

COMENTARIOS LECTURA #2

Investigación Forense y Digital

Daniel Alejandro Olarte Ávila

Universidad Sergio Arboleda

Universidad Sergio Arboleda Cl. 74 #14-14

Bogotá, Colombia

Correo: daniel.olarte01@correo.usa.edu.co

[Escuela de Ciencias Exactas e Ingeniería](#)

Profesor: Juan Carlos Galindo Piraquive

08/03/2022

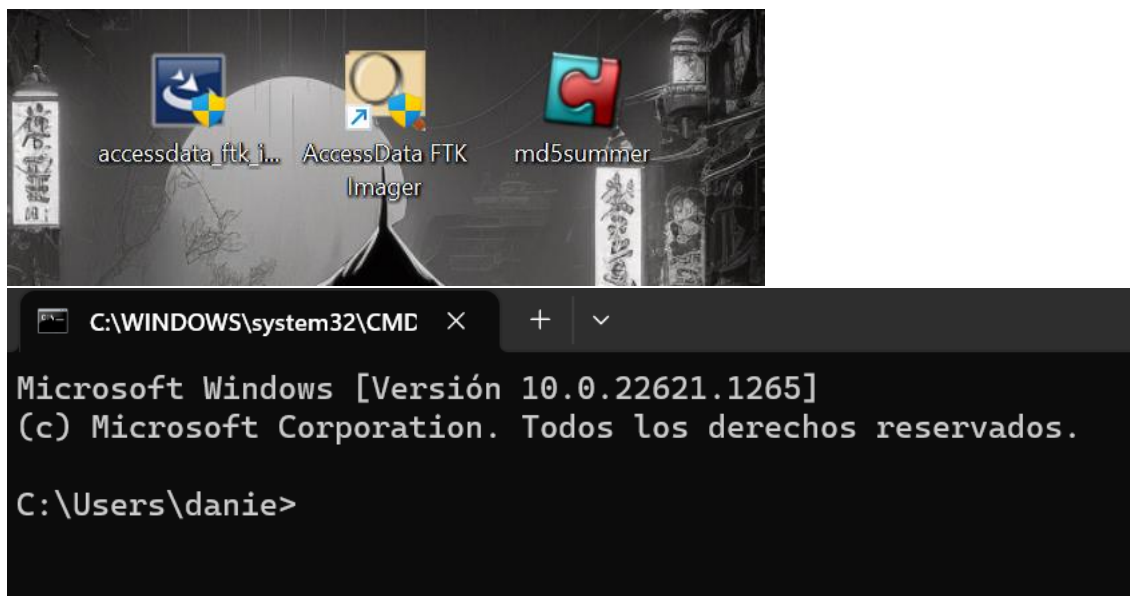
I. INTRODUCCION

En este laboratorio se va a evidenciar que son las huellas digitales hash y cómo podemos utilizar la herramienta FTK (Forensic ToolKit) para realizar una copia de la memoria RAM y el almacenamiento de un sistema digital.

Las huellas digitales hash son una herramienta esencial en la investigación digital y forense, ya que nos permiten identificar de manera única y precisa archivos y datos en un sistema. Al utilizar algoritmos matemáticos para generar una huella digital única para cada archivo, podemos verificar si dos archivos son iguales o diferentes, y detectar posibles manipulaciones o alteraciones.

En este laboratorio, vamos a aprender cómo utilizar la herramienta FTK para realizar una copia forense de la memoria RAM y el almacenamiento de un sistema digital. La copia forense nos permite hacer una copia bit a bit de todos los datos y archivos en un sistema, lo que nos permite analizarlos sin modificarlos y preservar su integridad.

II. HERRAMIENTAS: FTK – MD5SUMMER - CONSOLA



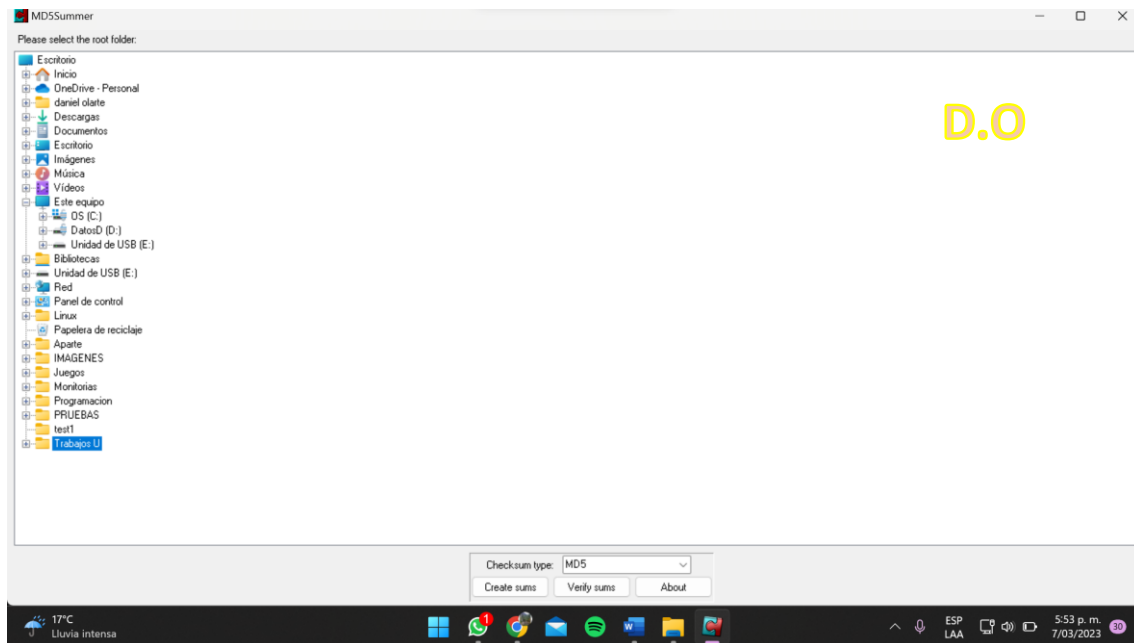
III. DESARROLLO

HUELLAS DIGITALES:

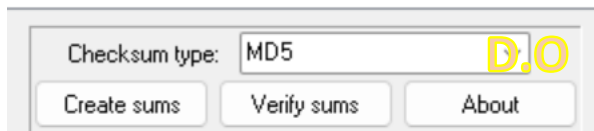
CREACIÓN:

LABORATORIO #1, Investigación Forense y Digital

- a. Se abre la herramienta de MD5Summer, se usa MD5 para hacer una huella digital de 32 caracteres

