

Práctica 2

Análisis de NTFS

Índice

Índice.....	2
1. Actividad:.....	4
a. Localiza una entrada cualquiera correspondiente al fichero borrado, por ejemplo yo he encontrado “texto - copia.txt”, y realiza una captura de pantalla. Posición de memoria. Pista: vete a la posición 03397XXXX.....	4
b. Recupera el fichero mediante la herramienta FTK Imager (se encuentra en la carpeta papelería).....	5
2. Actividad:.....	5
a. ¿Dónde puedo encontrar las fechas de creación, modificación y acceso?.....	5
b. ¿Qué significa la propiedad non-resident y sus valores asociados 0/1?.....	5
3. Actividad:.....	6
a. Exportar el fichero de metadatos \$MFT usando FTK, procesarla con la herramienta MFT2CSV e importarla en un editor de hojas de cálculo con el fin de analizar los atributos. Nos interesa estudiar qué archivos se han borrado y en qué fecha. Realiza un filtrado por el campo “in use” a estado ‘0’ (borrado) y/o por el campo “RecordActive” = DELETED/ALLOCATED para obtener las fecha/hora de borrado.....	6
4. Actividad:.....	9
a. Exportar el fichero de metadatos \$LogFile, que junto a la \$MFT del apartado anterior proporcionará datos sobre las transacciones realizadas en el sistema de archivos. Procesar los ficheros con la herramienta NTFS LogFileParse para decodificar la información y obtener un CSV. Buscar las transacciones donde el campo “lf_RedoOperation” valga “DeallocateFileRecordSegment” para localizar fichero borrados definitivamente puesto que como su nombre indica la operación fue desasignar el segmento del registro del fichero.....	9
5. Actividad:.....	11
a. Exportar el fichero de metadatos correspondiente al \$USNJournal (\$Extend -> \$USNjrl -> \$J). Procesado con la herramienta UsnJrnl2Csv para decodificar la información que almacena. Filtra la información resultante por el campo “Reason” = “CLOSE+DELETE” para obtener las fechas de cuando se produjo el borrado definitivo de los ficheros.....	11
6. Actividad:.....	12
a. En este apartado, vamos a utilizar la herramienta ANJP para realizar un procesamiento conjunto de la \$MFT, \$LogFile y \$USNjrl. Verás que trabaja con la misma información de los apartados anteriores de forma integrada en la misma herramienta. Dispone de una pestaña donde decodificar la información (Parse) y otra donde visualizar los resultados (Report). Se trata de una herramienta de pago. Se pide utilizarla y realizar un par de capturas de pantalla del informe de resultados que ofrece.....	12
7. Actividad:.....	14
a. Utiliza las herramientas “FTK Imager” y “AlternateDataViewer” para estudiar el origen de los ficheros que aparecen en la imagen “datos.dd”. Haz una captura de pantalla con cada herramienta donde se visualice un ejemplo.....	14
8. Actividad:.....	16
a. Exportar los ficheros de metadatos de tipo índice de directorios (\$I30) de los tres	

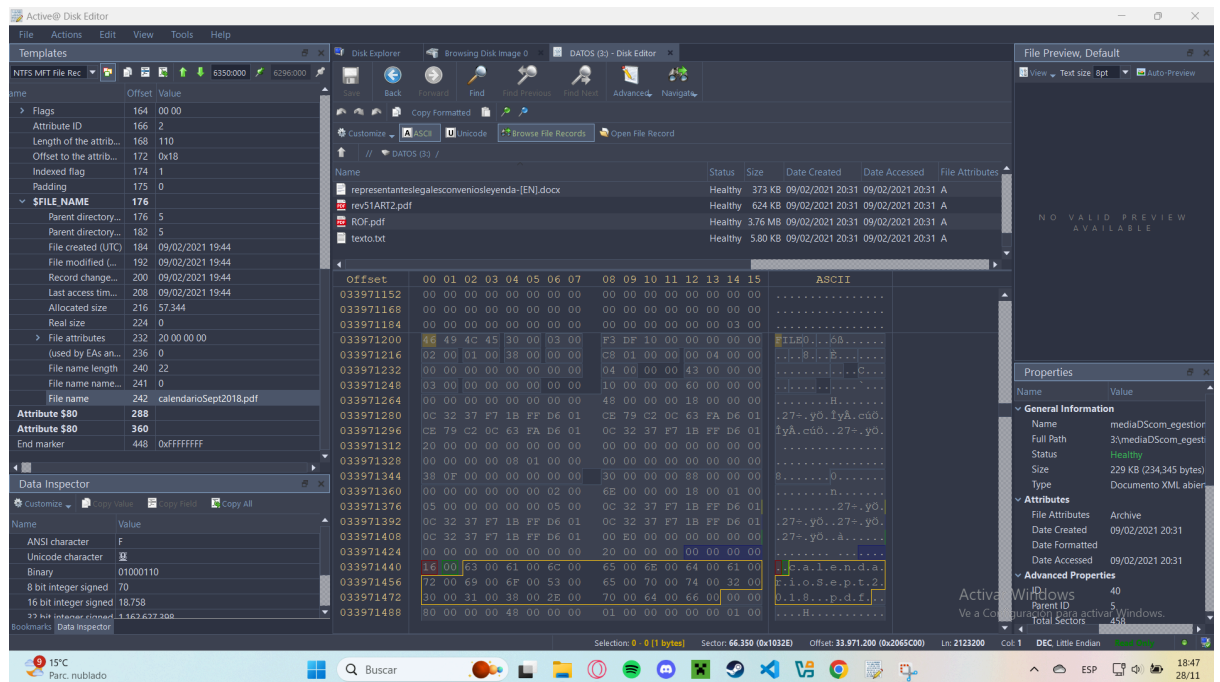
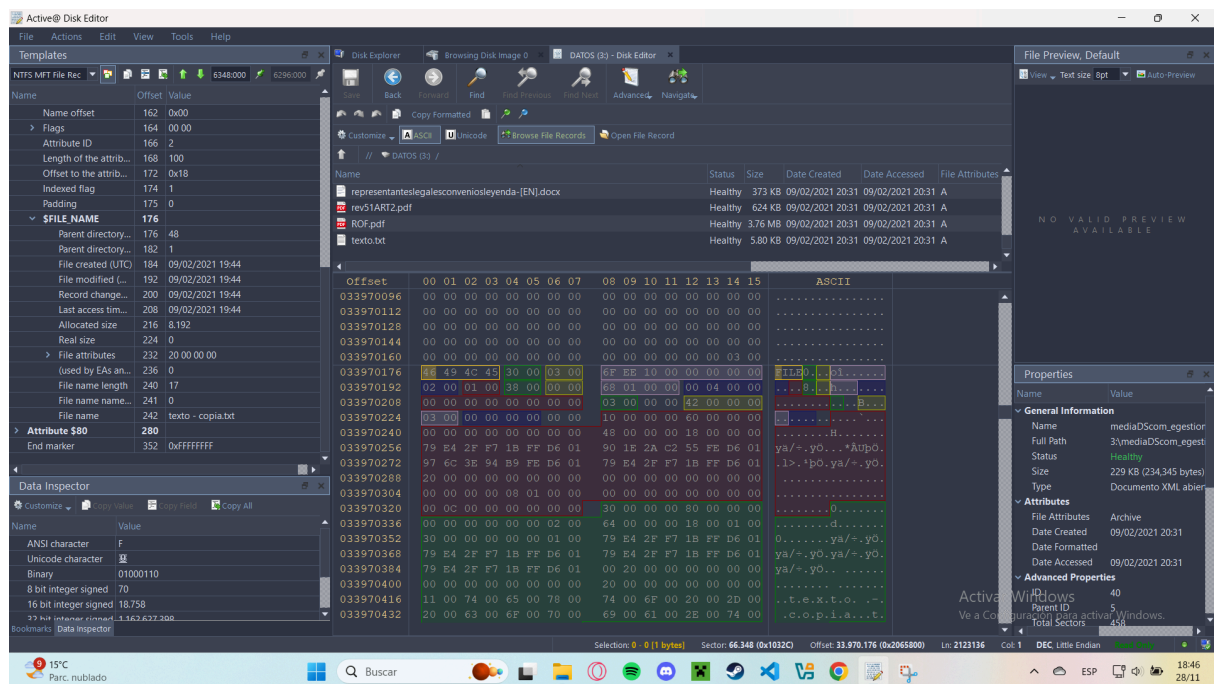
directorios que aparecen en la imagen de disco “datos.dd” de la presente práctica: el directorio raíz, el directorio “carpeta” y el directorio correspondiente a la papelera de reciclaje. Procesa estos ficheros con la herramienta “Indx2Csv”. Analiza qué ficheros hay y ha habido en los diferentes directorios..... 16

