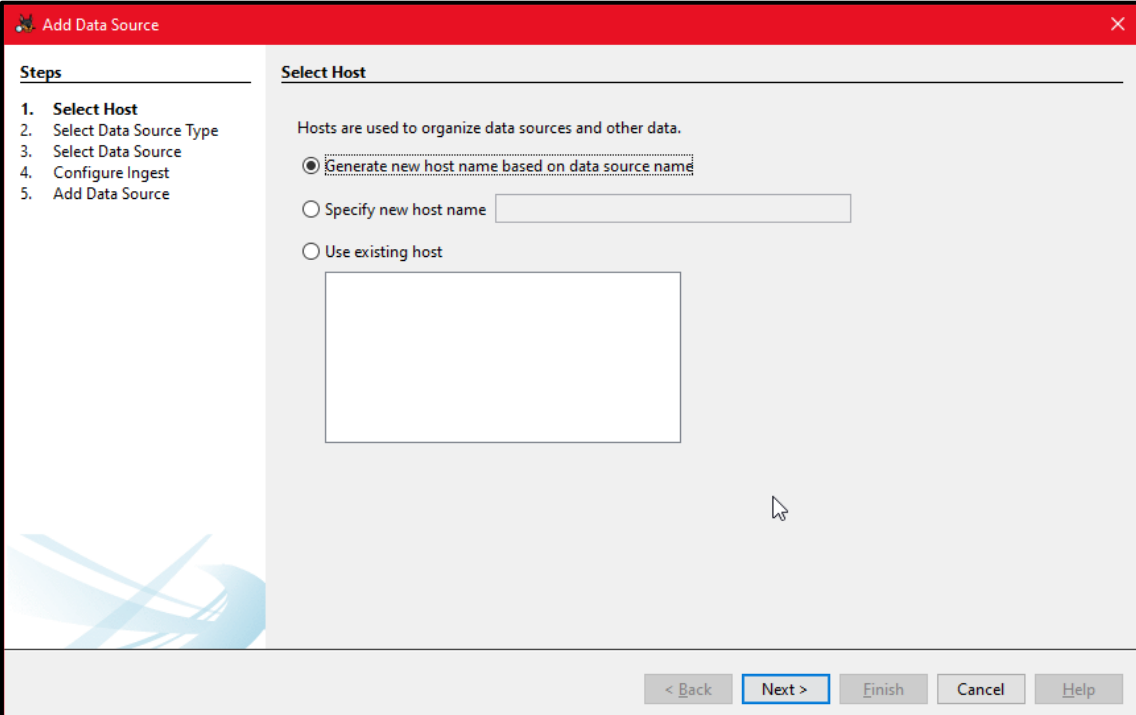
Email:

Notes:

Organization

Organization analysis is being done for:

< Back Next > **Finish** Cancel Help



Add Data Source

Steps

1. **Select Host**
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

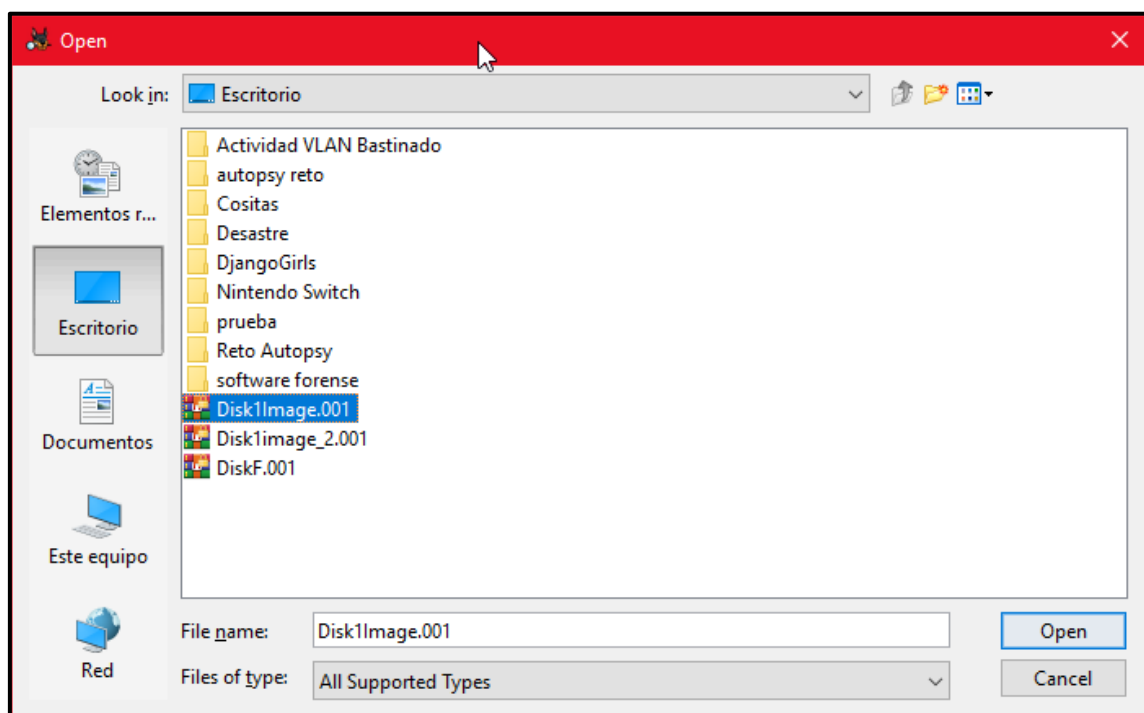
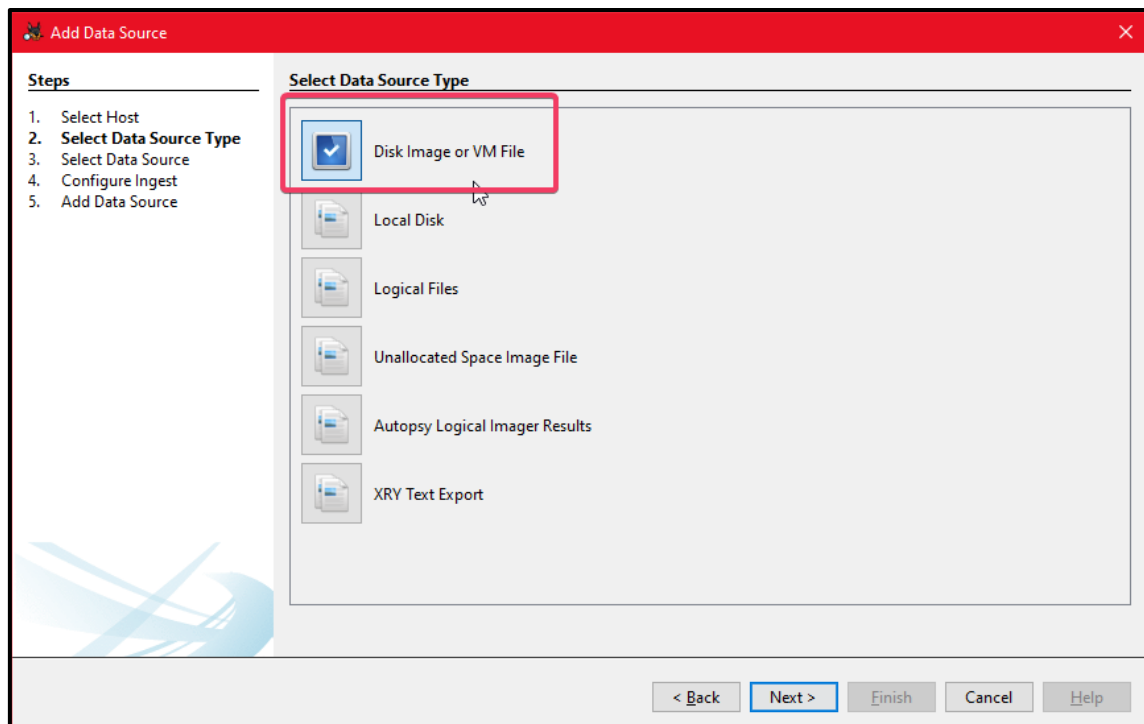
Hosts are used to organize data sources and other data.

