

# 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:-

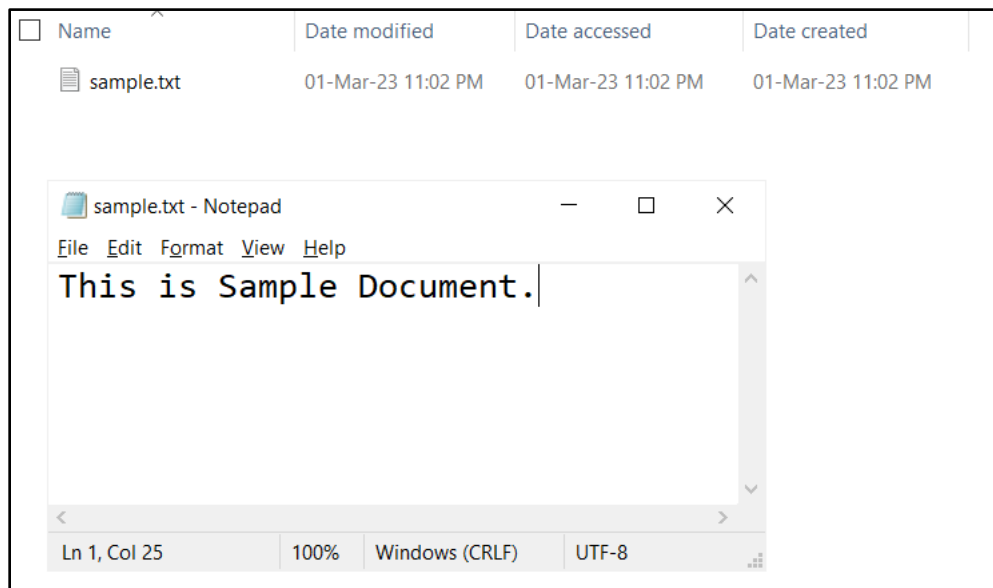
(a) \$STANDARD\_INFORMATION (\$SI) [File Explorer / CMD / PowerShell]

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

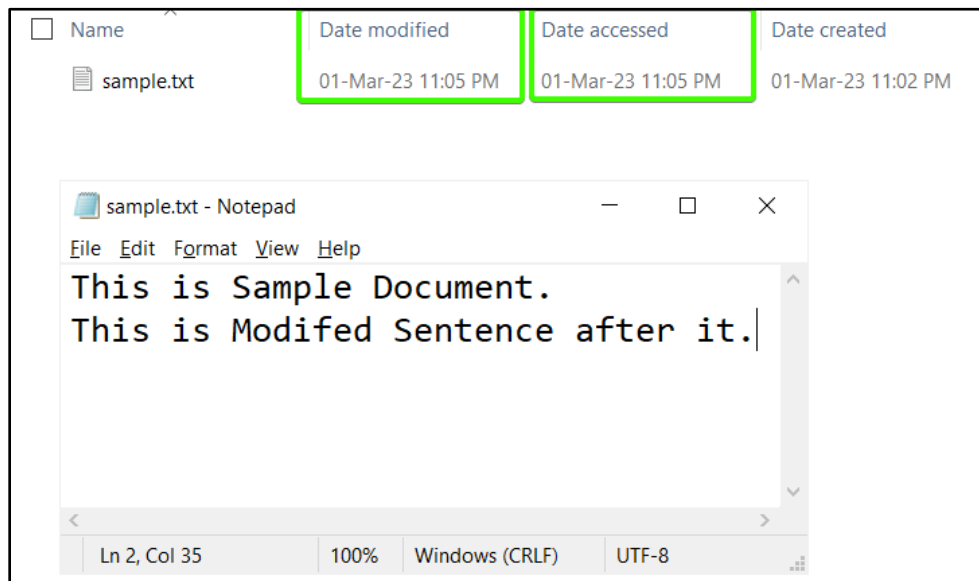
**Idea:** Compare the Timestamp of \$SI with \$FN to Check if File is Original / Copied / Modified?