9. Actividad:..... 19

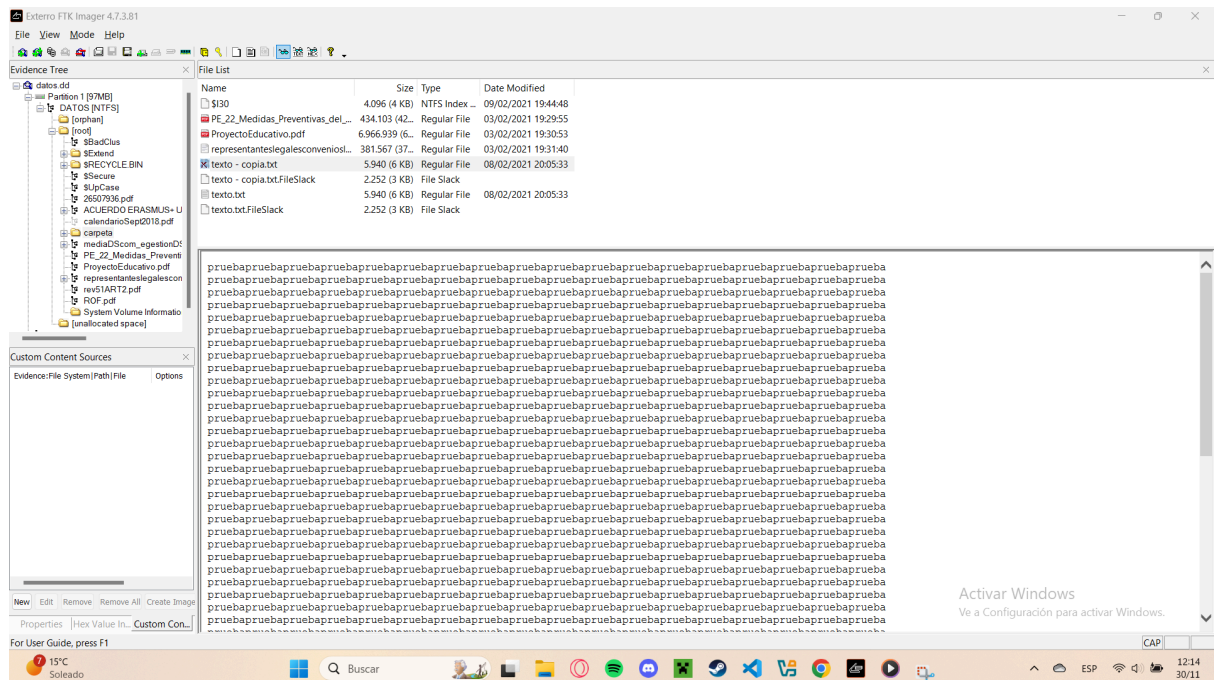
a. Instalar la herramienta de recuperación de ficheros automatizada “Recuva”. Monta con “FTK Imager” la imagen de disco “datos.dd” y usa la herramienta para recuperar todos los ficheros que te sea posible. Compara los resultados obtenidos con los ficheros que la herramienta “FTK Imager” es capaz de recuperar (Marcados con el símbolo aspa de eliminación)..... 19

1. Actividad:

a. Localiza una entrada cualquiera correspondiente al fichero borrado, por ejemplo yo he encontrado “texto - copia.txt”, y realiza una captura de pantalla. Posición de memoria. Pista: vete a la posición 03397XXXX.



b. Recupera el fichero mediante la herramienta FTK Imager (se encuentra en la carpeta papelera).



2. Actividad:

a. ¿Dónde puedo encontrar las fechas de creación, modificación y acceso?

Attribute \$10:

Attribute	Value	Offset
\$STANDARD_INFORMATION	080	
File created (UTC)	080	09/02/2021 19:44
File modified (UTC)	088	08/02/2021 20:05
Record changed (UTC)	096	09/02/2021 8:00
Last access time (UTC)	104	09/02/2021 19:44

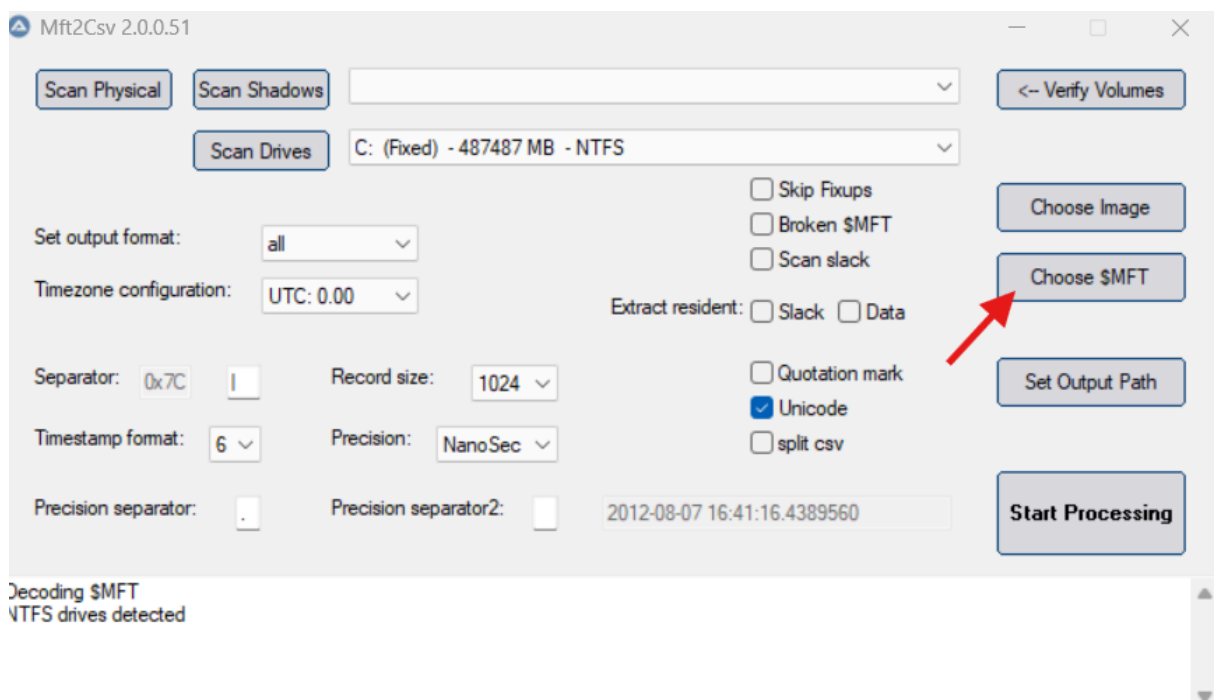
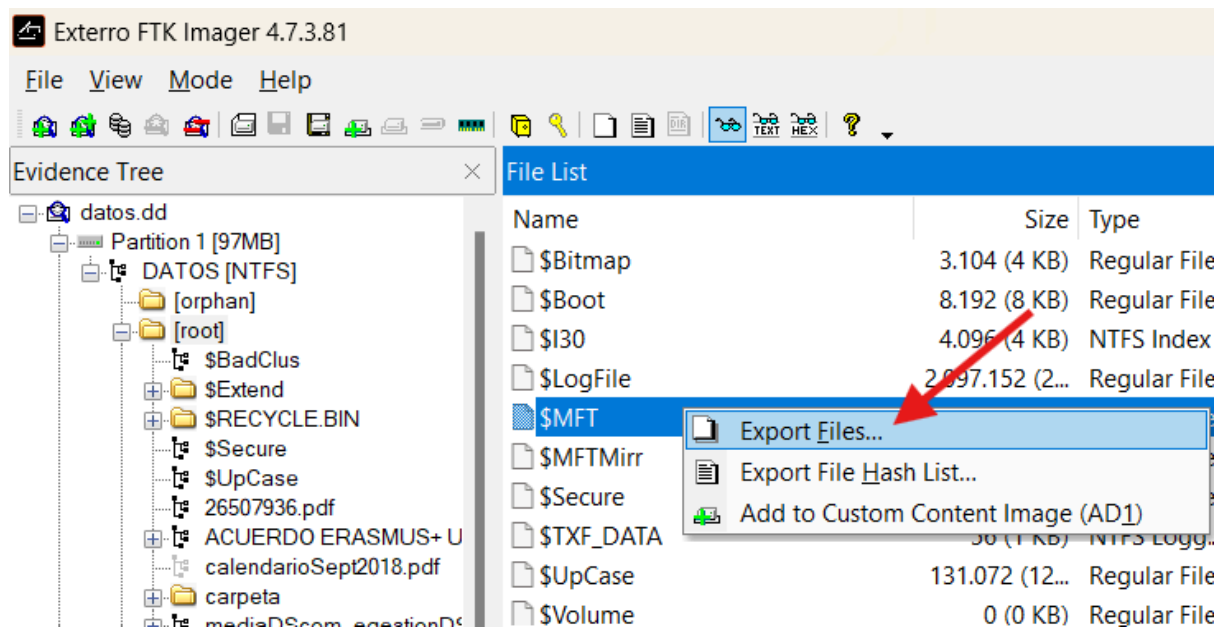
b. ¿Qué significa la propiedad non-resident y sus valores asociados 0/1?

