Esta herramienta sirve para descodificar el registro $MFT de archivos individuales. Es una combinación de mft2csv y NtfsFileExtracter. No escribe ningún CSV, sino que muestra la información en la consola. Es muy útil cuando se están probando cosas y aprendiendo NTFS, ya que se puede hacer cualquier cosa con un archivo en una unidad NTFS y obtener de inmediato la decodificación de la parte de la MFT correspondiente a ese archivo, sin necesidad de tener que extraer todo el $MFT y luego decodificarlo a un CSV. Entonces mientras que Mft2CSV es útil para extraer $MFT completo con todos sus registros, MftRcrd es para el volcado rápido de información de registro de archivos individuales.

Soporta tanto el nombre del archivo + ruta como el IndexNumber (registro MFT) como entrada (param1). Ahora también se puede especificar el desplazamiento del disco como alternativa. Ver ejemplos a continuación para la sintaxis. Param4 es para elegir si se desea hacer un hexdump de los registros INDX resueltos del atributo $INDEX_ALLOCATION

Atributos soportados:

- $STANDARD_INFORMATION
- $ATTRIBUTE_LIST
- $FILE_NAME
- $OBJECT_ID
- $SECURITY_DESCRIPTOR (sólo volcado hexadecimal crudo)
- $VOLUME_NAME
- $VOLUME_INFORMATION
- $DATA
- $INDEX_ROOT
- $INDEX_ALLOCATION
- $BITMAP (just raw hex dump)
- $REPARSE_POINT
- $EA_INFORMATION
- $EA
- $LOGGED_UTILITY_STREAM

CÓMO EJECUTAR MFTRCRD

MftRcrd64.exe param2 param3

- **param1** puede ser una ruta de archivo válida o un IndexNumber (número de registro $MFT).
- **param2** puede ser -d o -a:
  -d significa solo decodificar la entrada $MFT
  -a es lo mismo que -d pero también vuelca toda la entrada $MFT a la consola.
- **param3** para especificar si se quiere hacer un hexdump completo de los registros INDX y puede ser **indxdump=on** o **indxdump=off**. Tengan en cuenta que indxdump=on puede generar una gran cantidad de volcado en la consola para ciertos directorios.

Ejemplo para volcar una decodificación $MFT para boot.ini:

```
MFTRCRD C:\boot.ini -d indxdump=off
```

Ejemplo para volcar una decodificación $MFT + un volcado de registro de 1024 bytes $MFT para el propio $MFT en la unidad C:

```
MFTRCRD C:0 -a indxdump=off
```

Ejemplo para volcar una decodificación $MFT para $LogFile en la unidad D:

```
MFTRCRD D:2 -d indxdump=off
```

Ejemplo para volcar una decodificación de registro $MFT + hexdump de los registros INDX resueltos para el directorio raíz en C:, equivalente a la 'carpeta' llamada C:

```
MFTRCRD C:5 -d indxdump=on
```

Ejemplo para decodificar lo que se encuentra en el desplazamiento 3246809088 en la unidad c:

```
MFTRCRD C?3246809088 -a indxdump=off
```

(El desplazamiento especificado en hexadecimal debe estar precedido por «0x», es decir, C?0xC1866000)

Ejecutar la herramienta sin ningún parámetro mostrará la información de ayuda.