Cyber Law and Forensics (CS402)

Lab Assignment 4

**U19CS012**

A.) Identifying original timestamp by MFT analysis

(1) Basics behind Windows MACB Timestamp’s (NTFS)

**M** = Modification

**A** = Access

**C** = MFT Record **Change**

**B** = Birth (Creation)

Timestamps are stored in Metadata File called $MFT.

We can view it via 2 Ways:-

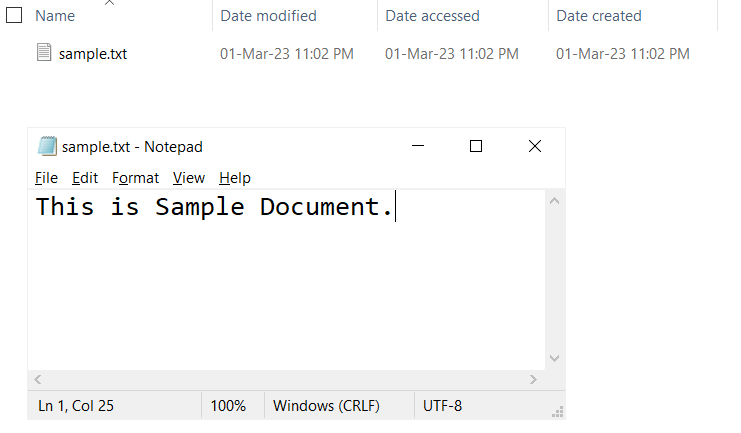
(a) $STANDARD\_INFORMATION ($SI) [File Explorer / CMD / PowerShell]

(b) $FILE\_NAME ($FN) [Only Modifiable by **Windows Kernel**]

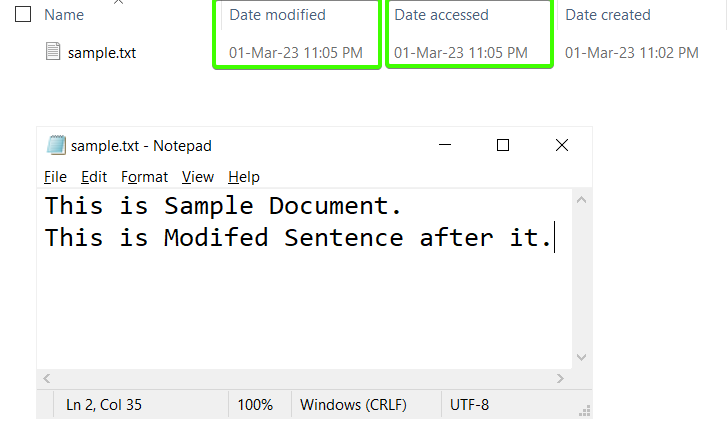
**Idea**: Compare the Timestamp of $SI with $FN to Check if File is Original / Copied / Modified?

|  |  |  |  |
| --- | --- | --- | --- |
| File Operation | Modified | Accessed | Birth (Creation) |
| File Create | Yes | Yes | Yes |
| File Modify | Yes | Yes | No |
| File Copy | No (Inherited) | Yes | Yes |
| File Access | No | No | No |