File Operation	Modified	Accessed	Birth (Creation)
<b>File Create</b>	Yes	Yes	Yes
<b>File Modify</b>	Yes	Yes	No
<b>File Copy</b>	No (Inherited)	Yes	Yes
<b>File Access</b>	No	No	No



## (I) File Create



## (II) File Modify



(III) File Copy

<input type="checkbox"/> Name	Date modified	Date accessed	Date created
 sample.txt	01-Mar-23 11:05 PM	01-Mar-23 11:05 PM	01-Mar-23 11:02 PM
<input checked="" type="checkbox"/>  sample.txt - Copy	01-Mar-23 11:05 PM	01-Mar-23 11:07 PM	01-Mar-23 11:07 PM

(IV) File Access (No Changes in Timestamp)

The screenshot shows a Windows File Explorer window with a table of files. The columns are 'Name', 'Date modified', 'Date accessed', and 'Date created'. The file 'sample.txt' is highlighted, showing timestamps of 01-Mar-23 11:05 PM for all three categories. Below the File Explorer is a Notepad window titled 'sample.txt - Notepad' containing the text: 'This is Sample Document.' and 'This is Modified Sentence after it.'

Name	Date modified	Date accessed	Date created
sample.txt	01-Mar-23 11:05 PM	01-Mar-23 11:05 PM	01-Mar-23 11:02 PM

sample.txt - Notepad

File Edit Format View Help

This is Sample Document.  
This is Modified Sentence after it.

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

[illegible]

## MFT Explorer (GUI Tool by Zimmerman)

SI_Created On	FN_Created On	SI_Modified On	FN_Modified On	SI_Last Accessed	FN_Last Accessed	SI_Record C
==	==	==	==	==	==	==
2022-11-15 21:05:32.9282943		2022-11-15 21:05:32.9282943		2023-02-22 07:28:04.5912340	2022-11-15 21:05:32.9282943	2023-02-22
2022-10-22 00:53:38.8194397		2022-10-22 00:53:38.8194397		2023-02-21 10:37:19.8317802	2022-10-22 00:53:38.8194397	2022-10-22
2022-11-15 21:05:32.9282943		2022-11-15 21:05:32.9282943		2023-01-18 03:57:37.1337487	2022-11-15 21:05:32.9282943	2022-11-15
2023-01-11 07:22:41.9544611		2023-01-11 07:22:41.9544611		2023-01-11 07:22:41.9544611		2023-01-11
2023-01-18 06:42:54.4528131		2023-01-18 06:42:54.4528131		2023-01-18 06:42:54.4528131		2023-01-18
2022-11-15 21:05:33.2251708		2022-11-15 21:05:33.2251708		2023-02-22 07:28:08.4998097	2022-11-15 21:05:33.2251708	2022-11-15
2022-11-15 21:05:31.1470448		2022-11-15 21:05:31.1470448		2023-02-08 03:48:38.7487359	2022-11-15 21:05:31.1470448	2022-11-15
2022-11-15 21:07:32.0695825		2022-11-15 21:07:32.0695825		2023-02-22 10:44:59.3297261	2022-11-15 21:07:32.0695825	2022-11-15
2022-11-15 21:06:38.2444989		2023-02-22 07:28:04.5726161	2022-11-15 21:06:38.2444989	2023-02-22 07:28:04.5726161	2022-11-15 21:06:38.2444989	2023-02-22
2022-11-15 21:06:38.2444989		2022-11-15 21:06:39.1292729	2022-11-15 21:06:38.2444989	2023-02-22 04:42:00.8105903	2022-11-15 21:06:38.2444989	2022-11-15
2022-11-15 21:06:38.2444989		2022-11-15 21:06:39.2073974	2022-11-15 21:06:38.2444989	2023-02-22 04:42:00.8206165	2022-11-15 21:06:38.2444989	2022-11-15
2022-11-15 21:06:38.2444989		2023-02-22 07:28:04.5569778	2022-11-15 21:06:38.2444989	2023-02-22 07:28:04.5569778	2022-11-15 21:06:38.2444989	2023-02-22
2022-11-15 21:06:38.2444989		2023-02-22 07:28:04.5726161	2022-11-15 21:06:38.2444989	2023-02-22 07:28:04.5726161	2022-11-15 21:06:38.2444989	2023-02-22
2022-11-15 21:06:38.2444989		2023-02-22 07:28:04.5726161	2022-11-15 21:06:38.2444989	2023-02-22 07:28:04.5726161	2022-11-15 21:06:38.2444989	2023-02-22
2022-11-15 21:06:38.2444989		2023-02-22 07:28:04.5726161	2022-11-15 21:06:38.2444989	2023-02-22 07:28:04.5726161	2022-11-15 21:06:38.2444989	2023-02-22
2023-01-10 11:45:17.1589976		2023-02-21 08:44:36.9186429	2023-01-10 11:45:17.1589976	2023-02-21 08:44:36.9186429	2023-01-10 11:45:17.1589976	2023-02-21