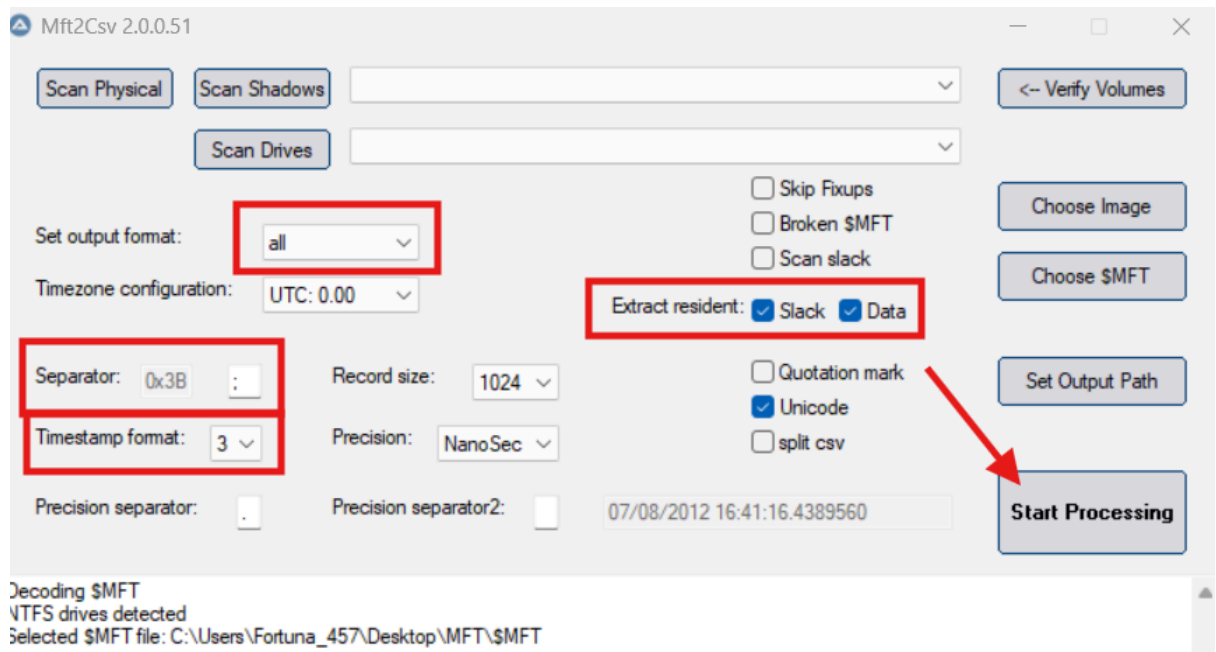
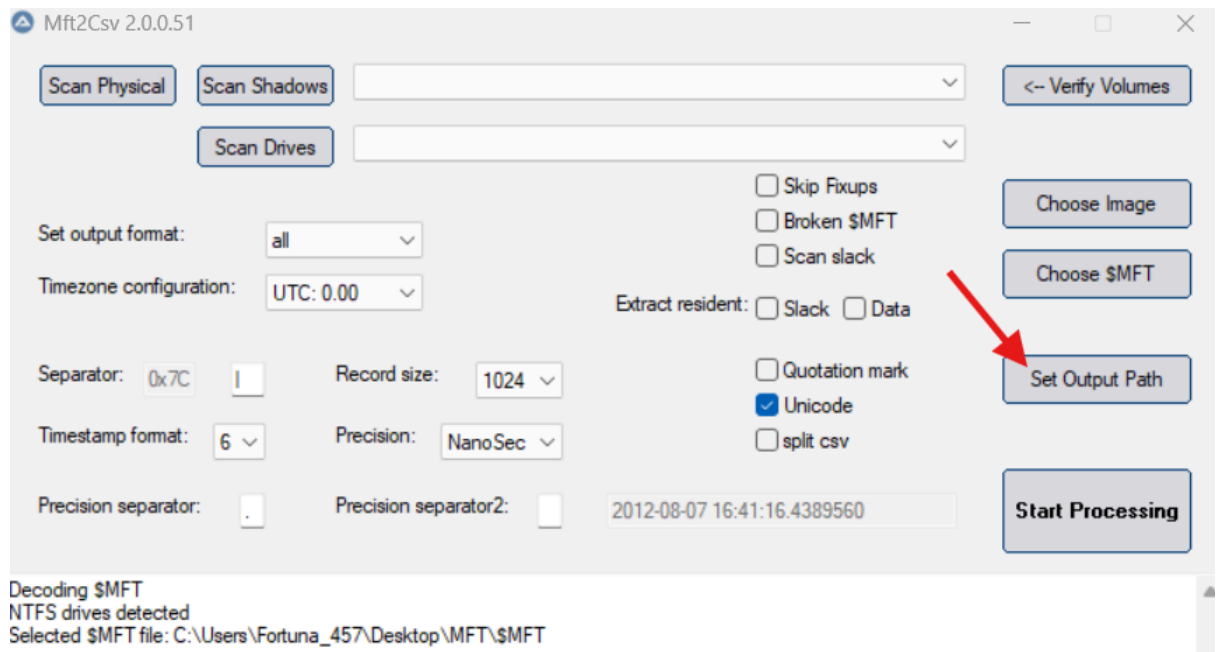
Attribute	Value	Offset
Attribute \$10	056	
Attribute type	056	0x10
Length (including header)	060	96
Non-resident flag	064	0

Significa que la información no está ahí, en el archivo en sí, sino en alguna otra parte del disco.

3. Actividad:

a. Exportar el fichero de metadatos \$MFT usando FTK, procesarla con la herramienta MFT2CSV e importarla en un editor de hojas de cálculo con el fin de analizar los atributos. Nos interesa estudiar qué archivos se han borrado y en qué fecha. Realiza un filtrado por el campo “in use” a estado ‘0’ (borrado) y/o por el campo “RecordActive” = DELETED/ALLOCATED para obtener las fecha/hora de borrado.





