

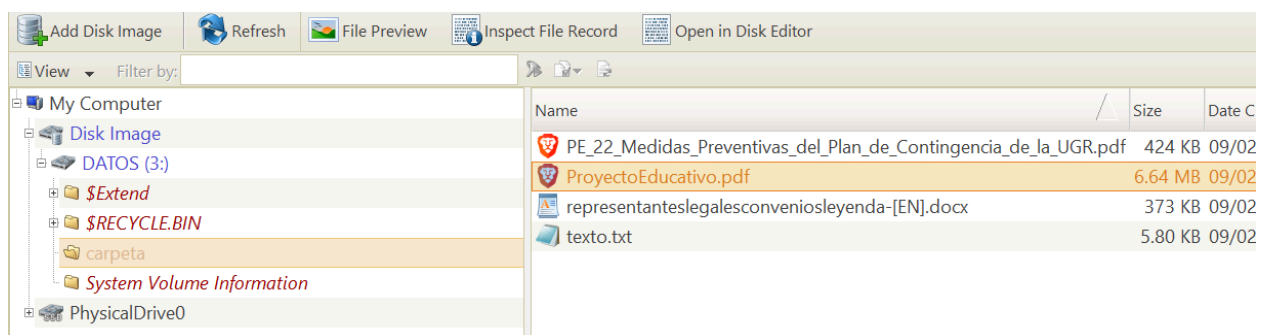
Practica 2

Análisis de NTFS

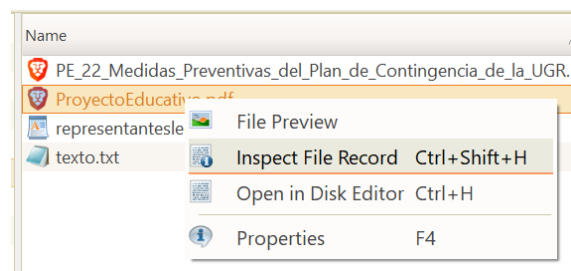
En esta instancia, se nos encomienda llevar a cabo un análisis forense de la imagen suministrada, la cual cuenta con un sistema de archivos NTFS.

1. Identificación de registros MFT borrados con Active Disk Editor

Podemos identificar archivos que han sido eliminados utilizando la herramienta [Active Disk Editor](#). Para lograrlo, una vez que hayamos abierto la herramienta y cargado la evidencia, nos dirigiremos al directorio '**carpeta**'.



Vamos a examinar estos archivos. Podemos abrir el que deseemos seleccionando '**botón secundario > Inspect File Record**'.



Cuando estemos en el inspector de registros de archivos, podremos identificar los registros eliminados observando la propiedad **FLAGS** (campo 'in use' = '0'). Como se puede apreciar en la imagen, el archivo que he seleccionado está en uso, lo que significa que no ha sido eliminado.

Sequence number	016	1	033968048	00 00 00 00 00 00 00 00
Hard link count	018	1	033968064	00 00 00 00 00 00 00 00
Offset to the first ...	020	0x38	033968080	00 00 00 00 00 00 00 00
Flags	022	01 00	033968096	00 00 00 00 00 00 00 00
In use	:0	1	033968112	00 00 00 00 00 00 00 00
Directory	:1	0	033968128	46 49 4C 45 30 00 03 00
Real size of the FIL...	024	456	033968144	01 00 01 00 38 00 01 00
Allocated size of t...	028	1.024	033968160	00 00 00 00 00 00 00 00
Base FILE record	032	0	033968176	03 00 00 00 00 00 00 00
Next attribute ID	040	4	033968192	00 00 00 00 00 00 00 00
ID of this record	044	64	033968208	C8 96 28 F7 1B FF D6 01
Update sequence ...	048	03 00	033968224	19 92 4E 94 B9 FE D6 01
Update sequence ...	050	00 00 00 00	033968240	20 00 00 00 00 00 00 00
Attribute \$10	056		033968256	00 00 00 00 00 00 01 00
Attribute \$30	152		033968272	58 07 00 00 00 00 00 00
Attribute \$80	288		033968288	00 00 00 00 00 00 02 00
Attribute \$80	360		033968304	30 00 00 00 00 00 01 00
End marker	448	0xFFFFFFFF	033968320	C8 96 28 F7 1B FF D6 01

Busquemos un archivo que coincida con la propiedad que hemos mencionado. Nos desplazamos por el inspector, observando el valor de 'File0', lo cual nos ayuda a identificar el inicio del fichero.

033967072	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
033967088	00 00 00 00 00 00 00 00	00 00 00 00 00 00 04 00
033967104	46 49 4C 45 30 00 03 00	F3 E9 10 00 00 00 00 00	FILE0...óé.....	.0.....
033967120	02 00 01 00 38 00 01 00	78 01 00 00 00 04 00 00	...8...x.....	..8.ÿ.È.
033967136	00 00 00 00 00 00 00 00	03 00 00 00 3F 00 00 00?...?
033967152	02 00 00 00 00 00 00 00	10 00 00 00 60 00 00 00``
033967168	00 00 00 00 00 00 00 00	48 00 00 00 18 00 00 00H.....H...
033967184	3E 0F FA 03 1C FF D6 01	3E 0F FA 03 1C FF D6 01	>.ú..ÿÖ.>.ú..ÿÖ.	.M.ũ.M.ũ
033967200	3E 0F FA 03 1C FF D6 01	3E 0F FA 03 1C FF D6 01	>.ú..ÿÖ.>.ú..ÿÖ.	.M.ũ.M.ũ

Podemos dirigirnos a estas posiciones para inspeccionarlas haciendo clic derecho sobre ellas y seleccionando 'Set Template Position'.

967104	46 49 4C 45 30 00 03 00	10
967120	Undo	Ctrl+Z
967136	Redo	Ctrl+Y
967152	Revert changes	
967168	Copy	Ctrl+C
967184	Copy Formatted	Ctrl+Shift+C
967200	Paste	Ctrl+V
967232	Set Template Position	
967248	Set Template Copy Position	

En la posición **033970176**, he identificado un registro eliminado que coincide con la propiedad de flags 'in use = 0'.

Offset to the first ...	020	0x38	033970144	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
Flags	022	00 00	033970160	00 00 00 00 00 00 00 00	00 00 00 00 00 00 03 00	
In use	:0	0	033970176	46 49 4C 45	30 00 03 00	6F EE 10 00 00 00 00 00	FILE0...01.....	..0....
Directory	:1	0	033970192	02 00 01 00	38 00 00 00	68 01 00 00 00 04 00 00	...8...h.....	..8.0.E.
Real size of the FIL...	024	360	033970208	00 00 00 00 00 00 00 00	03 00 00 00	42 00 00 00B...B.
Allocated size of t...	028	1.024	033970224	03 00 00 00 00 00 00 00	10 00 00 00	60 00 00 00
Base FILE record	032	0	033970240	00 00 00 00 00 00 00 00	48 00 00 00	18 00 00 00H.....H...
Next attribute ID	040	3	033970256	79 E4 2F F7	1B FF D6 01	90 1E 2A C2 55 FE D6 01	yä/÷.ÿÖ...*ÄÛö.	...ü?...ü

