🗀 1. USN Journal (`$UsnJrnl`)

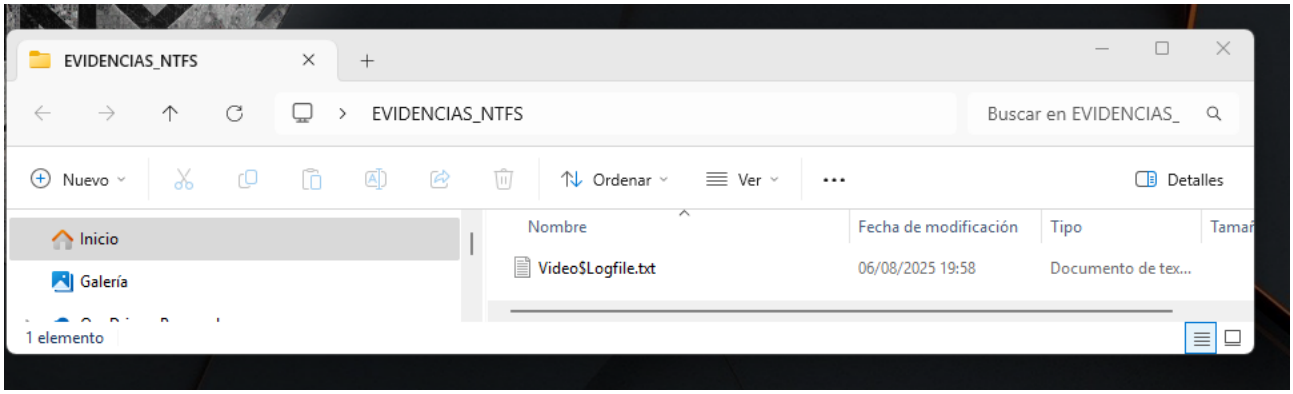
- Es un archivo **oculto del sistema** que registra cada cambio que ocurre en el volumen NTFS.
- Guarda eventos como:
    - Creación de archivos/carpetas
    - Cambios de nombre
    - Modificación de contenido
    - Eliminación
- Es extremadamente útil para saber **qué pasó en el sistema** incluso después de que el archivo original ha sido eliminado.

🧠 **Ejemplo forense**: puedes ver si un archivo fue copiado o modificado, y cuándo ocurrió.

🗃 2. Logfile (`$LogFile`)

- Es otro archivo oculto del sistema NTFS que registra operaciones de bajo nivel para recuperación ante fallos.
- Contiene información **transaccional** del sistema de archivos (similar a un journal en bases de datos).
- Puede revelar eventos que no aparecen en otros logs del sistema.

Empezamos creando un archivo txt y lo movemos dentro de una carpeta creada:

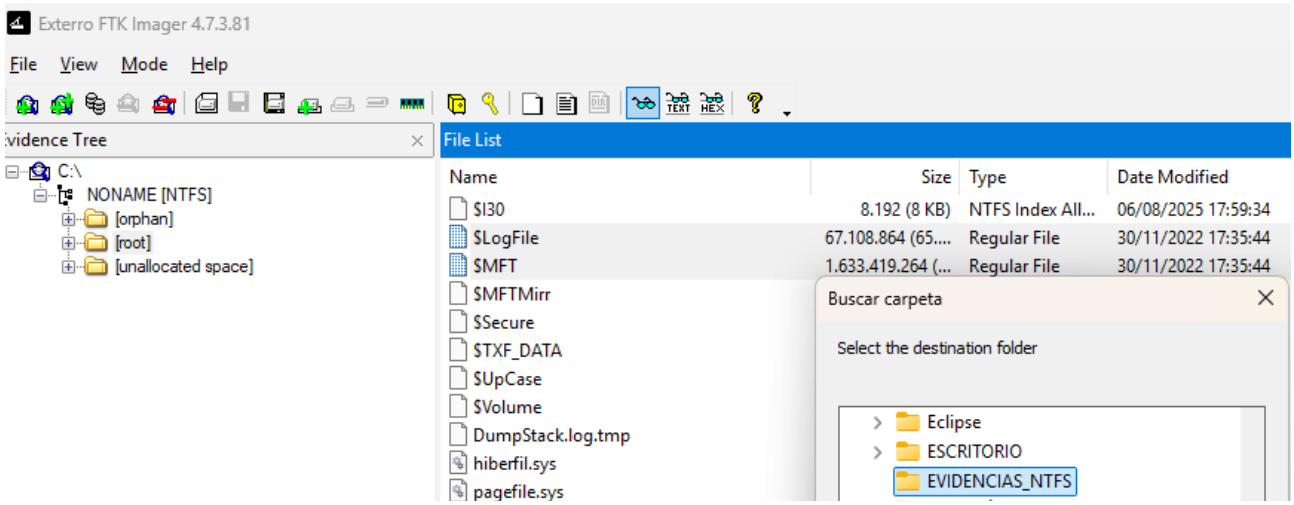


🔎 Extracción de artefactos con FTK Imager

Ejecutamos **FTK Imager** con el objetivo de realizar la **extracción de archivos relevantes para el análisis forense**. Una vez cargado el disco o la imagen de disco, realizamos un escaneo de su contenido.