☒ Generate new host name based on data source name

☐ Specify new host name

☐ Use existing host

< Back **Next >** Finish Cancel Help

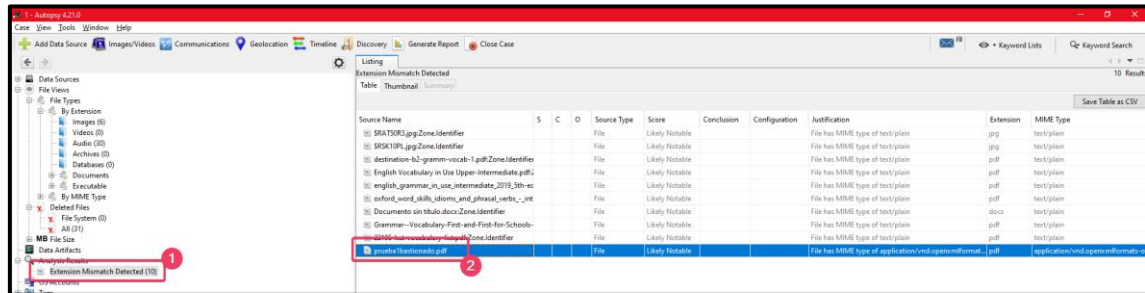


The screenshot shows the 'Add Data Source' window with the 'Select Data Source' step active. The 'Steps' list on the left includes: 1. Select Host, 2. Select Data Source Type, 3. **Select Data Source**, 4. Configure Ingest, and 5. Add Data Source. The 'Path' field contains 'C:\Users\Usuario\Desktop\Disk1Image.001' with a 'Browse' button. There is an unchecked checkbox for 'Ignore orphan files in FAT file systems'. The 'Time zone' is set to '(GMT+ 1:00) Europe/Madrid' and 'Sector size' is 'Auto Detect'. Under 'Hash Values (optional)', there are empty input fields for MD5, SHA-1, and SHA-256. A note states: 'NOTE: These values will not be validated when the data source is added.' At the bottom are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

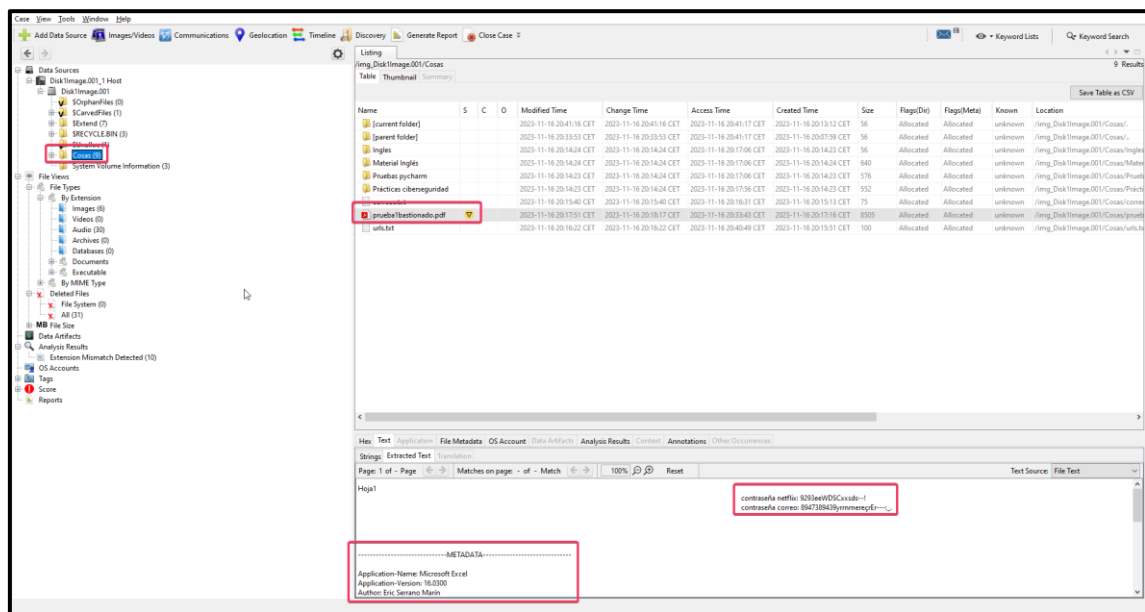
- Extension Missmatch: Para identificar extensiones que no coinciden con el archivo.
- PhotoRec Carver: Para los archivos eliminados.
- Picture Analyzer: Para poder ver el EXIF de la imagen.

The screenshot shows the 'Add Data Source' window with the 'Configure Ingest' step active. The 'Steps' list on the left includes: 1. Select Host, 2. Select Data Source Type, 3. Select Data Source, 4. **Configure Ingest**, and 5. Add Data Source. The 'Run ingest modules on:' dropdown is set to 'All Files, Directories, and Unallocated Space'. A list of modules is shown with checkboxes: Recent Activity, Hash Lookup, File Type Identification, **Extension Mismatch Detector** (highlighted with a red box), Embedded File Extractor, **Picture Analyzer** (highlighted with a blue box), Keyword Search, Email Parser, Encryption Detection, Interesting Files Identifier, **PhotoRec Carver** (highlighted with a red box), and Virtual Machine Extractor. At the bottom of the list are buttons for 'Select All', 'Deselect All', and 'History'. On the right, a text box states: 'The selected module has no per-run settings.' Below it, a description for the selected module reads: 'Performs general analysis on picture files, including ex...'. A 'Global Settings' button is at the bottom right. At the bottom of the window are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

En Extension Mismatch Detected, aparecen 10, uno de ellos es el que nosotros hemos cambiado de Excel a pdf.



Si nos vamos a la ubicación del archivo podremos ver lo siguiente:



La foto podemos encontrarla en la papelera, como podemos observar nos aparece la ubicación donde se ha tomado mi foto.

The screenshot displays the Autopsy forensic tool interface. At the top, there are tabs for 'File', 'Metadata', and 'Summary'. Below these, a table lists the source file: 'IMG_20231116_210233.jpg' with a source type of 'File'. The main panel shows the file's metadata, including its name, aggregate score, and two analysis results. The first analysis result, 'Analysis Result 1', provides detailed EXIF metadata such as altitude, creation date, device make, device model, latitude, and longitude. The second analysis result, 'Analysis Result 2', indicates that EXIF metadata exists for the file.

Source Name	S	C	O	Source Type	Score
IMG_20231116_210233.jpg				File	Not Notable

Item: IMG_20231116_210233.jpg
Aggregate Score: Not Notable

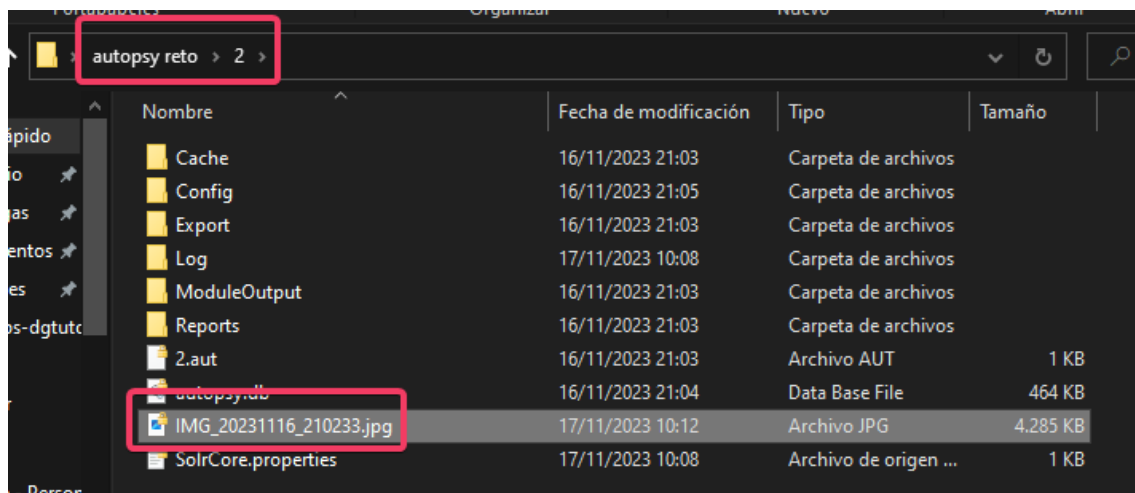
Analysis Result 1

Score: Not Notable
Type: EXIF Metadata
Configuration:
Conclusion:
Altitude: 93.2
Date Created: 2023-11-16 22:02:35 CET
Device Make: Xiaomi
Device Model: Mi 9 SE
Latitude: 37.66069397222222
Longitude: -5.520857

