Date- 16/09/2023

Roll No. - 13

Expt. No. - 7

K.M.S.P. Mandal’s

Sant Rawool Maharaj Mahavidyalaya, Kudal

**Department of Computer Science**

Signature

Detect hidden information or files within digital images using steganography analysis tools.

Title - \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Steganography:**

Steganography is the practice of concealing one piece of information within another to hide the existence of the hidden information. Unlike cryptography, which focuses on making the content of a message secret, steganography aims to hide the fact that a message or communication is taking place. The goal is to embed the hidden information in such a way that it is difficult to detect.

In digital steganography, the most common form, information is concealed within digital files like images, audio files, video files, or even text files. Here are some common techniques used in digital steganography:

**1. Image Steganography**: Concealing data within the pixels of an image without significantly altering its appearance.

**2. Audio Steganography:** Embedding data within audio files by slightly modifying the audio waveform.

**3. Video Steganography:** Hiding information within video files by manipulating certain frames or elements.

**4. Text Steganography:** Concealing information within a text document by, for example, using invisible characters or modifying the spacing between words.

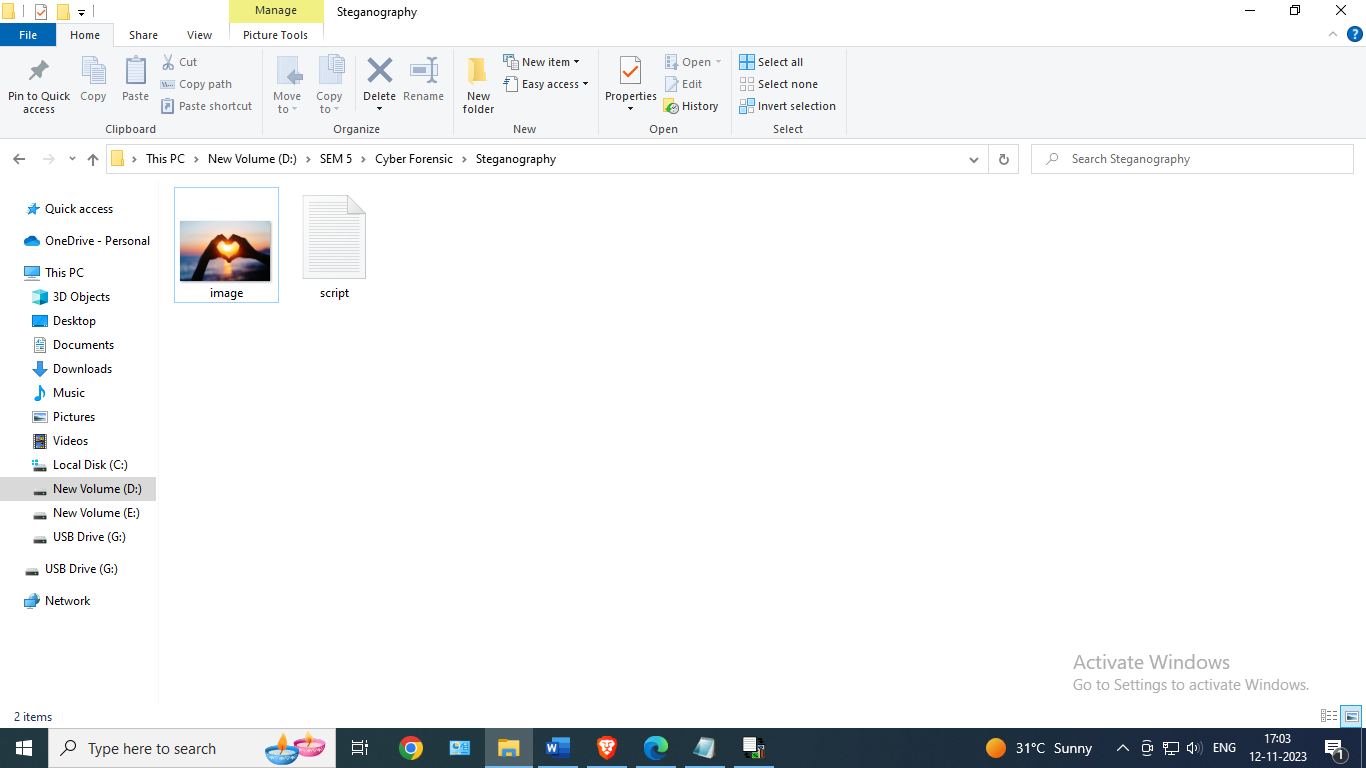
**5. File Steganography:** Embedding data within other types of files, such as documents or executables.

