MACB 101

An Introduction for developers


SCOTTISH SPRING WATER
STILL
MAC B
APPLE & BLACKCURRANT
SUGAR FREE • SUGAR FREE • SUGAR FREE

Modified

Accessed

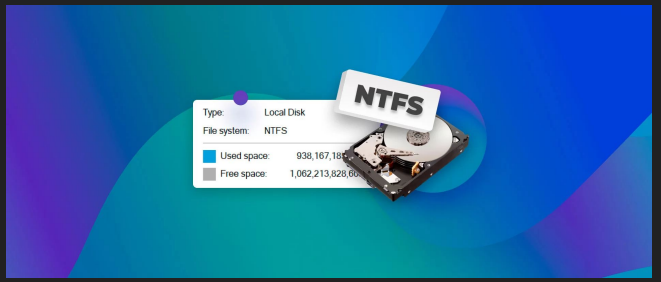
Changed (Windows / sometimes Linux) / **C**reated (sometimes Linux)

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

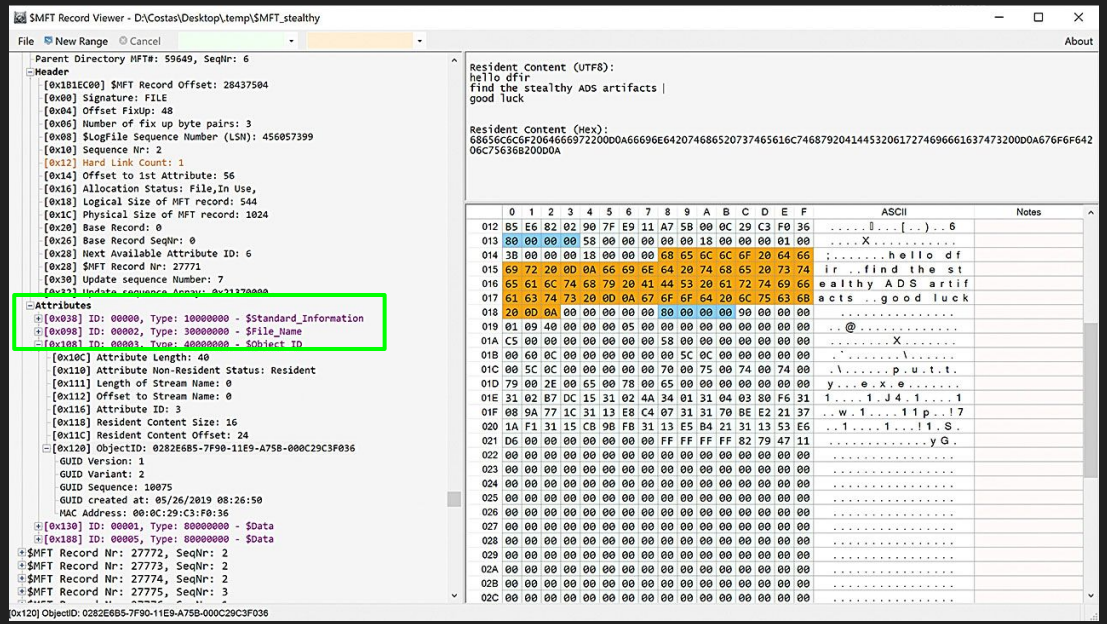
Windows

$STANDARD_INFORMATION

can be modified by user-level processes

$FILE_NAME

can only be modified by the system kernel



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