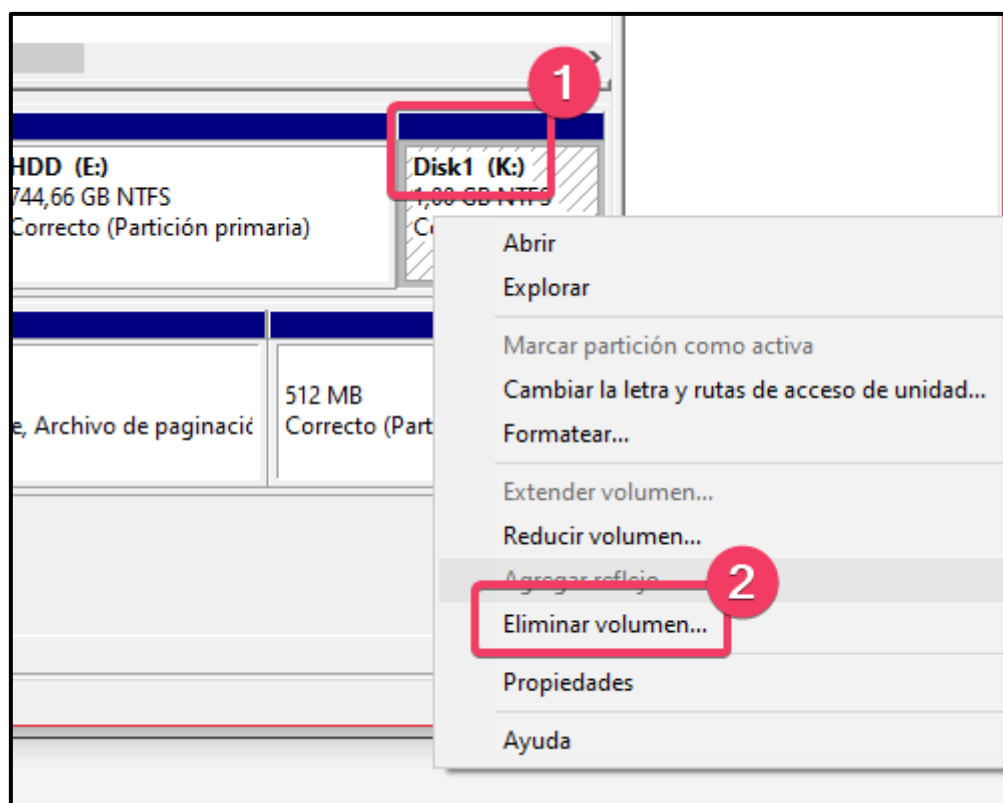
Analysis Result 2

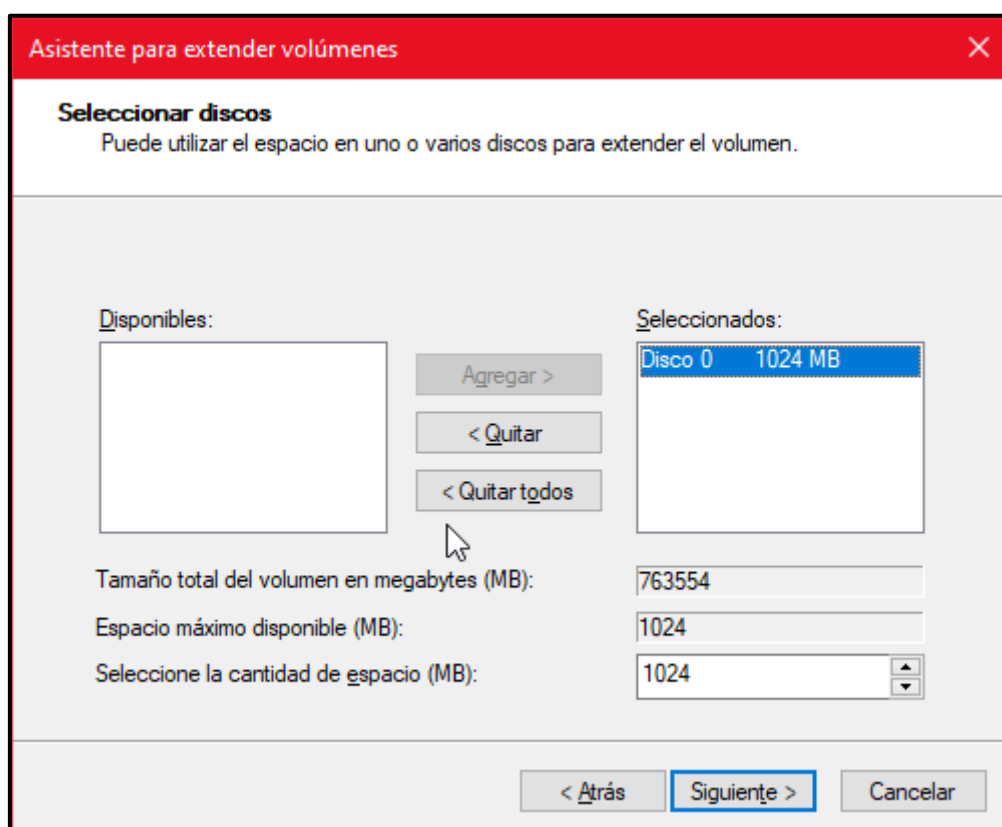
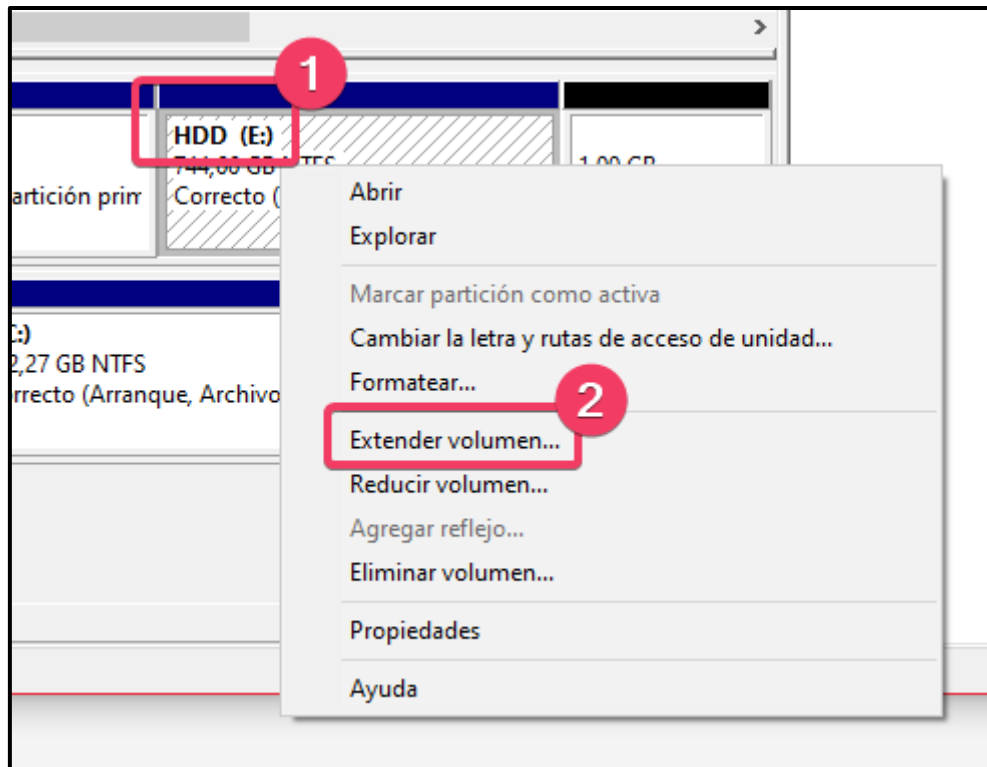
Score: Unknown
Type: User Content Suspected
Configuration:
Conclusion:
Comment: EXIF metadata data exists for this file.