En la raíz del sistema (`/`), localizamos los archivos `$MFT` y `$LogFile`, fundamentales para reconstruir la actividad del sistema de archivos NTFS. Estos archivos se exportan y se almacenan en nuestra carpeta destinada a evidencias.

A continuación, accedemos a la carpeta `$Extend`, donde se encuentra el archivo `$UsnJrnl`. Dentro de este, identificamos el archivo `$J`, que contiene la información más relevante del Journal. Procedemos igualmente a su extracción y lo guardamos junto al resto de evidencias recolectadas.



🩹 Análisis con NTFS Log Tracker

Una vez extraídos los archivos necesarios, procedemos a utilizar la herramienta **NTFS Log Tracker**. Para ello, abrimos la aplicación y **cargamos los archivos previamente obtenidos**, concretamente:

- `$MFT`
- `$LogFile`
- `$J` (ubicado dentro de `$UsnJrnl`)

Estos archivos permiten reconstruir y visualizar la actividad del sistema de archivos NTFS, facilitando el análisis cronológico de acciones realizadas en el disco, como creación, modificación o eliminación de archivos y carpetas.

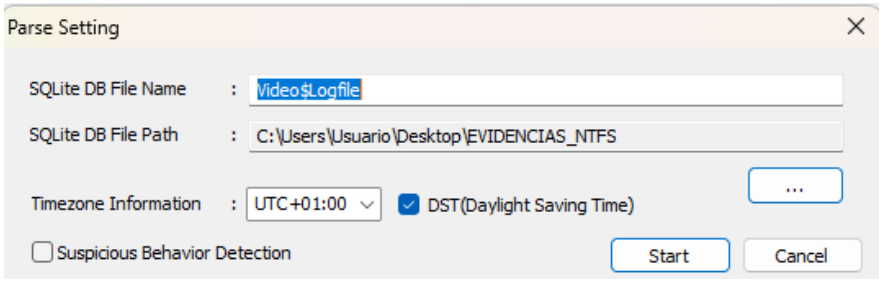
▶ Procesamiento de la información

Tras haber cargado los archivos en **NTFS Log Tracker**, hacemos clic en el botón `Parse` para iniciar el análisis. La herramienta procesará automáticamente la información contenida en los archivos cargados y generará una **vista detallada de las operaciones realizadas sobre el sistema de archivos**.

Podremos visualizar datos como:

- Archivos creados, modificados, renombrados o eliminados.
- Fechas y horas precisas de cada evento.
- Ruta completa de los archivos afectados.
- Tipo de operación registrada (Create, Modify, Delete, Rename…).

Esta información es esencial para reconstruir la línea temporal de actividad del dispositivo y detectar comportamientos sospechosos o relevantes para la investigación forense.

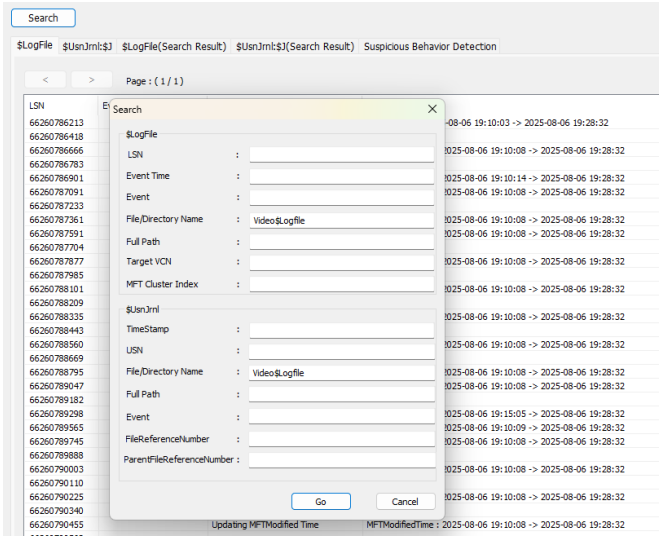


🔍 Búsqueda de eventos específicos en `$LogFile`

A continuación, accedemos a la pestaña `$LogFile` dentro de **NTFS Log Tracker**. En esta sección, realizamos una búsqueda específica utilizando el nombre del archivo `.txt` que fue creado previamente durante la práctica o simulación del caso.