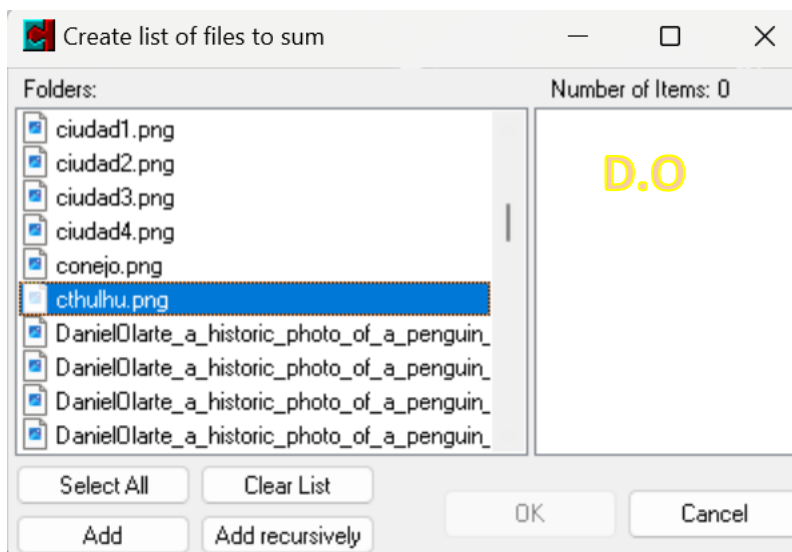


Herramienta MD5Summer 1

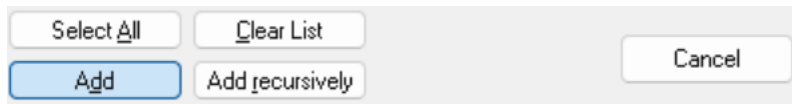


Escogiendo el tipo para hacer la huella digital

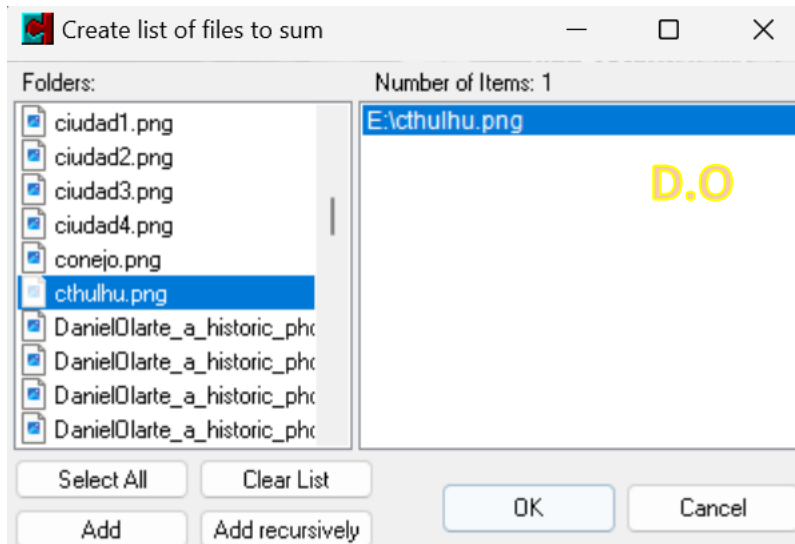
Después de seleccionar la carpeta seleccionamos el archivo 2ctulhu.png” (Imagen creada con Inteligencia Artificial) para generar el valor hash.



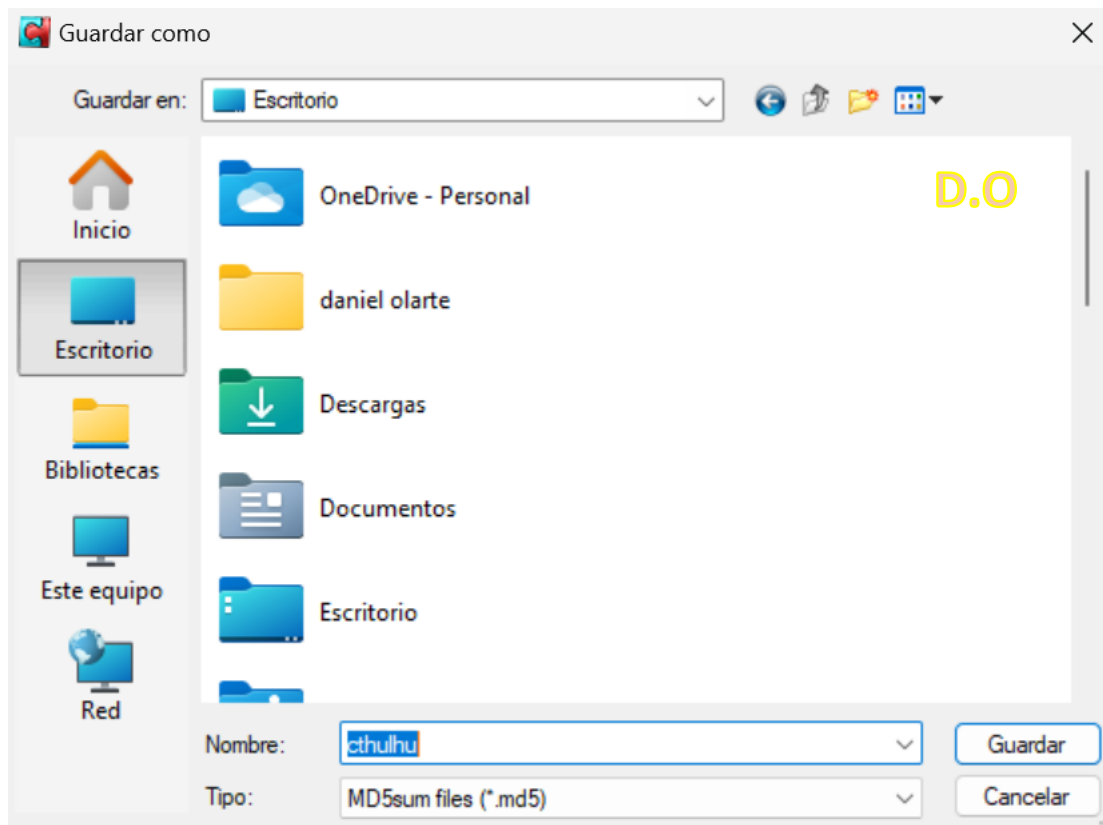
LABORATORIO #1, Investigación Forense y Digital



Herramienta MD5Summer, Se selecciona el archivo y Se Adiciona con el botón "Add"

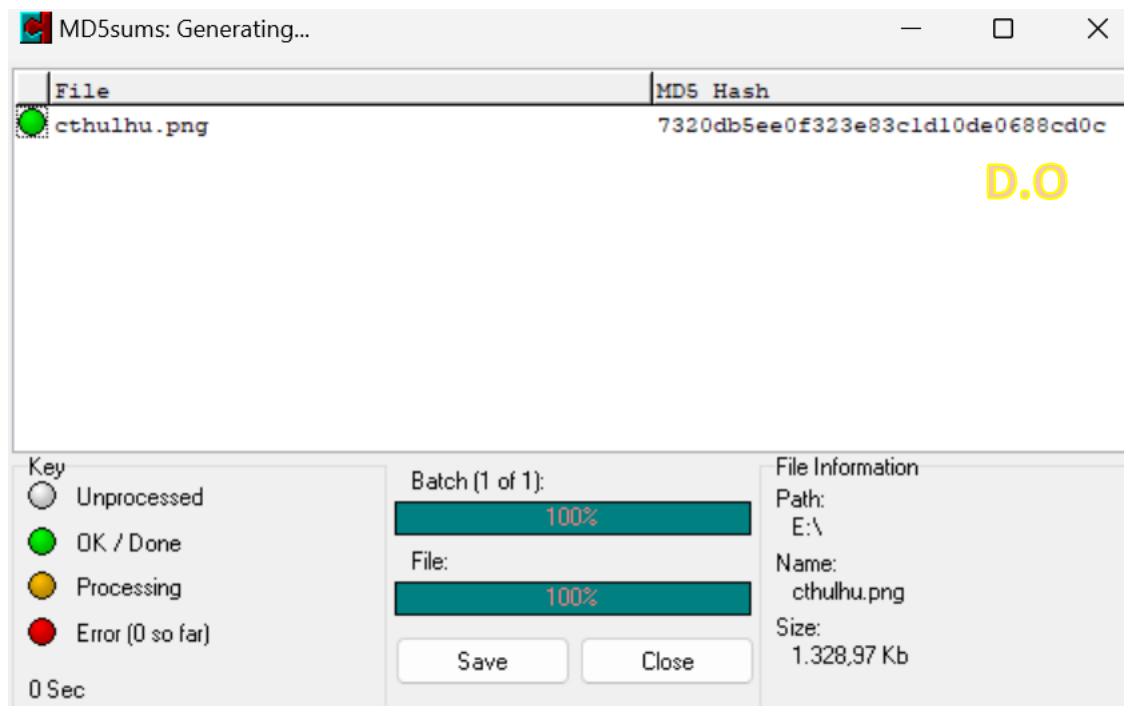


Se selecciona el archivo adicionado y se le da al botón "OK"