Steganography is often used for legitimate purposes, such as digital watermarking to protect intellectual property or embedding metadata in images. However, it can also be used for malicious activities, such as hiding malware or facilitating covert communication in cyber attacks.

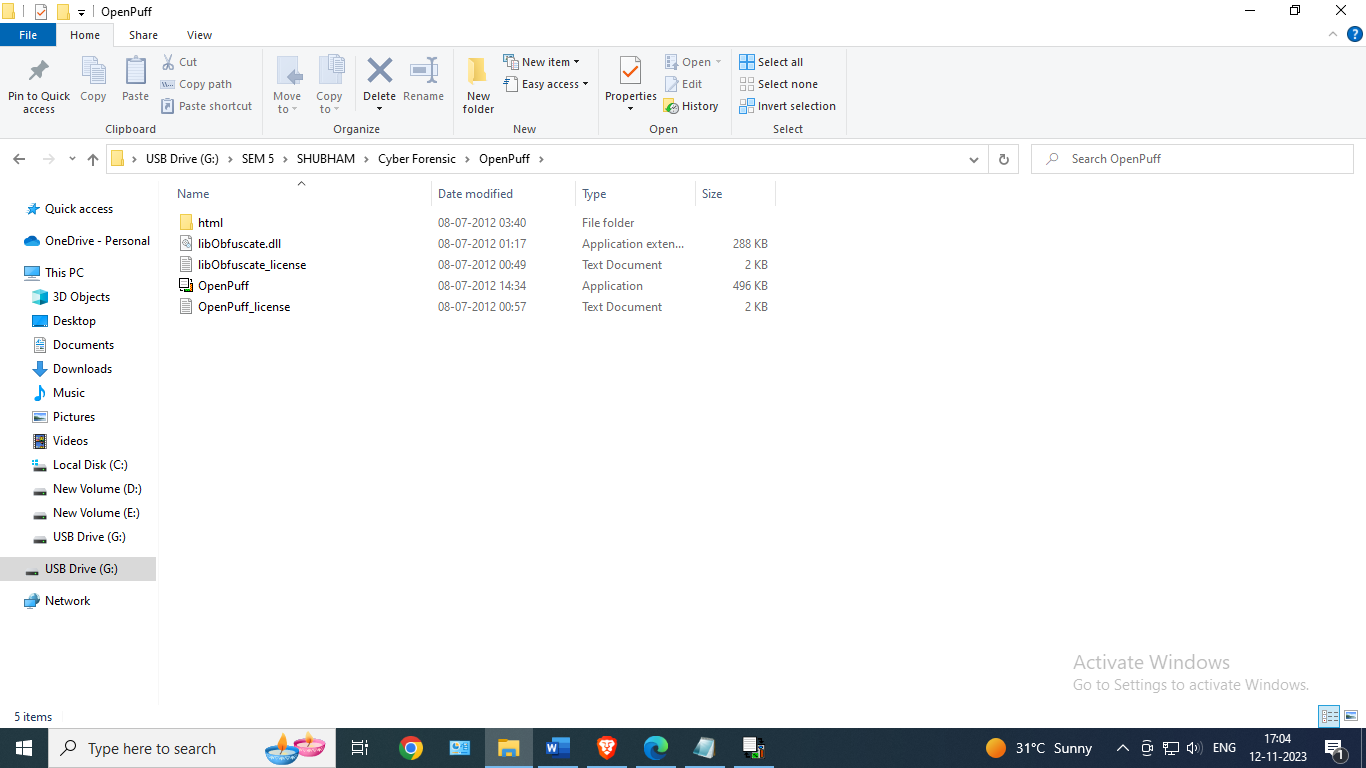
Detecting steganography can be challenging, as the alterations made to the carrier file are often subtle and designed to be undetectable to the human eye or ear. Specialized tools and techniques are used in digital forensics to identify and analyze potential instances of steganography.