Para recuperar la imagen clic derecho, extract y elegir donde quieres guardarla.



8. Eliminar la partición de 1GB y vuelva a insertarla en su partición original.

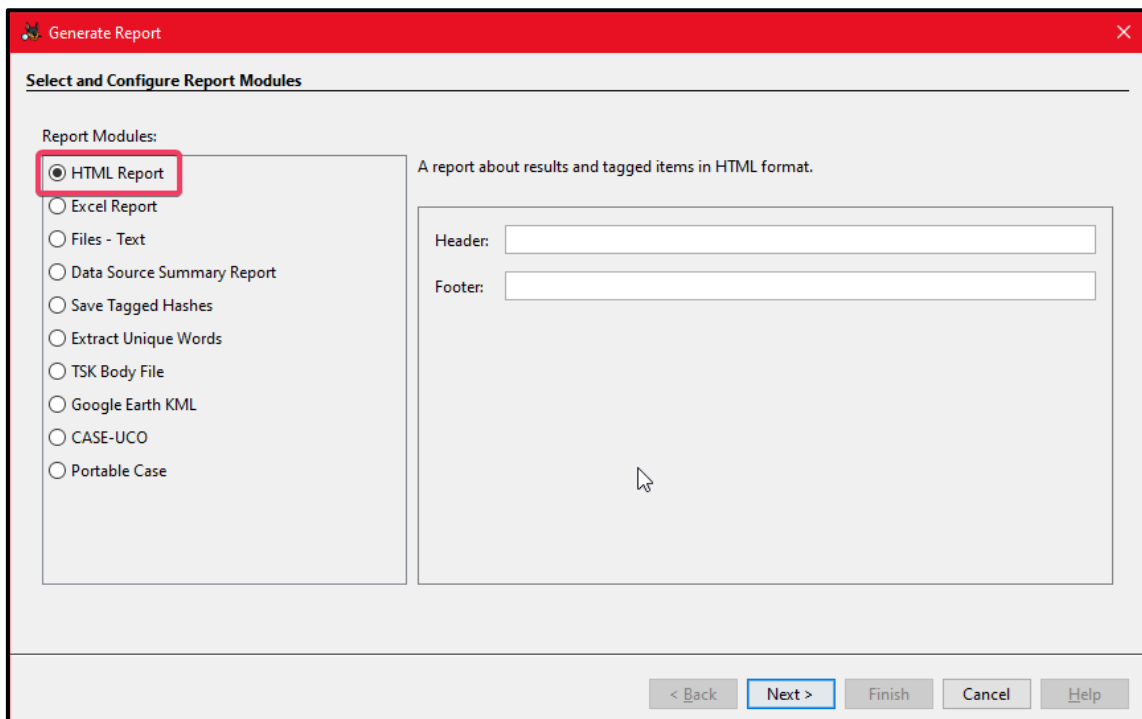
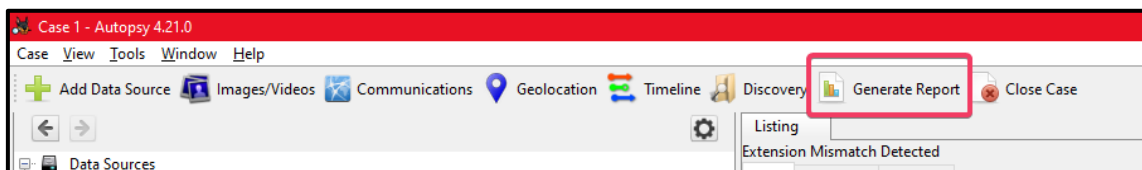




Y ya tendríamos la partición borrada y de vuelta a su partición original.

Disco 0 Básico 921,51 GB En pantalla	185,95 GB Correcto (Activo, Partición primaria)	HDD (E3) 745,66 GB NTFS Correcto (Partición primaria)
Disco 1 Básico 232,87 GB En pantalla	100 MB Correcto (Partición de sistema EFI)	IC3 232,27 GB NTFS Correcto (Arranque, Archivo de paginación, Volcado, Partición de datos básicos)
		512 MB Correcto (Partición de recuperación)

9. Generar un informe con Autopsy donde se refleje el análisis forense de lo sucedido. Detallar paso a paso en un documento.



Generate Report

Configure Report

Select which data to report on:

☒ All Results

☐ All Tagged Results

☐ Specific Tagged Results

Select All

Deselect All

Choose Result Types...

< Back

Next >

Finish

Cancel

Help

Report Generation Progress...

Complete

HTML Report : C:\Users\Usuario\Desktop\Case 1\Reports\Case 1 HTML Report 11-18-2023-02-07-40\report.html