Se selecciona la ruta donde se va a guardar el archivo creado con MD5Summer

Se visualizara el Hash en este ejemplo: 7320db5ee0f323e83c1d10de0688cd0c





```
cthulhu
Archivo  Editar  Ver

# MD5 checksums generated by MD5summer (http://www.md5summer.org)
# Generated 7/03/2023 6:05:18 p. m.

7320db5ee0f323e83c1d10de0688cd0c| *cthulhu.png
```

D.O

Se procede a realizar el hash de la misma imagen en terminal con el comando certutil -hashfile (nombre de archivo) (tipo de hash) para comparar ambos procesos:

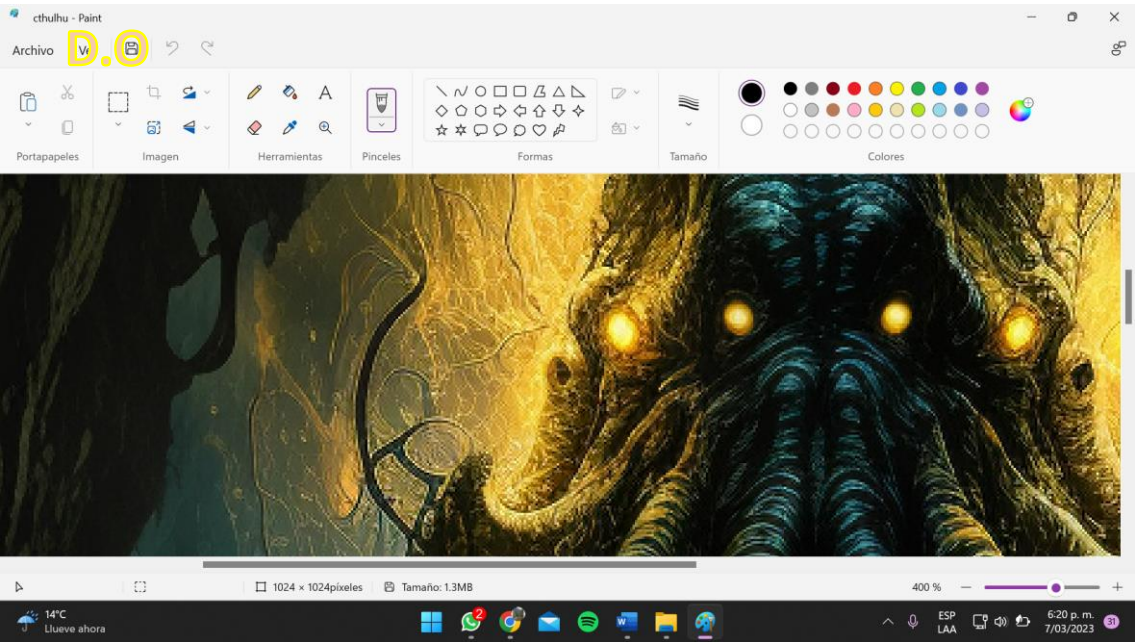
```
Windows PowerShell
PS E:\> certutil -hashfile .\cthulhu.png MD5
MD5 hash de .\cthulhu.png:
7320db5ee0f323e83c1d10de0688cd0c
CertUtil: -hashfile comando completado correctamente.
PS E:\>
```

D.O



MODIFICACIÓN:

Se realiza una modificación en la imagen para simular una manipulación de una prueba visual, en este caso se realizará con PAINT:

LABORATORIO #1, Investigación Forense y Digital

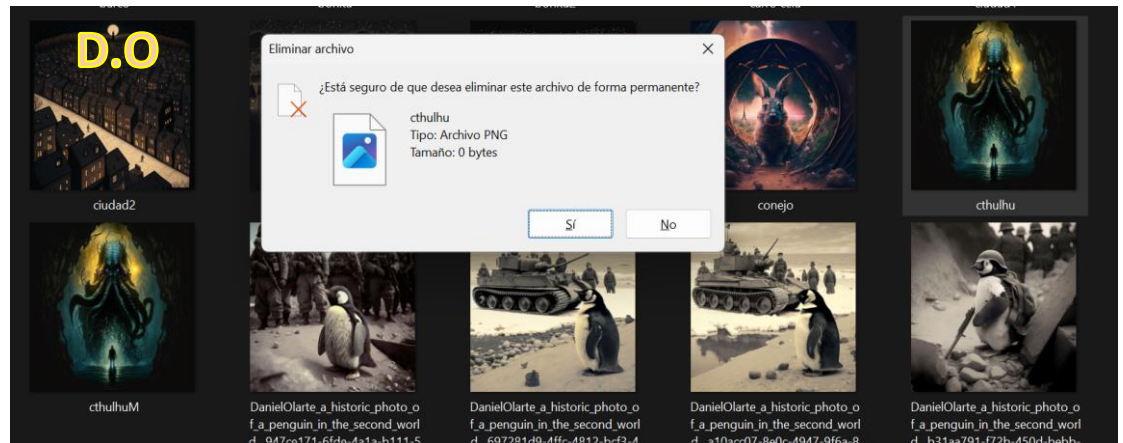


Modificando la imagen

ORIGINAL	MODIFICADA
 <pre data-bbox="240 1458 703 1608">PS E:\> certutil -hashfile .\cthulhu.png MD5 MD5 hash de .\cthulhu.png: 7320db5ee0f323e83cd10de0688cd0c CertUtil: -hashfile comando completado correctamente. PS E:\></pre>	 <pre data-bbox="743 1458 1358 1608">PS E:\> certutil -hashfile .\cthulhuM.png MD5 MD5 hash de .\cthulhuM.png: 66c1b6613be8dd8f643150c0ae35ec87 CertUtil: -hashfile comando completado correctamente. PS E:\></pre>

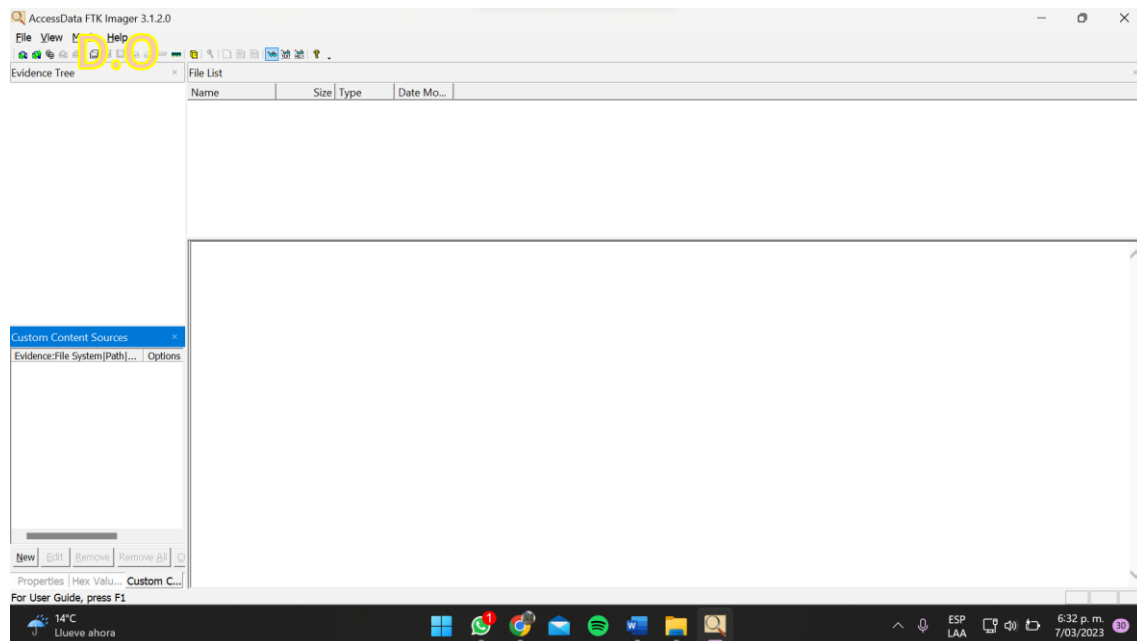
FTK IMAGE ROM:

Siguiendo el Proceso de las huellas digitales, se dirá que estamos trabajando en un caso de modificación de la imagen de prueba, en donde se habrá modificado la imagen original y se borrara, para el fin de poder recuperarla.