**Method 1**

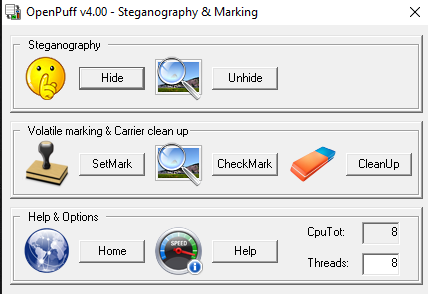
**Create a folder and with one image and script file:**

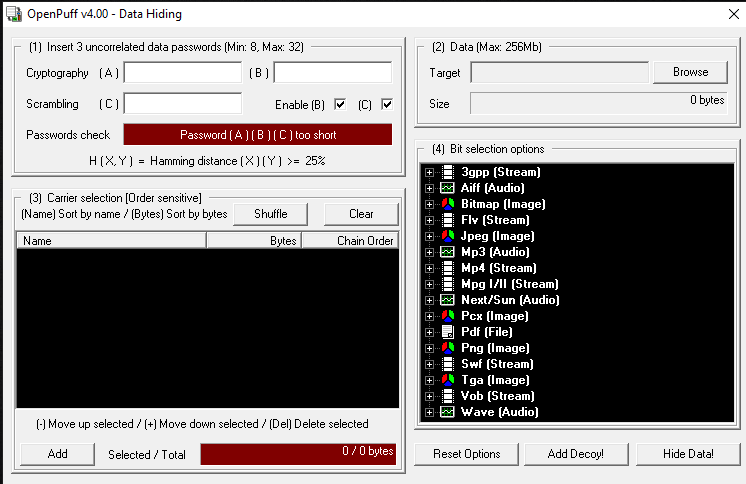


**Open OpenPuff Software:**

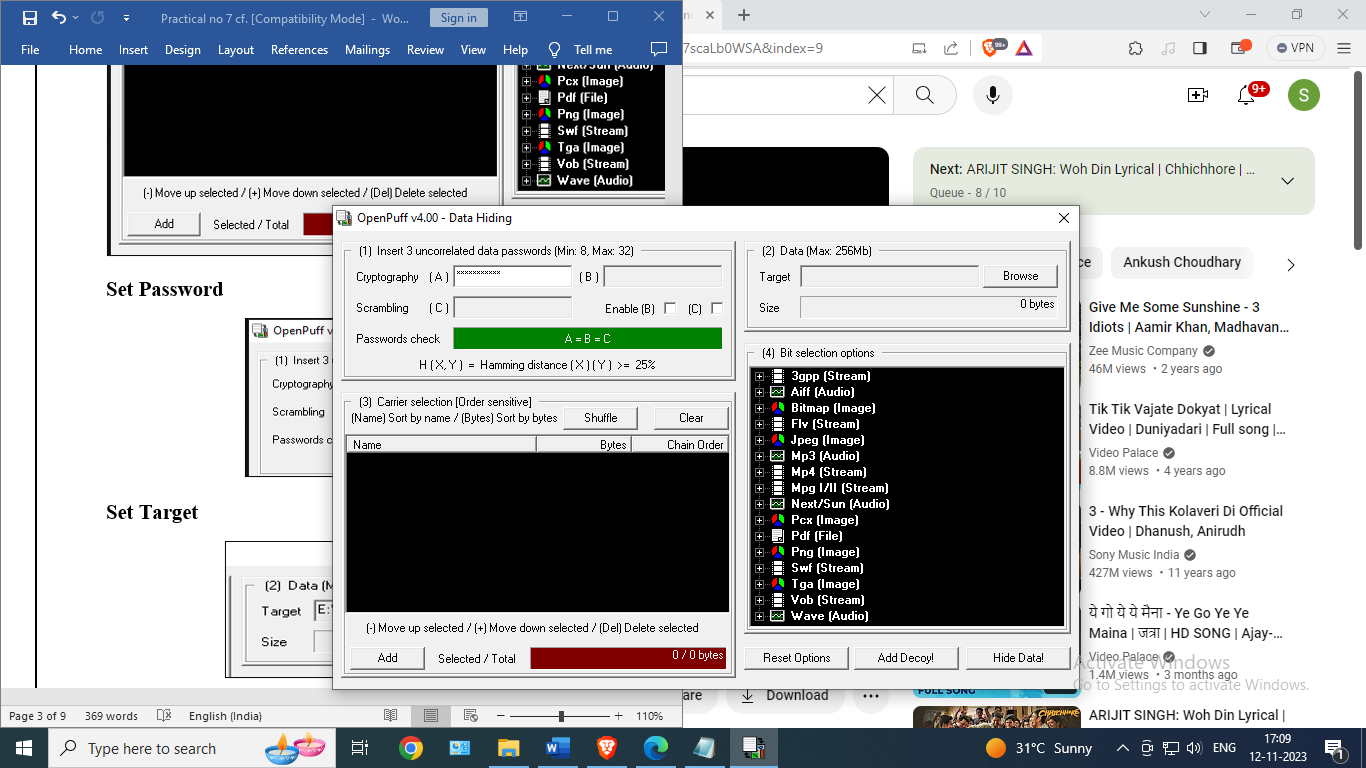


