“Universidad Internacional de La Rioja en México”

Informática Forense y Respuesta ante Incidentes

Proyecto:

Actividad 1: Adquisición de evidencias digitales

Profesor:

OSCAR MANUEL LIRA

Autor:

Juan Luis Cruz Aristeo.

Fecha de entrega:

17/06/2024

Adquisición de evidencias digitales.

Introducción

El objetivo de esta práctica es realizar la adquisición de forense de un dispositivo de almacenamiento externo, para poder comprender la importancia de lo que es la adquisición forense en una investigación, pues garantiza la preservación de la integridad y la autenticidad de evidencia digital, lo que permite su análisis sin alteraciones.

Para llevar a cabo este proceso se hace uso de técnicas y herramientas, proporcionadas por el docente de la materia de Informática Forense y Respuesta ante Incidentes. Este informe detalla cada paso realizado en el proceso de adquisición, como fueron utilizadas las herramientas, los resultados obtenidos y las medidas tomadas para verificar la integridad de las imágenes forenses generadas.

Procedimiento

Paso 1. Adquisición de herramientas

- Descargar e instalar FTK
- Descargar e instalar MD5summer.

Paso 2. Creación de archivos para guardar nuestras evidencias.

- Crear una carpeta con el nombre de UNIR en un lugar seguro dentro de nuestra PC, dentro de esta carpeta se crearán 3 carpetas con los siguientes nombres.
  1. Forense
  2. RAM
  3. Recuperados

Paso 3. adquisición en caliente del contenido de la memoria RAM

- Ejecutar FTK
- Buscamos el icono de (capture memory).
- Seleccionamos la ubicación en donde guardaremos el contenido, en este caso será en la carpeta de RAM, dentro de la carpeta UNIR.
- Le daremos el nombre de UNIR.mem.

Paso 4. Obtención del numero identificador HASH.

- Ejecutamos la herramienta MD5summer.
- Localizaremos nuestro archivo UNIR.mem dentro de la carpeta RAM, Seleccionamos la carpeta RAM y damos click en el botón Create Sums.
- Clic en add y luego ok
- Guardamos en la misma carpeta RAM

Paso 5. Obtención de evidencia de la Unidad Externa.

- Conectamos nuestra USB.
- Nos dirigimos a FTK y buscamos el icono de Add Evidence Item.
- Seleccionamos la opción de unidad física y damos siguiente.
- Seleccionamos la USB que conectamos.

Posteriormente de que carga el procedimiento anterior encontramos de lado izquierdo en la parte inferior las características particulares de nuestra UBS.

En la parte superior encontramos la información interna de la memoria, en el primer piso, seleccionamos Root, ahí encontraremos la información o contenido de nuestra memoria.

- Seleccionamos los documentos que queremos con la tecla CTRL, para seleccionar todos.
- Damos clic secundario y seleccionamos la opción de exportar archivos. Los colocamos en la carpeta de Recuperados, dentro de la carpeta UNIR.
- Volvemos a FTK y volvemos a seleccionas los archivos.
- Damos clic secundario y seleccionamos la opción de Export File Hash List

Paso 6. Creación de una imagen forense.

- Dentro de FTK debemos buscar el icono de Add Evidence Item
- Seleccionamos Image file
- Seccionamos Physical drive.
- Seleccionamos la USB
- Damos clic en ADD y seleccionamos E01 (Por cuestiones de seguridad)
- Llenamos los datos.
- Guardamos en la carpeta de forence.

Conclusión.

Conclusión

La adquisición forense es, sin lugar a dudas, una etapa crítica en cualquier investigación digital, ya que permite obtener evidencia sin alteraciones y de manera íntegra a lo largo de todo el proceso. Durante este procedimiento, se emplearon diversas técnicas de adquisición, ejecutando cada paso con extremo cuidado.

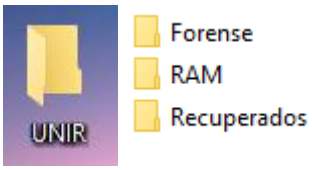
Es importante destacar que en la práctica utilizamos una USB de poco almacenamiento, lo cual fue útil para comprender el procedimiento sin consumir demasiado tiempo. Sin embargo, en un escenario real, donde se requiere la adquisición de un disco duro completo, el proceso puede durar varias horas, dependiendo del equipo utilizado para crear la imagen forense.

En definitiva, la adquisición forense es una herramienta fundamental en el ámbito de la ciberseguridad, proporcionando la base necesaria para una investigación efectiva y confiable.

