Anti-Forensic Techniques

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-