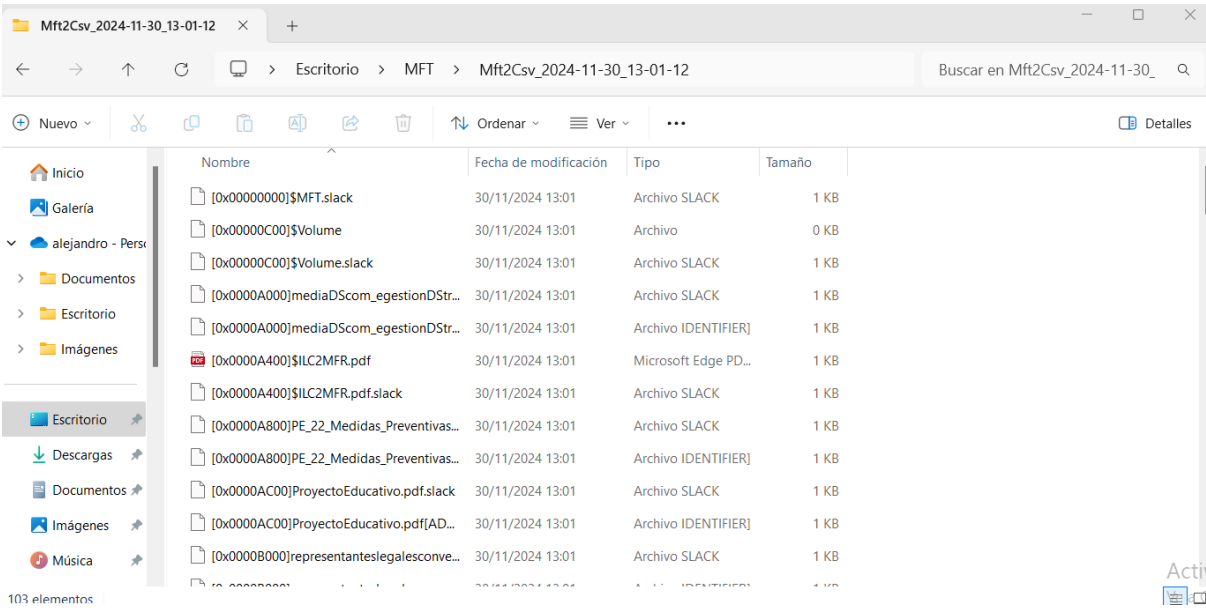
Parsing finished

Job took:
3 seg.

Output can be found in:
C:\Users\Fortuna_457\Desktop\MFT\Mft2Csv_2024-11-30_13-01-12

Aceptar

ANÁLISIS FORENSE



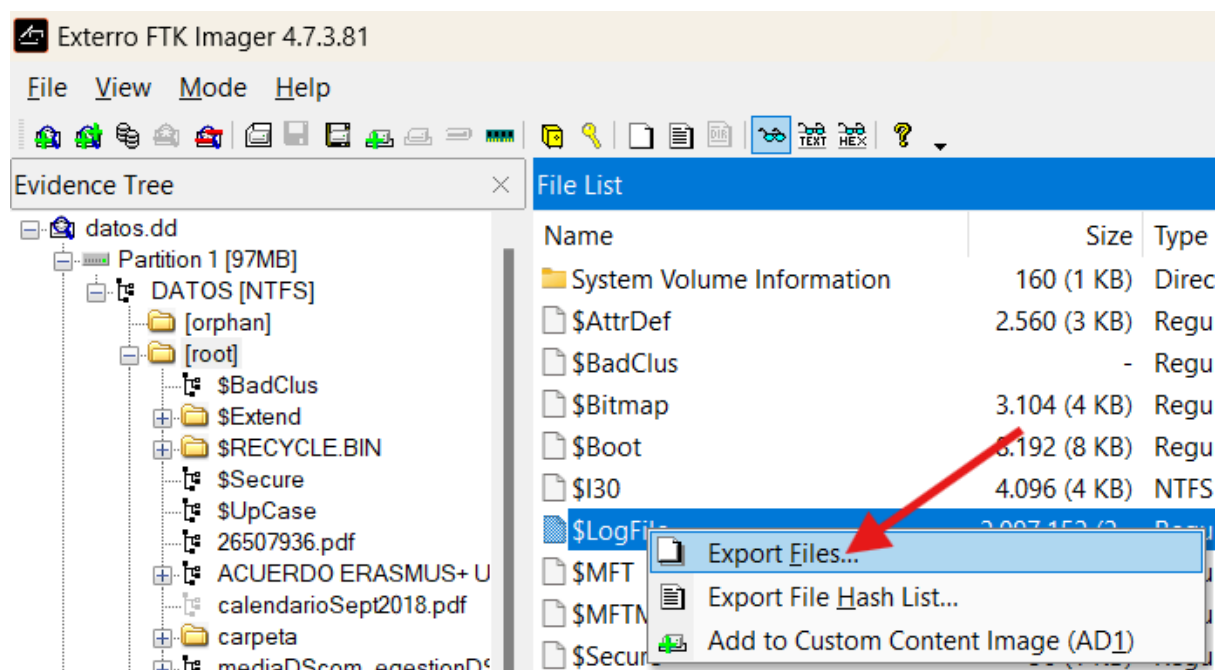
Archivo de origen Comma Separated Values

- Mft.csv
- Mft-All-I30-Entries.csv
- Mft-DATA.csv
- Mft-LOGGED_UTILITY_STREAM.csv
- Mft-ObjectId-Entries.csv
- Mft-TXF_DATA.csv

	J	M	V
1	FN_FileName	RecordActive	SI_RTime
68	texto - copia.txt	DELETED	09/02/2021 19:44:23.0319225
69	calendarioSept2018.pdf	DELETED	09/02/2021 19:44:23.0797836
258			
259			

4. Actividad:

a. Exportar el fichero de metadatos \$LogFile, que junto a la \$MFT del apartado anterior proporcionará datos sobre las transacciones realizadas en el sistema de archivos. Procesar los ficheros con la herramienta NTFS LogFileParse para decodificar la información y obtener un CSV. Buscar las transacciones donde el campo "If_RedoOperation" valga "DeallocateFileRecordSegment" para localizar fichero borrados definitivamente puesto que como su nombre indica la operación fue desasignar el segmento del registro del fichero.



NTFS \$LogFile Parser 2.0.0.46

Help

\$LogFile: C:\Users\Fortuna_457\Desktop\MFT\\$_LogFile Select \$LogFile

Fragment: Broken transaction fragment (optional) Select fragment

MFT: ers\Fortuna_457\Desktop\MFT\Mft2Csv_2024-11-30_13-17-29\Mft.csv Get MFT csv

Timestamp format: 3 Precision: NanoSec ☐ split csv Precision separator: .

Set decoded timestamps to specific region: UTC: 0.00 Precision separator2: ☐ skip sqlite3

Timestamp ErrorVal: 0000-00-00 00:00:00 07/08/2012 16:41:16.4389560 ☐ Skip Fixups

Set separator: : ☐ 0x3B ☐ Unicode ☐ Reconstruct data runs ☐ Rebuild headers (in slack) ☐ Broken \$LogFile

Sectors per cluster: 8 MFT record size: 1024 LSN error level: 0.1 10 % (up/down)