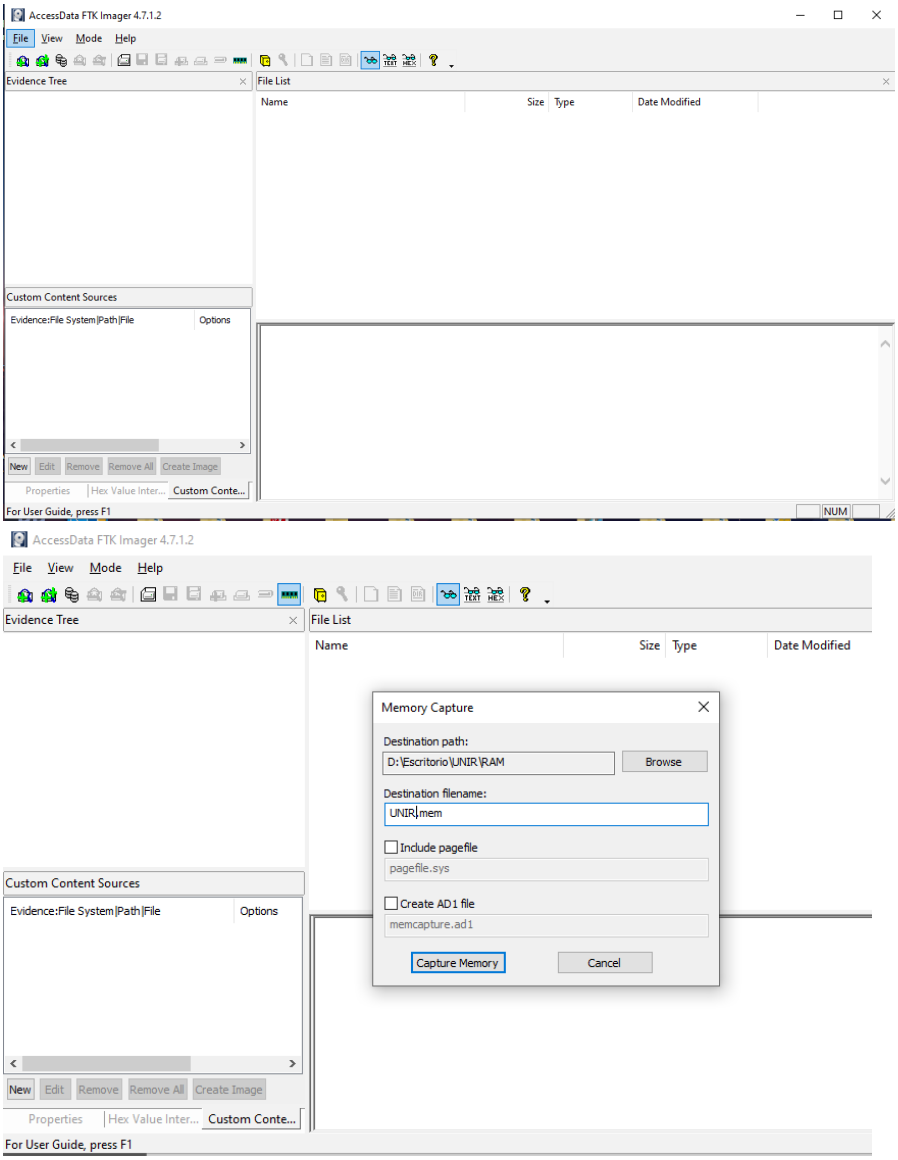
Evidencias:

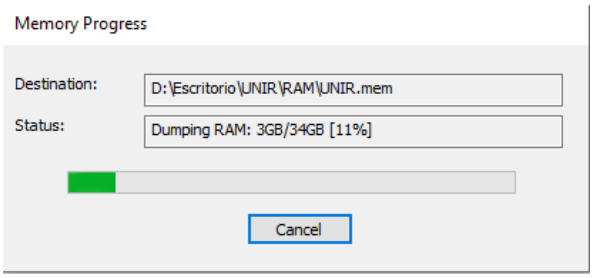
Paso 1: Adquisición de herramientas

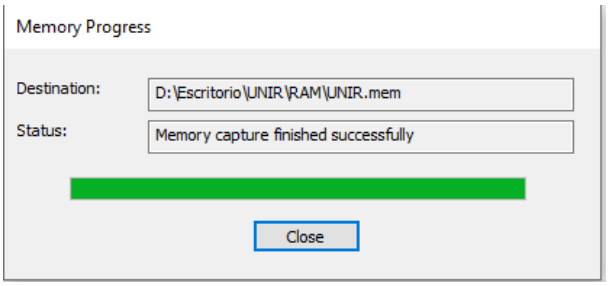
Paso 2: Creación de archivos para guardar nuestras evidencias.

