Digital Forensics Expert opinion

DFIR Report

File signature and File extension

Report No: 02

Report compiled by Muhsin Ali Shah

Date of investigation : 05/02/2024
Date report compiled : 05/02/2024

Endorsement:

- The contents of this report are the result of an investigation undertaken by myself, and I hereby confirm that:
- The investigation was conducted in accordance with the OWASP Top 10 Vulnerabilities.
- The software and hardware used to support this investigation were prepared and used in a manner designed to assure the forensic integrity of both the process and its outcomes.
- The opinions presented at the end of this report are mine and mine alone and are based solely on the evidence found.

Signed by: ***Muhsin Ali Shah***

Date [10/04/2024]

Credentials of the Investigator:

- My name Is Muhsin Ali Shah and I am student of Cyber Security:
- Internee {3 Months}
- Masters From UOP
- ItSolera Cyber Security Training
- Memberships
- https://www.linkedin.com/in/muhsinalishah/

Purpose of the Investigation:

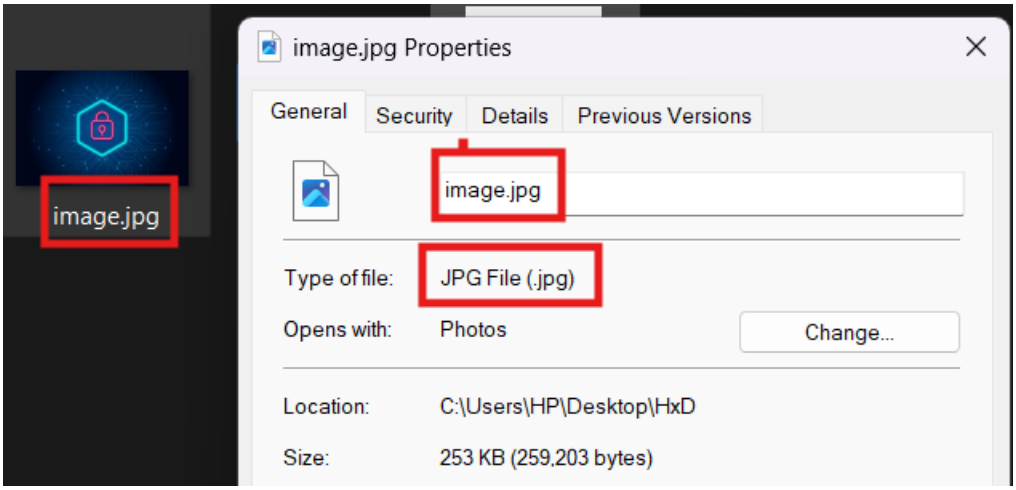
Case background: It is just for educational purposes:

Software to be used in investigation:

HxD Editor or Hxd Workshop and Autopsy.

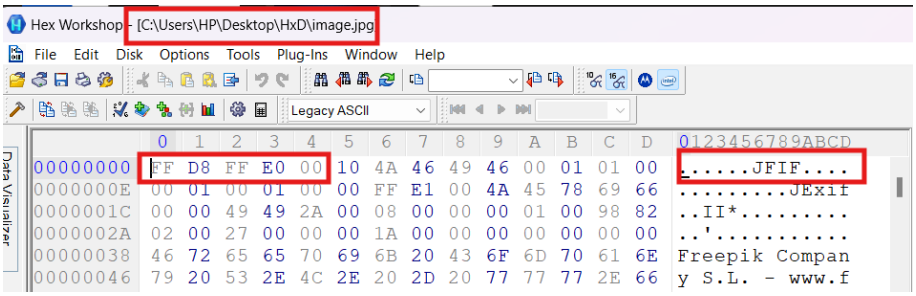
OBJECTIVES OF INVESTIGATION: OBJECTIVE OF FILE SIGNATURE AND EXTENSION ANALYSIS IN HXD:

1. **Identify File Type:** The main objective of analyzing file signatures is to determine the actual file type. File signatures, also known as "magic numbers," help identify files beyond just their extensions, which can be misleading or altered.