☐ Source is from 32-bit OS ☐ Extract non + resident updates of min size: 2

LSN's to trigger verbose output (comma separate): Start Exit

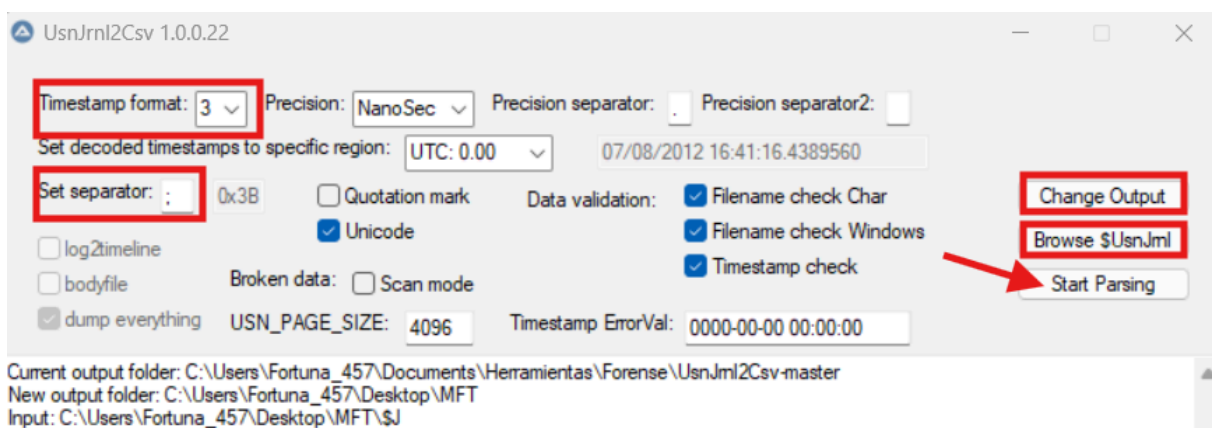
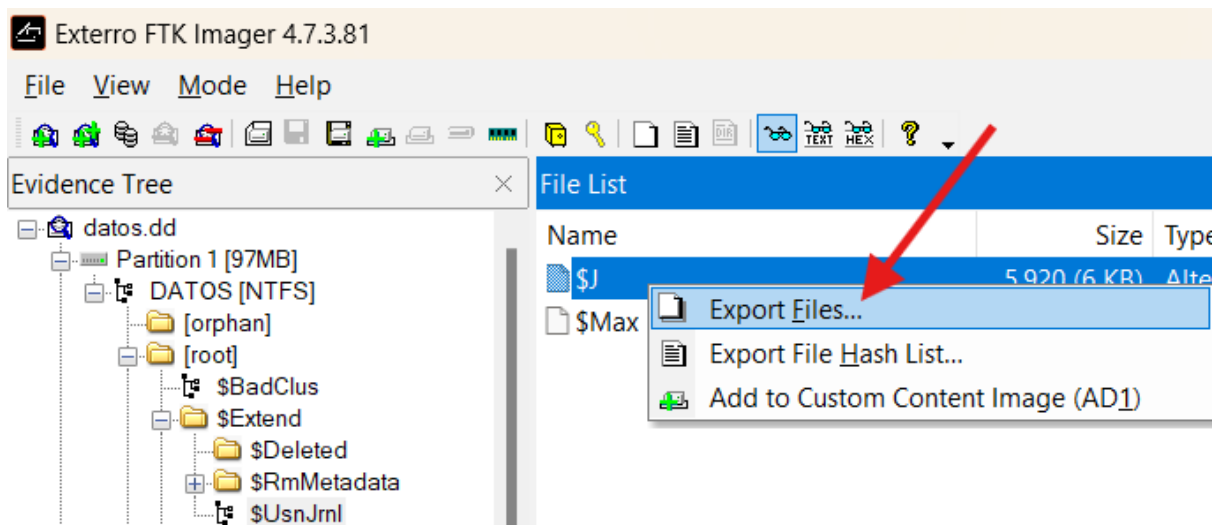
▼ Archivo de origen Comma Separated Values

LogFile.csv 30/11/2024 13:46 Archivo de origen ... 593 KB

	G	J
1	If_RedoOperation	If_FileName
5	DeallocateFileRecordSegment	
87	DeallocateFileRecordSegment	
1448	DeallocateFileRecordSegment	borrado_1.txt
1546	DeallocateFileRecordSegment	texto - copia.txt
1611	DeallocateFileRecordSegment	ProyectoEducativo.pdf
1666	DeallocateFileRecordSegment	\$UsnJrnl
1986	DeallocateFileRecordSegment	CuestionariodehabitoslectoresANALISIS.pdf
1997	DeallocateFileRecordSegment	calendarioSept2018.pdf
2023	DeallocateFileRecordSegment	nombre.txt

5. Actividad:

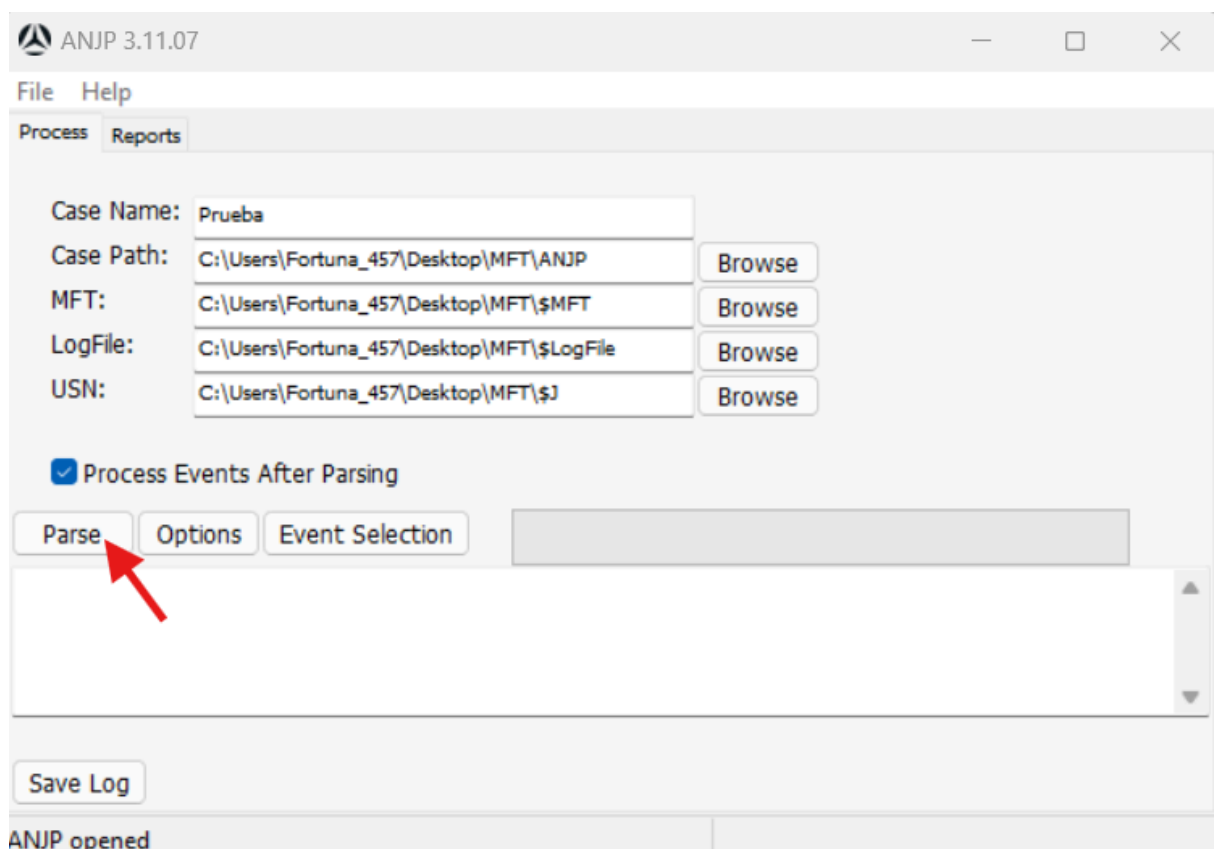
a. Exportar el fichero de metadatos correspondiente al \$USNJournal (\$Extend -> \$USNjrl -> \$J). Procesado con la herramienta UsnJrl2Csv para decodificar la información que almacena. Filtra la información resultante por el campo “Reason” = “CLOSE+DELETE” para obtener las fechas de cuando se produjo el borrado definitivo de los ficheros.



