

Artefacto \$MFT

⌚ Introducción

En esta práctica vamos a utilizar las herramientas **MFTECmd** y **Timeline Explorer** para realizar un análisis forense sobre un archivo **\$MFT** extraído de un sistema de archivos NTFS.

Mediante el uso conjunto de estas herramientas, seremos capaces de **extraer, visualizar y analizar la actividad completa del sistema de archivos**, identificando archivos:

- 📁 Activos
- 🗑 Eliminados
- 📈 Modificados
- 🔍 Accedidos
- 🕵️ Ocultos o potencialmente sospechosos

El objetivo principal es **reconstruir una línea de tiempo precisa** que nos permita detectar patrones relevantes, posibles manipulaciones o eventos críticos que hayan afectado al sistema.

Esta técnica es fundamental en tareas de análisis forense digital y respuesta ante incidentes, ya que nos proporciona **visibilidad total del historial del sistema**, incluso de archivos ya borrados.

💡 Paso 1: Lo primero es abrir el terminal en la carpeta donde tenemos descargada la herramienta:

🛠 Herramienta utilizada:

- **MFTECmd v1.3.0.0**
Autor: [Eric Zimmerman](#)

The screenshot shows a file explorer window titled 'EVIDENCIAS_NTFS > MFTECmd'. It displays three files: 'MFTECmd.dll' (modified 07/08/2025 18:42, 2.304 KB), 'MFTECmd.exe' (modified 07/08/2025 18:42, 297 KB), and 'MFTECmd.runtimeconfig.json' (modified 07/08/2025 18:42, 1 KB). A context menu is open over the files, listing options: Ver, Ordenar por, Agrupar por, Nuevo, Propiedades (Alt+Entrar), Abrir en Terminal, and Mostrar Más opciones.

Nombre	Fecha de modificación	Tipo	Tamaño
MFTECmd.dll	07/08/2025 18:42	Extensión de la apl...	2.304 KB
MFTECmd.exe	07/08/2025 18:42	Aplicación	297 KB
MFTECmd.runtimeconfig.json	07/08/2025 18:42	Archivo de origen ...	1 KB

📁 Estructura de carpetas usada:

```
bash
CopiarEditar
└─ EVIDENCIAS_NTFS
    ├─ $MFT.copy0           ← Archivo extraído previamente con Guymager o
similar
    └─ MFTECmd
        └─ MFTECmd.exe      ← Carpeta donde se encuentra MFTECmd.exe
```

📝 Objetivo:

Procesar el archivo \$MFT.copy0 para extraer todos los metadatos de los archivos y carpetas de una partición NTFS, generando la salida en formato **CSV** para su análisis forense.

```
PS C:\Users\Usuario\Desktop\EVIDENCIAS_NTFS\MFTECmd> .\MFTECmd.exe -f "..\$MFT.copy0" --csv .\ --csvf practica1NTFS.csv
MFTECmd version 1.3.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

Command line: -f ..\$MFT.copy0 --csv .\ --csvf practica1NTFS.csv

Warning: Administrator privileges not found!

File type: Mft

Processed ..\$MFT.copy0 in 11,9220 seconds

..\$MFT.copy0: FILE records found: 829.752 (Free records: 765.352) File size: 1,5GB
CSV output will be saved to .\practica1NTFS.csv
```

❖ Explicación del comando:

Parte	Descripción
.\MFTECmd.exe	Ejecuta la herramienta desde la carpeta actual.
-f "..\\$MFT.copy0"	Indica el archivo \$MFT.copy0, escapando \$ con acento grave (PowerShell interpreta \$MFT como variable si no se escapa). .. significa "carpeta anterior".
--csv .\	Genera la salida en formato CSV en el directorio actual.
--csvf	Define el nombre del archivo CSV de salida:
practica1NTFS.csv	practica1NTFS.csv.

```

PS C:\Users\Usuario\Desktop\EVIDENCIAS_NTFS\MFTECmd> dir

Directorio: C:\Users\Usuario\Desktop\EVIDENCIAS_NTFS\MFTECmd

Mode                LastWriteTime         Length Name
----                -----              ----  --
-a----   07/08/2025      18:42        2358912 MFTECmd.dll
-a----   07/08/2025      18:42        303232 MFTECmd.exe
-a----   07/08/2025      18:42          340 MFTECmd.runtimeconfig.json
-a----   07/08/2025      19:03      753175677 practicalNTFS.csv

```

Paso 2: Visualización con **Timeline Explorer**

¿Qué es Timeline Explorer?