In this image we can see the file type of this image is **.jpg** which is clearly visible in 3 locations.

2. **Verify File Integrity:** It ensures that the file has not been tampered with or renamed incorrectly. Even if the extension is changed, the file signature remains the same, providing a way to detect any inconsistencies.

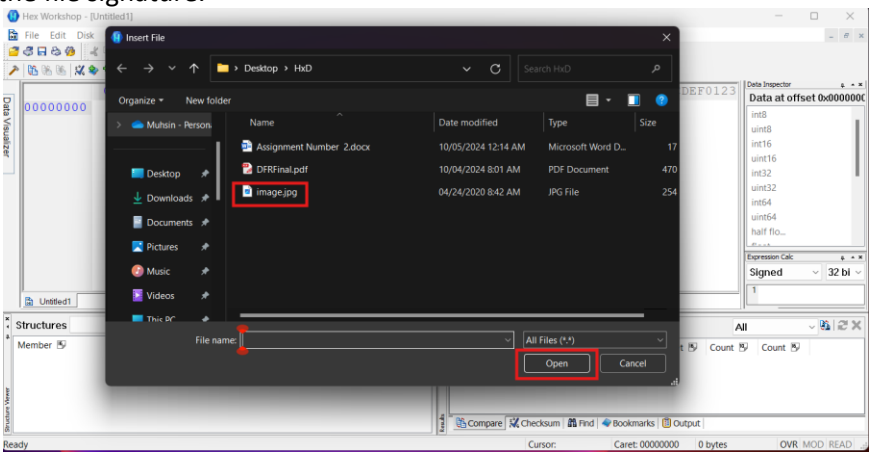


3. **File Recovery:** In forensic investigations, analyzing file signatures helps recover or reconstruct damaged or deleted files. HxD allows users to inspect the raw hex data to recognize the file's type and recover it even if the file system information is lost.

4. **Security and Malware Analysis:** File signature analysis aids in identifying hidden or malicious files. Malware can disguise itself by changing the file extension, but the file signature provides clues for accurate identification during malware investigations.

Investigation Process:

1. **Opening File in HxD:** Load the file in HxD and examine the first few bytes (hexadecimal values) to extract the file signature.



2. **Compare File Signature:** Use known file signature databases to compare the extracted signature with common file formats (e.g., JPEG: FF D8 FF, PDF: 25 50 44 46).

JPE, JPEG, JPG Generic JPEG image file
Trailer: FF D9 (ÿÙ)

NOTES on JPEG file headers: The proper JPEG header is the two-byte sequence, 0xFF-D8, aka *Start of Image (SOI)* marker. JPEG files end with the two-byte sequence, 0xFF-D9, aka *End of Image (EOI)* marker.

Between the SOI and EOI, JPEG files are composed of *segments*. Segments start with a two-byte *Segment Tag* followed by a two-byte *Segment Length* field and then a zero-terminated string identifier (i.e., a character string followed by a 0x00), as shown below with the JFIF, Exif, and SPIFF segments.

Segment Tags of the form 0x-FF-Ex (where x = 0..F) are referred to as APP0-APP15, and contain application-specific information. The most commonly seen APP segments at the beginning of a JPEG file are APP0 and APP1 although others are also seen. Some additional tags are shown below:

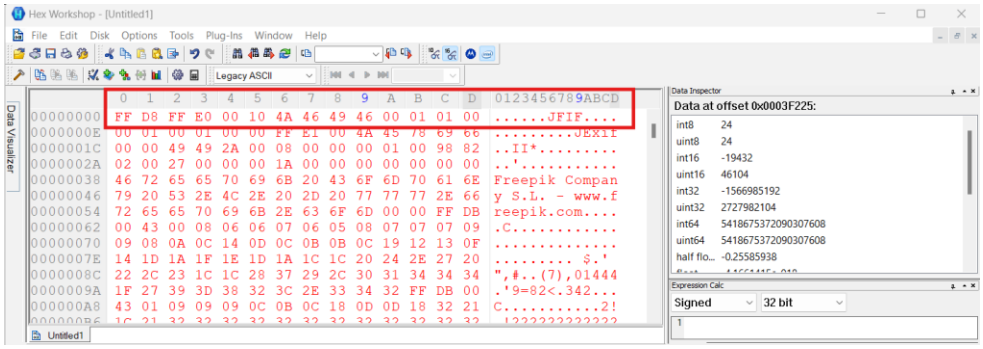
- 0xFF-D8-FF-E0 — Standard JPEG/JFIF file, as shown below.
- 0xFF-D8-FF-E1 — Standard JPEG file with Exif metadata, as shown below.
- 0xFF-D8-FF-E2 — Canon Camera Image File Format (CIFF) JPEG file (formerly used by some EOS and Powershot cameras).
- 0xFF-D8-FF-E8 — Still Picture Interchange File Format (SPIFF), as shown below.

```
FF D8 FF E0 xx xx 4A 46          ÿØÿà..JF
49 46 00                         IF.
```
JFIF, JPE, JPEG, JPG JPEG/JFIF graphics file
Trailer: FF D9 (ÿÙ)

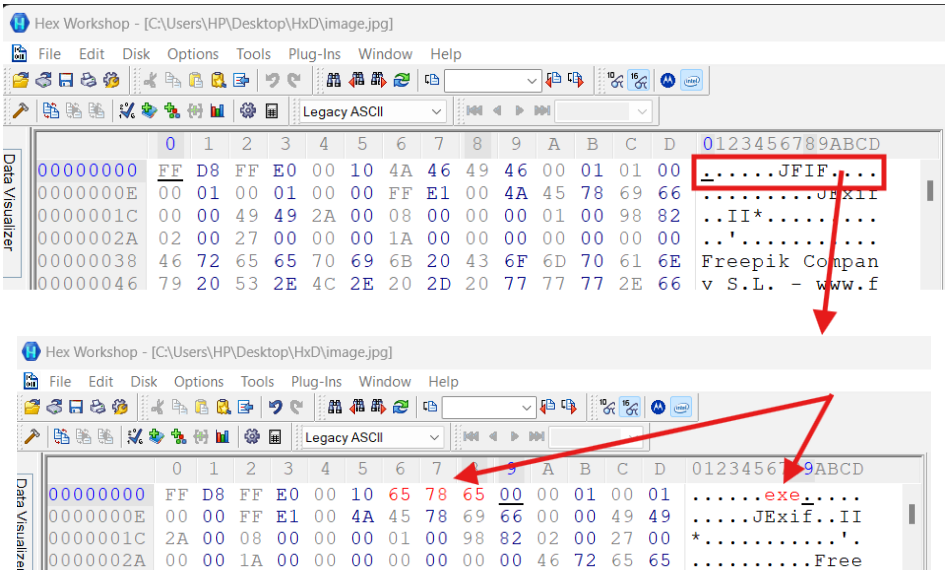
```
FF D8 FF E1 xx xx 45 78          ÿØÿá..Ex
69 66 00                         if.
```
JPG Digital camera JPG using Exchangeable Image File Format (EXIF)
Trailer: FF D9 (ÿÙ)
See "Using Extended File Information (EXIF) File Headers in Digital Evidence Analysis" (P. Alvarez, *IJDE*, *2*(3), Winter 2004) and ExifTool Tag Names

```
FF D8 FF E8 xx xx 53 50          ÿØÿè..SP
49 46 46 00                      IFF.
```
JPG Still Picture Interchange File Format (SPIFF)
Trailer: FF D9 (ÿÙ)