**Choose Hide:**

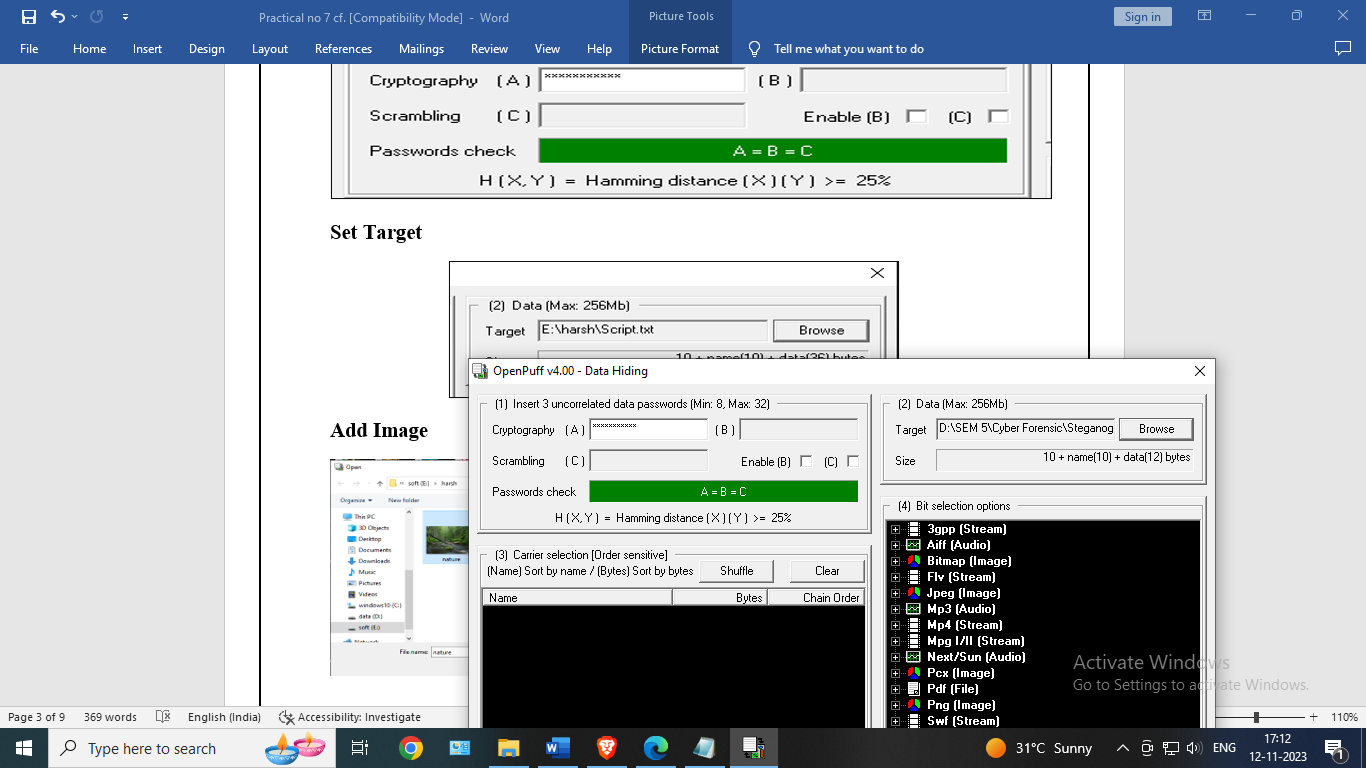
****

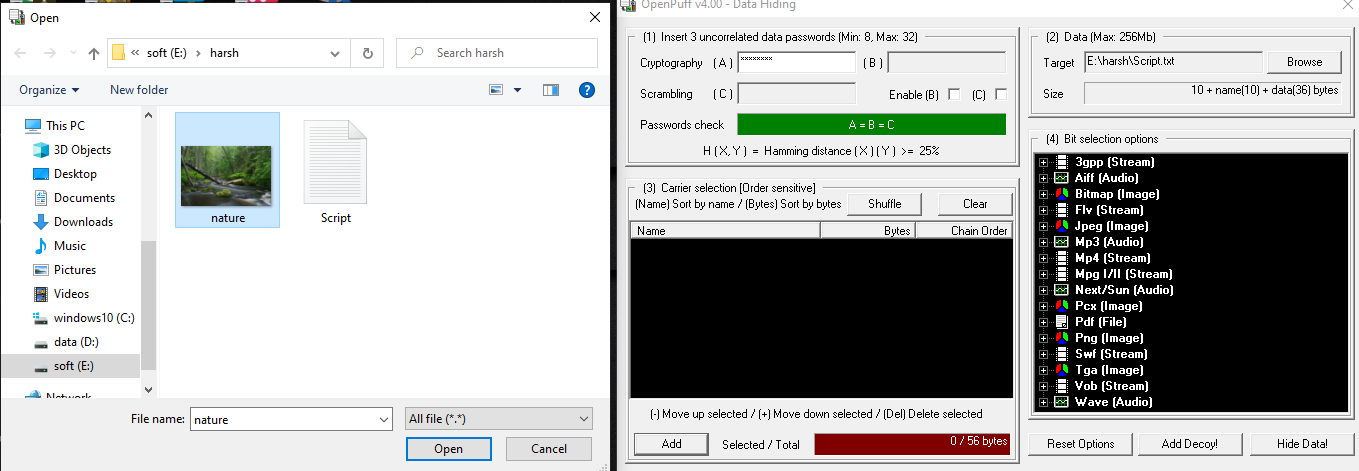
**Data Hiding**

**Set Password:**

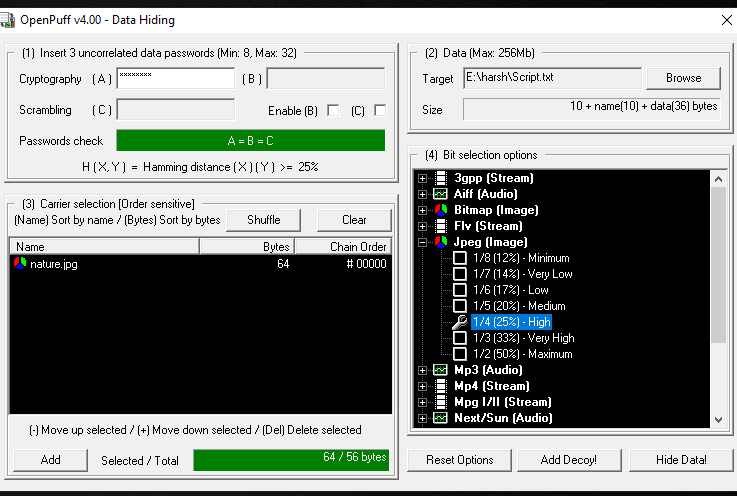