FN_Modified On	SI_Last Accessed	FN_Last Accessed	SI_Record Changed	FN_Record Changed	Timestamped	Copied
==	==	==	==	==	<input type="checkbox"/>	<input type="checkbox"/>
43 2023-02-22 07:28:04.5912340	2022-11-15 21:05:32.9282943	2023-02-22 07:28:04.5912340	2022-11-15 21:05:32.9282943	2022-11-15 21:05:32.9282943	<input type="checkbox"/>	<input type="checkbox"/>
97 2023-02-21 10:37:19.8317802	2022-10-22 00:53:38.8194397	2022-10-22 00:53:38.8194397	2022-10-22 00:53:38.8194397		<input type="checkbox"/>	<input type="checkbox"/>
43 2023-01-18 03:57:37.1337487	2022-11-15 21:05:32.9282943	2022-11-15 21:05:32.9282943	2022-11-15 21:05:32.9282943		<input type="checkbox"/>	<input type="checkbox"/>
11 2023-01-11 07:22:41.9544611		2023-01-11 07:22:41.9544611			<input type="checkbox"/>	<input type="checkbox"/>
31 2023-01-18 06:42:54.4528131		2023-01-18 06:42:54.4528131			<input type="checkbox"/>	<input type="checkbox"/>
08 2023-02-22 07:28:08.4998097	2022-11-15 21:05:33.2251708	2022-11-15 21:05:33.2251708	2022-11-15 21:05:33.2251708		<input type="checkbox"/>	<input type="checkbox"/>
48 2023-02-08 03:48:38.7487359	2022-11-15 21:05:31.1470448	2022-11-15 21:05:31.1470448	2022-11-15 21:05:31.1470448		<input type="checkbox"/>	<input type="checkbox"/>
25 2023-02-22 10:44:59.3297261	2022-11-15 21:07:32.0695825	2022-11-15 21:07:32.0695825	2022-11-15 21:07:32.0695825		<input type="checkbox"/>	<input type="checkbox"/>
61 2022-11-15 21:06:38.2444989	2023-02-22 07:28:04.5726161	2022-11-15 21:06:38.2444989	2023-02-22 07:28:04.5726161	2022-11-15 21:06:38.2444989	<input type="checkbox"/>	<input type="checkbox"/>
29 2022-11-15 21:06:38.2444989	2023-02-22 04:42:00.8105903	2022-11-15 21:06:38.2444989	2022-11-15 21:06:39.1292729	2022-11-15 21:06:38.2444989	<input type="checkbox"/>	<input type="checkbox"/>
74 2022-11-15 21:06:38.2444989	2023-02-22 04:42:00.8206165	2022-11-15 21:06:38.2444989	2022-11-15 21:06:39.2073974	2022-11-15 21:06:38.2444989	<input type="checkbox"/>	<input type="checkbox"/>
78 2022-11-15 21:06:38.2444989	2023-02-22 07:28:04.5569778	2022-11-15 21:06:38.2444989	2023-02-22 07:28:04.5569778	2022-11-15 21:06:38.2444989	<input type="checkbox"/>	<input type="checkbox"/>
61 2022-11-15 21:06:38.2444989	2023-02-22 07:28:04.5726161	2022-11-15 21:06:38.2444989	2023-02-22 07:28:04.5726161	2022-11-15 21:06:38.2444989	<input type="checkbox"/>	<input type="checkbox"/>
61 2022-11-15 21:06:38.2444989	2023-02-22 07:28:04.5726161	2022-11-15 21:06:38.2444989	2023-02-22 07:28:04.5726161	2022-11-15 21:06:38.2444989	<input type="checkbox"/>	<input type="checkbox"/>
61 2022-11-15 21:06:38.2444989	2023-02-22 07:28:04.5726161	2022-11-15 21:06:38.2444989	2023-02-22 07:28:04.5726161	2022-11-15 21:06:38.2444989	<input type="checkbox"/>	<input type="checkbox"/>
29 2023-01-10 11:45:17.1589976	2023-02-21 08:44:36.9186429	2023-01-10 11:45:17.1589976	2023-02-21 08:44:36.9186429	2023-01-10 11:45:17.1589976	<input type="checkbox"/>	<input type="checkbox"/>

**SUBMITTED BY:**

**U19CS012**

**BHAGYA VINOD RANA**