Esta búsqueda nos permitirá identificar las operaciones relacionadas con dicho archivo, tales como su **creación, modificación o eliminación**, junto con las fechas, horas y rutas asociadas.

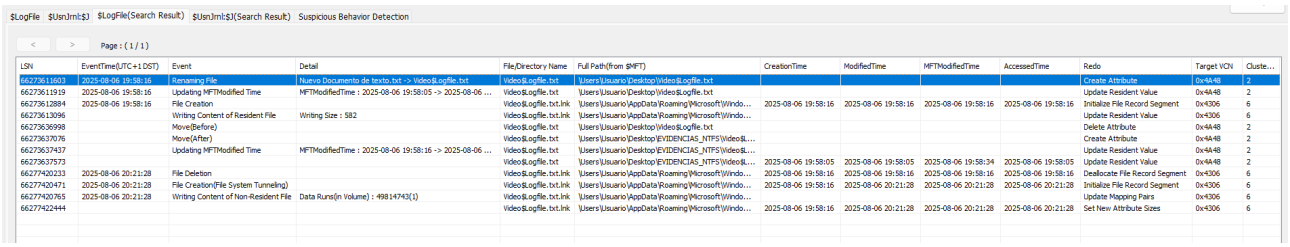
Este paso es crucial para **corroborar la existencia y manipulación del archivo**, así como para relacionar su actividad con otros eventos del sistema.



📝 `En la pestaña $LogFile (Search Result) podemos reconstruir la transacción completa almacenada en el` *transaction log* `de NTFS:`

1. **19:58:16** – Renombrado de *Nuevo Documento de texto.txt* a **Video$Logfile.txt**.
2. Actualización inmediata de tiempos MFT y creación del nuevo atributo de nombre.
3. Inicialización del File Record (FRS) y primera escritura (archivo residente, 582 bytes).
4. Registro de los movimientos *before/after* que acompañan al renombrado.
5. **20:21:28** – Escritura de 4,9 MB como datos no residentes y posterior cierre/eliminación del archivo, evidenciado por los eventos `File Deletion` y “File Creation (Tunneling)”.

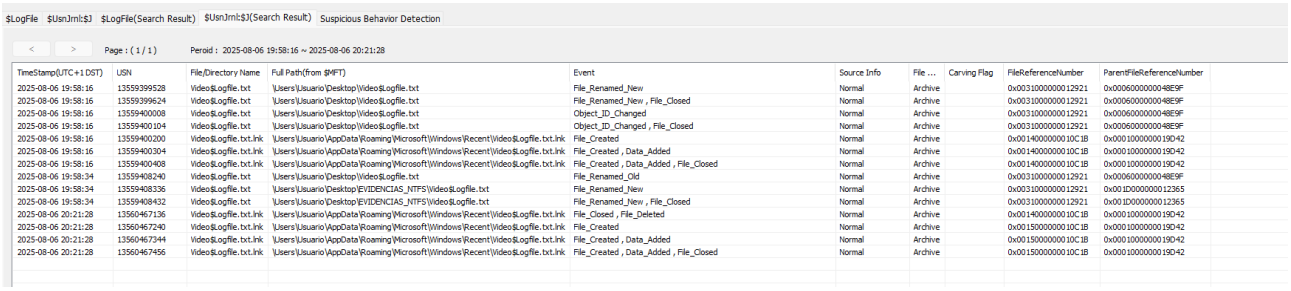
El `$LogFile` guarda estos eventos a nivel transaccional, permitiendo corroborar los hallazgos del **USN Journal** y detectar operaciones que el usuario pudiera intentar ocultar.



📝 Después de aplicar el filtro en `$UsnJrnl:$J`, se observa la cronología completa de *Video$Logfile.txt*:

1. **19:58:16** – Se crea el archivo con el nombre *Nuevo Documento de texto.txt*.
2. Se renombra inmediatamente a **Video$Logfile.txt** (`File_Renamed_New`).
3. NTFS actualiza su **Object ID** y registra la escritura de datos.
4. Windows crea los accesos directos en **Recent**, generando múltiples eventos `.lnk`.
5. **20:21:28** – El archivo es cerrado y, en algunos casos, eliminado o movido, lo que queda reflejado en los últimos registros.

