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

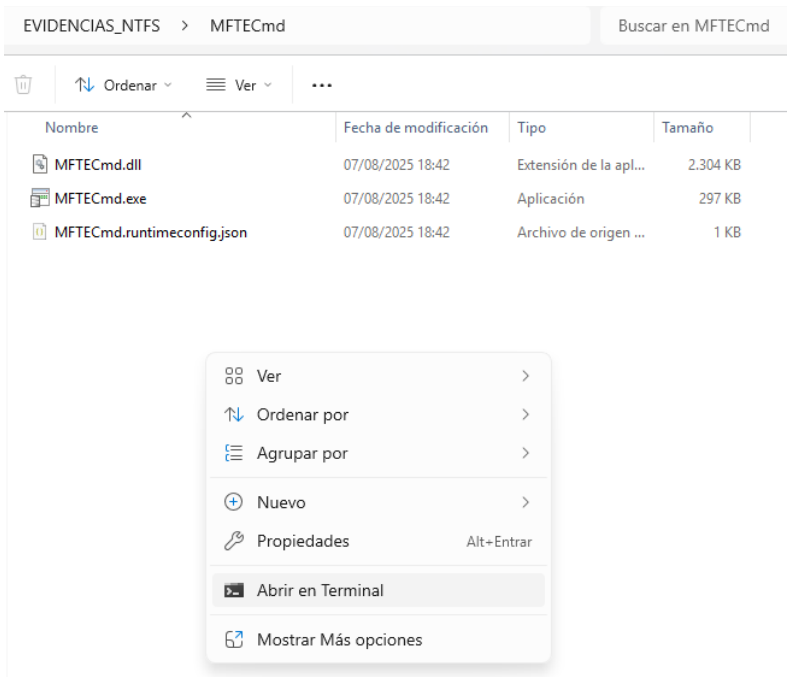
El objetivo principal es **reconstruir una línea de tiempo precisa** que nos permita detectar patrones relevantes, posibles manipulaciones o eventos críticos que hayan afectado al sistema.

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

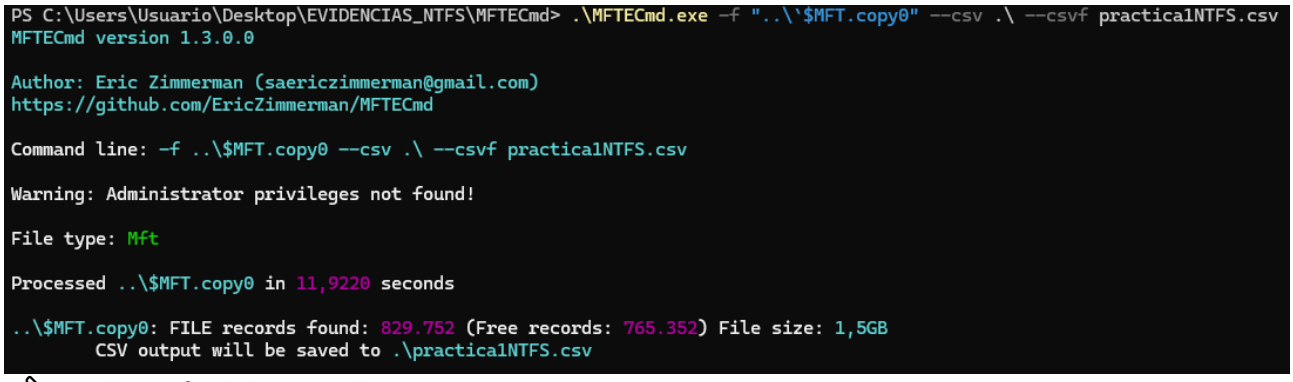


🗁 Estructura de carpetas usada:

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



📌 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 practica1NTFS.csv`	Define el nombre del archivo CSV de salida: `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 practica1NTFS.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?

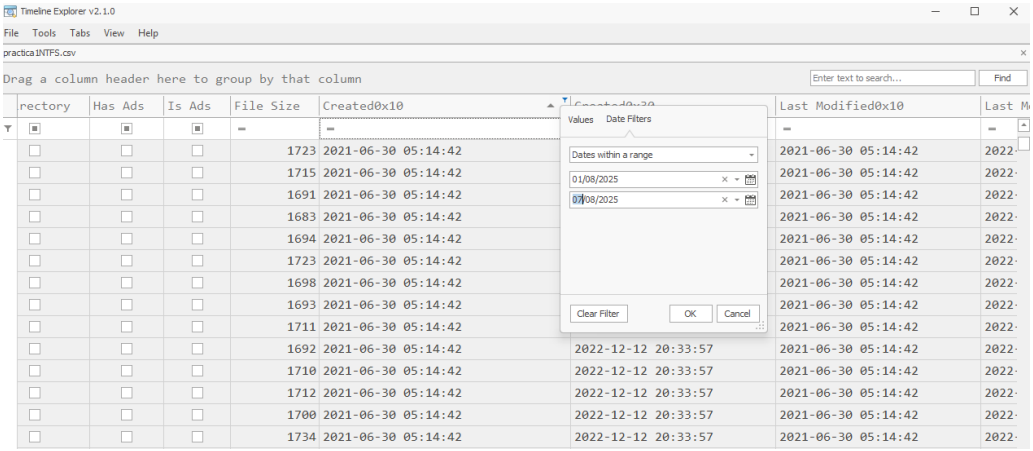
- Visualizar registros de tiempo de forma clara y ordenada.
- Aplicar **filtros avanzados** sin complicaciones.
- Ordenar por fechas de creación, modificación o eliminación.
- Ver múltiples columnas al mismo tiempo (fechas, rutas, nombres, tamaño...).
- Marcar eventos sospechosos o de interés.
- Exportar 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 `practica1NTFS.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)



💡 Ejemplos de análisis forense con Timeline Explorer

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