PRÁCTICA 2. ANÁLISIS DE NTFS

El sistema de archivos en cualquier dispositivo de almacenamiento es esencial para la organización general, los mecanismos de almacenamiento y el control de datos del dispositivo. Saber cómo funcionan estos sistemas de archivos y el diseño de estructuras clave, mecanismos de almacenamiento, metadatos asociados y características del sistema de archivos es esencial para ser capaz de realizar una investigación forense en una computadora u otro dispositivo. Los sistemas de archivos NTFS y FAT son dos sistemas de archivos clave que se utilizan activamente y se encuentran a menudo. Ambos sistemas ofrecen evidencia forense que es significativa y obligatoria en cualquier investigación.

Objetivos principales de la práctica:

- **Estudiar las metadatos que ofrece el sistema de archivos NTFS para el análisis forense.**

Software a utilizar:

- FTK imager 4.3 o superior
- Active Disk Editor v7.0
- MFT2Csv
- NTFSLogFile
- UsnJrl2Csv
- ANJP
- AlternateStreamViewer
- Indx2Csv

Imagen de disco a utilizar: Descárgatela desde este enlace.

Se pide:

1. Descargate la imagen de disco y abrela con Active Disk Editor (ADE). Intenta identificar con la herramienta ADE, mediante la inspección de los registros MFT (1KB), cuales de ellos han sido borrados en base a la propiedad FLAGS (campo “in use” = ’0’).

    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. Identificar los atributos a bajo nivel de alguno de los ficheros (registros de la MFT) mediante la herramienta **Active Disk Editor 7**. Los atributos que nos interesan son $10, $30 y $80.

    a. ¿Dónde puedo encontrar las fechas de creación, modificación y acceso?
    b. ¿Qué significa la propiedad non-resident y sus valores asociados 0/1?

3. 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.

4. 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 **NTFSLogFile** Parse 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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).