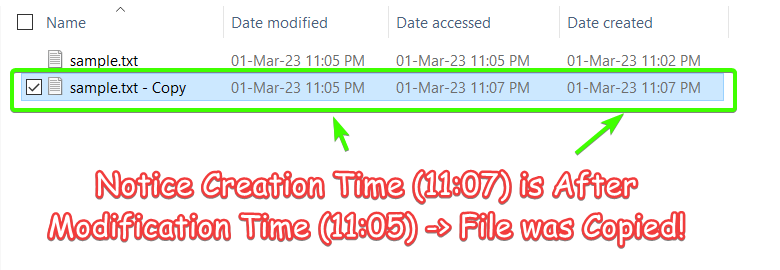
(I) File Create



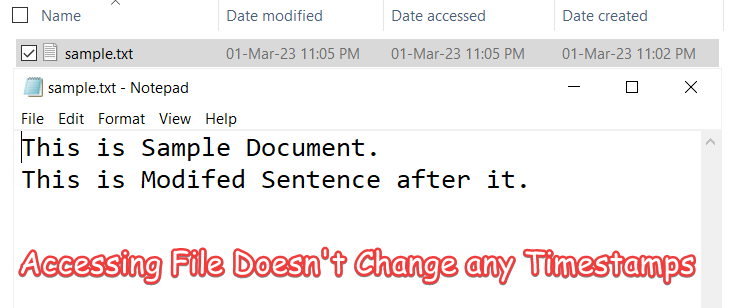
(II) File Modify



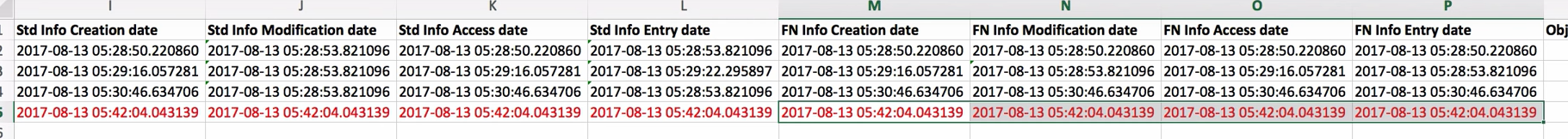
(III) File Copy



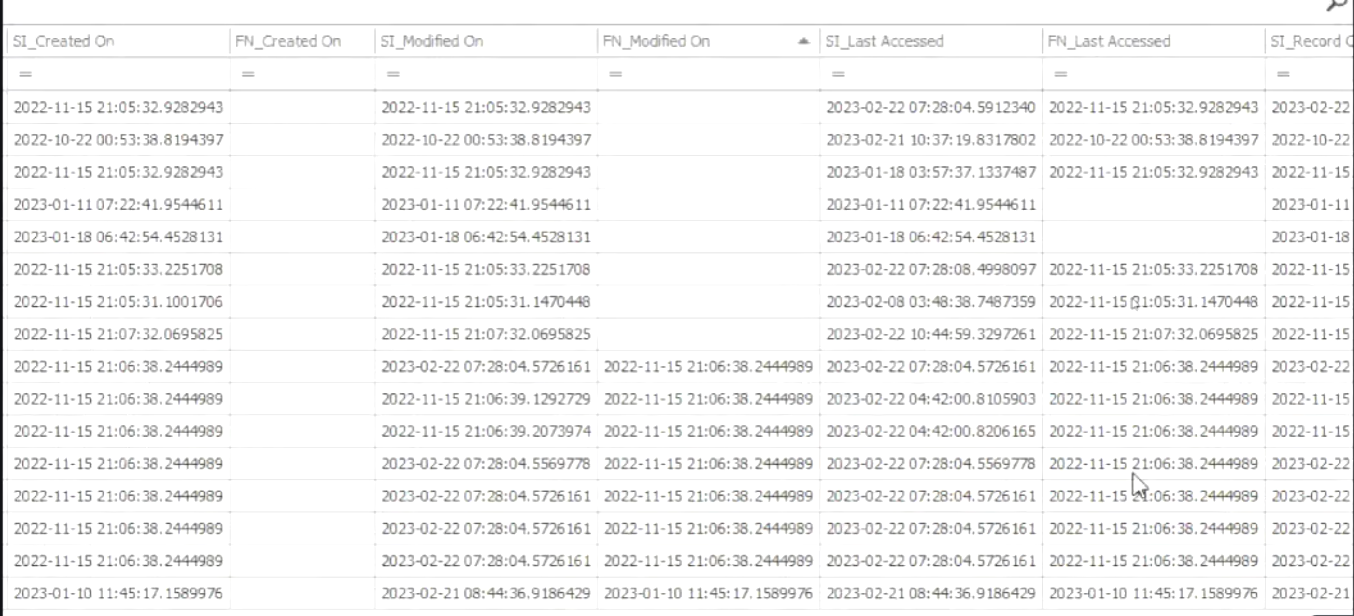
(IV) File Access (No Changes in Timestamp)

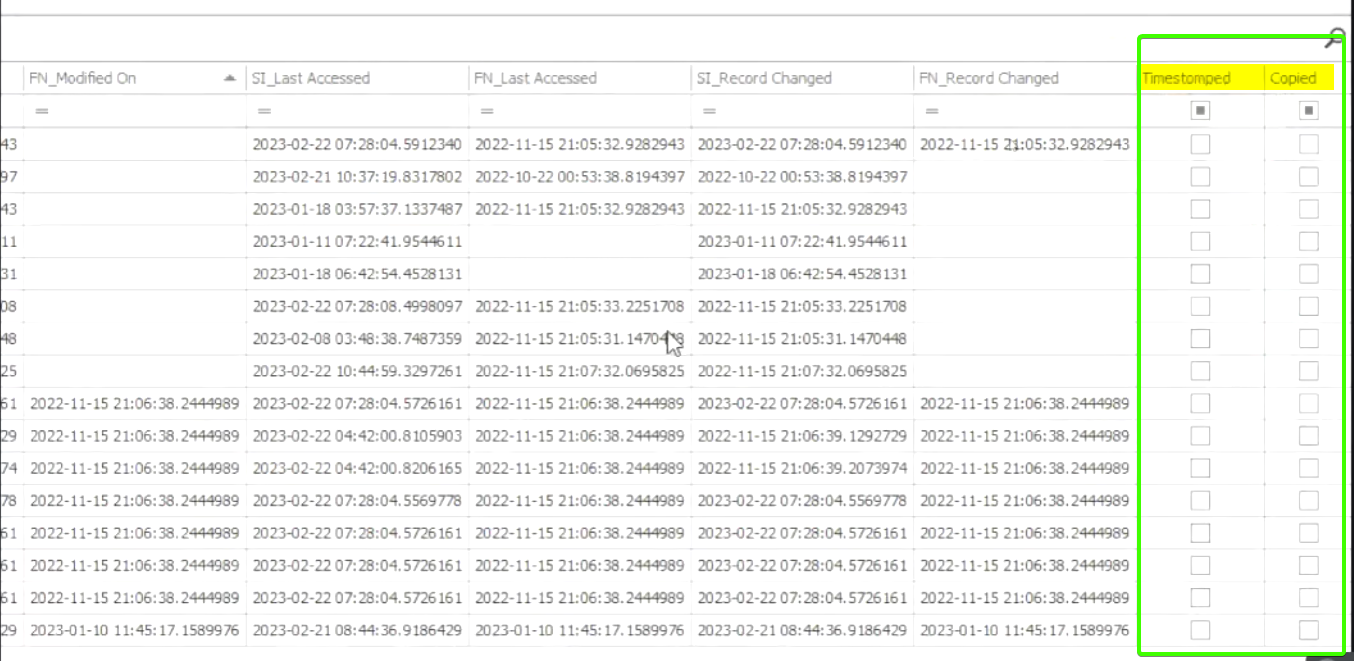


SI TimeStamps & FN Timestamps (Manually in Excel from MFT)



**MFT Explorer** (GUI Tool by Zimmerman)





**SUBMITTED BY**:

U19CS012

BHAGYA VINOD RANA