Share 0 More Next Blog» Create Blog Sign In

DigitalResidue's Forensics

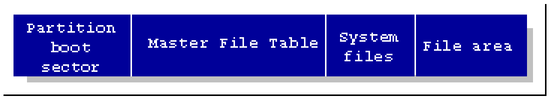
Thursday, March 7, 2013

Windows File System

Filesystems

Windows

- FAT12 This version is used specifically for floppy disks.
- FAT16 Supports disk partitions with a maximum capacity of 2 GB.
- FAT32 On versions of XP and Vista. Along with USB file systems.
- NTFS offers significant improvements over previous FAT file systems. It provides more information about a file, such as file ownership, along with more control over files and folders. NTFS takes advantage of Journaling, where a file system keeps track of the changes that would be made such as deleting or saving. Everything written to the disk is considered a file.
- Keeps track of many file **time stamps.** Create, Modify, Access,
- Compression, auditing, encryption EFS (when a file is added, then when read is unencrypted).
- There is less file slack space in NTFS.
- The Master File Table MFT, is the first file on the disk. MFT contains information about all files on the disk. An MFT is created at the same time a disk partition is formatted as an NTFS volume.
- Resident or non-resident files: If it's larger than 1024 bytes, the file is saved outside of the MFT. If the file is smaller it will be saved in the MFT (resident).
- The first data set is the Partition boot Sector(which starts at sector 0), followed immediately by the MFT.



Component	Description
NTFS Boot Sector	Contains the BIOS parameter block that stores information about the layout of the volume and the file system structures, as well as the boot code that loads Windows Server 2003.
Master File Table	Contains the information necessary to retrieve files from the NTFS partition, such as the attributes of a file.
File System Data	Stores data that is not contained within the Master File Table.
Master File Table Copy	Includes copies of the records essential for the recovery of the file system if there is a problem with the original copy.

Here is a link that shows how the Master File Table is constructed: This includes the NTFS Metafiles: http://www.writeblocked.org/resources/NTFS_CHEAT_SHEETS.pdf

- The MFT can expand but it never contracts. This is important for computer forensic investigators because it effects the recovery of data and the identification of deleted files.
- When a file is deleted the MFT entry is marked as ready to be re-used. This entry will continue to exist until it is overwritten bye a new file (Unallocated to Allocated).
- Here is a visual of these data clusters:

Blog Archive

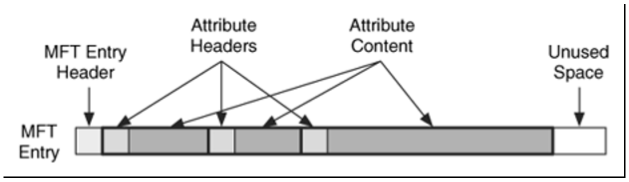
- ▼ 2013 (6)
  - ► July (1)
  - ► June (1)
  - ► April (1)
  - ▼ March (3)
    - Mac File System
    - Windows File System
    - Mac vs Windows pt.1

About Me

DigitalResidue

I've created this blog for the sole purpose of furthering my enjoyment of DFIR.

View my complete profile



- Data hiding techniques will take advantage of these unused areas and fake bad clusters.
- Tools such as Slueth Kit, among many other tools, can check for hidden data in these fake bad clusters.
- This process is also known as data carving. Which i wont be discussing here.

NTFS Journaling:

- NTFS uses $LogFile to record metadata changes that occur in a volume.
- This ensures when data is moved, it will remain consistent.
- USN Journal records all changes to all files, streams and directories in a volume, as well as their various attributes and security settings.

NTFS Data Streams:

- Also known as Alternate Data Streams, was developed in NTFS to be compatible with MAc. (Forks). They pose more of an alternative for Anti-Forensics, so i'll save that conversation for data hiding.
- Every file has a single $Data stream, but NTFS allows multiple data streams.
- You can hide data, which will not be displayed by Windows Explorer, or command dir.

$LogFile:

- Can be considered somewhat of a recovery log (in case of a crash).
- MTF records (which show a file header, and Standard Information Attribute, Filename Attribute, and resident data (all this can be found within the $LogFile) by searching for FILE0 which indicates the beginning of an MFT entry.

INDX Records:

- NTFS indexes directory metadata and stores it in a B+ tree.
- These files can be found in $LogFile.
- This is a blog that i found to be beyond informative for INDX file parsing. http://www.williballenthin.com/forensics/indx/
- Along with a post by Harlan Carvey: http://windowsir.blogspot.com/2013/02/binmode-parsing-java-idx-files-pt-trios.html

Sparse Files:

- To save space
- Important parts of a file are reserved as allocated, whereas the unnecessary parts to run the file can be located to unallocated spaces.
- This a form of Data Compression. (Used by Macs as well)

Reparse Points:

- These are files that essential function as links, and contains information about locations to which way they point.
- Linking files to files, or files to folders etc.. Hard linking (linked within MFT) or Soft Linking.
- Provide a filesystem with extra information to a directory within a folder.
- Reparse points are used to implement: **Volume Mount Points, Directory Junctions, Hierarchal Storage Management, Native Structured Storage, Single Instance Storage, and Symbolic Links**.
- Volume Mount Points: Used to mount and provide an entry point to other volumes. It can give a refernce to a root directory.
  - Volume Shadow Copies: or "snapshots" of files on a volume. Users can access these copies to recover accidentaly deleted or overwritten files without requiring a backup.
  - You can also use these copies to make comparison with other files.

These following areas of the Windows filesystem, will be discussed in depth at a later time.

FAT File Deletion: the OS inserts a HEX E5 (0xE5)_
NTFS File Deletion: $Bitmap is modified to show space occupied by the MFT record and

the space previously occupied by the file itself is now Unallocated and ready for reuse.
Encrypting Filesystems: Bitlocker is used From Vista to Win7.
Application Analysis
Swap or File Slack Analysis
Volume Analysis
Registry Analysis
NTFS metadata file analysis: Such as deleted or not deleted, whether a file is resident or non-resident, time stamps that get updated when a file or folder is copied, moved, or written to.

Sources
Guide to Computer Forensics and Investigations 3rd.
Handbook of Digital Forensics and Investigations.
Wikipedia.

Posted by DigitalResidue at 2:43 PM

g+1 Recommend this on Google

No comments:

Post a Comment

Enter your comment…

Comment as: Google Accou ▼

Publish Preview

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)