

HackTricks



WELCOME!

HackTricks

About the author

Getting Started in Hacking

GENERIC METHODOLOGIES & RESOURCES

Pentesting Methodology

External Recon Methodology >

Pentesting Network >

Pentesting Wifi >

Phishing Methodology >

Basic Forensic Methodology v

Baseline Monitoring

[Anti-Forensic Techniques](#)

Docker Forensics

Image Adquisition & Mount

Linux Forensics

Malware Analysis

Memory dump analysis >

Partitions/File Systems/Carving >



Powered By **GitBook**

Anti-Forensic Techniques



Support HackTricks and get benefits!

Timestamps

An attacker may be interested in **changing the timestamps of files** to avoid being detected.

It's possible to find the timestamps inside the MFT in attributes

`$STANDARD_INFORMATION` __ and __ `$FILE_NAME` .

Both attributes have 4 timestamps: **Modification, access, creation**, and **MFT registry modification** (MACE or MACB).

Windows explorer and other tools show the information from **`$STANDARD_INFORMATION`** .

TimeStomp - Anti-