# USE case two – Word File Time stamp manipulation

In this case, we modify the timestamp of a word document by a tool named timestomper.exe

<https://github.com/slyd0g/TimeStomper> that manipulates Windows file times using SetFileTime() API . This process is shown in figure 1, 2 , and 3

A screenshot of a computer

AI-generated content may be incorrect.

Figure 1: Properties of secret.docx before timestamp manipulation

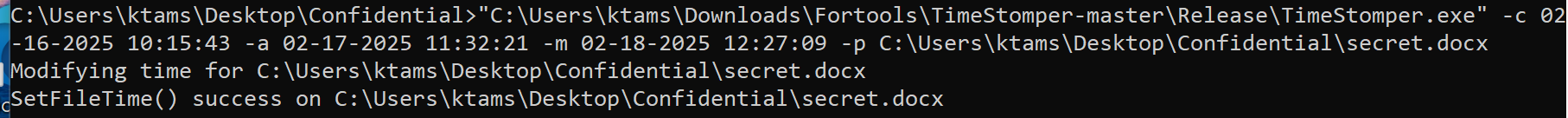


Figure 2: Implementing Timestomper.exe on secret.docx

A screenshot of a computer

AI-generated content may be incorrect.

Figure 3: Properties of secret.docx after timestamp manipulation

The mft record values that is to be noted for secret.docx before manipulation is shown below and figure 4.

Created0x10: 2/19/2025 17:24

Created0x30:

LastAccess0x10: 2/19/2025 17:24

LastAccess0x30:

A screenshot of a computer

AI-generated content may be incorrect.

Figure 4: MFT Record of the system before timestamp manipulation

The mft record values that is to be noted for secret.docx after manipulation is shown below and figure 5.

Created0x10: 2/16/2025 10:15

Created0x30: 2/19/2025 17:24

LastAccess0x10: 2/18/2025 12:27

LastAccess0x30: 2/19/2025 17:24

A screenshot of a computer screen

AI-generated content may be incorrect.

Figure 5: MFT Record of the system after timestamp manipulation

I have shared the raw MFT record with the hash **3974e9afc72a9d2a024699b98d4da0dd** and provided it in CSV format.

1. Start by testing the raw data.
2. Try asking without explicitly mentioning the word "file” for example, *"Can you find any time stomping based on this raw data?"* and then test the CSV version as well by asking, *"Can you find any time stomping based on this CSV data?"*
3. Next, you can be more specific by mentioning the file name **secret.docx**. For example:

* *"Can you find any time stomping on a file named secret.docx based on this raw data?"*
* *"Can you find any time stomping on a file named secret.docx based on this CSV data?"*

Additionally, I’ve shared the USNJRNL record with the hash **f00d8bcd76900680381c8e632ae4cb11**. Input this data using the same approach and check for any anomalies. Just different data same sets of questions

Finally, provide both datasets together to see if the LLMs can detect anti forensic techniques. This phase aims to assess their capability in identifying such manipulations.

1. Now I will provide you with both sets of raw, then csv, test accordingly.

Now it is coming to another phase where we check llm capabilities for inconsistencies in artifacts

**The first inconsistency** is identified through **LNK files** when analyzing the timestomping technique. In this case, the time values are nearly identical — with only milliseconds or seconds differing, while the minutes remain the same. This similarity is evident when comparing **secret.docx** and **secret.lnk** in the highlighted sections of the figure.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 6: Before changing secret.docx in mft with lnk file.

Interestingly, the key inconsistency is that while the associated **secret.docx** file gets modified, the **secret.lnk** file still has the previous timestamp. This is an abnormal system behavior that should not occur naturally unless the timestamp has been deliberately forged, as shown in Figure 7.A screenshot of a computer

AI-generated content may be incorrect.

Figure 7: After changing secret.docx in mft with its lnk file

Some examples for llm you can ask are as follows you can add accordingly.

1. **General Inconsistency Check:**
   * *"Can you identify any inconsistencies in any files based on this raw data?"*
   * *"This is an MFT record. Can you find any inconsistencies in any files from this raw data?"*
   * *"This is a parsed MFT record in CSV format. Can you find any inconsistencies or abnormalities?"*
2. **Specific File Check (secret.docx):**

*The file secret.docx is forged. Can you identify any inconsistencies in its timestamps that indicate abnormal behavior?"*

1. **LNK File Comparison (secret.docx vs. secret.lnk):**
   * *"Can you identify any inconsistencies between the timestamps of secret.docx and its associated shortcut file, secret.lnk?"*
   * *"Is there any abnormal behavior where secret.docx appears modified, but secret.lnk retains its original timestamp?"*

The second inconsistency is observed in the extracted XML structure of secret.docx, as shown in Figures 8 and 9. In Figure 9, the core.xml file reveals that the dcterms:created and dcterms:modified timestamps have the same previous values, even after timestomping. This inconsistency arises because the MFT record shows one value, while the XML metadata shows another.

Now, proceed by questioning LLMs as before, this time uploading both the Word file and the MFT record. Use a similar approach to test their ability to detect these inconsistencies.

A screenshot of a computer

AI-generated content may be incorrect.

Figure:8 – xml structure of secret.docx

A screenshot of a computer screen

AI-generated content may be incorrect.

Figure:8 – core.xml of secret.docx