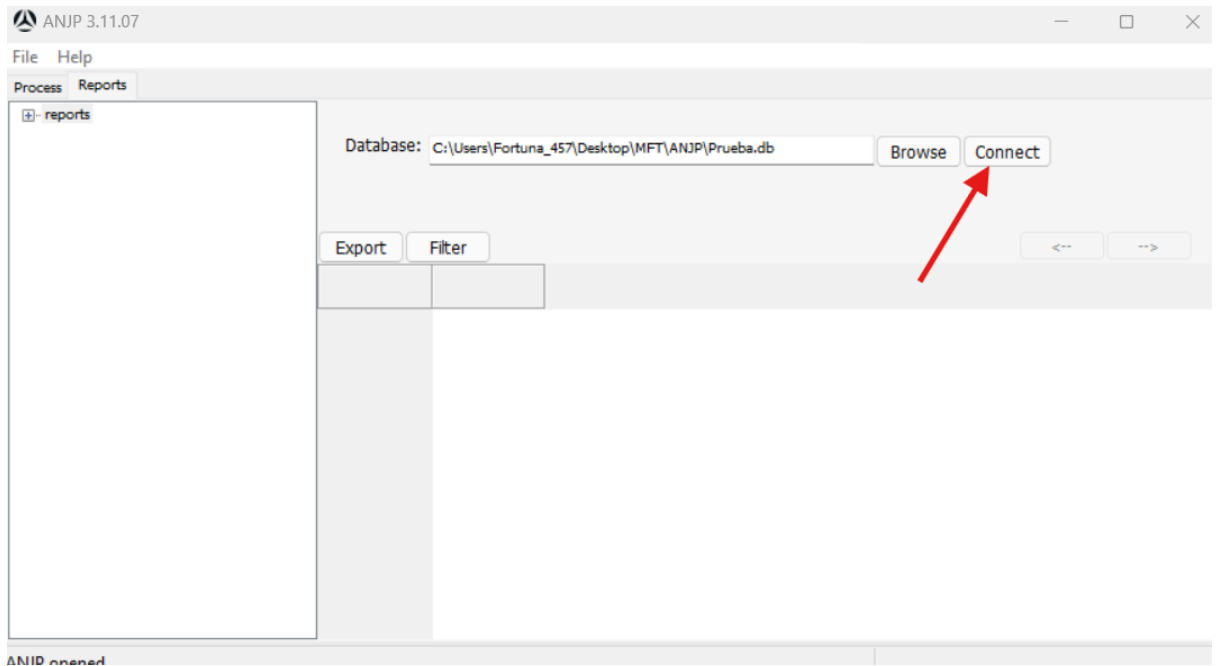
UsnJrnl_2024-11-30_15-12-24.csv	30/11/2024 15:12	Archivo de origen ...	9 KB
D58	fx	09/02/2021 19:44:48.2312284	
	B	D	E
1	FileName	Timestamp	Reason
39	CuestionariodehabitoslectoresANALISIS.pdf	09/02/2021 19:44:32.2920106	CLOSE+FILE_DELETE
40	calendarioSept2018.pdf	09/02/2021 19:44:32.2920106	CLOSE+FILE_DELETE
41	nombre.txt	09/02/2021 19:44:39.0896525	CLOSE+FILE_DELETE
58	texto - copia.txt	09/02/2021 19:44:48.2312284	CLOSE+FILE_DELETE

6. Actividad:

a. En este apartado, vamos a utilizar la herramienta ANJP para realizar un procesamiento conjunto de la \$MFT, \$LogFile y \$USNjrnl. Verás que trabaja con la misma información de los apartados anteriores de forma integrada en la misma herramienta. Dispone de una pestaña donde decodificar la información (Parse) y otra donde visualizar los resultados (Report). Se trata de una herramienta de pago. Se pide utilizarla y realizar un par de capturas de pantalla del informe de resultados que ofrece.



ANÁLISIS FORENSE



\$USNjrl:

	USN Evt Type	USN Evt ID	USN Evt Hit	USN Evt Rule File	USN Rcd File Name	USN E Fulln
1	Transaction Event	Deletions	1		CuestionariodehabitoslectoresANALISIS.pdf	\Cuestionariodehabitosle
2	Transaction Event	Deletions	2		calendarioSept2018.pdf	\calendarioSept2018.pdf
3	Transaction Event	Deletions	3		nombre.txt	\nombre.txt
4	Transaction Event	Deletions	4		texto - copia.txt	\carpeta\texto - copia.tx

\$MFT:

	Record Name	MFT Hdr Entry Ref	MFT Hdr Entry #	MFT Hdr Seq #	MFT Hdr Link Count	MFT Hdr Flags	MFT Hdr Active	MFT LS
1	\carpeta\texto - copia.txt	66-2	66	2	1	File	Unallocated	11096
2	\calendarioSept2018.pdf	67-2	67	2	1	File	Unallocated	11059
3	\calendarioSept2018.pdf:Zone.Identifier	67-2	67	2	1	File	Unallocated	11059

\$LogFile:

	LogFile Rcd Name	LSN Redo Op_b	LSN Redo Op	LSN Undo Op_b	LSN Undo Op	LogFile Rcd LSN	Log Tarç
1		0300	DeallocateFileRecordSegment	0200	InitializeFileRecordSegment	1109615	66

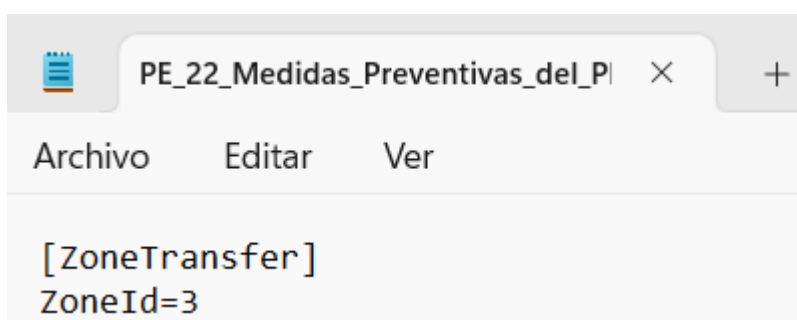
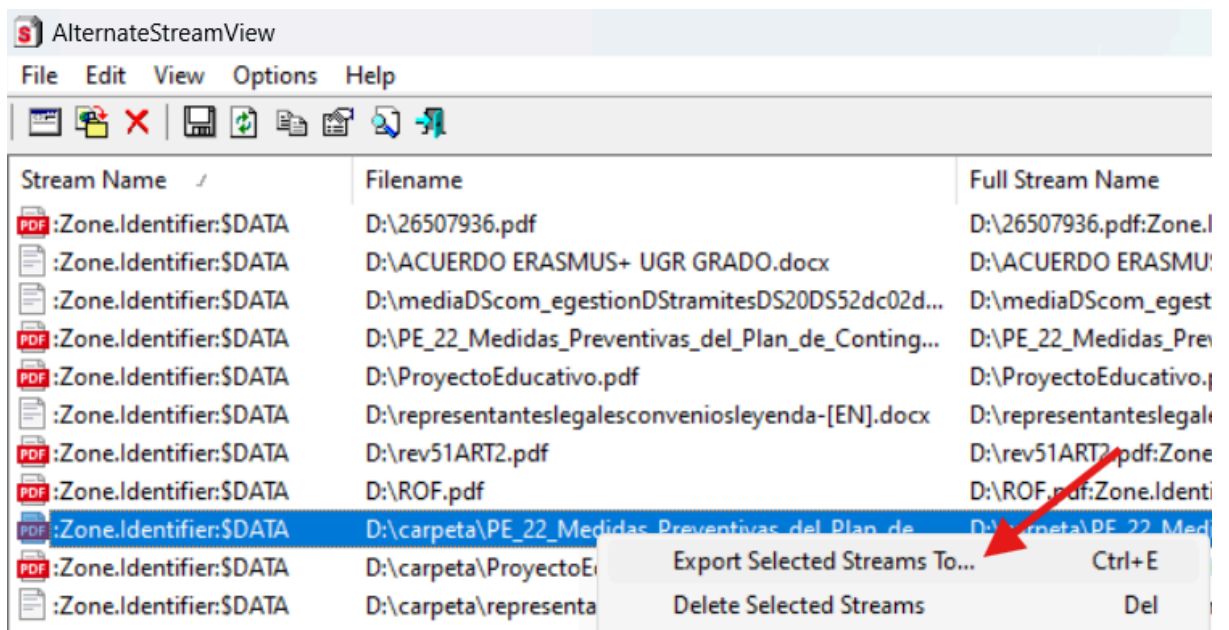
7. Actividad:

a. Utiliza las herramientas “FTK Imager” y “AlternateDataViewer” para estudiar el origen de los ficheros que aparecen en la imagen “datos.dd”. Haz una captura de pantalla con cada herramienta donde se visualice un ejemplo.