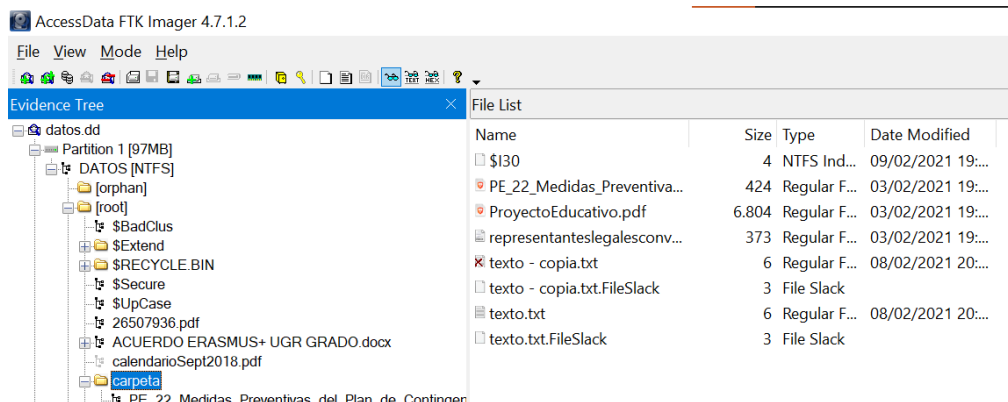
Podemos ver que se llama **'texto - copia.txt'**

File attribu...	232	20 00 00 00	033970224
(used by E...	236	0	033970240
File name l...	240	17	033970256
File name ...	241	0	033970272
File name	242	texto - copia.txt	033970288
Attribute \$80	280		033970304
End marker	283	0xFFFFFFFF	033970320

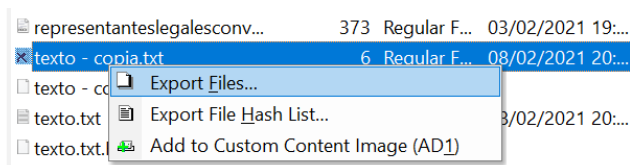
He encontrado otro registro eliminado en la posición **033971200**, denominado **'calendarioSept2019.pdf'**.

Real size	224	0	033971120	00 00 00 00
File attribu...	232	20 00 00 00	033971136	00 00 00 00
(used by E...	236	0	033971152	00 00 00 00
File name l...	240	22	033971168	00 00 00 00
File name ...	241	0	033971184	00 00 00 00
File name	242	calendarioSept2018.pdf	033971200	46 49 4C 45
Attribute \$80	288		033971216	02 00 00 00
Attribute \$80	360		033971232	00 00 00 00
End marker	448	0xFFFFFFFF	033971248	03 00 00 00

Podemos recuperar estos archivos utilizando FTK Imager. Para ello, cargamos la evidencia, y con esta herramienta nos resultará sumamente fácil localizar los elementos eliminados, ya que la propia herramienta los señala con una **'X'**.



Podemos exportar los archivos haciendo clic derecho en el botón 'Export Files...!.



Finalmente, estos son los archivos que hemos recuperado, los cuales habían sido eliminados.

Nombre	Fecha de modificación	Tipo	Tamaño
calendarioSept2018	03/02/2021 20:30	Brave HTML Document	53 KB
texto - copia	08/02/2021 21:05	Documento de texto	6 KB

2. Identificación de atributos a bajo nivel

Con la herramienta que hemos utilizado anteriormente, Active Disk Editor, también podemos visualizar los atributos a nivel bajo. Gracias a esto, hemos podido ver previamente los nombres de los archivos. Ahora vamos a explorar qué información contienen estos atributos.

- **\$10**: Contiene información estándar
- **\$30**: Contiene el nombre del fichero
- **\$80**: Hace referencia al data

Mediante el atributo **\$10**, podemos identificar las fechas de creación, modificación y acceso del archivo.

Attribute ID	070	0	033970176	4
Length of the attribute	072	72	033970192	0
Offset to the attribute data	076	0x18	033970208	0
Indexed flag	078	0	033970224	0
Padding	079	0	033970240	0
\$STANDARD_INFORMATION	080		033970256	7
File created (UTC)	080	09/02/2021 19:44	033970272	9
File modified (UTC)	088	08/02/2021 20:05	033970288	2
Record changed (UTC)	096	09/02/2021 8:00	033970304	0
Last access time (UTC)	104	09/02/2021 19:44	033970320	0
File Permissions	112	20 00 00 00	033970336	0
Maximum number of versi...	116	0	033970352	3
Version number	120	0	033970368	7

Cuando el **"Non-Resident Flag"** está activado (establecido en 1), significa que los datos asociados al atributo en cuestión no se almacenan directamente dentro del MFT, sino que se encuentran fuera de este, en sectores fuera de la tabla maestra de archivos. Este caso se presenta cuando los datos son demasiado grandes para almacenarse directamente en el MFT.

Por otro lado, cuando el **"Non-Resident Flag"** está desactivado (establecido en 0), los datos están almacenados directamente dentro del MFT. Esto es más eficiente para datos pequeños, ya que se evita el acceso a sectores adicionales fuera del MFT.

ID of this record	044	66	033970144
Update sequence number	048	03 00	033970160
Update sequence array	050	00 00 00 00	033970176
Attribute \$10	056		033970192
Attribute \$30	152		033970208
Attribute \$80	280		033970224
Attribute type	280	0x80	033970240
Length (including header)	284	72	033970256
Non-resident flag	288	1	033970272
Name length	289	0	033970288
Name offset	290	0x00	033970304
Flags	292	00 00	033970320
Attribute ID	294	1	033970336
First VCN	296	0	

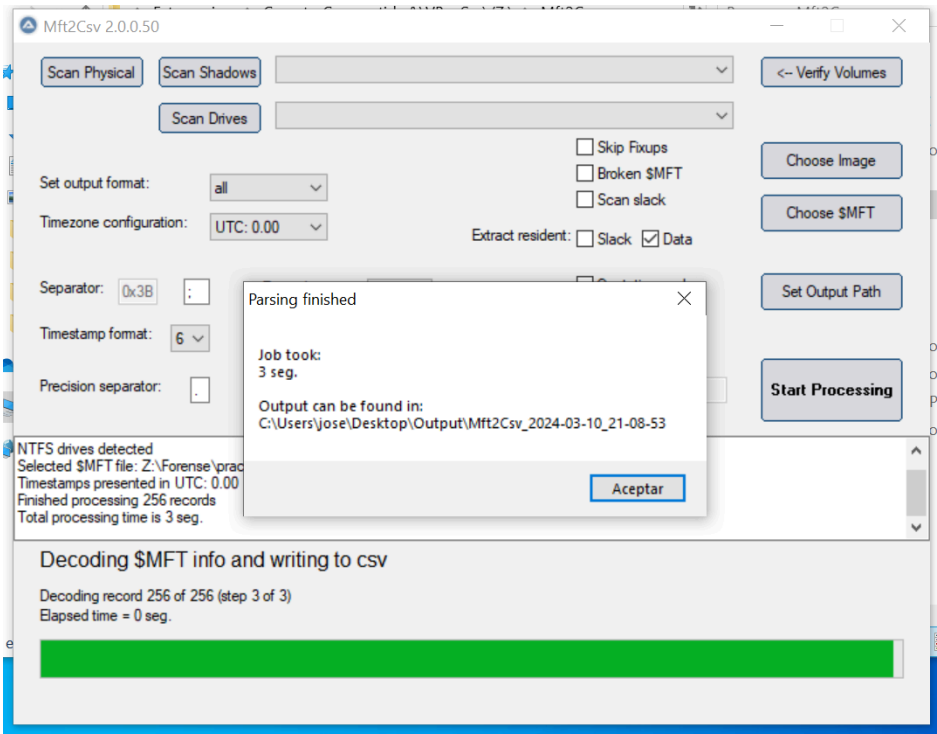
3. Análisis de MFT

En este escenario, exportaremos el archivo **\$MFT** y lo examinaremos. Para lograrlo, utilizaremos la herramienta FTK Imager para realizar la exportación.

3.

The screenshot shows the AccessData FTK Imager 4.7.1.2 interface. On the left, the 'Evidence Tree' shows a partition named 'Partition 1 [97MB]' containing a file system 'DATOS [NTFS]'. Under 'DATOS [NTFS]', there is a folder '[orphan]' and a folder '[root]'. The '[root]' folder contains several files and folders, including '\$BadClus', '\$Extend', '\$RECYCLE.BIN', '\$Secure', '\$UpCase', '26507936.pdf', 'ACUERDO ERASMUS+ UGR GRADO.docx', 'calendarioSept2018.pdf', 'carpeta', 'mediaDScorn_egestionDStramitesDS20DS52dc02dc1f6', 'PE_22_Medidas_Preventivas_del_Plan_de_Contingencia', 'ProyectoEducativo.pdf', 'representanteslegalesconveniosleyenda-[EN].docx', 'rev5TART2.pdf', 'ROF.pdf', 'System Volume Information', and '[unallocated space]'. On the right, the 'File List' shows a table of files. The file '\$MFT' is selected, showing a size of 256 bytes, type 'Regular F...', and date modified '09/02/2021 19:00'. Other files listed include '\$Bitmap', '\$Boot', '\$I30', '\$LogFile', '\$MFTMirr', '\$Secure', '\$TXF_DATA', '\$UpCase', '\$Volume', '26507936.pdf', 'ACUERDO ERASMUS+ UG...', 'ACUERDO ERASMUS+ UG...', and 'calendarioSept2018.pdf'.

A continuación, procederemos a procesar este archivo con la herramienta MFT2CSV para convertir estos datos en un archivo .csv. Para ello, seleccionaremos el archivo \$MFT utilizando la opción 'Choose \$MFT' y también especificaremos un directorio donde se almacenará el volcado.



Este sería el resultado que hemos obtenido. Utilizaremos el archivo .csv para crear una hoja de cálculo y así poder examinar los atributos.

[0x00009400]WPSettings.dat	10/03/2024 21:08	Archivo DAT	1 KB
[0x00009800]\$RQPCWVG.pdf[ADS_Zone.Id...	10/03/2024 21:08	Archivo IDENTIFIER]	1 KB
[0x00010000]ProyectoEducativo.pdf[ADS_Z...	10/03/2024 21:08	Archivo IDENTIFIER]	1 KB
[0x00010400]\$RLC2MFR.pdf[ADS_Zone.Ide...	10/03/2024 21:08	Archivo IDENTIFIER]	1 KB
Mft.csv	10/03/2024 21:14	Archivo de origen Co...	64 KB
Mft.log	10/03/2024 21:08	Documento de texto	195 KB
Mft-All-I30-Entries.csv	10/03/2024 21:08	Archivo de origen Co...	4 KB
Mft-DATA.csv	10/03/2024 21:08	Archivo de origen Co...	5 KB

	B	C	D	E	F	G	H	I	J	K	L	M
1	Signature	IntegrityChe	Style	HEADER_MI	HEADER_Se	Header_Har	FN_ParentR	FN_ParentSc	FN_FileNam	FilePath	HEADER_Fl	RecordActiv
2	GOOD	OK		66	2	1	48	1	texto - copia.txt	:\carpeta\texto -	FILE	DELETED
3	GOOD	OK		67	2	1	5	5	calendarioSept2	:\calendarioSept	FILE	DELETED
4	GOOD	OK		0	1	1	5	5	\$MFT	:\\$MFT	FILE	ALLOCATED
5	GOOD	OK		1	1	1	5	5	\$MFTMirr	:\\$MFTMirr	FILE	ALLOCATED
6	GOOD	OK		2	2	1	5	5	\$LogFile	:\\$LogFile	FILE	ALLOCATED
7	GOOD	OK		3	3	1	5	5	\$Volume	:\\$Volume	FILE	ALLOCATED
8	GOOD	OK		4	4	1	5	5	\$AttrDef	:\\$AttrDef	FILE	ALLOCATED
9	GOOD	OK		5	5	1	5	5	.	:\.	FOLDER	ALLOCATED
10	GOOD	OK		6	6	1	5	5	\$Bitmap	:\\$Bitmap	FILE	ALLOCATED
11	GOOD	OK		7	7	1	5	5	\$Boot	:\\$Boot	FILE	ALLOCATED
12	GOOD	OK		8	8	1	5	5	\$BadClus	:\\$BadClus	FILE	ALLOCATED

Finalmente, en la hoja de cálculo, podremos aplicar un filtro para mostrar solo aquellos elementos que han sido eliminados. De esta manera, podremos examinar las fechas y verificar cuándo fueron eliminados.

	S	T	U	V
	SI_CTime	SI_ATime	SI_MTime	SI_RTime
0	2021-02-09 19:44:23.0319225	2021-02-08 20:05:33.7223824	2021-02-09 08:00:06.3532183	2021-02-09 19:44:23.0319225
1	2021-02-09 19:44:23.0797836	2021-02-03 19:30:37.6786382	2021-02-03 19:30:37.6786382	2021-02-09 19:44:23.0797836

	X	Y	Z	AA
	FN_CTime	FN_ATime	FN_MTime	FN_RTime
0	2021-02-09 19:44:23.0319225	2021-02-09 19:44:23.0319225	2021-02-09 19:44:23.0319225	2021-02-09 19:44:23.0319225
0	2021-02-09 19:44:23.0797836	2021-02-09 19:44:23.0797836	2021-02-09 19:44:23.0797836	2021-02-09 19:44:23.0797836

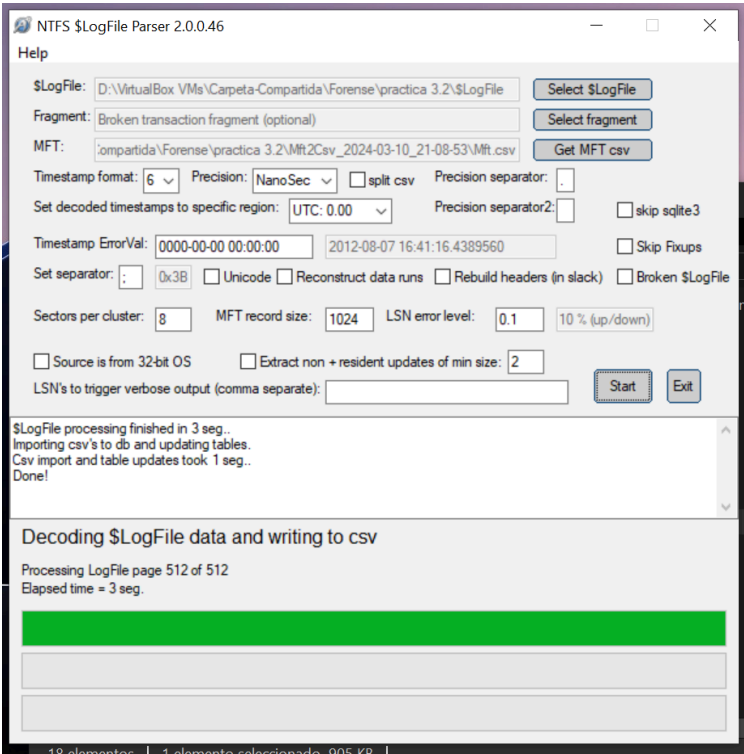
4. Análisis de LogFile

Continuemos examinando el archivo **\$LogFile**, tal como hicimos en la instancia previa. Exportemos utilizando FTK Imager para facilitar su procesamiento.

The screenshot shows the AccessData FTK Imager 4.7.1.2 interface. On the left, the 'Evidence Tree' displays a hierarchy starting with 'datos.dd', followed by 'Partition 1 [97MB]', 'DATOS [NTFS]', '[orphan]', and '[root]'. Under '[root]', various files and folders are listed, including '\$BadClus', '\$Extend', '\$RECYCLE.BIN', '\$Secure', '\$UpCase', '26507936.pdf', 'ACUERDO ERASMUS+ UGR GRADO.docx', 'calendarioSept2018.pdf', 'carpeta', 'mediaDScom_egestionDStramitesDS20DS52dc02dc1f6', 'PE_22_Medidas_Preventivas_del_Plan_de_Contingencia', 'ProyectoEducativo.pdf', 'representanteslegalesconveniosleyenda-[EN].docx', 'rev51ART2.pdf', and 'ROF.pdf'. On the right, the 'File List' pane shows a table of files and folders. The file '\$LogFile' is highlighted in blue.

Name	Size	Type	Date Modified
\$Extend	1	Directory	09/02/2021 19:...
\$RECYCLE.BIN	1	Directory	09/02/2021 19:...
carpeta	1	Directory	09/02/2021 19:...
System Volume Information	1	Directory	09/02/2021 19:...
\$AttrDef	3	Regular F...	09/02/2021 19:...
\$BadClus	0	Regular F...	09/02/2021 19:...
\$Bitmap	4	Regular F...	09/02/2021 19:...
\$Boot	8	Regular F...	09/02/2021 19:...
\$I30	4	NTFS Ind...	09/02/2021 19:...
\$LogFile	2.048	Regular F...	09/02/2021 19:...
\$MFT	256	Regular F...	09/02/2021 19:...
\$MFTMirr	4	Regular F...	09/02/2021 19:...
\$Secure	1	Regular F...	09/02/2021 19:...
\$TXF_DATA	1	NTFS Log...	09/02/2021 19:...

Utilizaremos la herramienta **NTFSLogFileParser** para decodificar la información y generar un archivo .CSV. Para ello, dentro de la herramienta, seleccionamos el archivo \$LogFile previamente importado en la opción '**Select \$LogFile**', luego elegimos la opción '**Get MFT.csv**' y especificamos el archivo CSV generado en el ejercicio anterior. Una vez configurado, podemos iniciar el proceso clicando en 'Start', y así obtendremos un archivo CSV con la información necesaria.

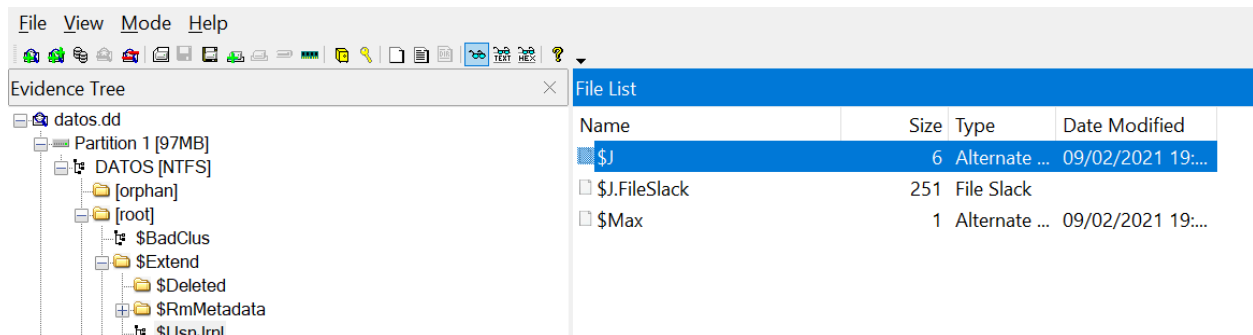


Al aplicar un filtro según el valor '**DeallocateFileRecordSegment**' en la propiedad '**If_RedoOperation**', seremos capaces de identificar los archivos que han sido eliminados de forma permanente.

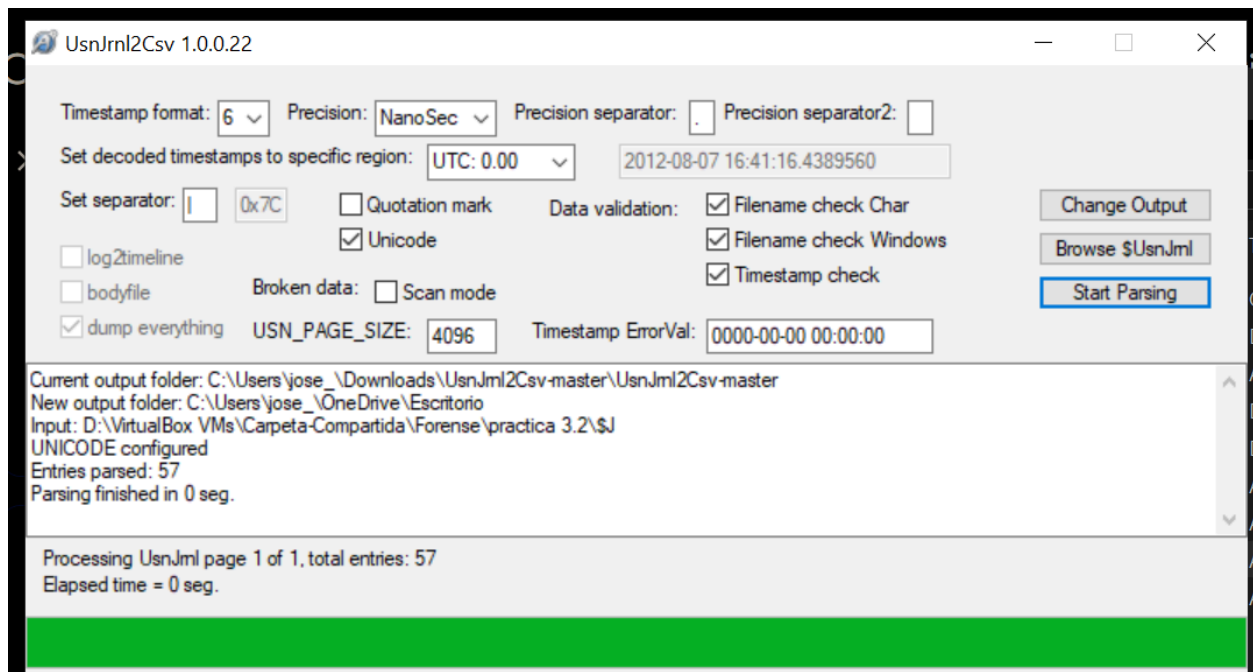
	G	H	I	J
5	If_RedoOperation	If_UndoOperation	If_OffsetInMft	If_FileName
3	DeallocateFileRecordSegment	InitializeFileRecordSegment	0	
3	DeallocateFileRecordSegment	InitializeFileRecordSegment	0	
7	DeallocateFileRecordSegment	InitializeFileRecordSegment	0	borrado_1.txt
1	DeallocateFileRecordSegment	InitializeFileRecordSegment	0	texto - copia.txt
3	DeallocateFileRecordSegment	InitializeFileRecordSegment	0	ProyectoEducativo.pdf
2	DeallocateFileRecordSegment	InitializeFileRecordSegment	0	\$UsnJrnl
3	DeallocateFileRecordSegment	InitializeFileRecordSegment	0	CuestionariodehabitoslectoresANALISIS.pdf
0	DeallocateFileRecordSegment	InitializeFileRecordSegment	0	calendarioSept2018.pdf
3	DeallocateFileRecordSegment	InitializeFileRecordSegment	0	nombre.txt

5. Análisis de USNJOURNAL

En este caso, procederemos a exportar el archivo correspondiente al **\$USNJournal** (ubicado en **\$Extend -> \$USNjrl -> \$J**) utilizando la herramienta FTK Imager.