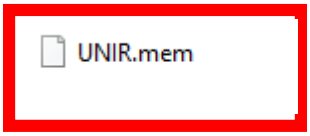


Paso 3: adquisición en caliente del contenido de la memoria RAM

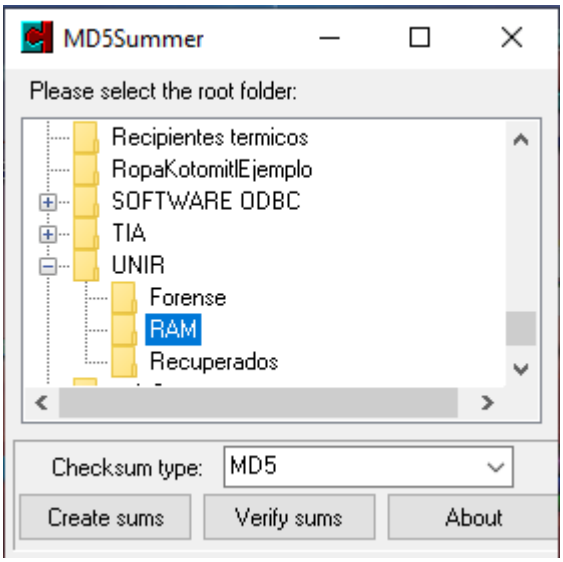


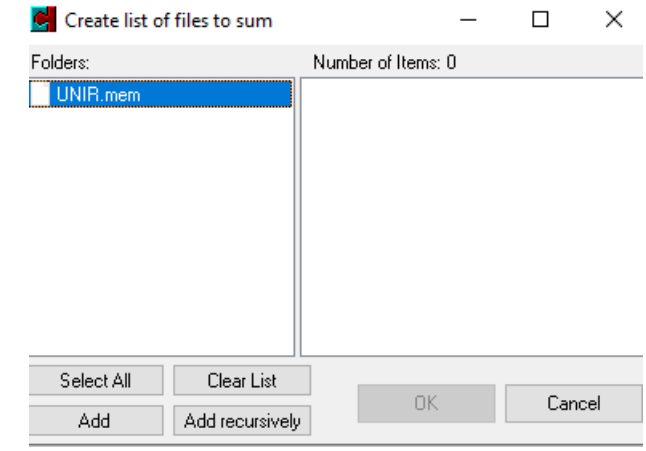


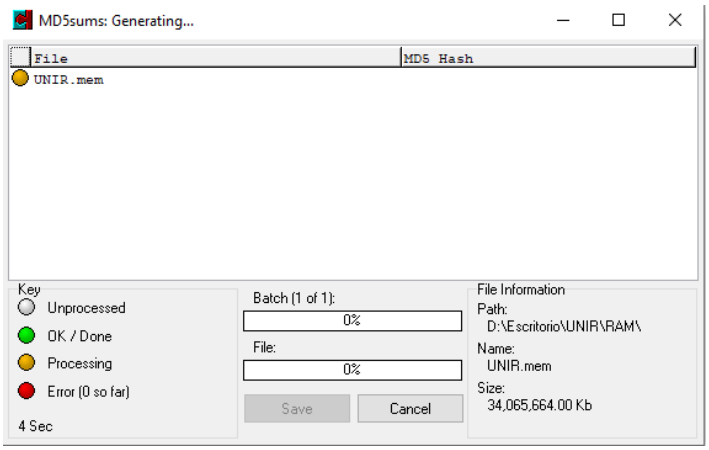


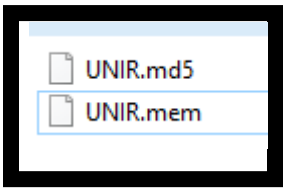


Paso 4: Obtención del numero identificador HASH.