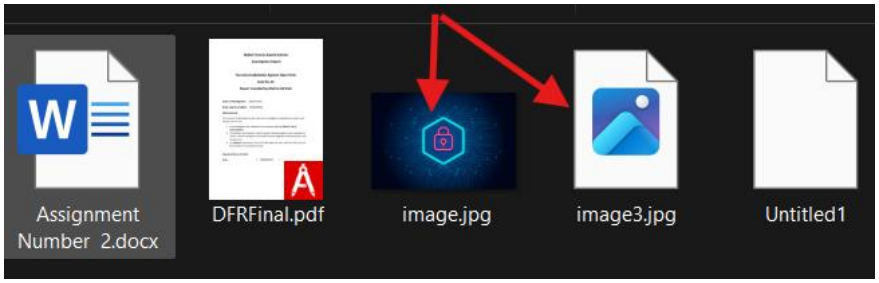
3. **Check Consistency with Extension:** Verify if the file's signature matches its extension. If not, this could indicate a mislabelled or potentially malicious file.



6. Visualizing Changes:
If we change the signatures of any image just as like this :



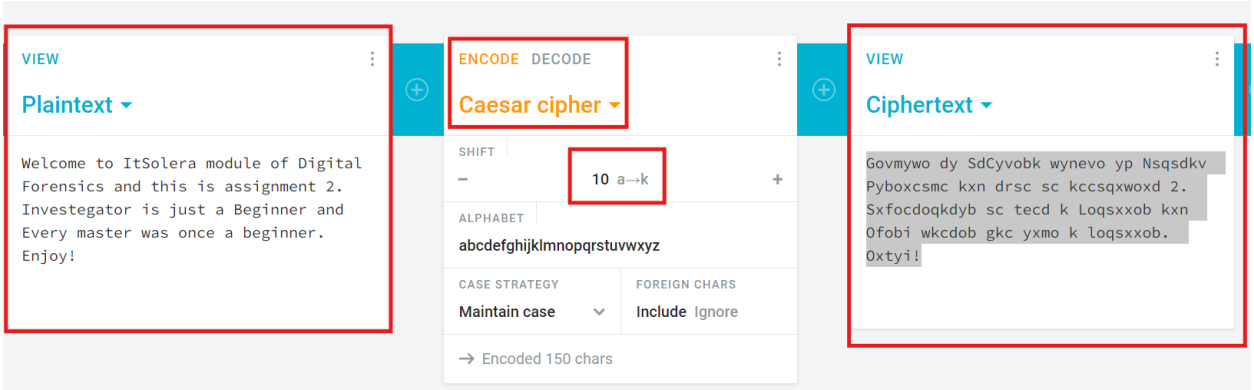
Now we can clearly see the changes in signature of the extension we changed from jfif to exe
And if we save it the file will be showed as with exe extension.



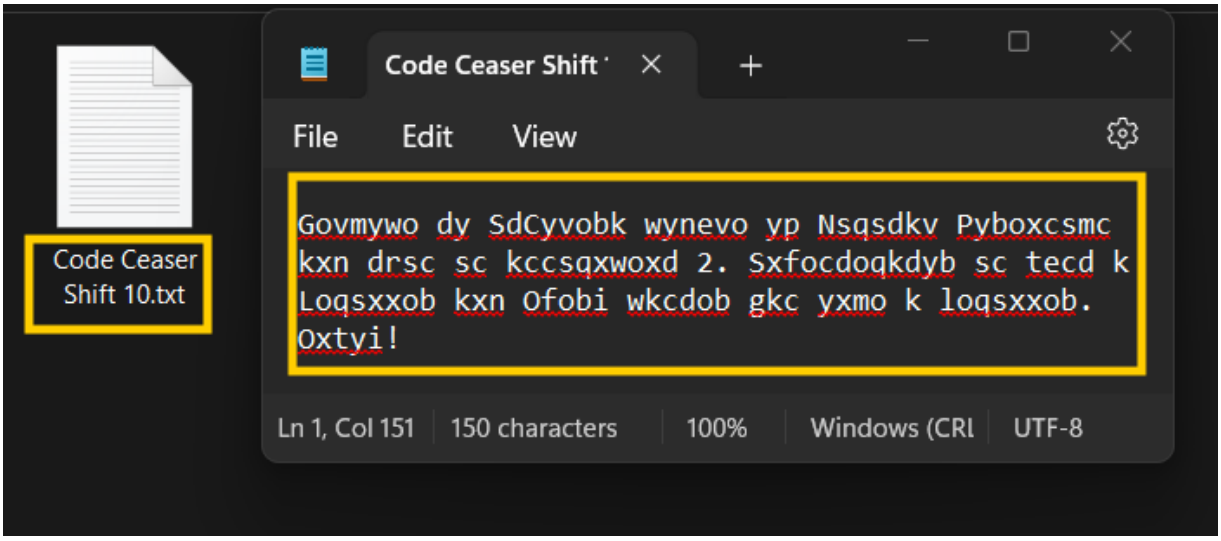
So, in this image it shows clearly how we changed its signature value and now is unable for preview.
Its extension is still the same but not available more if we have such files extension we can recover them by knowing their type of signature value and changing it. We can Encrypt/Decrypt file in this way.