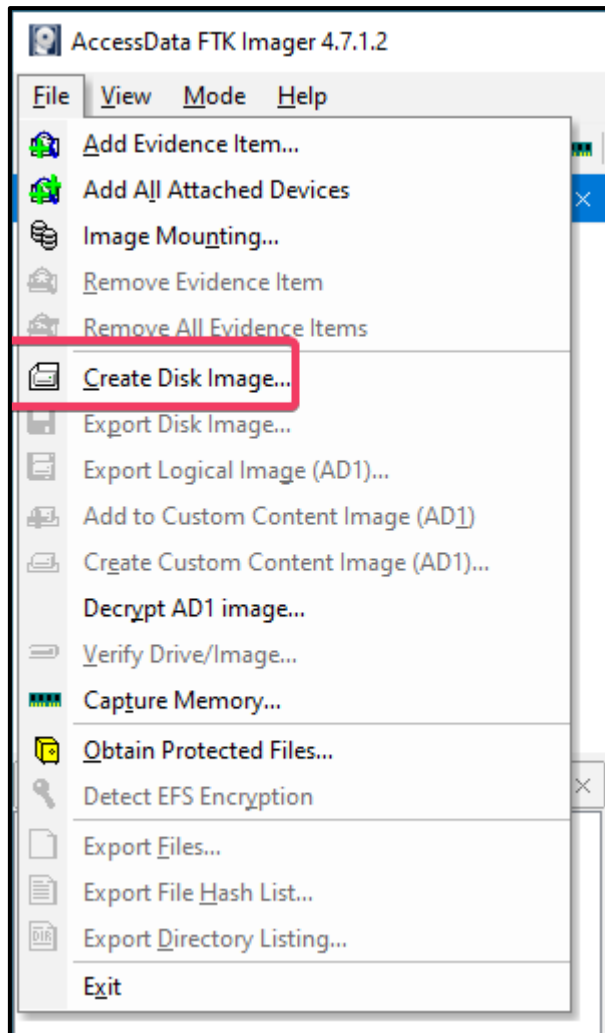
Complete

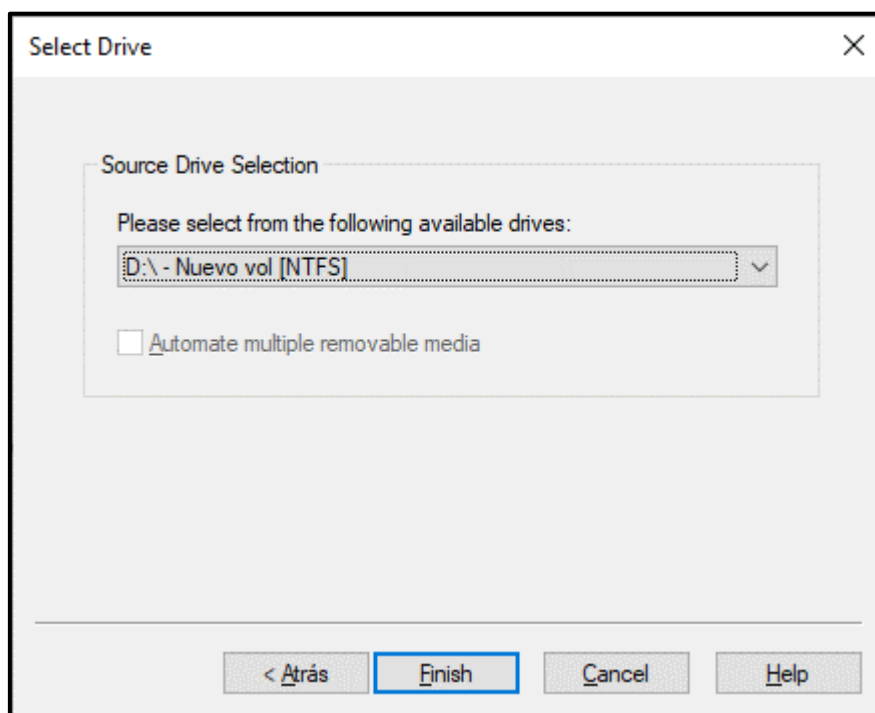
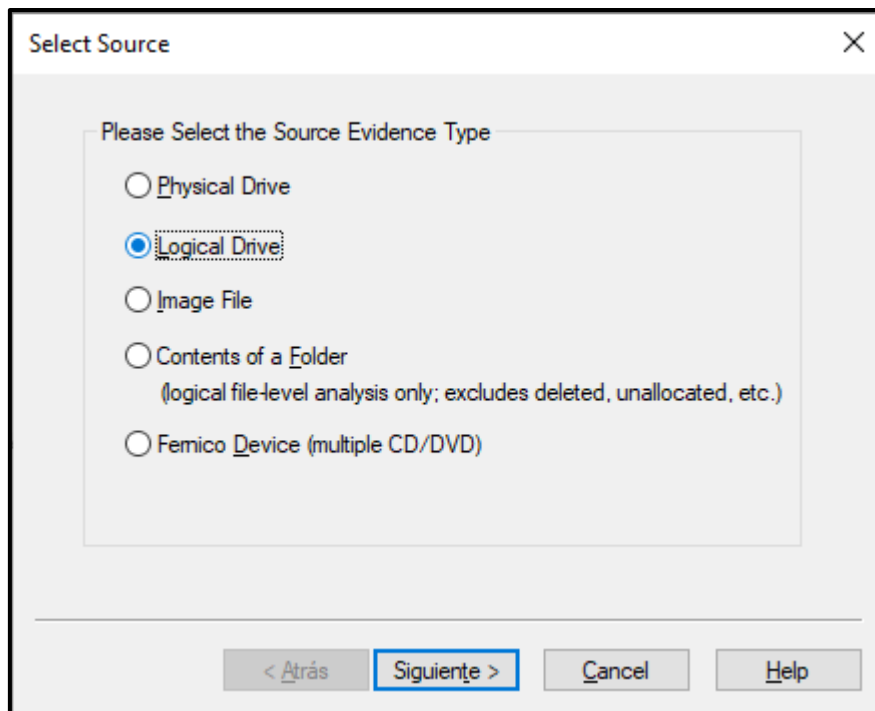
Cancel

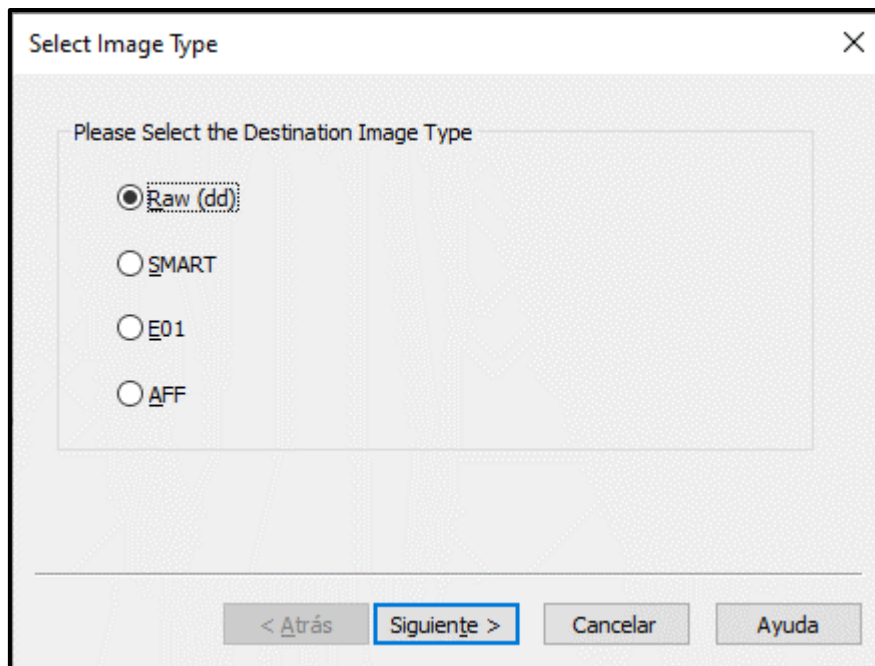
Close

Ejercicio 2

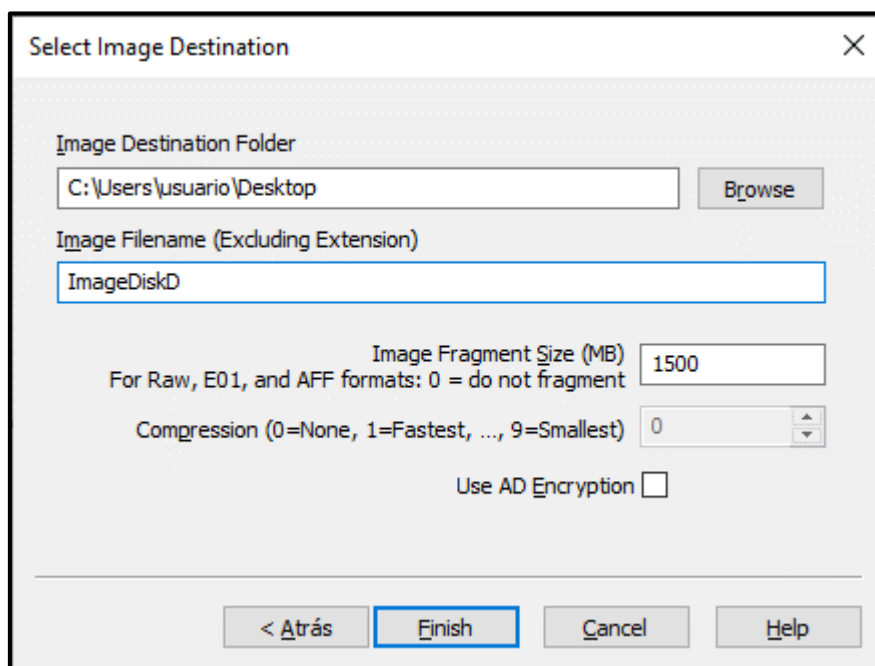
1. Creación de imagen del disco duro de 5GB.



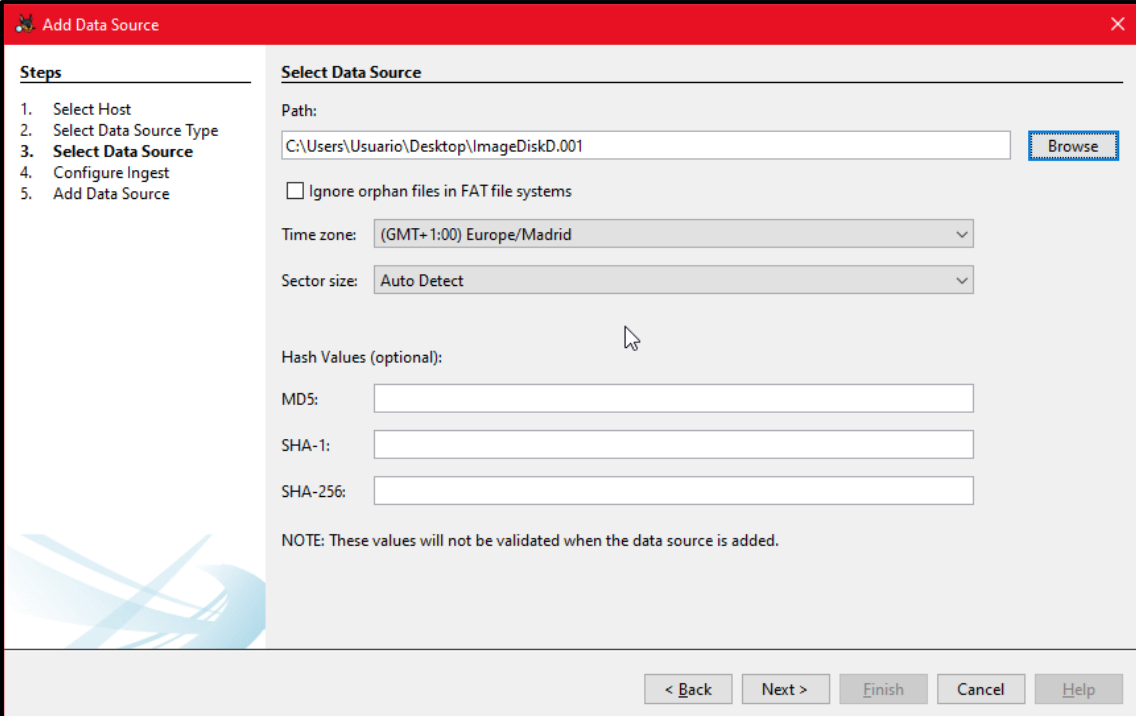




Después de este paso ya tendríamos nuestra imagen ImageDiskD.001.



2. Usar autopsy para encontrar la imagen.

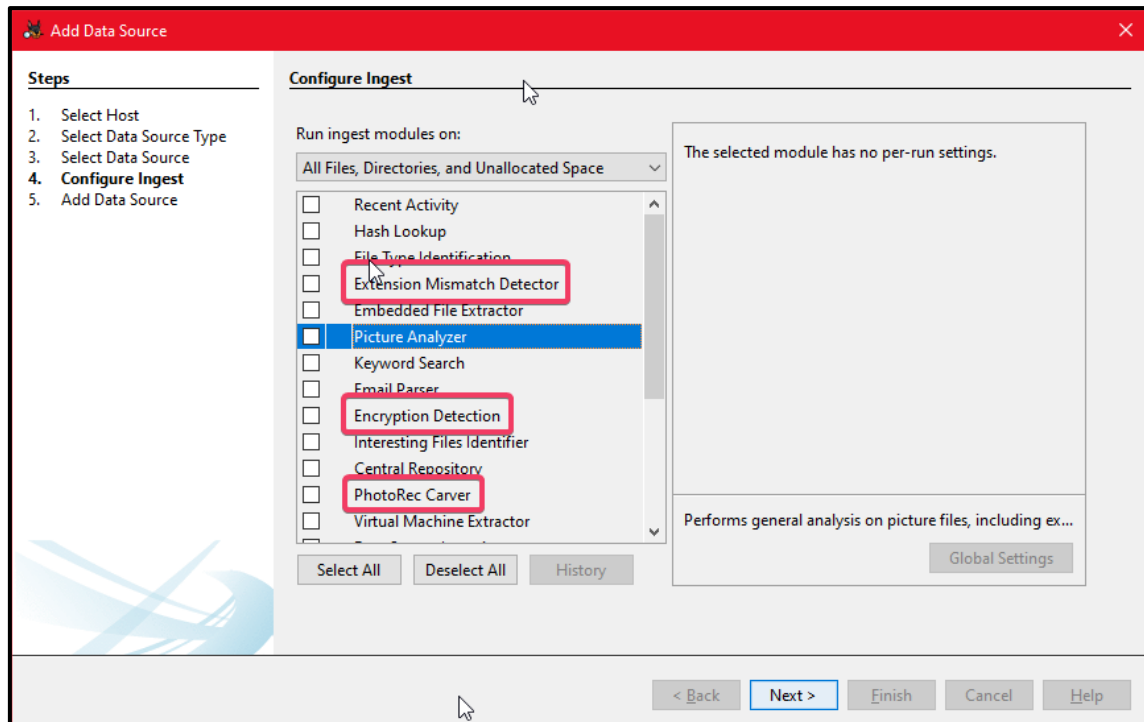


The screenshot shows the 'Add Data Source' window in the Autopsy software. The window has a red title bar with the text 'Add Data Source' and a close button. On the left, there is a 'Steps' panel with a list of five steps: 1. Select Host, 2. Select Data Source Type, 3. **Select Data Source** (highlighted), 4. Configure Ingest, and 5. Add Data Source. The main area is titled 'Select Data Source' and contains the following fields and options:

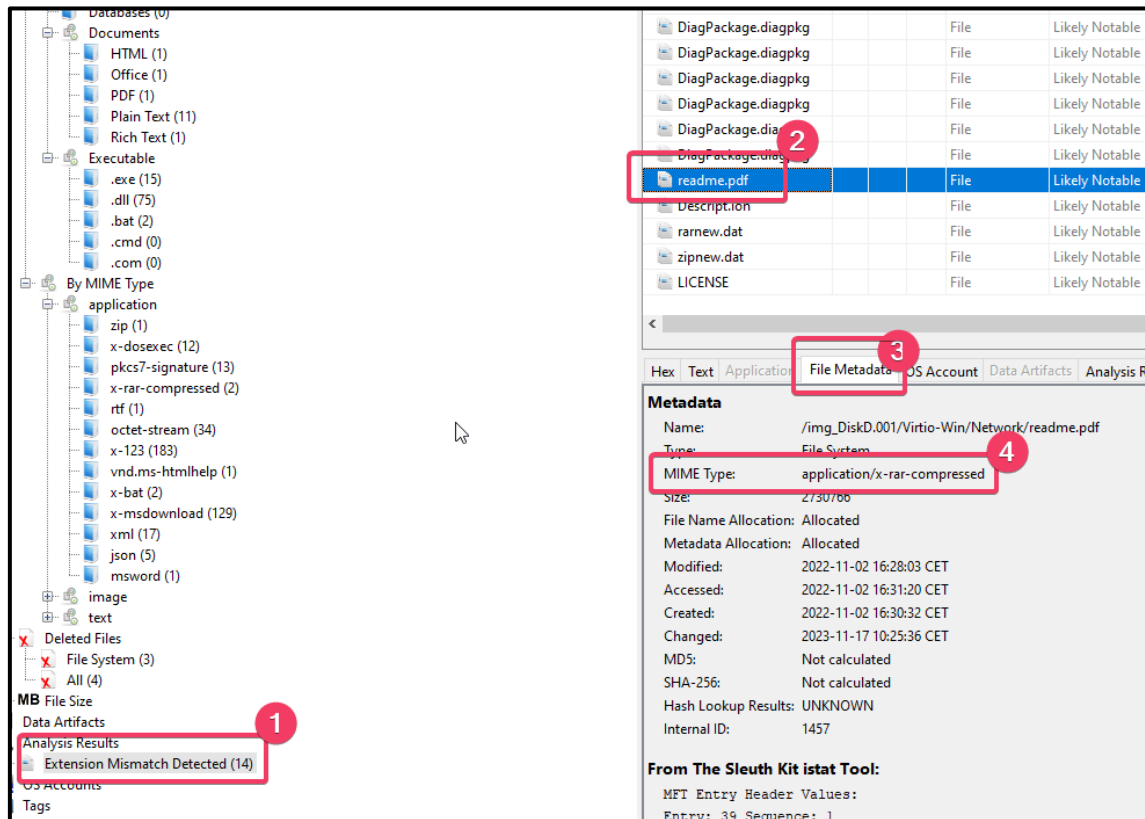
- Path:** A text box containing 'C:\Users\Usuario\Desktop\ImageDiskD.001' and a 'Browse' button.
- ☐ Ignore orphan files in FAT file systems
- Time zone:** A dropdown menu showing '(GMT+ 1:00) Europe/Madrid'.
- Sector size:** A dropdown menu showing 'Auto Detect'.
- Hash Values (optional):** Three text boxes for 'MD5:', 'SHA-1:', and 'SHA-256:'.
- NOTE:** These values will not be validated when the data source is added.