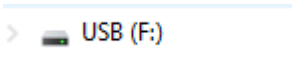


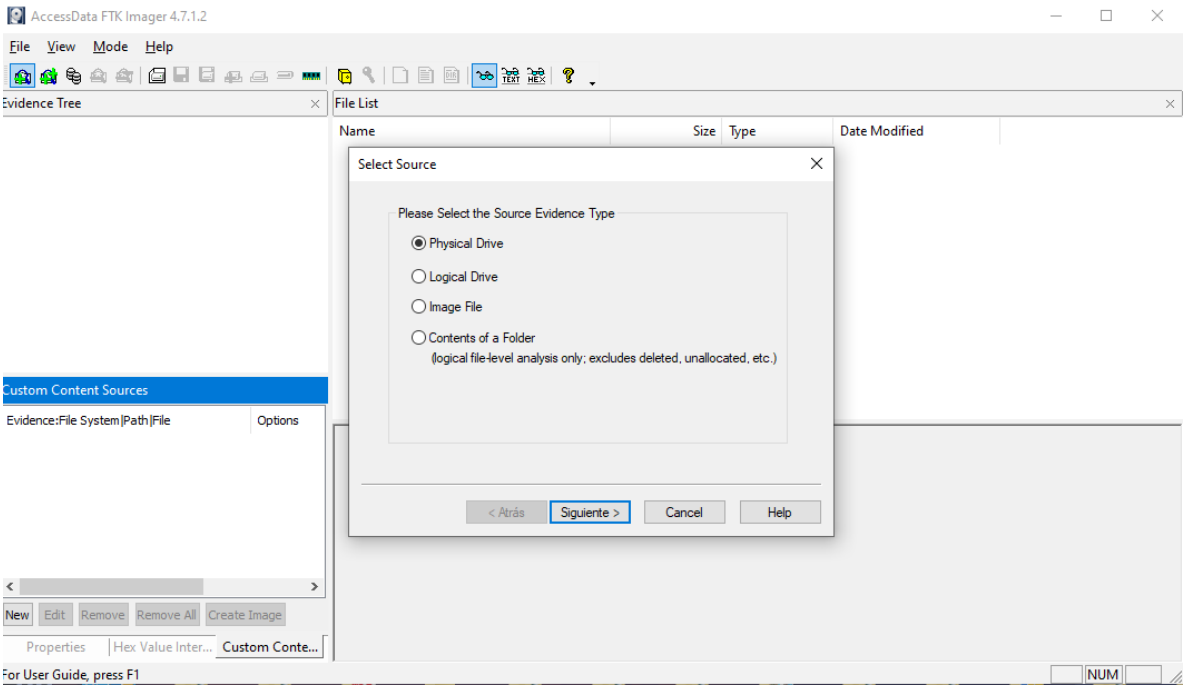


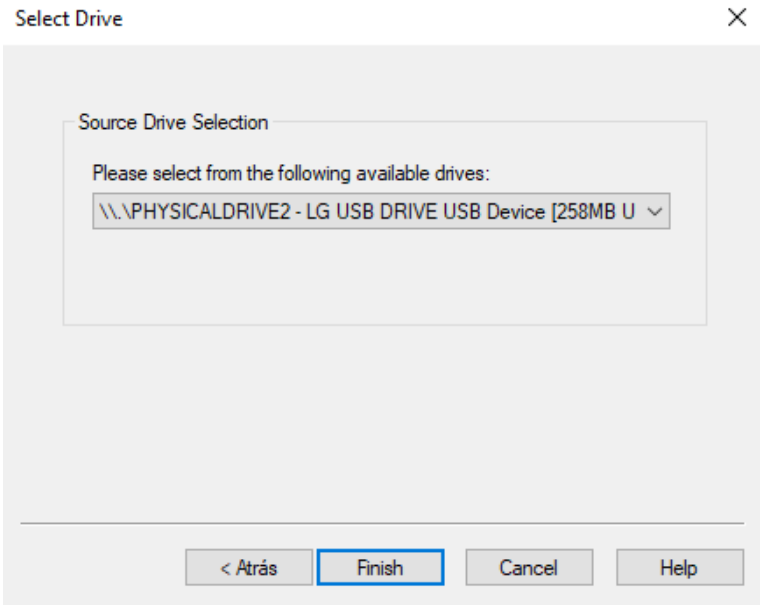


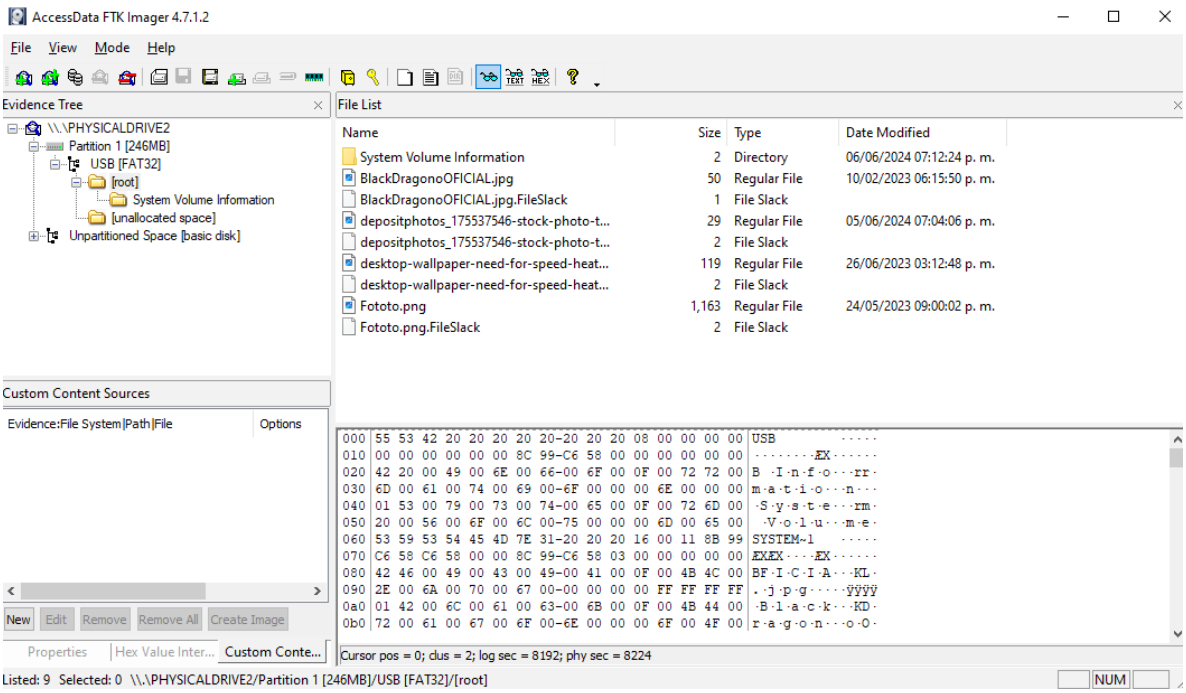


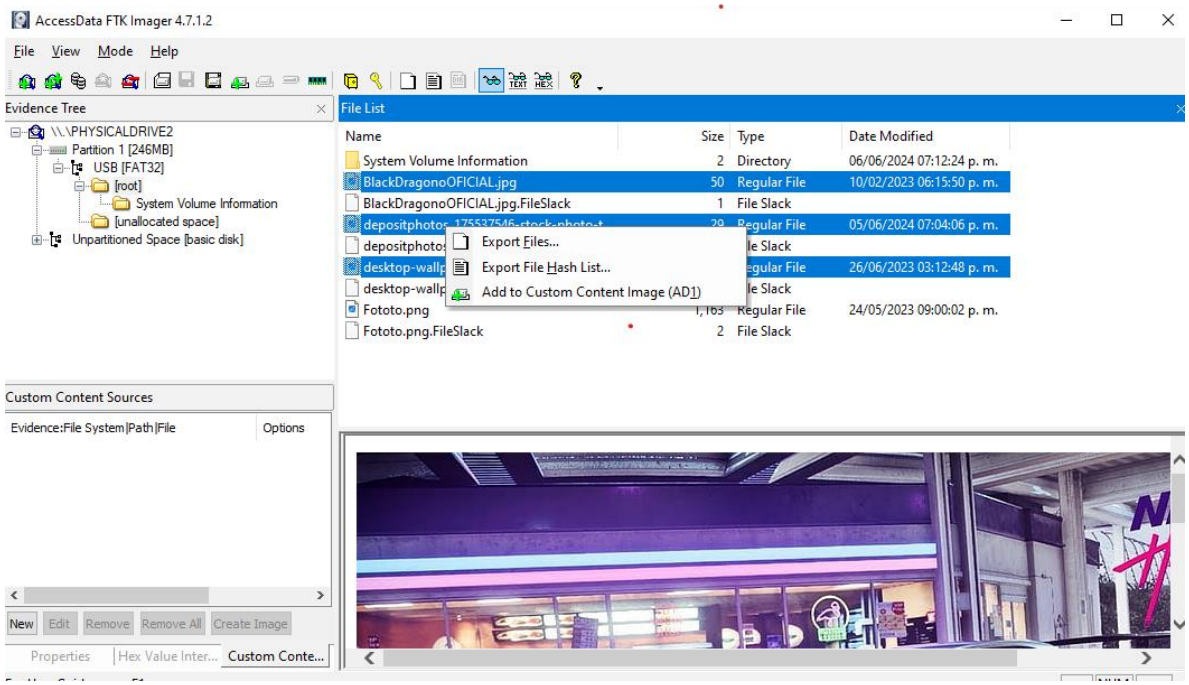
Paso 5: Obtención de evidencia de la Unidad Externa.