Practicle Example of Encrypting Files through HxD and decrypting Back

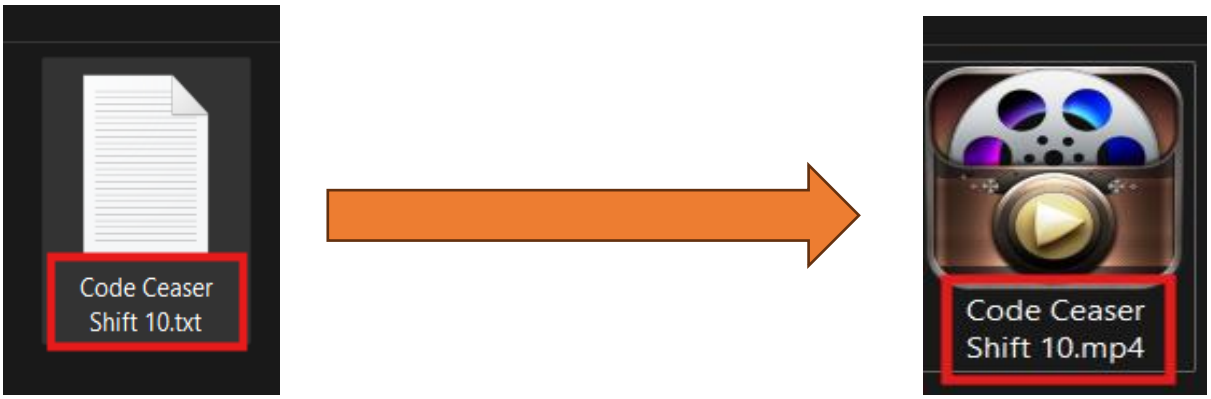
For Example, we have a document File remember its extension and the shifted creaser message in it. Create a file and save ceaser cifier decode text in it as below method ;