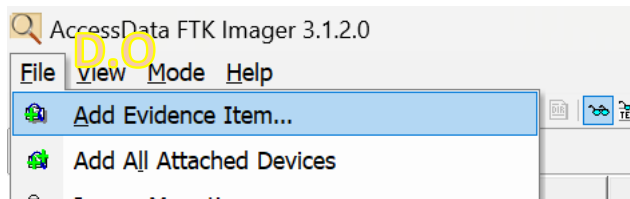
Se elimina la prueba original y se deja la modificada

Para el desarrollo de FTK Image se utiliza una USB de 8 gigabytes de almacenamiento.

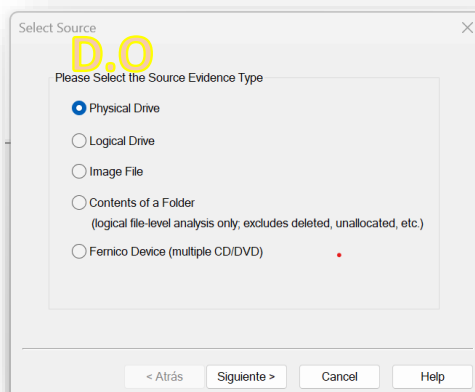


Herramienta FTK Image

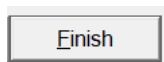
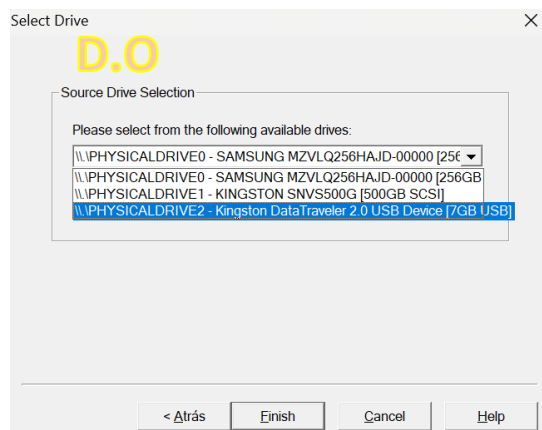
LABORATORIO #1, Investigación Forense y Digital



Para la elección y configuración de la imagen en la herramienta FKT Image, se selección una imagen “Physical Drive” también se eligió el dispositivo de almacenamiento, a continuación, se observa la culminación de la imagen



Se selecciona la opción “Physical Drive”



Se selecciona el dispositivo a hacer la Imagen

LABORATORIO #1, Investigación Forense y Digital

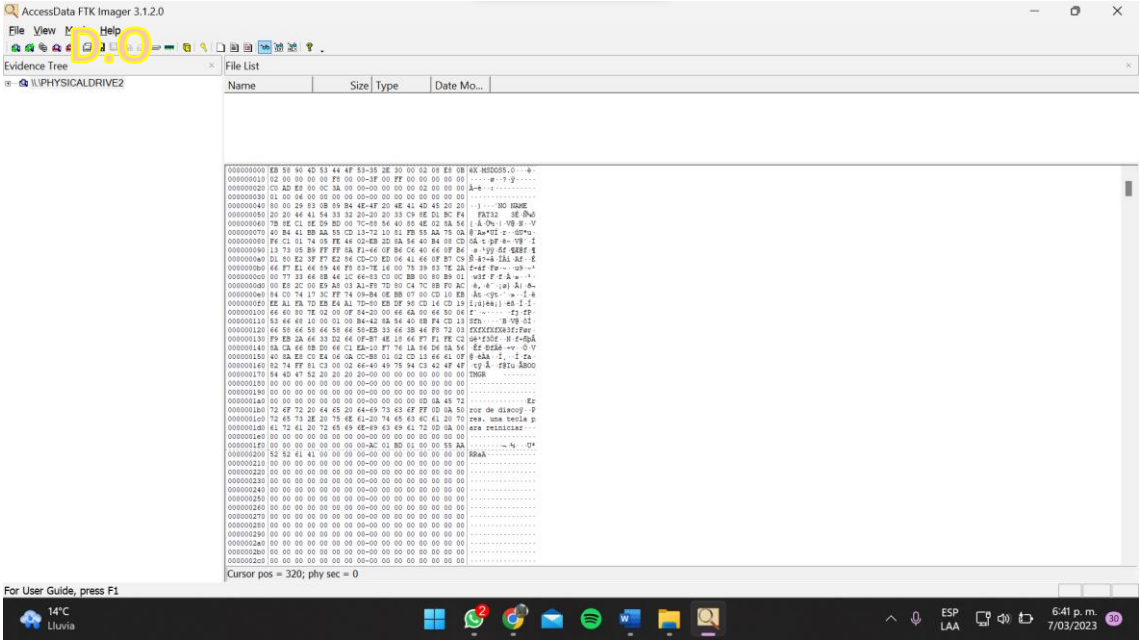
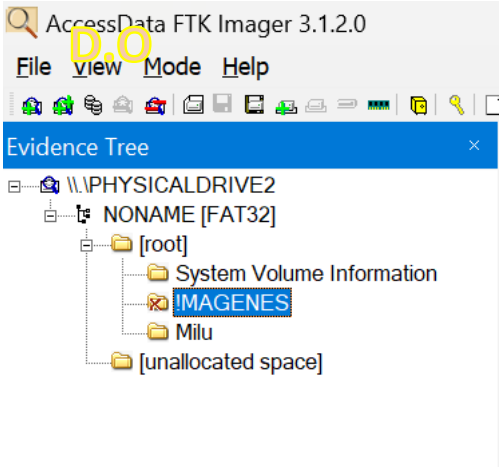


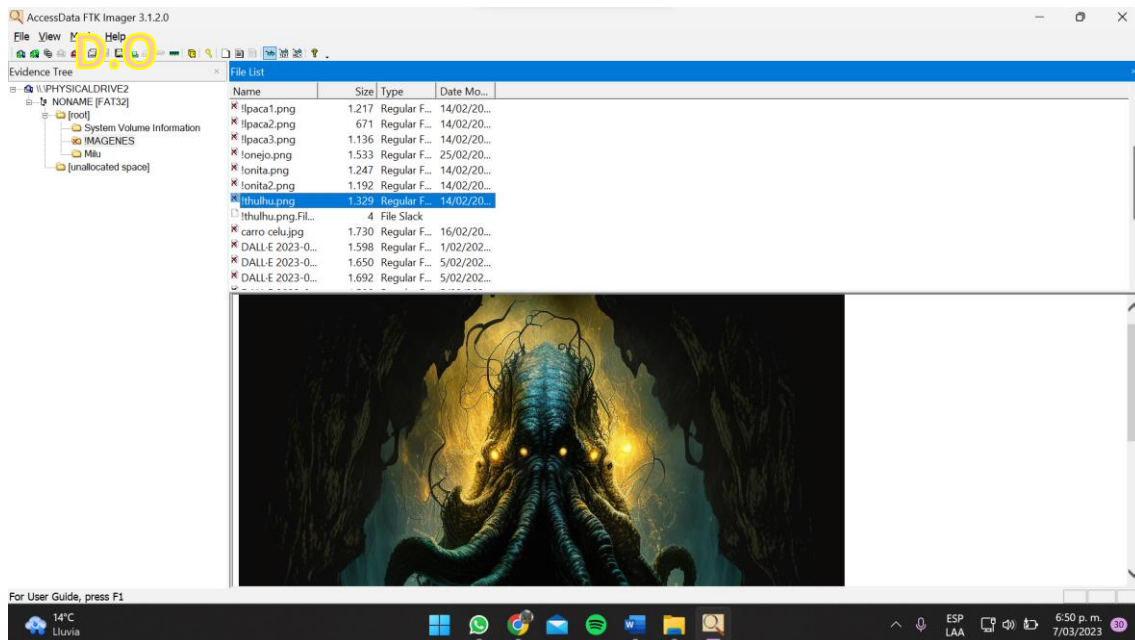
Imagen evidenciando el resultado

Para proceder a recuperar la prueba original, se busca dentro de la imagen hasta llegar al root y buscar el archivo que se desea recuperar.