**Set Target:**

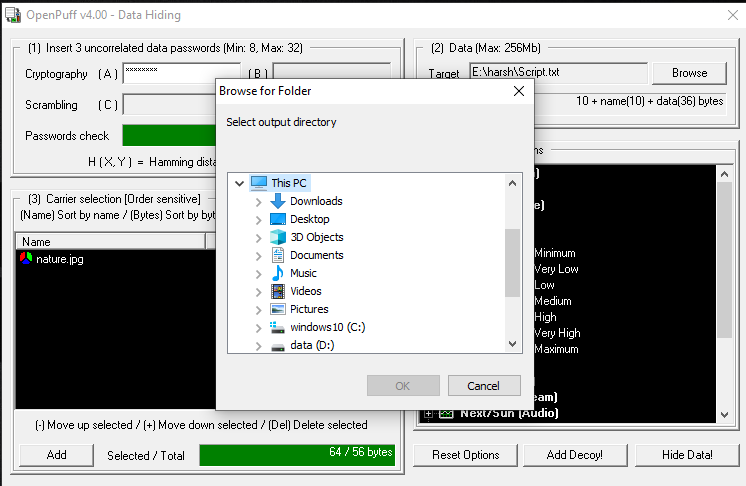
**Add Image**



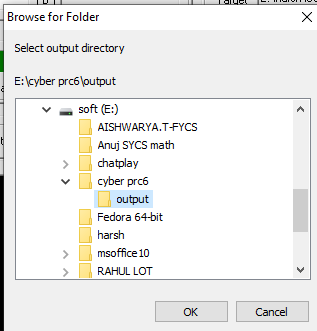
**Data hiding**



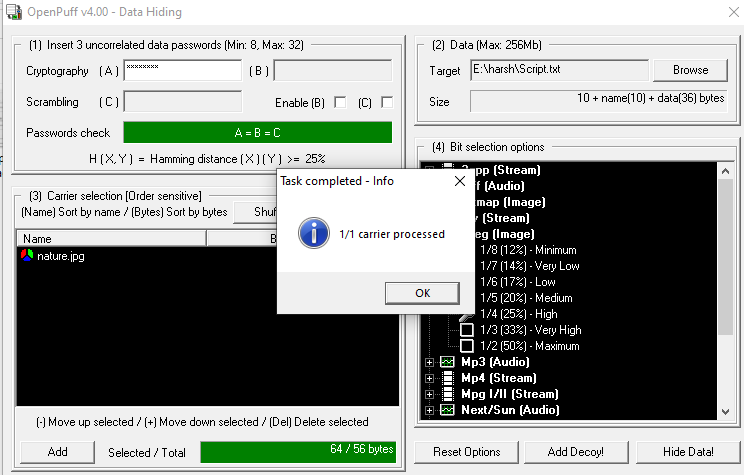
**Select Output directory**