Timeline Explorer es una herramienta gratuita creada por Eric Zimmerman (el mismo autor de MFTECmd), que permite **analizar archivos CSV con información forense** en una interfaz amigable.

¿Para qué sirve?

- Visualizar registros de tiempo de forma clara y ordenada.
- Aplicar **filtros avanzados** sin complicaciones.
- Ordenar por fechas de creación, modificación o eliminación.
- Ver múltiples columnas al mismo tiempo (fechas, rutas, nombres, tamaño...).
- Marcar eventos sospechosos o de interés.
- Exportar vistas filtradas a nuevos archivos CSV para informes.

Cómo usarlo paso a paso:

1. Abre Timeline Explorer
2. Haz clic en "File" > "Open" y selecciona `practicalNTFS.csv`
3. Verás una tabla con todos los registros del archivo \$MFT
4. Usa la barra de búsqueda o el botón "Filter" para:

- Ver solo archivos **eliminados** (`InUse = false`)
- Filtrar por una extensión concreta (`.jpg, .exe, .zip, etc.`)
- Buscar archivos creados o modificados en fechas específicas

5. Ordena columnas haciendo clic sobre los encabezados (por ejemplo, `Created0x10` para reconstruir la cronología, Ej: Filtramos la semana previa si se ha producido algún incidente)

The screenshot shows the Timeline Explorer interface with a file list titled 'practicaNTFS.csv'. A filter dialog is open over the list, specifically for the 'Created0x10' column. The dialog has two tabs: 'Values' and 'Date Filters'. Under 'Date Filters', there is a dropdown set to 'Dates within a range' with two date fields: '01/08/2025' and '07/08/2025'. At the bottom of the dialog are 'Clear Filter', 'OK', and 'Cancel' buttons. The main table lists various files with their creation times, such as '1723 2021-06-30 05:14:42' and '1734 2021-06-30 05:14:42'.

rectory	Has Ads	Is Ads	File Size	Created0x10	Last Modified0x10	Last M
				1723 2021-06-30 05:14:42	2021-06-30 05:14:42	2022-
				1715 2021-06-30 05:14:42	2021-06-30 05:14:42	2022-
				1691 2021-06-30 05:14:42	2021-06-30 05:14:42	2022-
				1683 2021-06-30 05:14:42	2021-06-30 05:14:42	2022-
				1694 2021-06-30 05:14:42	2021-06-30 05:14:42	2022-
				1723 2021-06-30 05:14:42	2021-06-30 05:14:42	2022-
				1698 2021-06-30 05:14:42	2021-06-30 05:14:42	2022-
				1693 2021-06-30 05:14:42	2021-06-30 05:14:42	2022-
				1711 2021-06-30 05:14:42	2022-12-12 20:33:57	2022-
				1692 2021-06-30 05:14:42	2022-12-12 20:33:57	2022-
				1710 2021-06-30 05:14:42	2022-12-12 20:33:57	2022-
				1712 2021-06-30 05:14:42	2022-12-12 20:33:57	2022-
				1700 2021-06-30 05:14:42	2022-12-12 20:33:57	2022-
				1734 2021-06-30 05:14:42	2022-12-12 20:33:57	2022-

💡 Ejemplos de análisis forense con Timeline Explorer

Objetivo	Filtro o acción
Ver archivos eliminados	<code>InUse == false</code>
Buscar archivos creados justo antes del incidente	Filtrar por fecha en <code>Created0x10</code>
Detectar uso de pendrives o instalación de software	Filtrar por <code>Extension</code> o <code>FileName</code> sospechoso
Encontrar accesos a carpetas ocultas	Buscar en <code>Flags</code> o rutas como <code>\\$RECYCLE.BIN</code> o <code>System Volume Information</code>