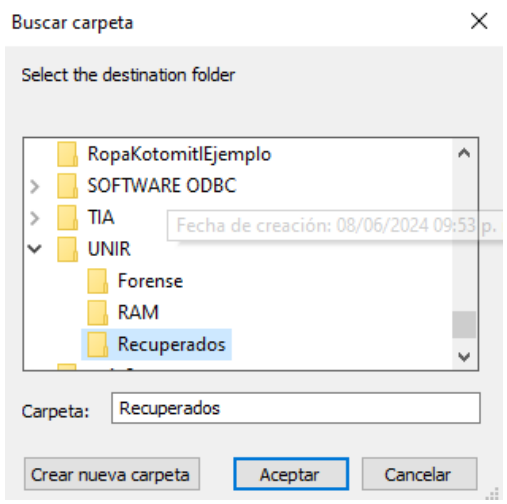


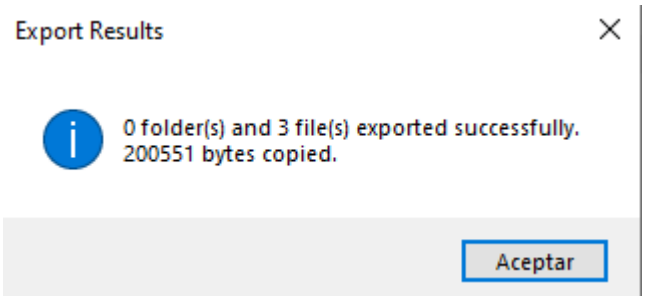


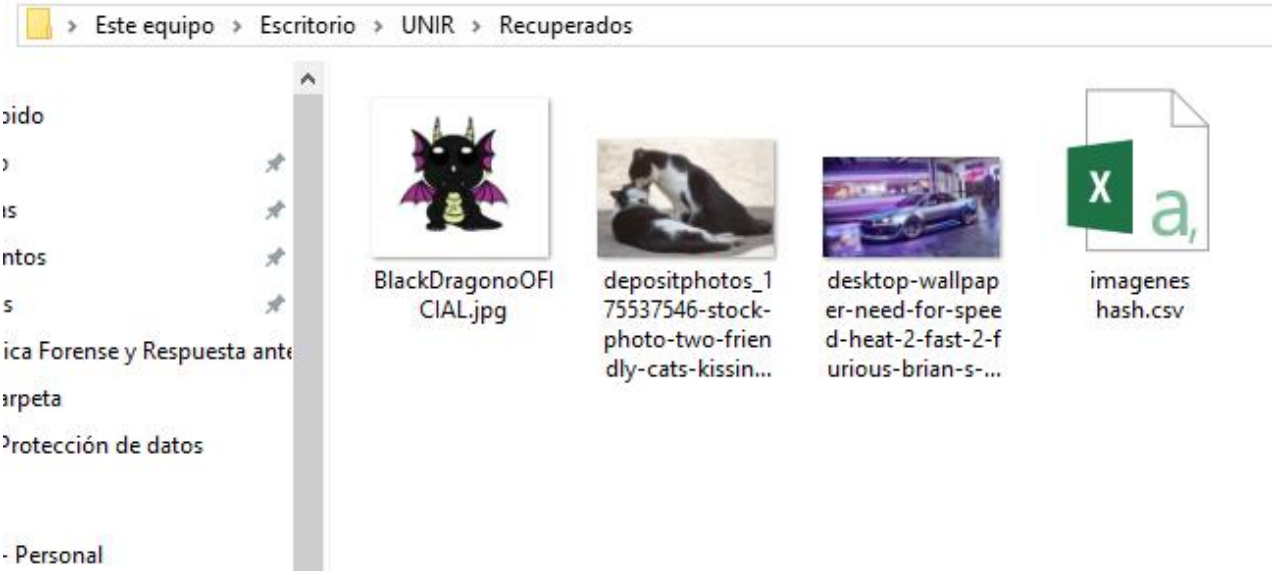

Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE2 - LG USB DRIVE USB Device [258MB U
< Atrás
Finish
Cancel
Help


AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE2
Partition 1 [246MB]
USB [FAT32]
[root]
System Volume Information
[unallocated space]
Unpartitioned Space [basic disk]
File List
Name Size Type Date Modified
System Volume Information 2 Directory 06/06/2024 07:12:24 p. m.
BlackDragonoOFICIAL.jpg 50 Regular File 10/02/2023 06:15:50 p. m.
BlackDragonoOFICIAL.jpg.FileSlack 1 File Slack
depositphotos_175537546-stock-photo-t... 29 Regular File 05/06/2024 07:04:06 p. m.
depositphotos_175537546-stock-photo-t... 2 File Slack
desktop-wallpaper-need-for-speed-heat... 119 Regular File 26/06/2023 03:12:48 p. m.
desktop-wallpaper-need-for-speed-heat... 2 File Slack
Fototo.png 1,163 Regular File 24/05/2023 09:00:02 p. m.
Fototo.png.FileSlack 2 File Slack
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
000 55 53 42 20 20 20 20 20-20 20 20 08 00 00 00 00 USB
010 00 00 00 00 00 00 8C 99-C6 58 00 00 00 00 00 00 ÆX
020 42 20 00 49 00 6E 00 66-00 6F 00 0F 00 72 72 00 B I n f o rr
030 6D 00 61 00 74 00 69 00-6F 00 00 00 6E 00 00 00 m a t i o n
040 01 53 00 79 00 73 00 74-00 65 00 0F 00 72 6D 00 S y s t e rm
050 20 00 56 00 6F 00 6C 00-75 00 00 00 6D 00 65 00 V o l u m e
060 53 59 53 54 45 4D 7E 31-20 20 20 16 00 11 8B 99 SYSTEM~1
070 C6 58 C6 58 00 00 8C 99-C6 58 03 00 00 00 00 00 ÆXÆX ÆX
080 42 46 00 49 00 43 00 49-00 41 00 0F 00 4B 4C 00 BF I C I A KL
090 2E 00 6A 00 70 00 67 00-00 00 00 00 FF FF FF FF . j p g ÿÿÿÿ
0a0 01 42 00 6C 00 61 00 63-00 6B 00 0F 00 4B 44 00 B l a c k KD
0b0 72 00 61 00 67 00 6F 00-6E 00 00 00 6F 00 4F 00 r a g o n o O
Cursor pos = 0; clus = 2; log sec = 8192; phy sec = 8224
Listed: 9 Selected: 0 \\.\PHYSICALDRIVE2/Partition 1 [246MB]/USB [FAT32]/[root]
NUM

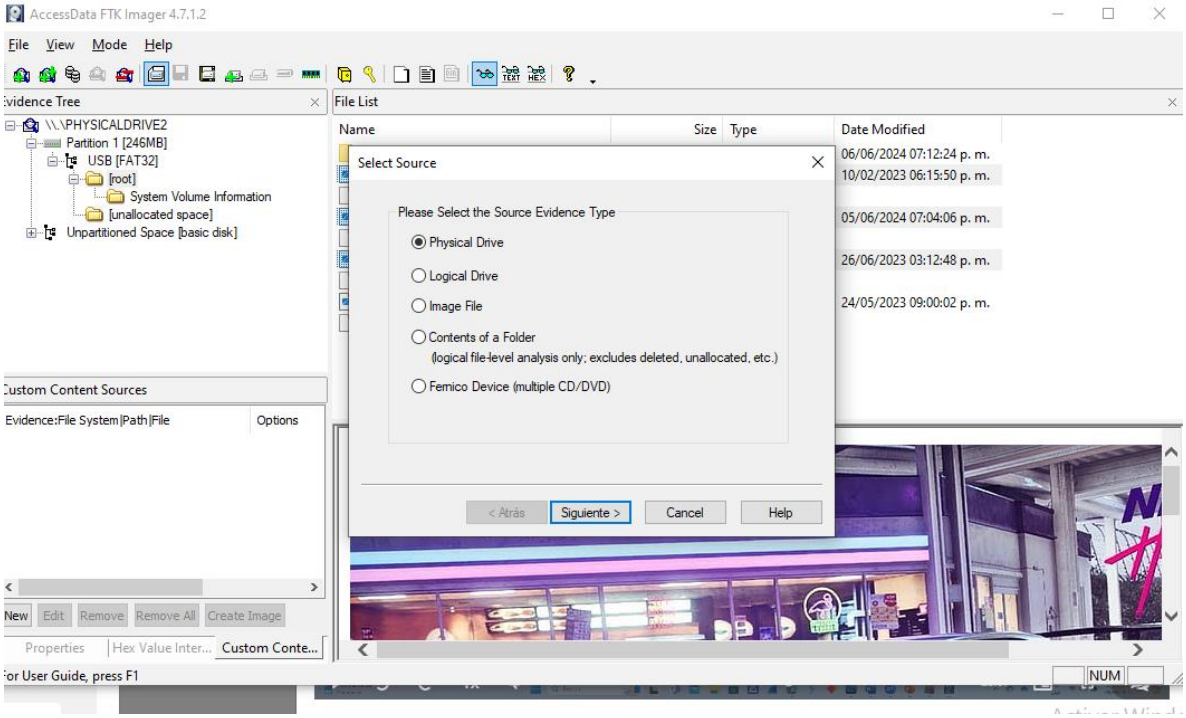

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE2
Partition 1 [246MB]
USB [FAT32]
[root]
System Volume Information
[unallocated space]
Unpartitioned Space [basic disk]
File List
Name Size Type Date Modified
System Volume Information 2 Directory 06/06/2024 07:12:24 p. m.
BlackDragonoOFICIAL.jpg 50 Regular File 10/02/2023 06:15:50 p. m.
BlackDragonoOFICIAL.jpg.FileSlack 1 File Slack
Export Files...
Export File Hash List...
Add to Custom Content Image (AD1)
Fototo.png 24/05/2023 09:00:02 p. m.
Fototo.png.FileSlack 2 File Slack
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...