****

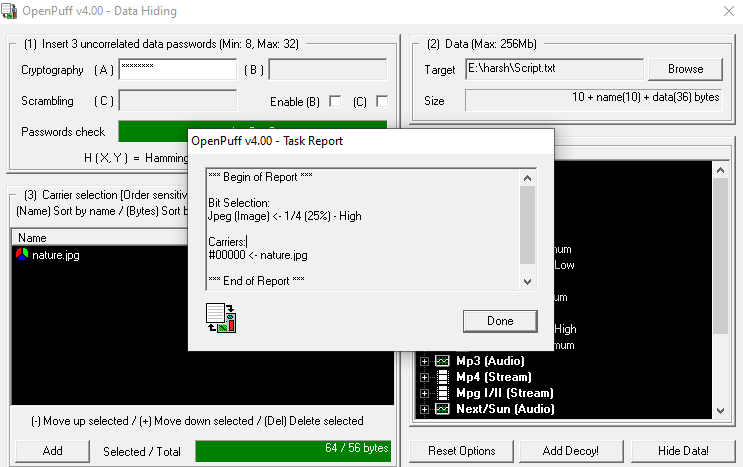
**Choose Folder**

****

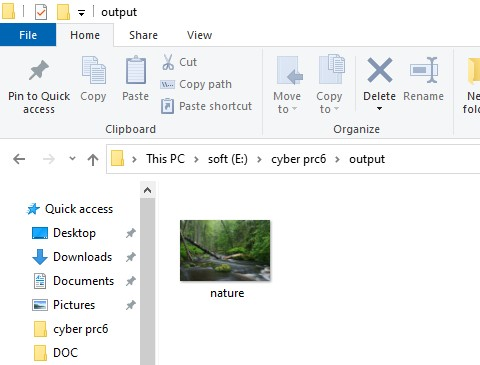
**Data Hiding process**

****

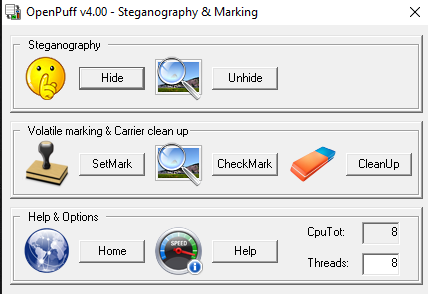