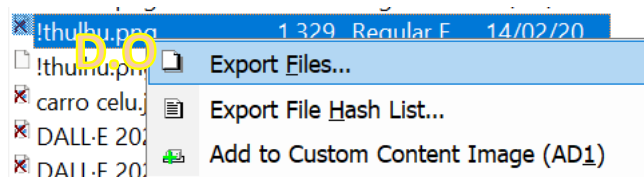
D.O

File List				
Name	Size	Type	Date Mo...	
!lpaca1.png	1.217	Regular F...	14/02/20...	
!lpaca2.png	671	Regular F...	14/02/20...	
!lpaca3.png	1.136	Regular F...	14/02/20...	
!onejo.png	1.533	Regular F...	25/02/20...	
!onita.png	1.247	Regular F...	14/02/20...	
!onita2.png	1.192	Regular F...	14/02/20...	
!thulhu.png	1.329	Regular F...	14/02/20...	
!thulhu.png.Fil...	4	File Slack		
carro celu.jpg	1.730	Regular F...	16/02/20...	
DALL-E 2023-0...	1.598	Regular F...	1/02/202...	
DALL-E 2023-0...	1.650	Regular F...	5/02/202...	
DALL-E 2023-0...	1.692	Regular F...	5/02/202...	



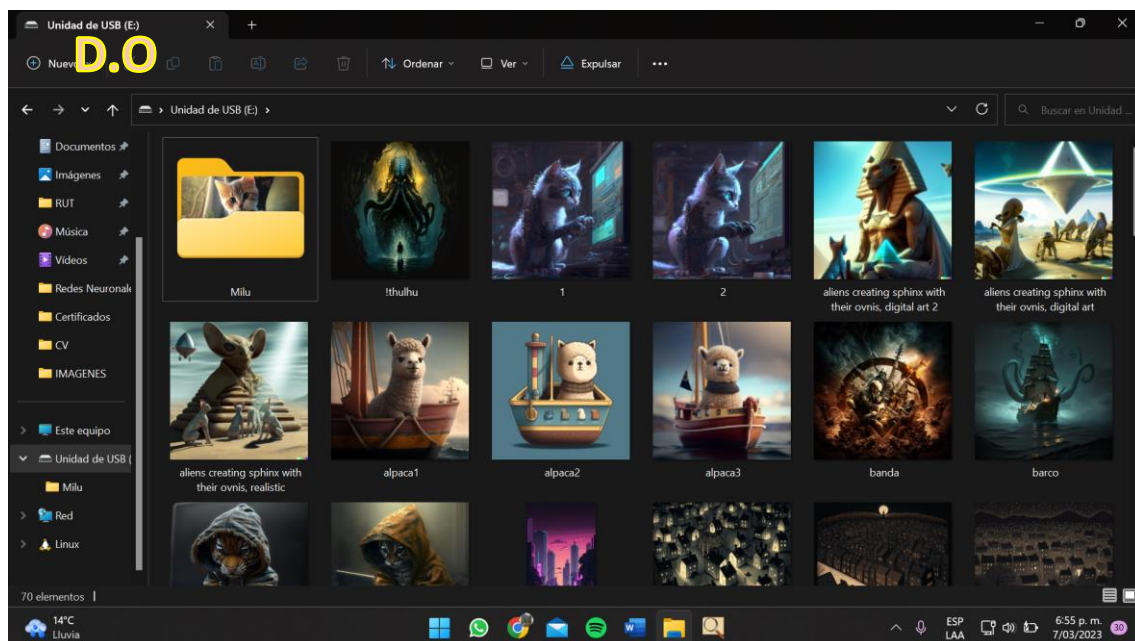
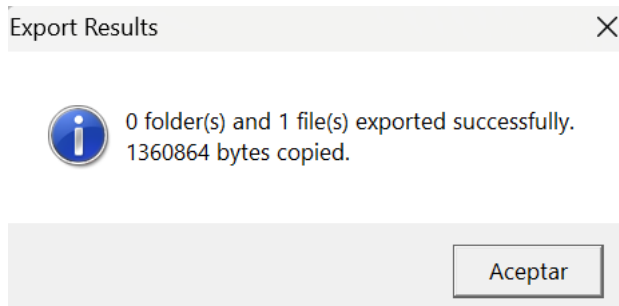
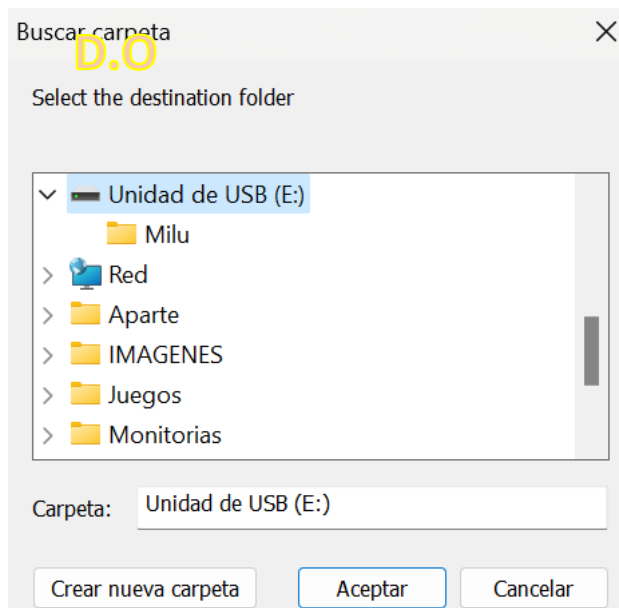
RECUPERACIÓN:

Para recuperar las pruebas eliminadas se selecciona Exportar archivo y se selecciona donde guardar



Se exporta la prueba borrada

LABORATORIO #1, Investigación Forense y Digital





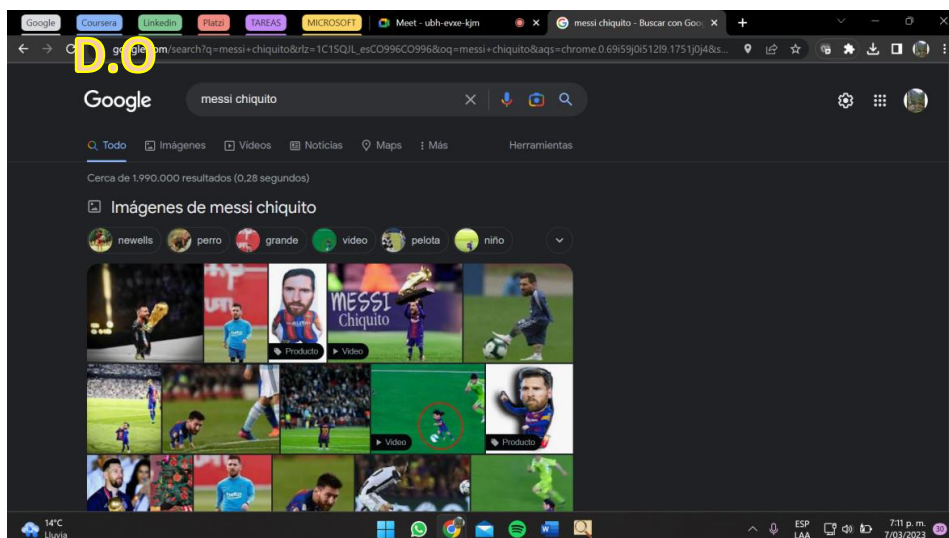
Se procede a comprobar el HASH del archivo recuperado