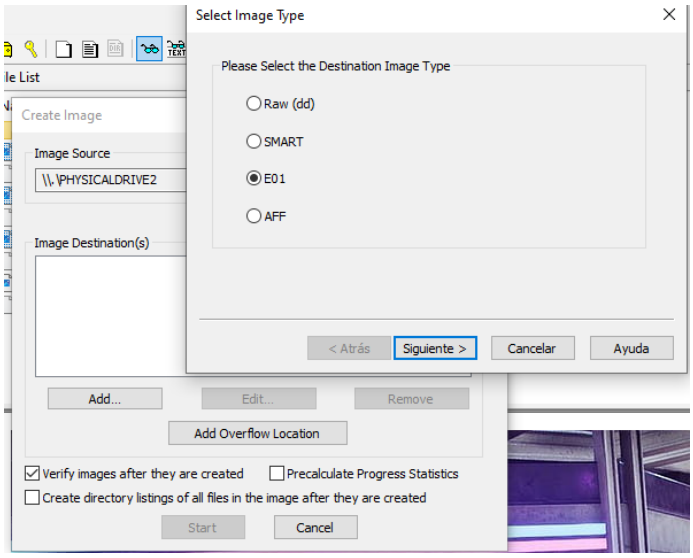

Buscar carpeta
Select the destination folder
RopaKotomitlEjemplo
SOFTWARE ODBC
TIA
UNIR
Forense
RAM
Recuperados
Carpeta: Recuperados
Crear nueva carpeta
Aceptar
Cancelar

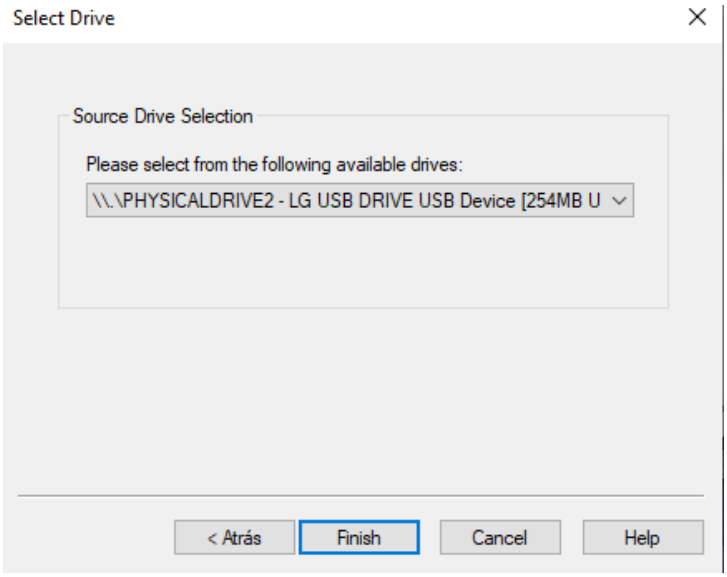

Export Results
0 folder(s) and 3 file(s) exported successfully.
200551 bytes copied.
Aceptar

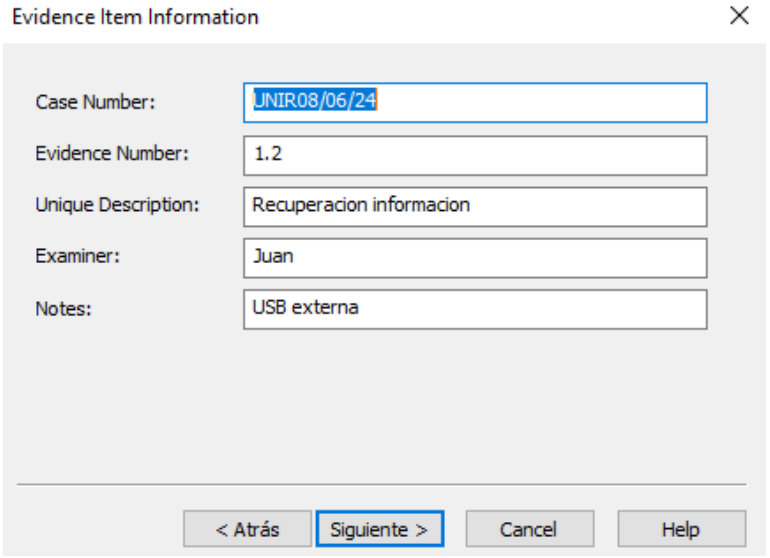

Este equipo › Escritorio › UNIR › Recuperados
BlackDragonoOFICIAL.jpg
depositphotos_175537546-stock-photo-two-friendly-cats-kissin...
desktop-wallpaper-need-for-speed-heat-2-fast-2-furious-brian-s-...
imagenes hash.csv
Protección de datos
- Personal

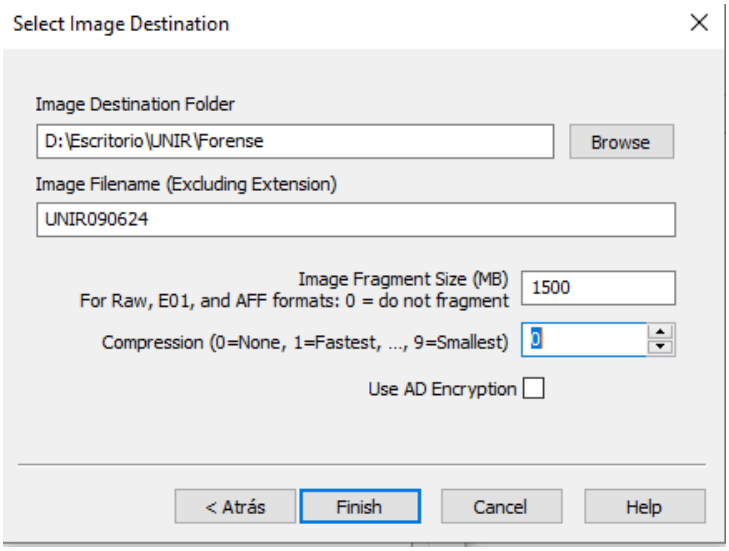
Paso 6: Creación de una imagen forense.