**Task Report**

****

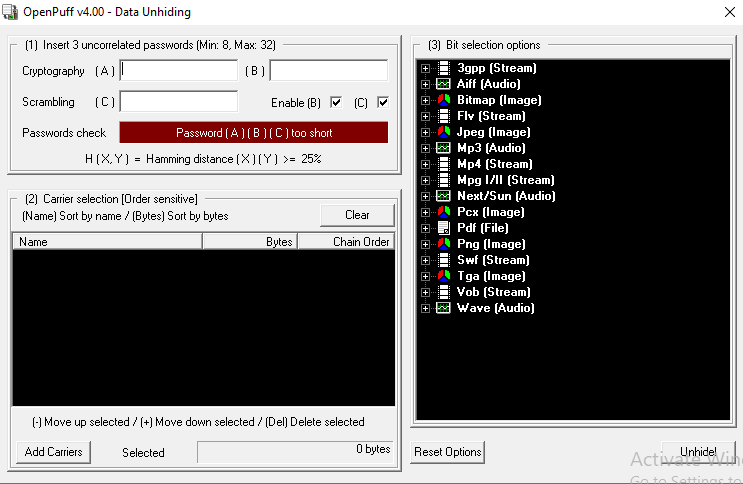
**Output**



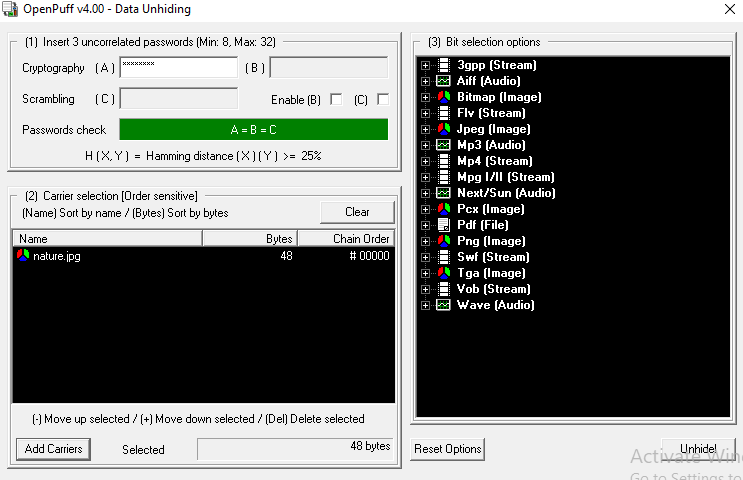
**Unhide Process – Choose Unhide**



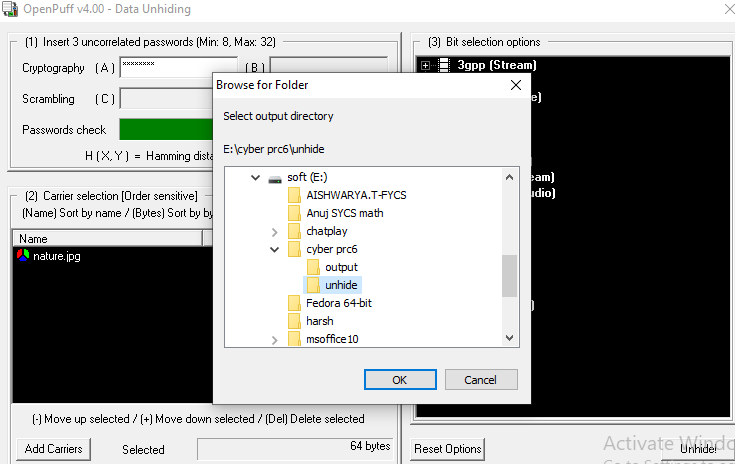
**Data Unhiding**



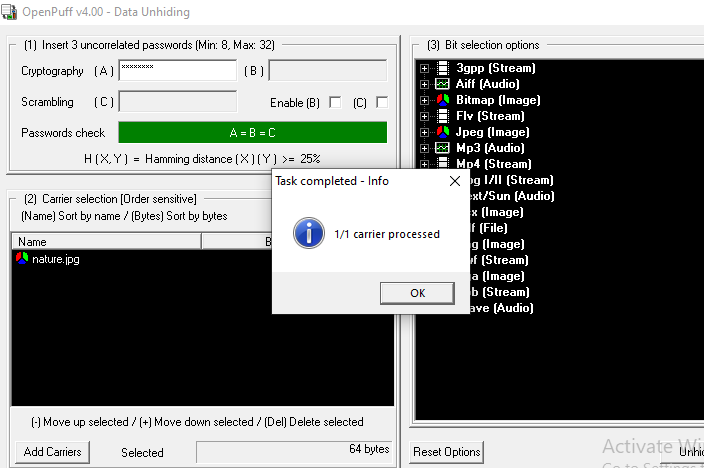