ORIGINAL	RECUPERADO
<pre>Windows PowerShell PS E:\> certutil -hashfile .\cthulhu.png MD5 MD5 hash de .\cthulhu.png: 7320db5ee0f323e83c1d10de0688cd0c CertUtil: -hashfile comando completado correctamente. PS E:\></pre>	<pre>Windows PowerShell PS E:\> certutil -hashfile .\!thulhu.png MD5 MD5 hash de .\!thulhu.png: 7320db5ee0f323e83c1d10de0688cd0c CertUtil: -hashfile comando completado correctamente. PS E:\></pre>

Hash Generado Exactamente el mismo al ORIGINAL

FTK IMAGE RAM:

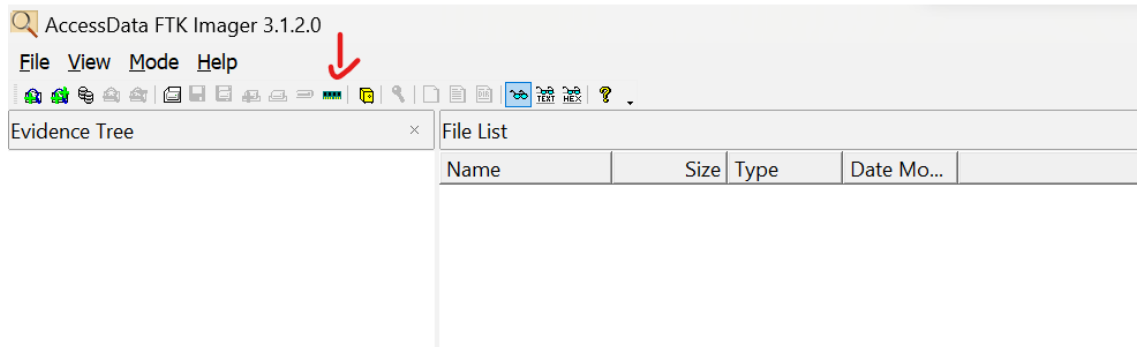
Para este proceso se realizo anteriormente búsquedas en Google para “alimentar” la RAM y poder evidenciarlo al hacer la copia de esta. En el ejemplo a ver se busco en el navegador “Messi chiquito”



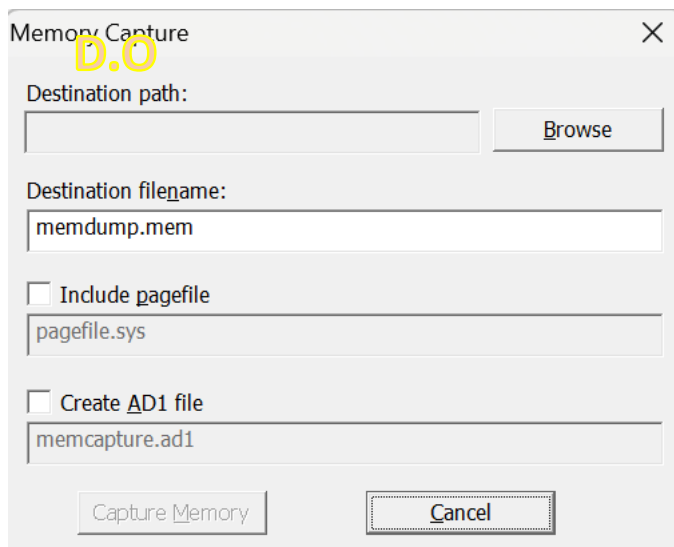
BUSQUEDA REALIZADA QUE QUEDA EN LA RAM DEL DISPOSITIVO A ANALIZAR

Se selecciona el botón CAPTURE MEMORY para realizar una copia de la RAM y se selecciona la dirección donde se desea guardar

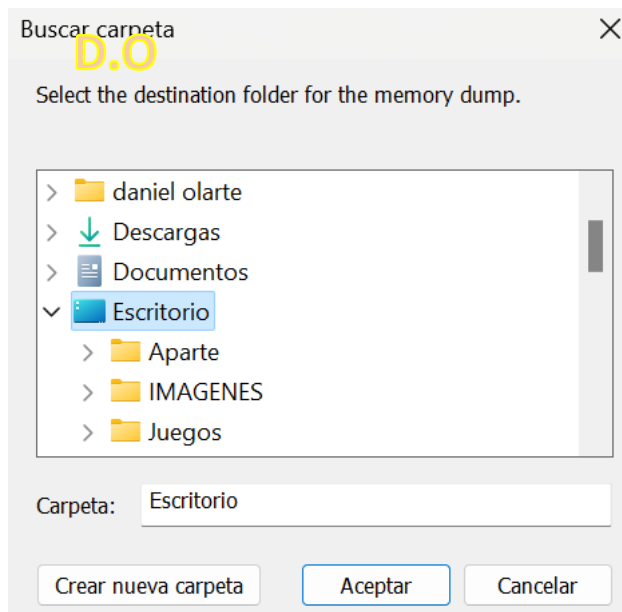
D.O



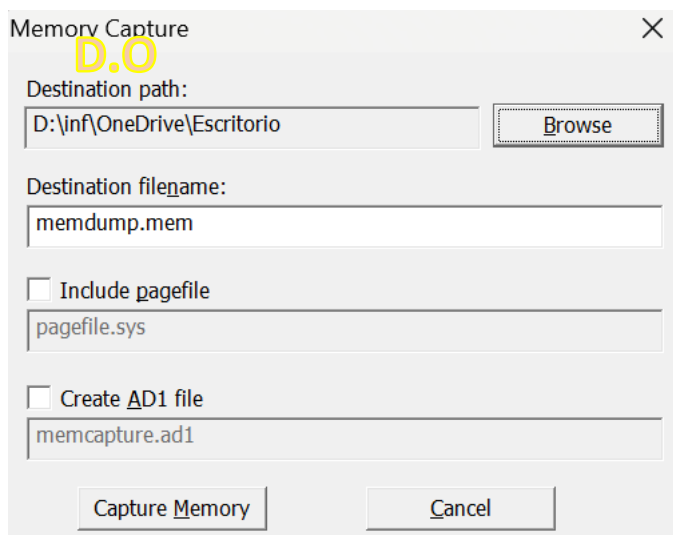
Se selecciona el botón CAPTURE MEMORY



Se selecciona "Browse"

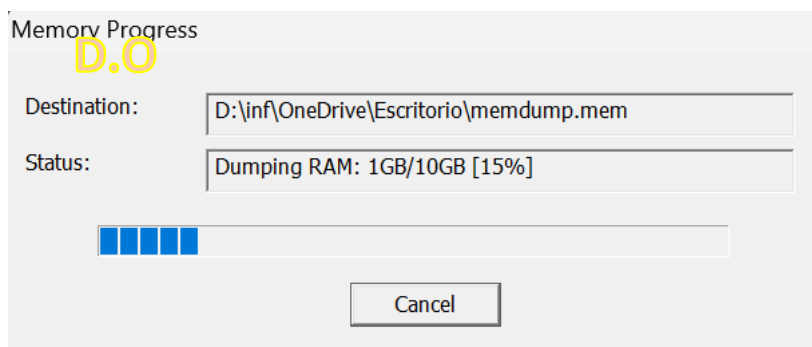


Se selecciona la ruta para guardar

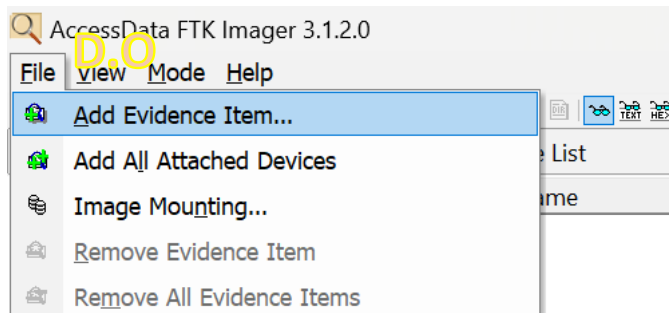


Se selecciona "Capture Memory"