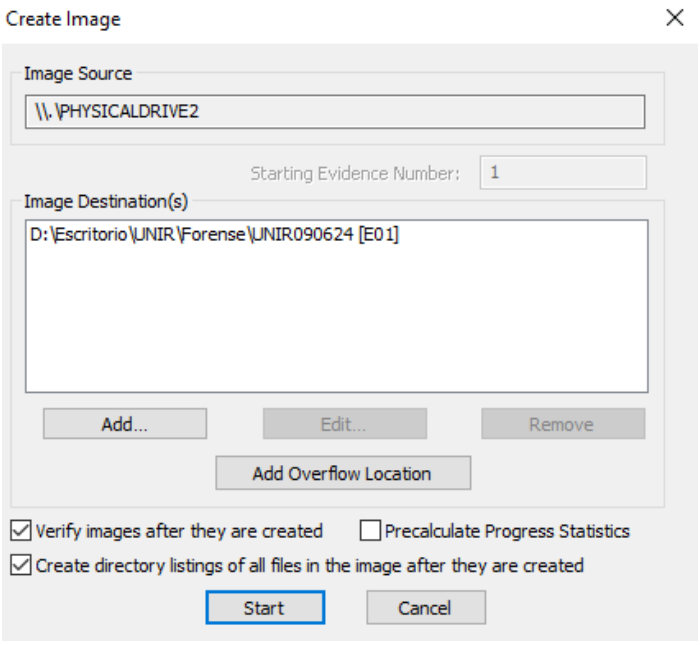


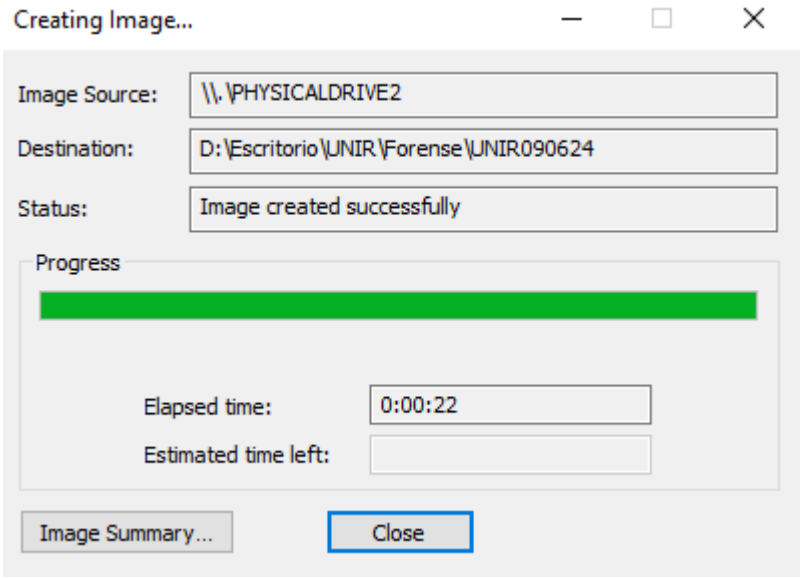


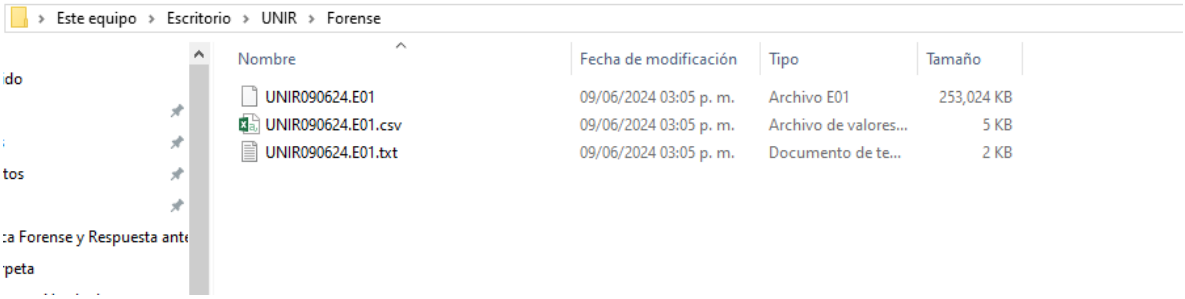

Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE2 - LG USB DRIVE USB Device [254MB U
< Atrás
Finish
Cancel
Help


Evidence Item Information
Case Number:
UNIR08/06/24
Evidence Number:
1.2
Unique Description:
Recuperacion informacion
Examiner:
Juan
Notes:
USB externa
< Atrás
Siguiente >
Cancel
Help


Select Image Destination
Image Destination Folder
D:\Escritorio\UNIR\Forense
Browse
Image Filename (Excluding Extension)
UNIR090624
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment
1500
Compression (0=None, 1=Fastest, ..., 9=Smallest)
0
Use AD Encryption
< Atrás
Finish
Cancel
Help


Create Image
Image Source
\\.\PHYSICALDRIVE2
Starting Evidence Number:
1
Image Destination(s)
D:\Escritorio\UNIR\Forense\UNIR090624 [E01]
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


Creating Image...
Image Source:
\\.\PHYSICALDRIVE2
Destination:
D:\Escritorio\UNIR\Forense\UNIR090624
Status:
Image created successfully
Progress
Elapsed time:
0:00:22
Estimated time left:
Image Summary...
Close



Resultado de esta imagen forense.