At the bottom of the window, there are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

- **Extension Mismatch Detector:** Para detectar extensiones que no sean del archivo.
- **Picture Analyzer:** Para saber EXIF y metada de la foto.
- **PhotoRec Carver:** Por si la imagen ha sido eliminada.
- **Encryption Detection:** Para detectar encriptación.



Con Extension Missmatch hemos encontrado este readme.pdf, que según File Metadata es un rar.



Al extraerlo a nuestro Escritorio le cambiamos la extensión a .rar.



Pero está protegido por contraseña, como no tenemos contraseña y sabemos que la contraseña que se ha usado para cifrar es la misma que la del usuario ciber, vamos a intentar sacar la contraseña.

3. Encontrar los hashes de las contraseñas del usuario ciber.

Usamos pwdump8.exe para saber los hashes de los usuarios.

```

C:\Users\usuario\Desktop\pwdump\pwdump8-8.2>dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: E402-C872

Directorio de C:\Users\usuario\Desktop\pwdump\pwdump8-8.2
17/11/2023  11:06    <DIR>          .
17/11/2023  11:06    <DIR>          ..
17/07/2020  14:44    <DIR>          pwdump8
                0 archivos                0 bytes
                3 dirs      8.563.081.216 bytes libres

C:\Users\usuario\Desktop\pwdump\pwdump8-8.2>cd pwdump8
C:\Users\usuario\Desktop\pwdump\pwdump8-8.2\pwdump8>pwdump8.exe

Pwdump v8.2 - dumps windows password hashes - by Fulvio Zanetti & Andrea Petralia @ http://www.blackMath.it

Administrador:500:AAD3B435B51404eeaAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
Invitado:501:AAD3B435B51404eeaAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
DefaultAccount:503:AAD3B435B51404eeaAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
WDAGUtilityAccount:504:AAD3B435B51404eeaAD3B435B51404EE:DDE136F209D537A893888D7EC7D8C76B
usuario:1001:AAD3B435B51404eeaAD3B435B51404EE:F2AB082FA1B21C772FEA4193D454D7B0
ciber:1002:AAD3B435B51404eeaAD3B435B51404EE:CEB9AFACDAF52F05BD7AAF66DA973D34

C:\Users\usuario\Desktop\pwdump\pwdump8-8.2\pwdump8>
  
```

4. Sacar la contraseña del hash con john the Ripper y extraer el .rar.

Copiaremos el hash en un .txt, lo copiaremos tal y como vemos en la captura. Después usaremos el comando john.exe y le añadiremos el .txt

```

C:\Users\Usuario\Desktop\john-1.9.0-jumbo-1-win64\john-1.9.0-jumbo-1-win64>run:john.exe C:\Users\Usuario\Desktop\hash.txt
Warning: detected hash type "NT", but the string is also recognized as "NT-opencl"
Use the "--format=NT-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 20 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 1 candidate buffered for the current salt, minimum 24 needed for performance.
Warning: Only 23 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 21 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 13 candidates buffered for the current salt, minimum 24 needed for performance.
ciber22 (ciber)
ig 0.00.00.00 DONE 1/3 (2023-11-17 13:48) 142.8g/s 62857p/s 62857c/s 62857C/s ciber81..Ciber74
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed

C:\Users\Usuario\Desktop\john-1.9.0-jumbo-1-win64\john-1.9.0-jumbo-1-win64>run>
  
```

hash.txt: Bloc de notas

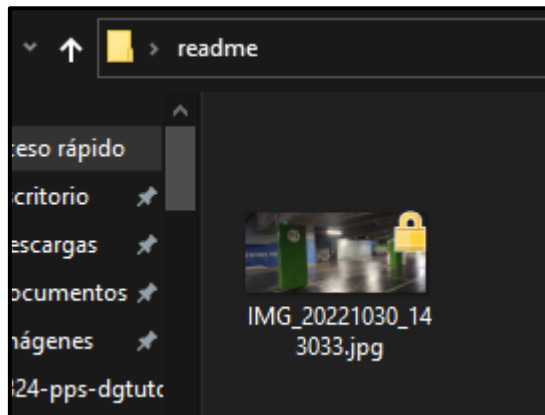
Archivo Edición Formato Ver Ayuda

ciber:1002::CEB9AFACDAF52F05BD7AAF66DA973D34

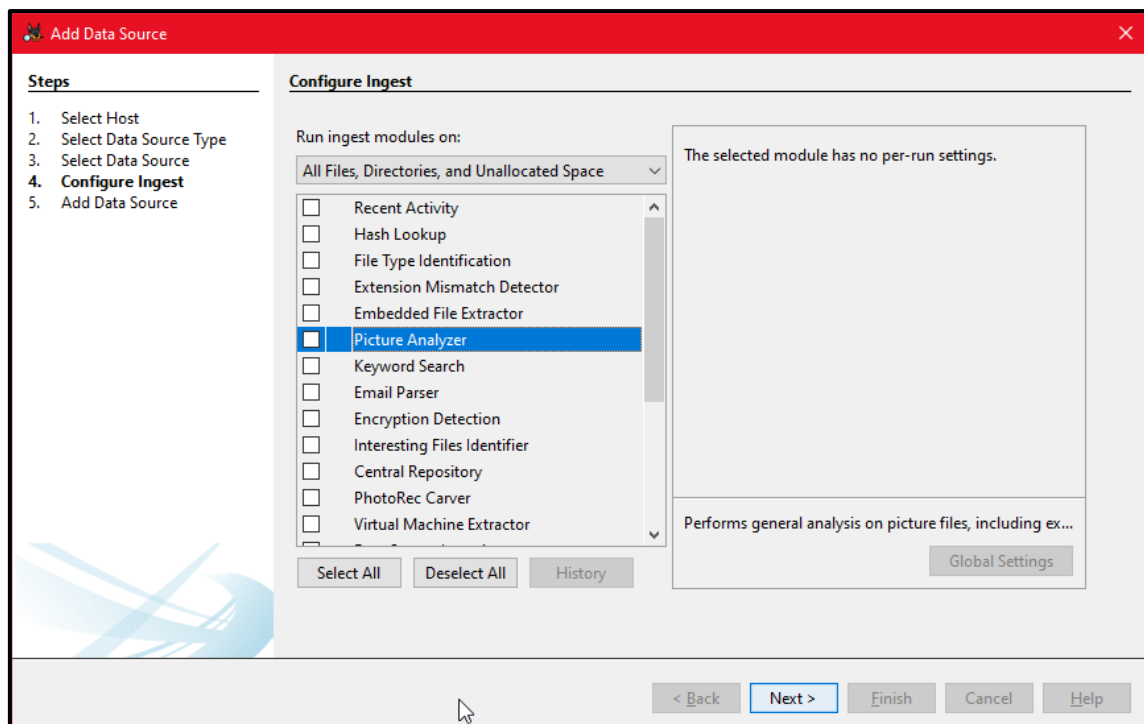
Como podemos observar nos ha sacado la **contraseña ciber22**, por lo que ya podremos abrir el .rar.