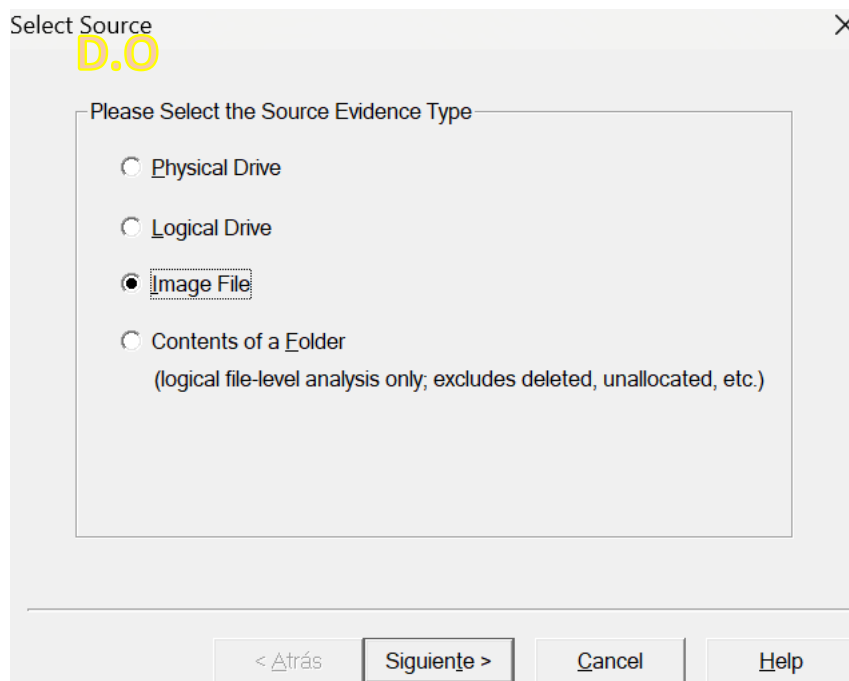
Se podrá evidenciar el proceso del vaciado de RAM



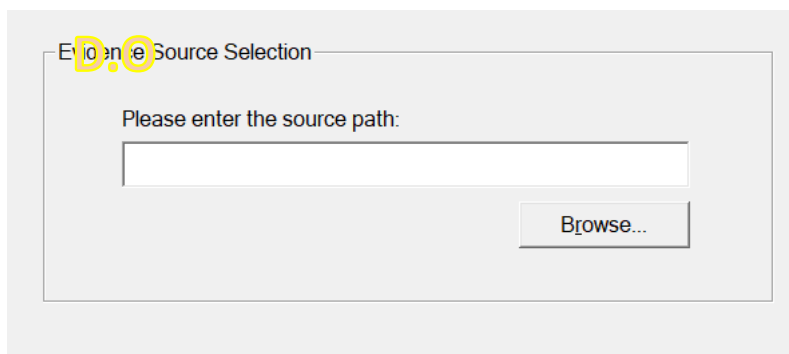
Se selecciona agregar evidencia y IMAGE FILE para agregar la imagen anteriormente guardada



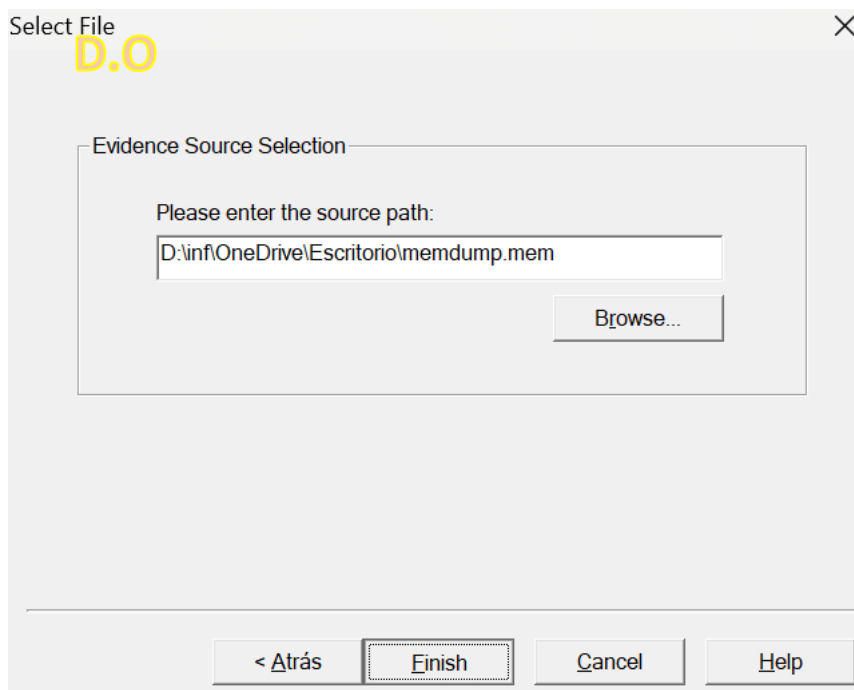
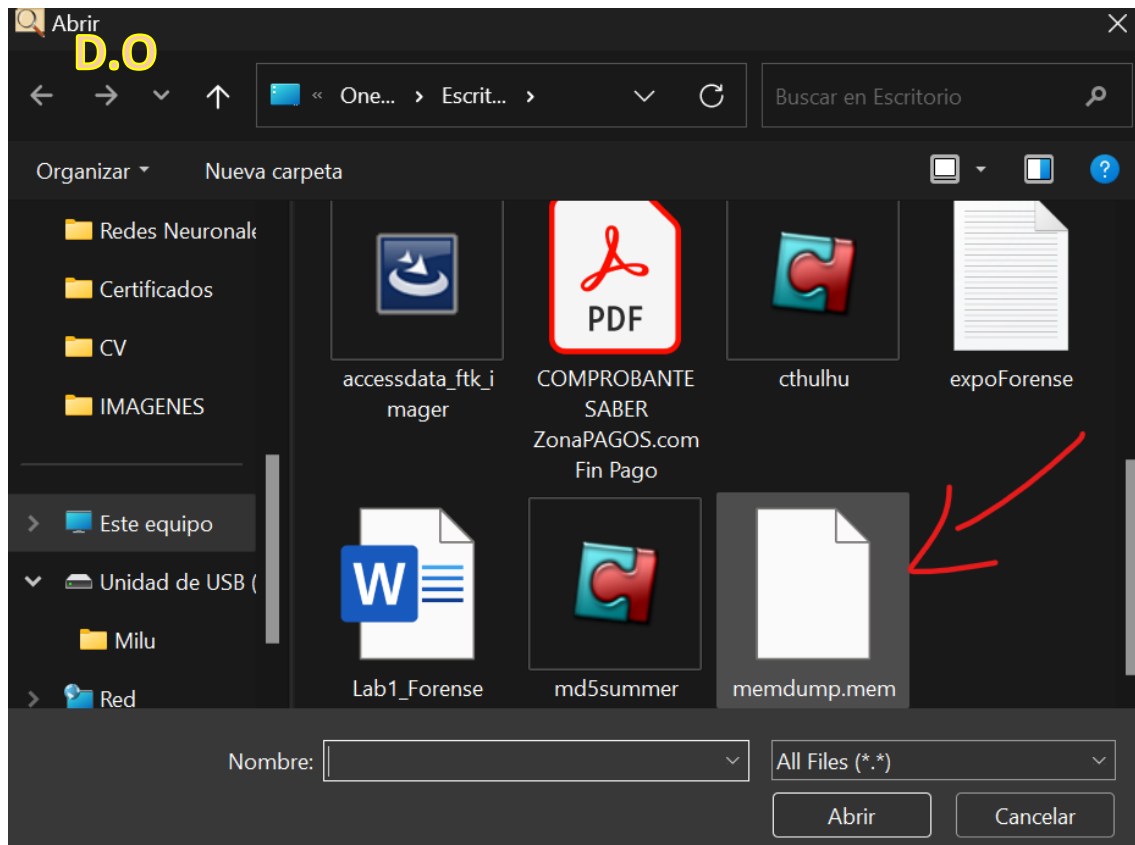
Se selecciona "Add Evidence Item" para empezar el análisis