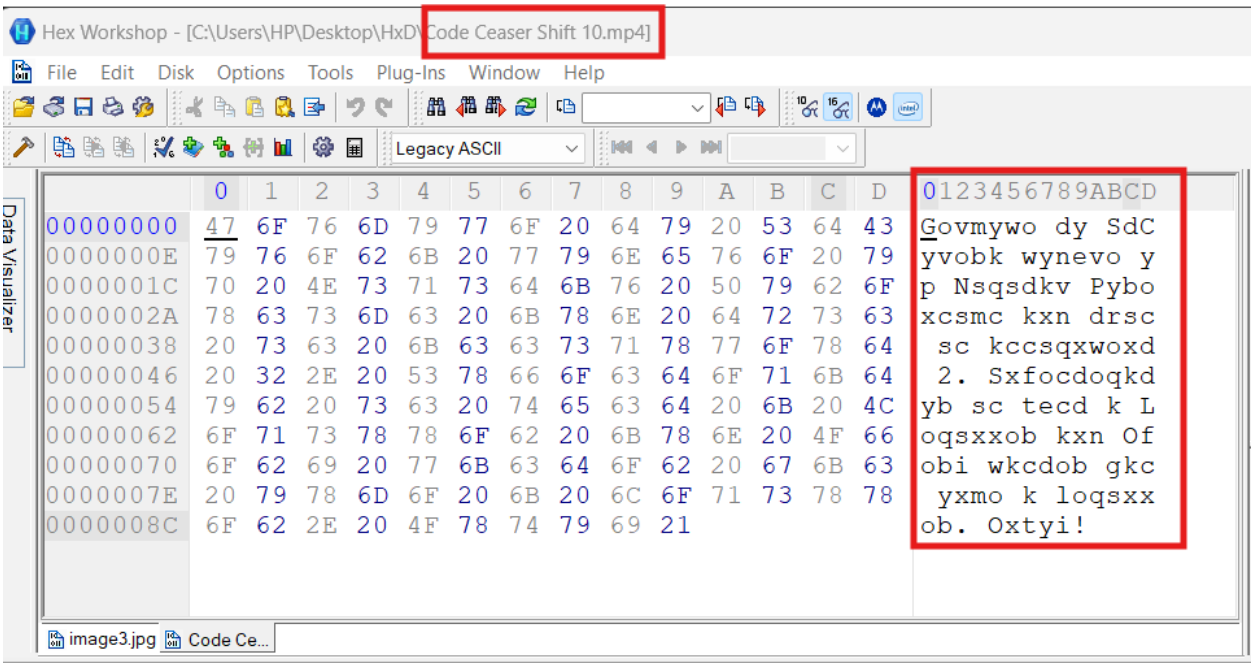
We have written plain text and copied the Cipher into text file as shown in below image: and save the file.



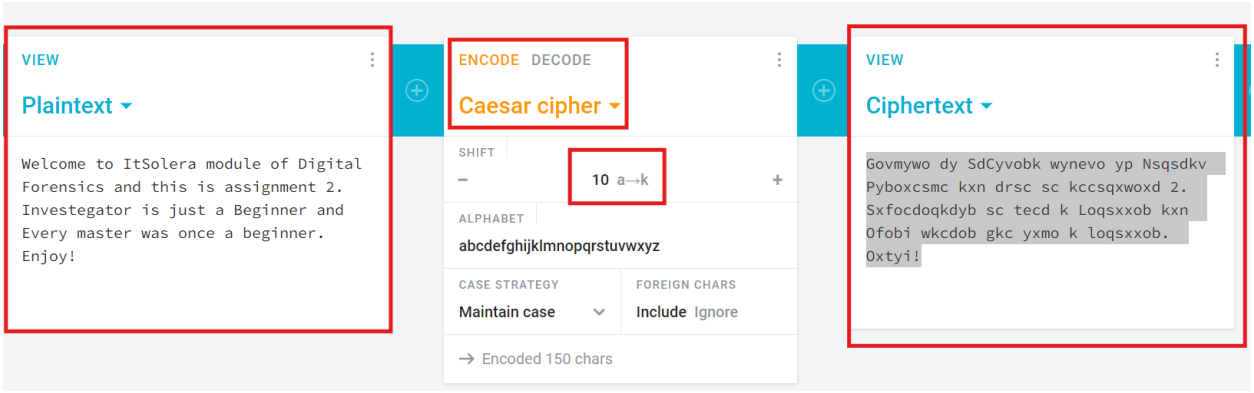
Now change the file extension from original to any other as shown in image:



As you can see, we have changed the file extension from text to mp4 and now the computer thinks its not a notepad file but it's a video file that's how we have tempered the extension type.
In this way the scripts are evolved after we click them it flashes our data and spreads **viruses** this is just a simple method how to ***temper with signature and extensions***, we can *encrypt decrypt* and make **exploits** in a such away for victims too. Now open that file in HxD and visualize it.