Posteriormente, procesaremos dicho archivo con la herramienta **UsnJrnl2Csv** para descifrar la información que contiene. Seleccionaremos el archivo **\$J** previamente exportado en '**Browse \$UsnJrnl**' y especificaremos el directorio donde se volcará la información obtenida en '**Change Output**'.



Una vez obtengamos el archivo .csv, tendremos la opción de exportarlo a una hoja de cálculo. En este contexto, observamos que en la columna **'Reason'** se registra detalladamente cada acción realizada con respecto a cada archivo.

	B	C	D	E
	FileName	USN	Timestamp	Reason
30	CuestionariodehabitoslectoresANALISIS.pdf	0	2021-02-09 19:44:22.8150781	FILE_CREATE
30	CuestionariodehabitoslectoresANALISIS.pdf	144	2021-02-09 19:44:22.8150781	DATA_EXTEND+FILE_CREATE
20	CuestionariodehabitoslectoresANALISIS.pdf	288	2021-02-09 19:44:22.8150781	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE
30	CuestionariodehabitoslectoresANALISIS.pdf	432	2021-02-09 19:44:22.8150781	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+STREAM_CHANGE
10	CuestionariodehabitoslectoresANALISIS.pdf	576	2021-02-09 19:44:22.8150781	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+NAMED_DATA_EXTEND+STREAM_CHANGE
30	CuestionariodehabitoslectoresANALISIS.pdf	720	2021-02-09 19:44:22.8150781	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+NAMED_DATA_EXTEND+NAMED_DATA_OVERWRITE
30	CuestionariodehabitoslectoresANALISIS.pdf	864	2021-02-09 19:44:22.8150781	BASIC_INFO_CHANGE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+NAMED_DATA_EXTEND+NAM
70	CuestionariodehabitoslectoresANALISIS.pdf	1008	2021-02-09 19:44:22.8150781	BASIC_INFO_CHANGE+CLOSE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+NAMED_DATA_EXTEN
30	ProyectoEducativo.pdf	1152	2021-02-09 19:44:22.9840584	FILE_CREATE
58	ProyectoEducativo.pdf	1256	2021-02-09 19:44:22.9840584	DATA_EXTEND+FILE_CREATE
30	ProyectoEducativo.pdf	1360	2021-02-09 19:44:22.9840584	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE
38	ProyectoEducativo.pdf	1464	2021-02-09 19:44:22.9909246	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+STREAM_CHANGE
20	ProyectoEducativo.pdf	1568	2021-02-09 19:44:22.9909246	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+NAMED_DATA_EXTEND+STREAM_CHANGE
38	ProyectoEducativo.pdf	1672	2021-02-09 19:44:22.9909246	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+NAMED_DATA_EXTEND+NAMED_DATA_OVERWRITE
70	ProyectoEducativo.pdf	1776	2021-02-09 19:44:22.9909246	BASIC_INFO_CHANGE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+NAMED_DATA_EXTEND+NAM
58	ProyectoEducativo.pdf	1880	2021-02-09 19:44:22.9909246	BASIC_INFO_CHANGE+CLOSE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+NAMED_DATA_EXTEN
20	rev51ART2.pdf	1984	2021-02-09 19:44:23.0153384	FILE_CREATE
18	rev51ART2.pdf	2072	2021-02-09 19:44:23.0153384	DATA_EXTEND+FILE_CREATE
70	rev51ART2.pdf	2160	2021-02-09 19:44:23.0153384	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE
38	rev51ART2.pdf	2248	2021-02-09 19:44:23.0153384	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+STREAM_CHANGE
20	rev51ART2.pdf	2336	2021-02-09 19:44:23.0153384	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+NAMED_DATA_EXTEND+STREAM_CHANGE
78	rev51ART2.pdf	2424	2021-02-09 19:44:23.0153384	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+NAMED_DATA_EXTEND+NAMED_DATA_OVERWRITE
30	rev51ART2.pdf	2512	2021-02-09 19:44:23.0153384	BASIC_INFO_CHANGE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+NAMED_DATA_EXTEND+NAM
28	rev51ART2.pdf	2600	2021-02-09 19:44:23.0153384	BASIC_INFO_CHANGE+CLOSE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+NAMED_DATA_EXTEN

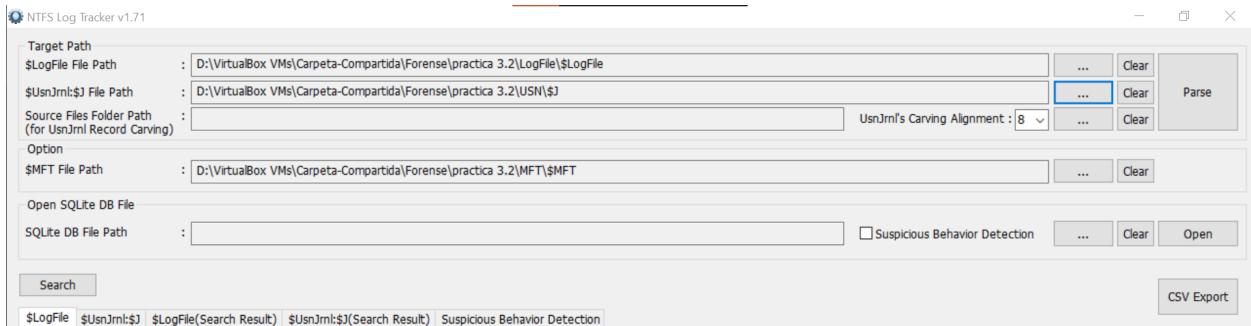
Si filtramos el campo **'Reason'** con el valor **'CLOSE+FILE_DELETE'**, podremos visualizar la fecha en la que se eliminaron definitivamente los archivos.

	B	C	D	E	Mi
	FileName	USN	Timestamp	Reason	
00	CuestionariodehabitoslectoresANALISIS.pdf	4096	2021-02-09 19:44:32.2920106	CLOSE+FILE_DELETE	
90	calendarioSept2018.pdf	4240	2021-02-09 19:44:32.2920106	CLOSE+FILE_DELETE	
F8	nombre.txt	4344	2021-02-09 19:44:39.0896525	CLOSE+FILE_DELETE	
C0	texto - copia.txt	5824	2021-02-09 19:44:48.2312284	CLOSE+FILE_DELETE	

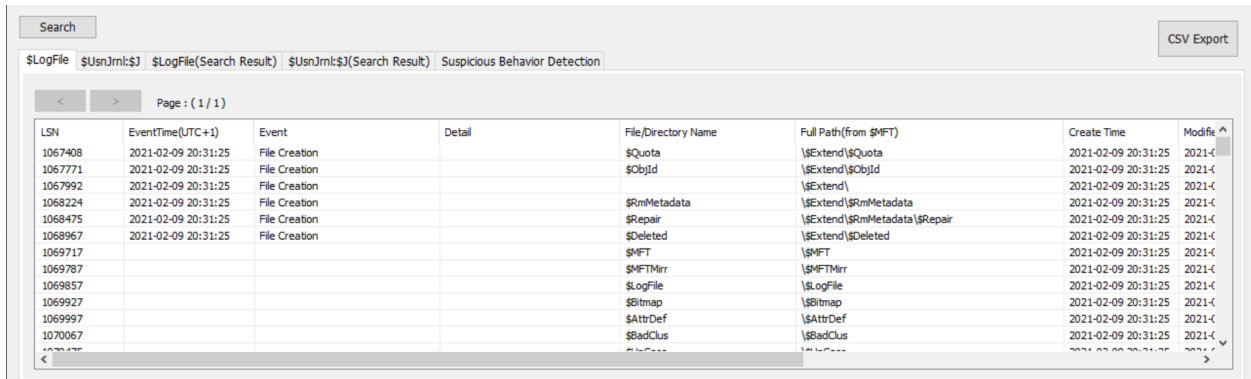
6. Herramienta ANJP: \$UsnJml + \$Logfile + \$MFTE

En este escenario, se solicitaba el uso de la herramienta ANJP, sin embargo, no he encontrado información al respecto. En su lugar, he identificado un foro que presenta alternativas similares, por lo que optaré por utilizar [NTFSLogTracker](#).



Una vez dentro de la herramienta, seleccionaremos los archivos con los que hemos estado trabajando, como el archivo de registro (Logfile), \$J y \$MFT, y procederemos a hacer clic en 'Parse'.



Esta herramienta simplifica la revisión de nuestras acciones anteriores al proporcionar toda la información en un solo lugar. Una vez que el proceso de análisis (parse) concluya, la información resultante se presentará en la parte inferior de la interfaz.



Al acceder al directorio que hemos especificado, podemos notar que la herramienta genera una base de datos que contiene la información de estos archivos.

Nombre	Estado	Fecha de modificación	Tipo	Tamaño
 ANJP_2024-03-11 12-59-45.db		11/03/2024 12:59	Data Base File	128 KB

Podemos emplear SQLite para una visualización más efectiva de la información. Lo destacado de esta opción es la posibilidad de utilizar consultas SQL para ubicar la información de manera más eficiente.

Databases			
Filter by name			
<div> <div>ANJP_2024-03-11 12-59-45 (SQLite 3)</div> <div> <div>Tables (4)</div> <div> <div>LogFile</div> <div>MFT</div> <div>TimeZone</div> <div>UsnJrnl</div> <div>Views</div> </div> </div> </div>			
Structure			
Vista de rejilla			
Vista de formulario			
Filtrar datos			
Total rows loaded: 125			
FileName	FullPath	CreationTime	
CuestionariodehabitoslectoresANALISIS.pdf	\\CuestionariodehabitoslectoresANALISIS.pdf	2021	
mediaDScom_egestionDStramitesDS20DS52dc02dc1f6359fa654797289a31938f.docx	\\mediaDScom_egestionDStramitesDS20DS52dc02dc1f6359fa654797289a31938f.docx	2021	
nombre.txt	\\nombre.txt	2021	
PE_22_Medidas_Preventivas_del_Plan_de_Contingencia_de_la_UGR.pdf	\\PE_22_Medidas_Preventivas_del_Plan_de_Contingencia_de_la_UGR.pdf	2021	
ProyectoEducativo.pdf	\\ProyectoEducativo.pdf	2021	
representanteslegalesconveniosleyenda-[EN].docx	\\representanteslegalesconveniosleyenda-[EN].docx	2021	
rev51ART2.pdf	\\rev51ART2.pdf	2021	
ROF.pdf	\\ROF.pdf	2021	
texto.txt	\\texto.txt	2021	
carpeta	\\carpeta	2021	
PE_22_Medidas_Preventivas_del_Plan_de_Contingencia_de_la_UGR.pdf	\\carpeta\\PE_22_Medidas_Preventivas_del_Plan_de_Contingencia_de_la_UGR.pdf	2021	
ProyectoEducativo.pdf	\\carpeta\\ProyectoEducativo.pdf	2021	
representanteslegalesconveniosleyenda-[EN].docx	\\carpeta\\representanteslegalesconveniosleyenda-[EN].docx	2021	
rev51ART2.pdf	\\carpeta\\rev51ART2.pdf	2021	
ROF.pdf	\\carpeta\\ROF.pdf	2021	
texto - copia.txt	\\carpeta\\texto - copia.txt	2021	
texto.txt	\\carpeta\\texto.txt	2021	

7. Análisis de Alternate Data Stream

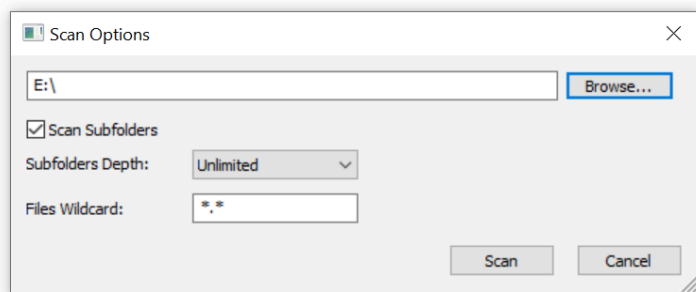
FTK Imager es una herramienta que podemos utilizar para examinar el origen de los archivos presentes en la imagen. Utilizando esta herramienta, el proceso es tan simple como dirigirse a un archivo específico y hacer doble clic sobre él para obtener más detalles.

File View Mode Help			
Evidence Tree			
File List			
Name	Size	Type	Date Modified
\$I30	4	NTFS Ind...	09/02/2021 19:...
PE_22_Medidas_Preventiva...	424	Regular F...	03/02/2021 19:...
ProyectoEducativo.pdf	6.804	Regular F...	03/02/2021 19:...
representanteslegalesconv...	373	Regular F...	03/02/2021 19:...
texto - copia.txt	6	Regular F...	08/02/2021 20:...
texto - copia.txt.FileSlack	3	File Slack	
texto.txt	6	Regular F...	08/02/2021 20:...
texto.txt.FileSlack	3	File Slack	

Así, podremos notar la presencia de un archivo **ZoneIdentifier** que nos proporcionará información sobre su origen. Un valor como "**ZoneId=3**" señala que el archivo proviene de la Zona de Internet.

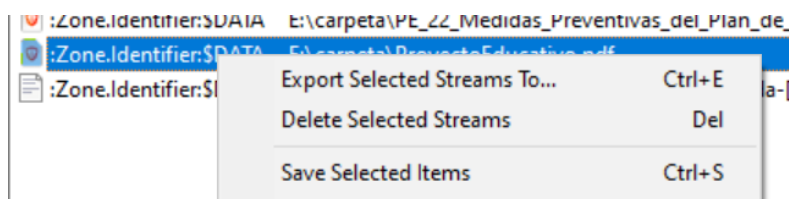
Evidence Tree			
File List			
Name	Size	Type	Date Modified
Zone.Identifier	1	Alternate ...	03/02/2021 19:...
[ZoneTransfer] ZoneId=3			

Podemos llevar a cabo la misma acción utilizando la herramienta AlternateDataStreamViewer. Basta con seleccionar el volumen que hemos montado previamente con FTK Imager.



En la interfaz de la herramienta, podemos visualizar los archivos almacenados en la imagen. Al hacer clic en uno de ellos, podemos exportarlo seleccionando la opción '**Export Selected Streams To...**'.

Stream Name	Filename	Full Stream Name	Stream Size	Stream Allocated S...	Extension	File Modified Time	File Created Time	Entr
:Zone.Identifier:\$DATA	E:\26507936.pdf	E:\26507936.pdf:Zone.Identifier	26	32	pdf	03/02/2021 20:30:05	09/02/2021 20:31:55	03/0
:Zone.Identifier:\$DATA	E:\ACUERDO ERASMUS+ UGR GRADO.docx	E:\ACUERDO ERASMUS+ UGR GRADO.docx:Zone.Id...	26	32	docx	03/02/2021 20:33:08	09/02/2021 20:31:55	03/0
:Zone.Identifier:\$DATA	E:\mediaDScom_egestionDStramitesDS20DS52dc02d...	E:\mediaDScom_egestionDStramitesDS20DS52dc02d...	26	32	docx	03/02/2021 20:31:30	09/02/2021 20:31:55	03/0
:Zone.Identifier:\$DATA	E:\PE_22_Medidas_Preventivas_del_Plan_de_Conting...	E:\PE_22_Medidas_Preventivas_del_Plan_de_Conting...	26	32	pdf	03/02/2021 20:29:55	09/02/2021 20:31:55	03/0
:Zone.Identifier:\$DATA	E:\ProyectoEducativo.pdf	E:\ProyectoEducativo.pdf:Zone.Identifier	26	32	pdf	03/02/2021 20:30:53	09/02/2021 20:31:55	03/0
:Zone.Identifier:\$DATA	E:\representanteslegalesconveniosleyenda-[EN].docx	E:\representanteslegalesconveniosleyenda-[EN].docx...	26	32	docx	03/02/2021 20:31:40	09/02/2021 20:31:55	03/0
:Zone.Identifier:\$DATA	E\rev51ART2.pdf	E\rev51ART2.pdf:Zone.Identifier	26	32	pdf	03/02/2021 20:29:44	09/02/2021 20:31:55	03/0
:Zone.Identifier:\$DATA	E\ROF.pdf	E\ROF.pdf:Zone.Identifier	26	32	pdf	03/02/2021 20:30:49	09/02/2021 20:31:55	03/0
:Zone.Identifier:\$DATA	E\carpeta\PE_22_Medidas_Preventivas_del_Plan_de_...	E\carpeta\PE_22_Medidas_Preventivas_del_Plan_de_...	26	32	pdf	03/02/2021 20:29:55	09/02/2021 20:31:55	09/0
:Zone.Identifier:\$DATA	E\carpeta\ProyectoEducativo.pdf	E\carpeta\ProyectoEducativo.pdf:Zone.Identifier	26	32	pdf	03/02/2021 20:30:53	09/02/2021 20:44:22	09/0
:Zone.Identifier:\$DATA	E\carpeta\representanteslegalesconveniosleyenda-[...	E\carpeta\representanteslegalesconveniosleyenda-[...	26	32	docx	03/02/2021 20:31:40	09/02/2021 20:31:55	09/0



Al abrir el archivo exportado, observaremos que contiene la misma información que obtuvimos utilizando FTK Imager.

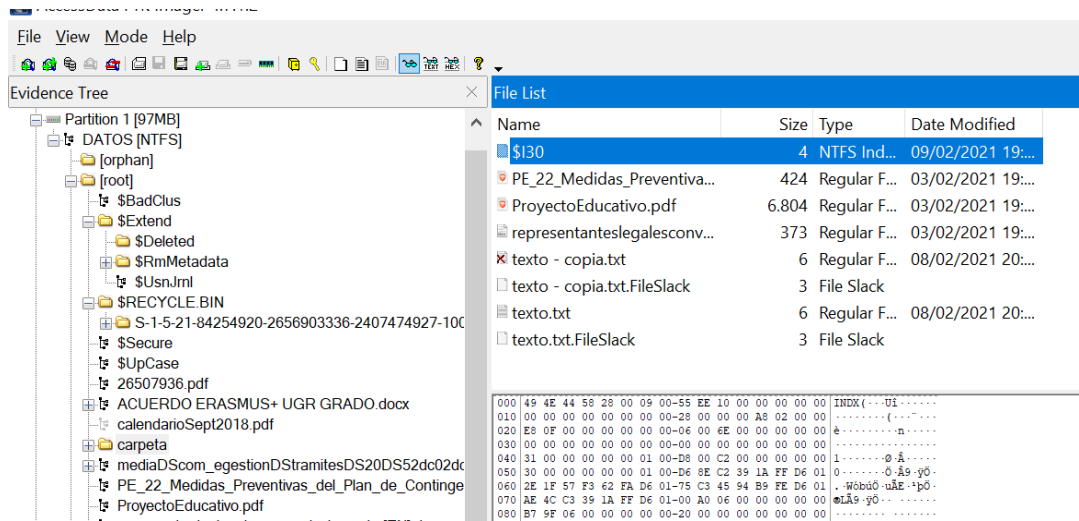
```

D: > VirtualBox VMs > Carpeta-Compartida > Forense > practica 3.2 > ProyectoEducativo.pdf_Zone.Identifier
1 [ZoneTransfer]
2 ZoneId=3
3

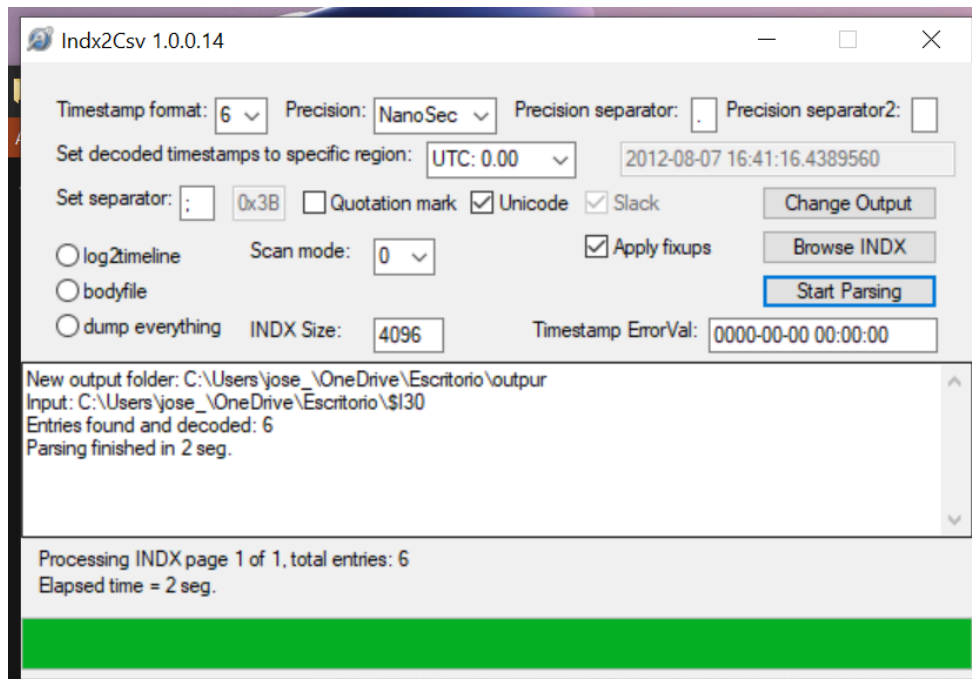
```

8. Análisis de INDX/\$i30

En este caso, procederemos a exportar los archivos de tipo índice de directorios (**\$i30**).