Se selecciona "Image File"

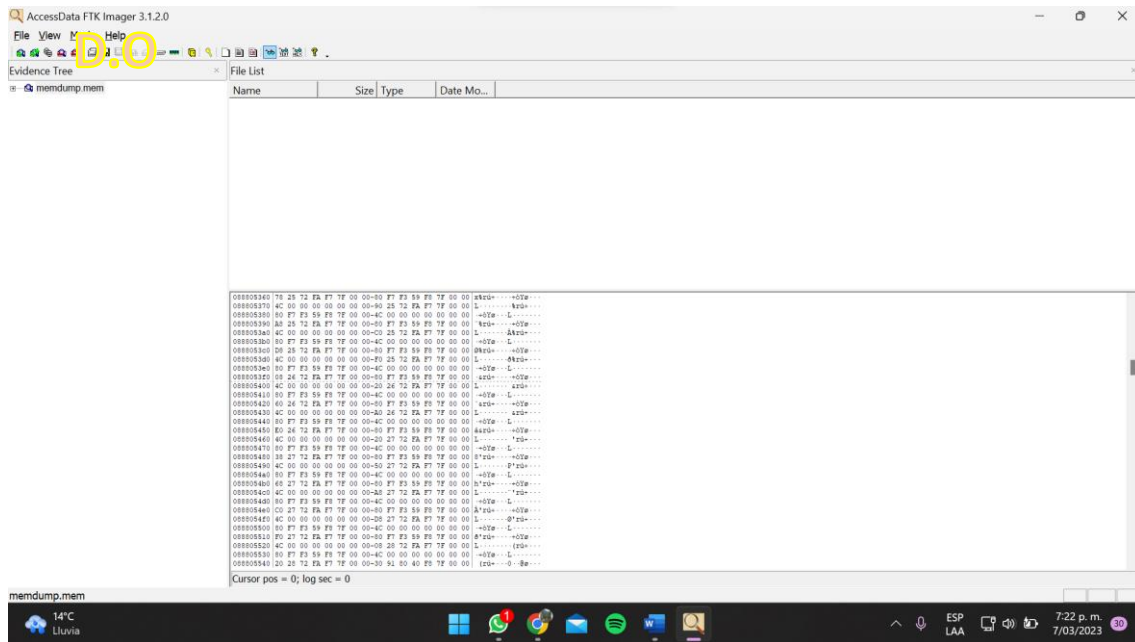


Se agrega la memoria guardada



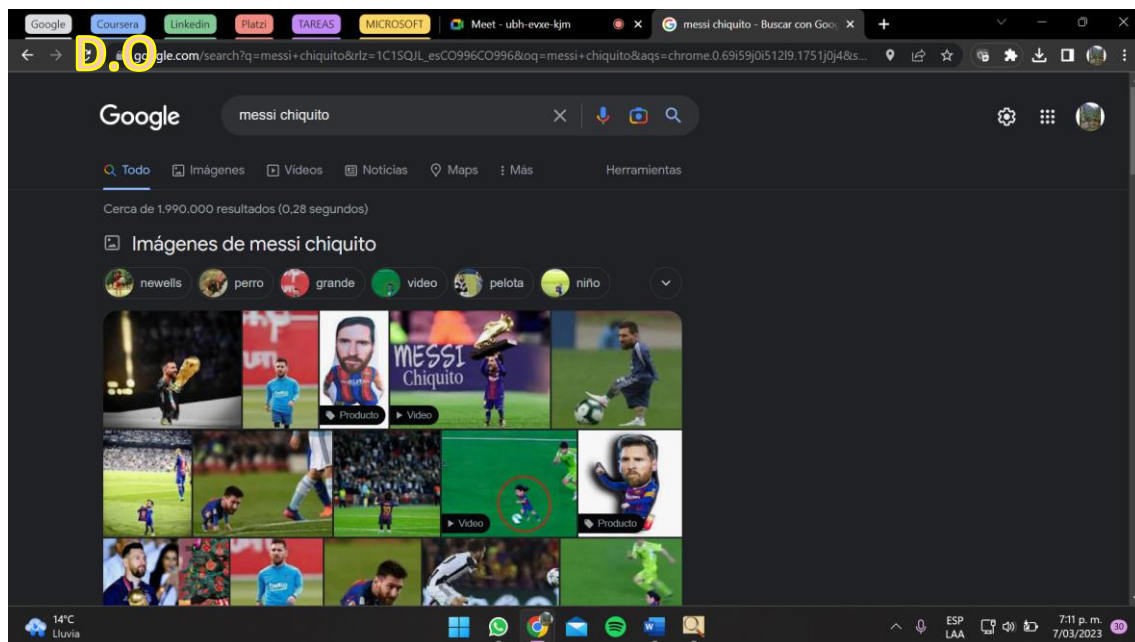
Se puede evidenciar el resultado

LABORATORIO #1, Investigación Forense y Digital



Memoria RAM visualizada

Para analizar la RAM vamos a hallar la búsqueda que se realizó en el equipo desde la Imagen de la RAM, con CTRL+F se abre la herramienta para buscar a detalle y se digita lo que se desea buscar



Evidencia de prueba realizada antes de la memoria



Opción CTRL+F para la búsqueda

Evidenciamos el resultado “Messi chiquito”

```
000bbcb00 | 50 65 73 74 61 C3 B1 61-3A 20 6D 65 73 73 69 20 | Pestaña: messi
000bbcb10 | 63 68 69 71 75 69 74 6F-20 2D 20 42 75 73 63 61 | chiquito - Busca
```

Se evidencia Messi chiquito en la memoria de la RAM

CONCLUSIONES

1. Las huellas digitales hash son herramientas útiles para la verificación de integridad de archivos y datos digitales, permitiendo detectar si han sido modificados o alterados de alguna forma.
2. La modificación de una imagen en este caso una generada por IA puede alterar la huella digital original de la imagen, lo que puede dificultar su verificación de integridad y su autenticidad.
3. La herramienta FTK es una herramienta de análisis forense que permite la recuperación de datos eliminados y la verificación de huellas digitales hash, lo que resulta valioso en casos de investigación forense y litigios.
4. Es importante entender cómo funcionan las huellas digitales hash y las herramientas de análisis forense como FTK para poder realizar investigaciones digitales efectivas.
5. La combinación de técnicas de análisis forense y de verificación de huellas digitales hash puede proporcionar una mayor fiabilidad en la recuperación y verificación de datos digitales, lo que puede resultar valioso en la investigación digital y forense.
6. La herramienta FTK es una herramienta útil para la investigación digital y forense, ya que permite la copia de la RAM y el almacenamiento, así como la recuperación de datos borrados y la visualización de huellas digitales.

IV. REFERENCIAS

<https://www.accessdata.com/products-services/forensic-toolkit-ftk> - Sitio oficial de la herramienta Forensic Toolkit (FTK).

<https://www.sciencedirect.com/topics/computer-science/digital-forensic-toolkit> - Artículo científico sobre herramientas de investigación digital y forense, incluyendo FTK.

<https://www.forensicfocus.com/articles/ftk-imager-how-and-why-to-use-this-free-tool/> - Artículo sobre la herramienta FTK Imager y su uso en la creación de imágenes forenses.

<https://www.blackbagtech.com/blog/understanding-the-importance-of-hash-values-in-digital-forensics> - Artículo sobre la importancia de los valores hash en la investigación digital forense.

<https://www.forensicmag.com/article/2016/03/real-life-case-why-hash-values-are-critical-digital-forensics> - Artículo que describe un caso real en el que los valores hash fueron críticos en la investigación digital forense.