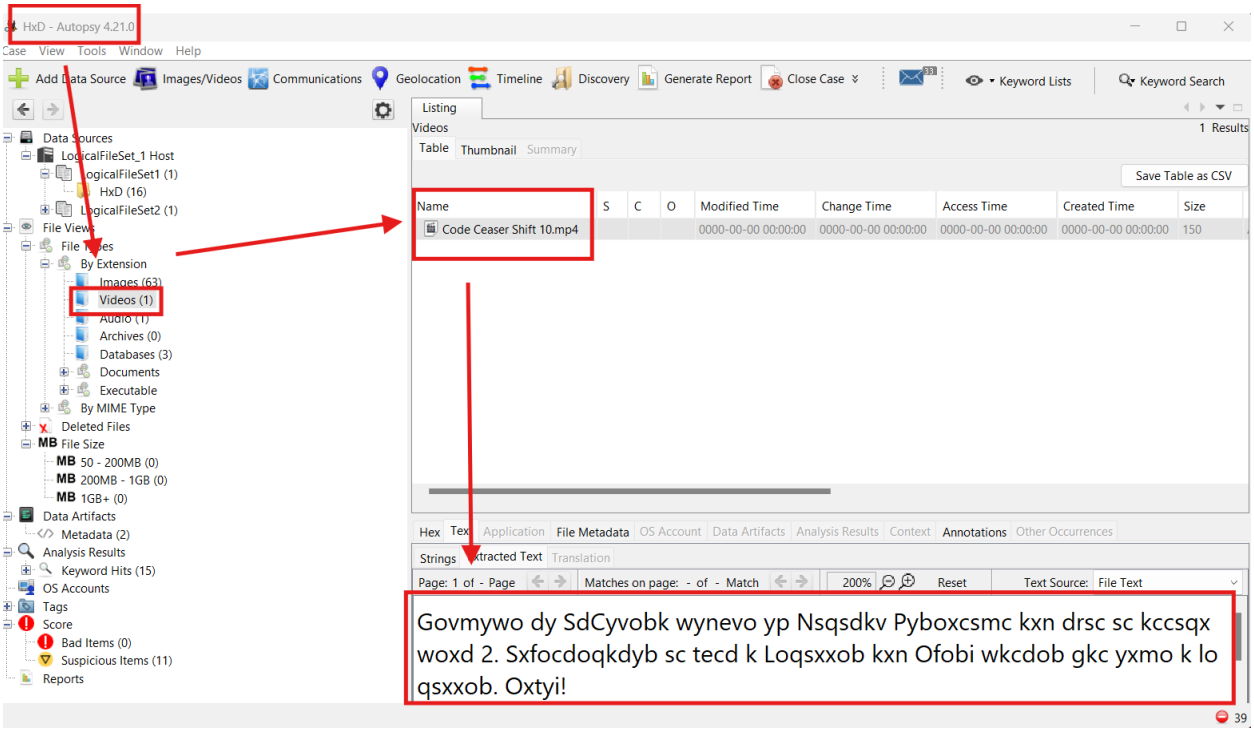
Its clear we can see the file type and our code that was injected before tempering Filetype Extension, Secondly, we don't have any signature in display as coz text files don't support it by default. In Reality nothing is tempered just we needed the secret message to decode it back to we can copy it and through cypher we can see the code back. As it's a text file text files don't owns Signatures.



Second Method of Evidence Looking using Autopsy:

Open your file in autopsy which is tempered of extension has changed we can see what it has as below.

This file we opened clearly shows us what our temple file is consisting of.



Conclusion:

In today Digital Forensics and Incident Response (DFIR), We used HxD and Autopsy for file extension and signatures as it serves as a vital tool for analyzing file signatures and extensions by allowing the inspection of a file's raw binary data. By examining file headers and signatures in hex format, forensic investigators can confirm file types, detect manipulation, or uncover hidden data, regardless of misleading extensions.