Utilizaremos la herramienta **INDX2CSV** para decodificar su información y obtener un archivo .csv. Para ello, seleccionaremos el fichero exportado anteriormente y especificaremos un directorio para su volcado.



En última instancia, podemos importar este archivo .csv en una hoja de cálculo para facilitar el trabajo con la información. Con estos datos, podremos visualizar todo lo que está y ha estado presente en cada directorio. En este caso, la imagen corresponde al directorio 'carpeta'.

A	B	C	D	E	F	G	H	I	J
1 Offset	Vcn	IsNotLeaf	LastLsn	FromIndexSlack	FileName	MFTReference	MFTReferenceSeqNo	IndexFlags	MFTParentReference
2 0x00000040	0	0	1109589	0	PE_22_Medidas_Preventivas_del_Plan_de_Contingencia_de_la_UGR.pdf	49	1	0	48
3 0x00000118	0	0	1109589	0	ProyectoEducativo.pdf	64	1	0	48
4 0x00000198	0	0	1109589	0	representanteslegalesconveniosleyenda-[EN].docx	51	1	0	48
5 0x00000248	0	0	1109589	0	texto.txt	55	1	0	48
6 0x000002C0	0	0	-1	1	texto.txt	55	1	0	48
7 0x00000390	0	0	-1	1	texto.txt	8589934608	0	0	48

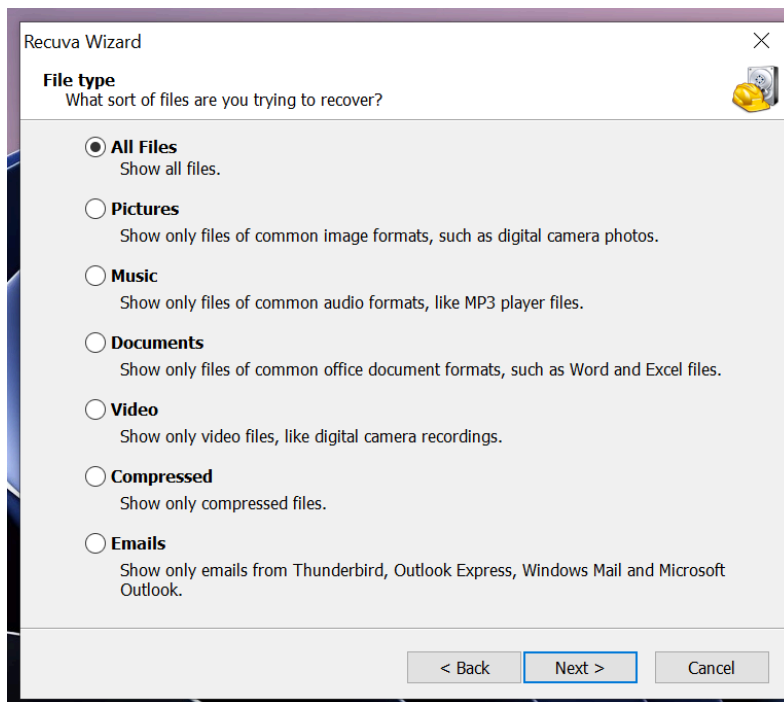
Este sería el mismo ejemplo pero en el directorio raíz

10 0x00000370	0	0	1106595	0	\$RECYCLE.BIN	30
11 0x000003E8	0	0	1106595	0	\$Secure	9
12 0x00000448	0	0	1106595	0	\$UpCase	10
13 0x000004A8	0	0	1106595	0	\$Volume	3
14 0x00000508	0	0	1106595	0	.	5
15 0x00000560	0	0	1106595	0	26507936.pdf	56
16 0x000005D0	0	0	1106595	0	ACUERDO ERASMUS+ UGR GRADO.docx	57
17 0x00000660	0	0	1106595	0	carpeta	48
18 0x000006C0	0	0	1106595	0	mediaDScom_egestionDStramitesDS20DS52dc02dc1f6359fa654797289a31938f.docx	40
19 0x000007A8	0	0	1106595	0	PE_22_Medidas_Preventivas_del_Plan_de_Contingencia_de_la_UGR.pdf	42
20 0x00000880	0	0	1106595	0	ProyectoEducativo.pdf	43
21 0x00000900	0	0	1106595	0	representanteslegalesconveniosleyenda-[EN].docx	44
22 0x000009B0	0	0	1106595	0	rev51ART2.pdf	45
23 0x00000A20	0	0	1106595	0	ROF.pdf	46
24 0x00000A80	0	0	1106595	0	System Volume Information	36
25 0x00000B08	0	0	1106595	0	texto.txt	47
26 0x00000B70	0	0	-1	1	texto.txt	0
27 0x00000BF0	0	0	-1	1	texto.txt	47
28 0x00000C98	0	0	-1	1	texto.txt	47
29 0x00000D08	0	0	-1	1	texto.txt	8589934608

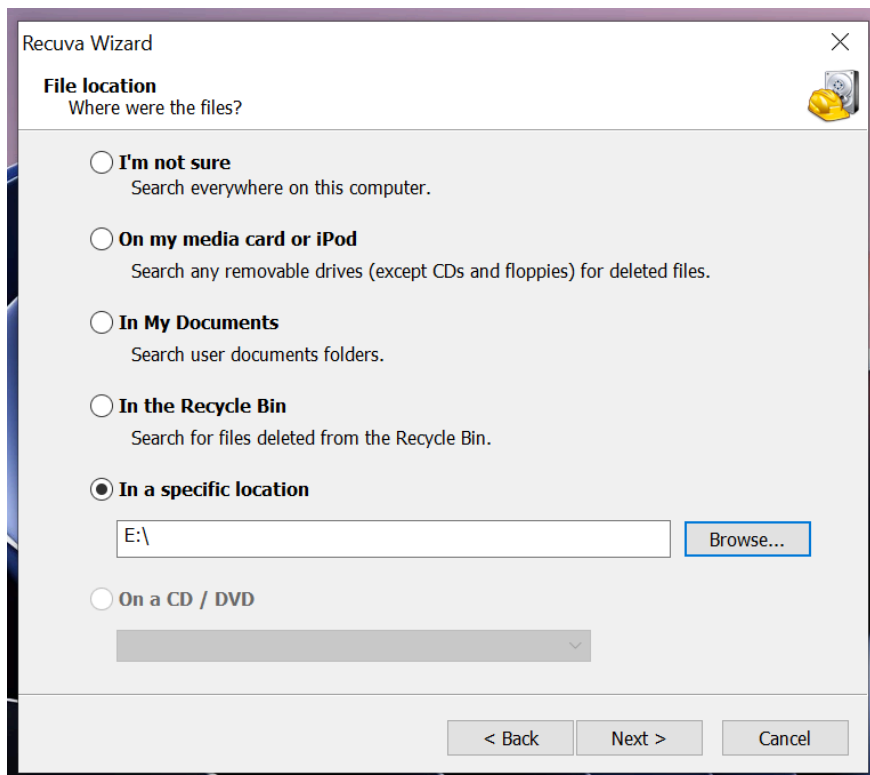
9. Recuperación de ficheros con Recuva

Para concluir esta práctica, hemos constatado que FTK Imager nos permite recuperar archivos. No obstante, es importante destacar que existen herramientas automatizadas, como **Recuva**, que facilitan este proceso de recuperación de manera más eficiente.

Una vez instalada la herramienta, procedemos a abrirla. En este punto, seleccionaremos que busque todos los archivos.



En este caso seleccionamos el volumen E que es donde tenemos montada la evidencia.



Page 10 of 10