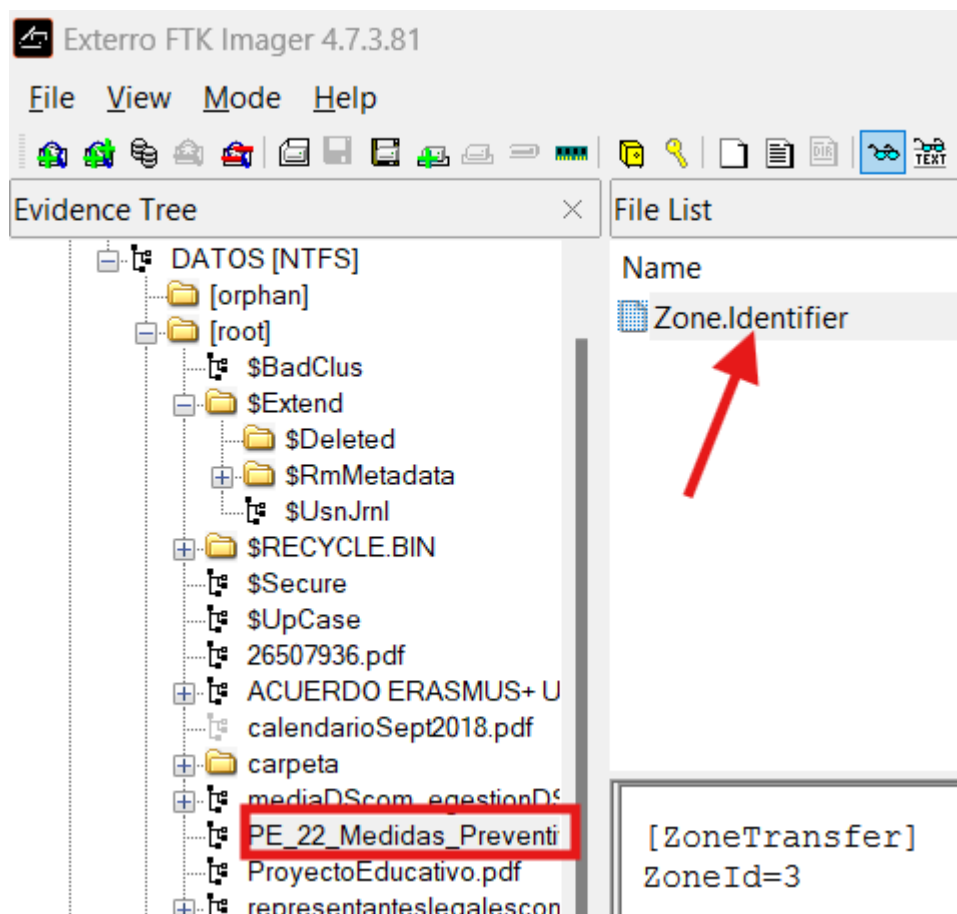
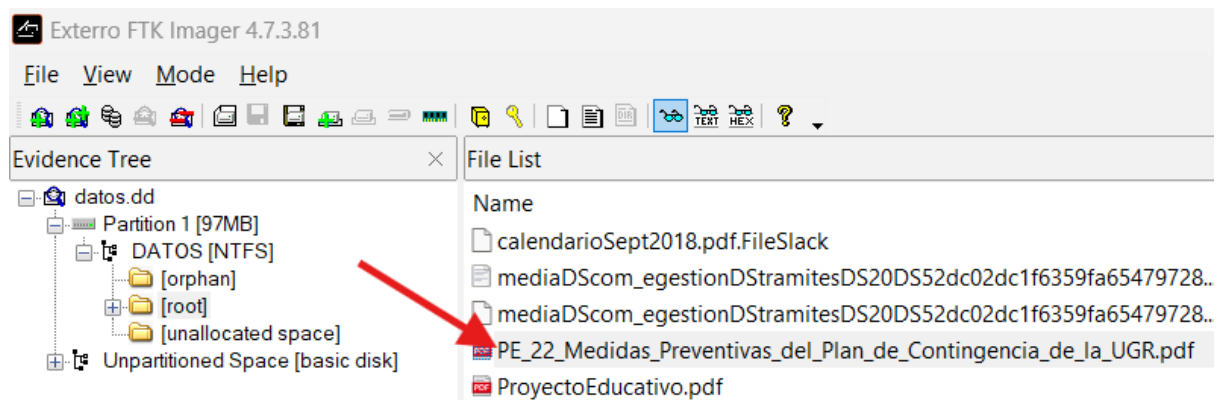
Zone Identifiers:

- ZoneId=0: Local machine.
- ZoneId=1: Local intranet.
- ZoneId=2: Trusted sites.
- ZoneId=3: Internet.
- ZoneId=4: Restricted sites.

AlternateDataViewer:

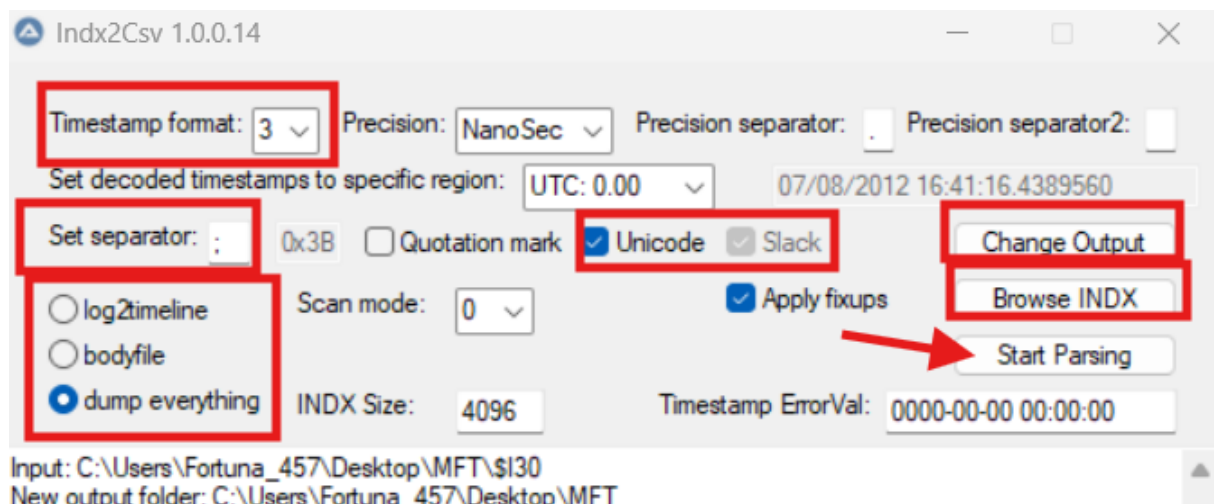


FTK Imager:



8. Actividad:

a. Exportar los ficheros de metadatos de tipo índice de directorios (\$I30) de los tres directorios que aparecen en la imagen de disco “datos.dd” de la presente práctica: el directorio raíz, el directorio “carpeta” y el directorio correspondiente a la papelera de reciclaje. Procesa estos ficheros con la herramienta “Indx2Csv”. Analiza qué ficheros hay y ha habido en los diferentes directorios.



Indx_2024-12-01_12-21-11.log

Indx_I30_Entries_2024-12-01_12-21-11.csv

Indx_ObjIdO_Entries_2024-12-01_12-21-11.csv

Indx_ReparsR_Entries_2024-12-01_12-21-11.csv

Root:

L10 ▾ | fx 09/02/2021 19:31:56.1979542

	E	F
1	FromIndxSlack	FileName
2	0	\$AttrDef
3	0	\$BadClus
4	0	\$Bitmap
5	0	\$Boot
6	0	\$Extend
7	0	\$LogFile
8	0	\$MFT
9	0	\$MFTMirr
10	0	\$RECYCLE.BIN
11	0	\$Secure
12	0	\$UpCase
13	0	\$Volume
14	0	.
15	0	26507936.pdf
16	0	ACUERDO ERASMUS+ UGR GRADO.docx
17	0	carpeta
18	0	mediaDScom_egestionDStramitesDS20DS52dc02dc1f6359fa654797289a31938f.docx
19	0	PE_22_Medidas_Preventivas_del_Plan_de_Contingencia_de_la_UGR.pdf
20	0	ProyectoEducativo.pdf
21	0	representanteslegalesconveniosleyenda-[EN].docx
22	0	rev51ART2.pdf
23	0	ROF.pdf
24	0	System Volume Information
25	0	texto.txt
26	1	texto.txt
27	1	texto.txt
28	1	texto.txt
29	1	texto.txt
30		

Carpeta:

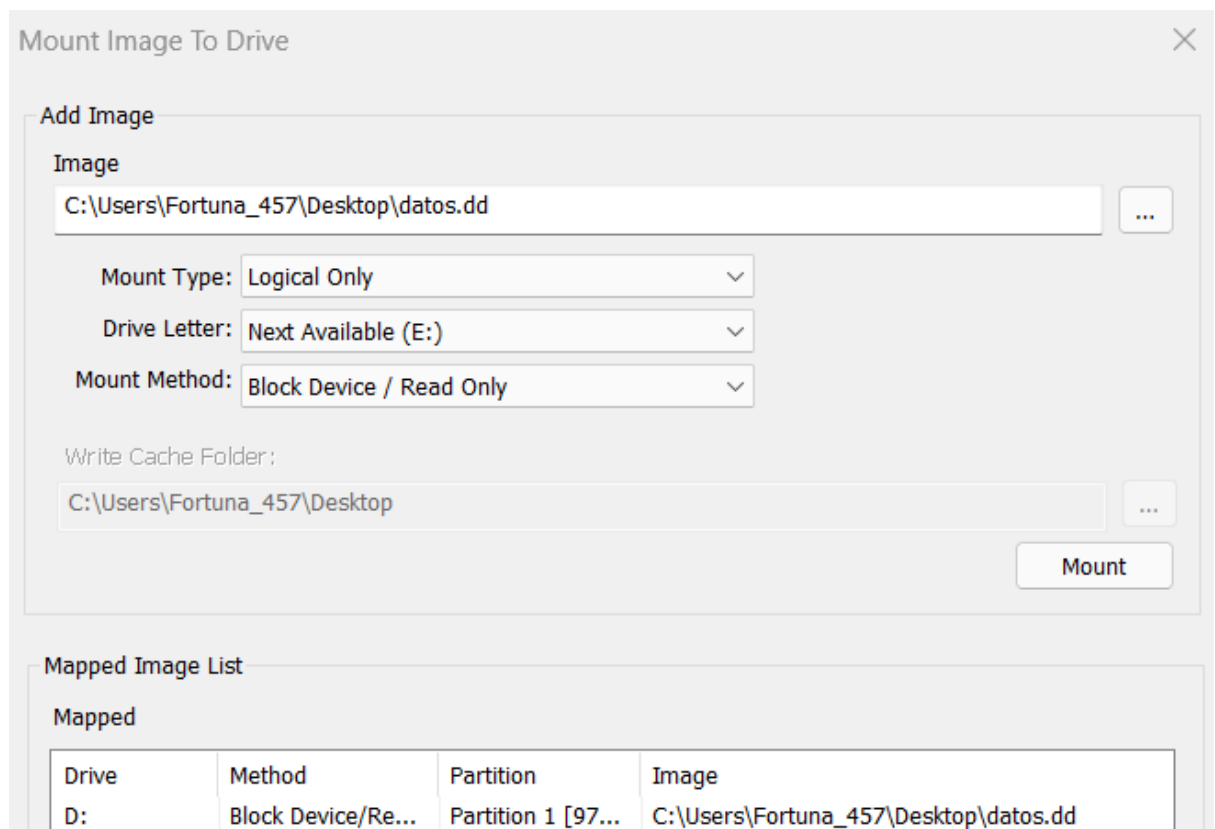
E	F
FromIndxSlack	FileName
0	PE_22_Medidas_Preventivas_del_Plan_de_Contingencia_de_la_UGR.pdf
0	ProyectoEducativo.pdf
0	representanteslegalesconveniosleyenda-[EN].docx
0	texto.txt
1	texto.txt
1	texto.txt

\$RECYCLE.BIN:

E	F
FromIndxSlack	FileName
0	\$IBHU4I1.pdf
0	\$IL8AQ5K.pdf
0	\$ILC2MFR.pdf
0	\$IQPCWVG.pdf
0	\$IXU6R2O.pdf
0	\$RBHU4I1.pdf
0	\$RL8AQ5K.pdf
0	\$RLC2MFR.pdf
0	\$RQPCWVG.pdf
0	\$RXU6R2O.pdf
0	desktop.ini

9. Actividad:

a. Instalar la herramienta de recuperación de ficheros automatizada “Recuva”. Monta con “FTK Imager” la imagen de disco “datos.dd” y usa la herramienta para recuperar todos los ficheros que te sea posible. Compara los resultados obtenidos con los ficheros que la herramienta “FTK Imager” es capaz de recuperar (Marcados con el símbolo aspa de eliminación).



Recuva:

Recuva Wizard

File type
What sort of files are you trying to recover?

☒ **All Files**
Show all files.

☐ **Pictures**
Show only files of common image formats, such as digital camera photos.

☐ **Music**
Show only files of common audio formats, like MP3 player files.

☐ **Documents**
Show only files of common office document formats, such as Word and Excel files.

☐ **Video**
Show only video files, like digital camera recordings.

☐ **Compressed**
Show only compressed files.

☐ **Emails**
Show only emails from Thunderbird, Outlook Express, Windows Mail and Microsoft Outlook.

< Back Next > Cancel

Recuva Wizard

File location
Where were the files?

☐ **I'm not sure**
Search everywhere on this computer.

☐ **On my media card or iPod**
Search any removable drives (except CDs and floppies) for deleted files.

☐ **In My Documents**
Search user documents folders.

☐ **In the Recycle Bin**
Search for files deleted from the Recycle Bin.


☒ **In a specific location**


D:\


Browse...

☐ **On a CD / DVD**

< Back Next > Cancel



**Recuva**

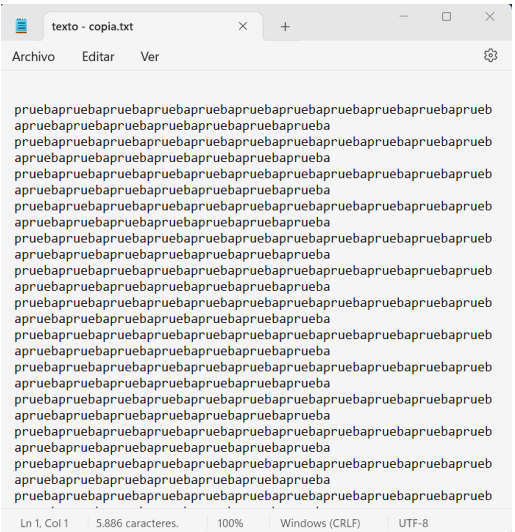
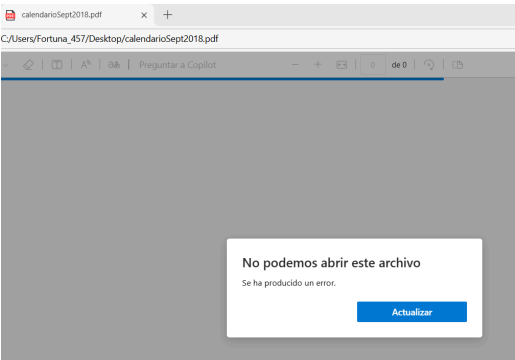
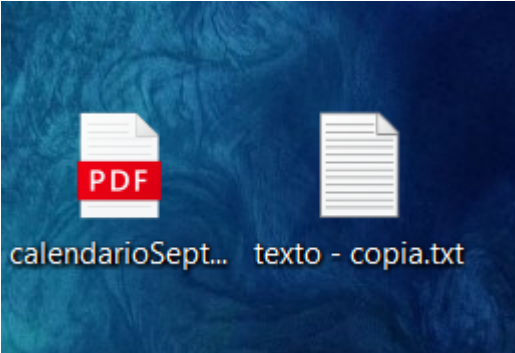
**Recuva** v1.53.1087 (64-bit)
Windows 10 64-bit
12th Gen Intel Core i5-12450H, 16,0GB RAM, Intel UHD Graphics



Select the files you want to Recover by ticking the boxes and then pressing Recover.
For the best results, restore the files to a different drive.

Switch to advanced mode

<input type="checkbox"/>	Filename	Path	Last Modified	Size	State	Comments
<input type="checkbox"/>	 texto - copia.txt	D:\carpeta\	08/02/2021 2...	6 KB	Excellent	No overw...
<input type="checkbox"/>	 calendarioSept2018.pdf	D:\	03/02/2021 2...	53 KB	Excellent	No overw...



FTK Imager:

