

MACB 101

An Introduction for developers



Modified

Accessed

Changed (Windows / sometimes Linux) / **Created** (sometimes Linux)

Birth (Windows only)

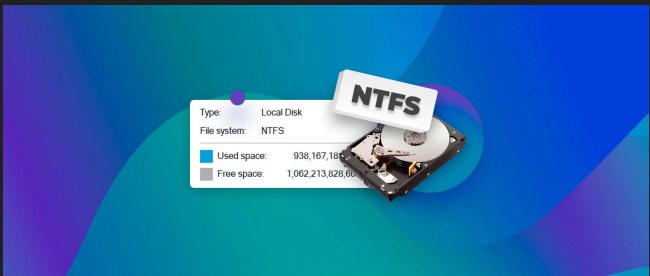
Where are they stored?

Well it depends!



Windows

Windows file systems are “NTFS” file systems



This means that they contain a file called \$MFT aka Master File Table

This file contains things with the two attributes \$STANDARD_INFORMATION and \$FILE_NAME that will contain MACB information for all the files on the system

Windows

\$STANDARD_INFORMATION

can be modified by user-level processes

\$FILE_NAME

can only be modified by the system kernel

The screenshot displays the SMFT Record Viewer application, which is used to inspect and modify file system metadata. The window title is "SMFT Record Viewer - D:\Costas\Desktop\temp\SMFT_stealthy".

The interface is divided into several panes:

- Parent Directory MFT:** Shows the parent directory's MFT entry (59649, SeqNr: 6).
- Header:** Displays file system headers, including the MFT record offset (28437504), signature (FILE), offset fixup (48), number of fix-up byte pairs (3), \$LogFile Sequence Number (LSN) (456057399), sequence number (2), hard link count (1), offset to 1st attribute (56), allocation status (File, In Use), logical size of MFT record (544), physical size of MFT record (1024), base record (0), base record seqnr (0), next available attribute ID (6), MFT record number (27771), and update sequence number (7).
- Attributes:** A list of file attributes. The attribute **\$STANDARD_INFORMATION** (ID: 00000, Type: 100000000) is highlighted with a green box. Other attributes include \$FILE_NAME (ID: 00002, Type: 300000000) and \$OBJECT_ID (ID: 00003, Type: 400000000).
- Resident Content (UTF8):** Shows the file's content, which is "Hello dfr find the stealthy ADS artifacts | good luck".
- Resident Content (hex):** Shows the hexadecimal representation of the file's content.
- Table:** A table showing the file's data blocks, including their addresses, sizes, and offsets.

Linux differences

Lots of possible file system types! No \$MFT by default

Typically there is no “Birth” time - although this varies depending on file system

The “C” time normally describes the last time that the file’s metadata was altered.

Regular files / folders

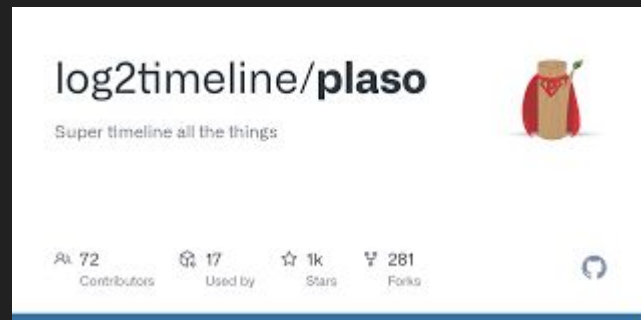
os.stat

Zips:

```
ZipFile(file).infolist()
```

Plaso's log2timeline

Parses a lot of specific file types and binaries



Timezones??

Most tools will either automatically convert timestamps to UTC based on system information or will assume that everything is in UTC