Féidearthachtaí as Cuimse
Infinite Possibilities

# NTFS and MTF

Digital Forensics- Week 5 – 18th Oct 2024

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
TECHNOLOGICAL UNIVERSITY DUBLIN

# Overview

NTFS File System

Master File Table Records

Resident and non-resident files

NTFS Journaling

# NTFS

- NTFS - New Technology File System
- NTFS is the primary file system for recent versions of Windows and Windows Server
- It offers security descriptors, encryption, disk quotas, and rich metadata.
- NTFS can support volumes as large as 8 petabytes on Windows Server 2019 and newer and Windows 10

# How NTFS Works

- A  hard drive needs to be formatted with to work with a particular file system.
- An operating system will be capable of working with a particular file system to perform storage and retrieval operations.
- clusters range from 512 bytes to 64 KB

# NTFS features

- Organizational efficiency - b-tree directory scheme
- Accessible data - via MFT
- Capacity for very large files
- User Permissions
- File compression
- Security - place permissions on certain data
- Logging - extensive logs on the file system operation

# How is this useful in Digital Forensics?

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
TU DUBLIN
TECHNOLOGICAL UNIVERSITY DUBLIN

- Over the last couple of weeks we have seen how content cna be recovered from a file system (carving, Autopsy, headers, footers etc...)
- For a given machine the Hard Drive and File System are the data persistence mechanism. Anything saved or retrieved comes through here.
- The exact operation of a File System can offer information to a digital forensic investigation.

# What is available via NTFS

- File System Analysis - Master File Table (MFT) and File metadata
- Recovery - deleted content (carving and unallocated space)
- Timestamps - Analyzing timestamps (creation, modification, access)
- Journal Analysis - the journals document the changes made to the file system

# Master File Table MFT

- MFT is a relational database
- The new Resiliant File System (ReFS) will be the replacement for NTFS
- Every file and folder has a record in the MFT (including the MFT itself and its copy)
- A MFT record contains date/time stamps, the file size, file status and the memory addresses for the file content (even if the file is deleted)

# NTFS Reserved Files

- $MFT
- SMFTMirr
- $LogFile
- $Volume
- $AttrDef
- Root Directory
- $Bitmap
- $Extend/$Quota
- $Extend/$ObjId
- SBoot
- $BadClus
- $Secure
- $UpCase
- $Extend
- Reserves for $MFT
- Extension Endties
- $Extend§Reparse

# MFT Record

- A MFT record is 1024 bytes in size, in 2 contiguous 512 sectors
- The first sector contains most of the useful forensic data
- The second sector contains file data (if we are dealing with a resident file)
- If the file data (size) is greater than 512 bytes the file in sot stored in the MTF record but somewhere on the drive.

# Overview of a MFT Record

- The 2 MFT sectors both finish with F7 04
- The MFT Records need to deal with:
  - files and folders
  - parent and child relationships

# Overview of a MFT Record

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
TECHNOLOGICAL UNIVERSITY DUBLIN

Header – starting with 46 49 4C 45 (spells FILE)

Standard Info – starting with 10 00 00 00

Filename – starting with 30 00 00 00

Additional file name entry

Data – starting with 80 00 00 00

# General Info on NFTS

- It can be difficult to find tutorials online for NTFS digital forensics
- There can be small differences in the operation of NTFS for different OS versions.
- A new reference chart would be needed for each operating system
- A forensics examiner would need to be familiar with the differences.

# What is file system journaling?

- The journal is a transactional log of all changes mode to a given volume.
- If there is an issue with the system (eg power off / crash), the operating system can use the journal information to roll back changes or to continue the operation.
- The main focus is to try maintain file system integrity and prevent catastrophic events from occurring.

- Demo: MFTECmd tool by Eric Zimmerman

# Why is system journaling relevant?

- We can use the journal to find evidence of file creations, deletions, changes etc…
- The journal may be the only way to prove if a file existed on a given machine (even if anti-forensics techniques were used)

# $UsrJrnl

- Located in $Extend\$UsrJrnl
- Tracks high level changes
- Provides an efficient change monitoring solution, this is used by AV / Backups software to monitor changes to files.
- Typical size is 32MB
- Example Operation Codes:
  - fileCreate, fileDelete, Rename, Data Override etc….

# $LogFile

- Located in Root
- Tracks the detailed low lever transactional changes for NTFS
- Provides file system integrity and resilience.
    - Records actual data that changed
- May only last hours to days on a primary boot brive.
- Typical size is 64MB
- Example Operation Codes:
    - AddIndexEntryAllocation
    - InitializeFileRecordSegment
    - DeleteIndexEntryAllocation
    - Etc…

# Demo

- Tools by Eric Zimmerman
- KAPE
- MFTECmd
- Timeline Explorer

# NTFS Attributes

| Code | Attribute Name |
|---|---|
| 10 00 00 00 | $Standard_Information |
| 20 00 00 00 | $Attribute_List |
| 30 00 00 00 | $File_Name |
| 40 00 00 00 | $Object_Id |
| 50 00 00 00 | $Security_Descriptor |
| 60 00 00 00 | $Volume_Name |
| 70 00 00 00 | $Volume_Information |
| 80 00 00 00 | $Data |
| 90 00 00 00 | $Index_Root |
| A0 00 00 00 | $Index_Allocation |
| B0 00 00 00 | $Bitmap |
| C0 00 00 00 | $ReparsePoint |
| D0 00 00 00 | $Ea_Information |
| E0 00 00 00 | $EA |
| 00 01 00 00 | $Logged_Utility_Stream |

# $Data Attribute

- 80 00 00 00 xx xx xx xx yy
- As for all attributes, they come with 4 bytes standing for its length (xx xx xx xx).
- The byte that follows this indicates whether the attribute is resident or not (yy)
- When it is resident its value is 0
- When it is not resident its value is 1

# Resident files

- The data for a resident file is contained within the MFT record.

# Non-resident files

- If a file is non-resident, information (data) is stored elsewhere on the disk drive.
- For this to happen the data size will be greater than 512
- The data is stored in groups (data runs). A data run specifies a range of clusters where the file's data is stored, and it includes information about the starting cluster, the number of clusters, and the run's length.
- To retrieve a file, NTFS follows the data runs to retrieve the data from the designated clusters.
- There is no single cut off size for a file to be resident or not, it depends on several factors. Depending on how the file is created (eg by the system, there may be more space for it to be a resident file.

# Summary

- Being able to understand MFT records is an important part of drive analysis in digital forensics.
- This offers insights into data recovery and drive analysis.
- It can show what operations were performed and when.
- If offers different attributes within the MFT records
- Its probably best to use specialized tools to work with the MFT, but the investigators understanding of NTFS and MFT may offer something good to the investigation not detected by the tools.

# Questions