Esta secuencia confirma **creación → renombrado → edición → cierre** y demuestra la utilidad del USN Journal para reconstruir actividades incluso si el archivo se borra posteriormente.



$LogFile | $UsnJrnl:$J | $LogFile(Search Result) | $UsnJrnl:$J(Search Result) | Suspicious Behavior Detection

< > Page : (1 / 1) Peroid : 2025-08-06 19:58:16 ~ 2025-08-06 20:21:28

TimeStamp(UTC+1 DST)	USN	File/Directory Name	Full Path(from $MFT)	Event	Source Info	File ...	Carving Flag	FileReferenceNumber	ParentFileReferenceNumber
2025-08-06 19:58:16	13559399528	Video$Logfile.txt	\Users\Usuario\Desktop\Video$Logfile.txt	File_Renamed_New	Normal	Archive		0x0031000000012921	0x0006000000048E9F
2025-08-06 19:58:16	13559399624	Video$Logfile.txt	\Users\Usuario\Desktop\Video$Logfile.txt	File_Renamed_New , File_Closed	Normal	Archive		0x0031000000012921	0x0006000000048E9F
2025-08-06 19:58:16	13559400008	Video$Logfile.txt	\Users\Usuario\Desktop\Video$Logfile.txt	Object_ID_Changed	Normal	Archive		0x0031000000012921	0x0006000000048E9F
2025-08-06 19:58:16	13559400104	Video$Logfile.txt	\Users\Usuario\Desktop\Video$Logfile.txt	Object_ID_Changed , File_Closed	Normal	Archive		0x0031000000012921	0x0006000000048E9F
2025-08-06 19:58:16	13559400200	Video$Logfile.txt.lnk	\Users\Usuario\AppData\Roaming\Microsoft\Windows\Recent\Video$Logfile.txt.lnk	File_Created	Normal	Archive		0x0014000000010C1B	0x0001000000019D42
2025-08-06 19:58:16	13559400304	Video$Logfile.txt.lnk	\Users\Usuario\AppData\Roaming\Microsoft\Windows\Recent\Video$Logfile.txt.lnk	File_Created , Data_Added	Normal	Archive		0x0014000000010C1B	0x0001000000019D42
2025-08-06 19:58:16	13559400408	Video$Logfile.txt.lnk	\Users\Usuario\AppData\Roaming\Microsoft\Windows\Recent\Video$Logfile.txt.lnk	File_Created , Data_Added , File_Closed	Normal	Archive		0x0014000000010C1B	0x0001000000019D42
2025-08-06 19:58:34	13559408240	Video$Logfile.txt	\Users\Usuario\Desktop\Video$Logfile.txt	File_Renamed_Old	Normal	Archive		0x0031000000012921	0x0006000000048E9F
2025-08-06 19:58:34	13559408336	Video$Logfile.txt	\Users\Usuario\Desktop\EVIDENCIAS_NTFS\Video$Logfile.txt	File_Renamed_New	Normal	Archive		0x0031000000012921	0x001D000000012365
2025-08-06 19:58:34	13559408432	Video$Logfile.txt	\Users\Usuario\Desktop\EVIDENCIAS_NTFS\Video$Logfile.txt	File_Renamed_New , File_Closed	Normal	Archive		0x0031000000012921	0x001D000000012365
2025-08-06 20:21:28	13560467136	Video$Logfile.txt.lnk	\Users\Usuario\AppData\Roaming\Microsoft\Windows\Recent\Video$Logfile.txt.lnk	File_Closed , File_Deleted	Normal	Archive		0x0014000000010C1B	0x0001000000019D42
2025-08-06 20:21:28	13560467240	Video$Logfile.txt.lnk	\Users\Usuario\AppData\Roaming\Microsoft\Windows\Recent\Video$Logfile.txt.lnk	File_Created	Normal	Archive		0x0015000000010C1B	0x0001000000019D42
2025-08-06 20:21:28	13560467344	Video$Logfile.txt.lnk	\Users\Usuario\AppData\Roaming\Microsoft\Windows\Recent\Video$Logfile.txt.lnk	File_Created , Data_Added	Normal	Archive		0x0015000000010C1B	0x0001000000019D42
2025-08-06 20:21:28	13560467456	Video$Logfile.txt.lnk	\Users\Usuario\AppData\Roaming\Microsoft\Windows\Recent\Video$Logfile.txt.lnk	File_Created , Data_Added , File_Closed	Normal	Archive		0x0015000000010C1B	0x0001000000019D42