5. Usaremos autopsy para averiguar donde se realizó la imagen.

Podemos observar que es la foto que estábamos buscando.



Vamos a seleccionar Picture Analyzer.



Podemos observar que gracias al modulo Picture Analyzer sabemos las coordenadas donde se tomó la foto.

The screenshot displays the Autopsy software interface. On the left, the 'File Views' pane shows a hierarchical tree of file types. Under 'Analysis Results', 'EXIF Metadata (1)' is highlighted. The main pane on the right shows a table with the file 'IMG_20221030_143033.jpg' selected. Below the table, the 'Analysis Result 1' section provides detailed EXIF data for the image.

Source Name	S	C	O	Source T
IMG_20221030_143033.jpg				File

Item: IMG_20221030_143033.jpg
Aggregate Score: Not Notable

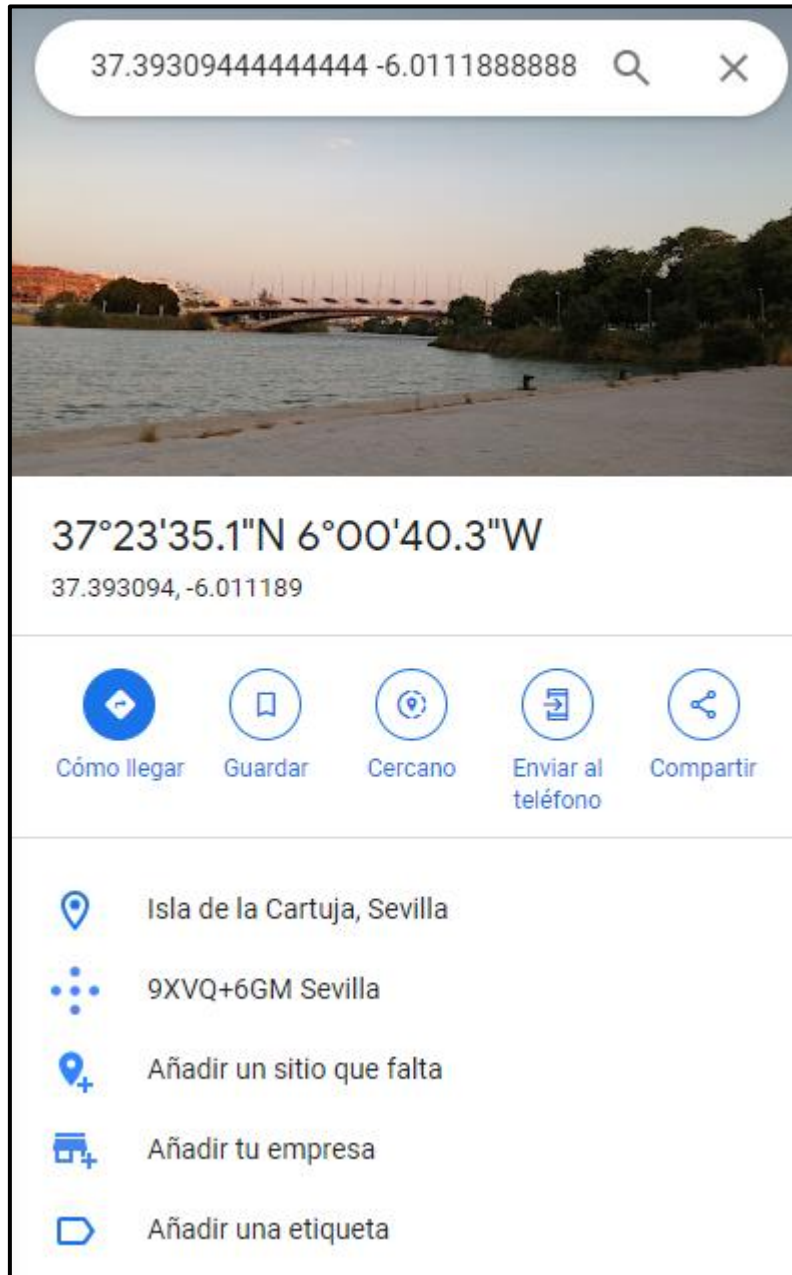
Analysis Result 1

Score: Not Notable
Type: EXIF Metadata
Configuration:
Conclusion:
Altitude: 0.0
Date Created: 2022-10-30 15:30:34 CET
Device Make: Xiaomi
Device Model: M2007J20CG
Latitude: 37.39309444444444
Longitude: -6.011188888888885

Analysis Result 2

Score: Unknown
Type: User Content Suspected
Configuration:

Si ponemos las coordenadas en Google maps nos dice que es Isla de la Cartuja, Sevilla.



6. Guardar en todo momento la cadena de custodia del análisis forense a realizar.

Cadena de Custodia para Análisis Forense.

Información general:

- Nombre del Caso: Análisis Forense de PC con 2 discos duros
- Fecha de Inicio: 18/11/2023
- Fecha de Finalización: 18/11/2023
- Persona Responsable del Análisis: Eric Serrano Marín

Descripción de la Evidencia:

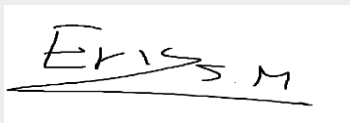
- Tipo de Evidencia: Sistema Operativo y Datos del Disco Duro de 5GB
- Descripción Detallada de los Datos: Sistema Operativo, Usuarios (Administrador, Usuario, Ciber, Invitado), Disco Duro de 5GB con información diversa.
- Ubicación y Estado Inicial de la Evidencia: PC con 2 discos duros, estado inicial al inicio del análisis.

Registro de Acciones y Actividades:

Fecha y Hora	Acción Realizada	Persona Responsable	Observaciones
10:00	Inicio del Análisis Forense	Eric Serrano Marín	Inicio del proceso de análisis en el PC objetivo
10:10	Adquisición de la evidencia	Eric Serrano Marín	Creación de copias forenses de los discos duros
10:30	Búsqueda de imagen	Eric Serrano Marín	Uso de Autopsy
10:45	Recopilación de HASH de usuarios.	Eric Serrano Marín	Obtención de HASHES con pwdump

11:15	Contraseña de usuario user	Eric Serrano Marín	Uso de John the Ripper
11:30	Análisis de Archivos y Metadata	Eric Serrano Marín	Búsqueda de la fotografía y metadatos relevantes.
11:40	Identificación de la Fotografía	Eric Serrano Marín	Identificación y verificación de la fotografía específica
12:00	Determinación del Lugar de la Fotografía	Eric Serrano Marín	Localización geográfica identificada a través de datos EXIF
12:15	Fin del Análisis Forense	Eric Serrano Marín	Conclusión del análisis y cierre del proceso

Registro de Firmas:

Nombre de la Persona	Firma	Fecha
Eric Serrano Marín		18/11/2023

Observaciones finales:

- Conclusiones del Análisis: Identificación de la fotografía y su ubicación geográfica.
- Estado Final de la Evidencia: Evidencia analizada y conclusiones obtenidas.
- Nombre del Responsable: Eric Serrano Marín.
- Fecha de Finalización: 18/11/2023