**Set Password and Add Carrier**



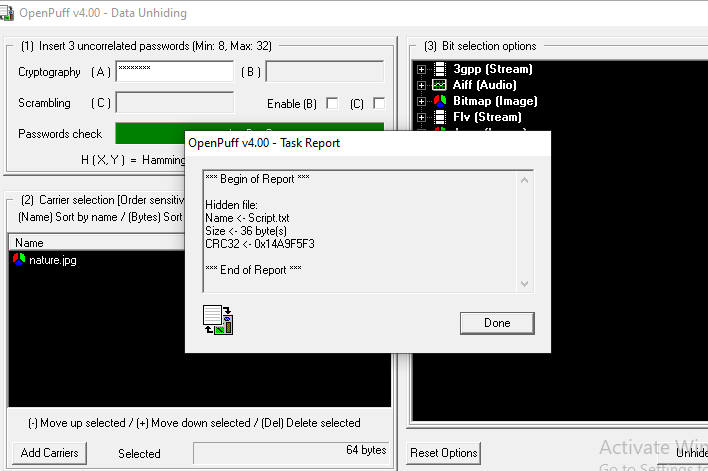
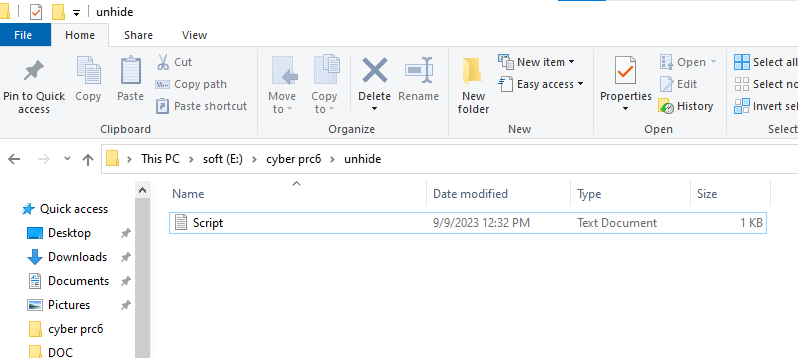
**Choose Output directory For Unhide**



**Data Unhide**

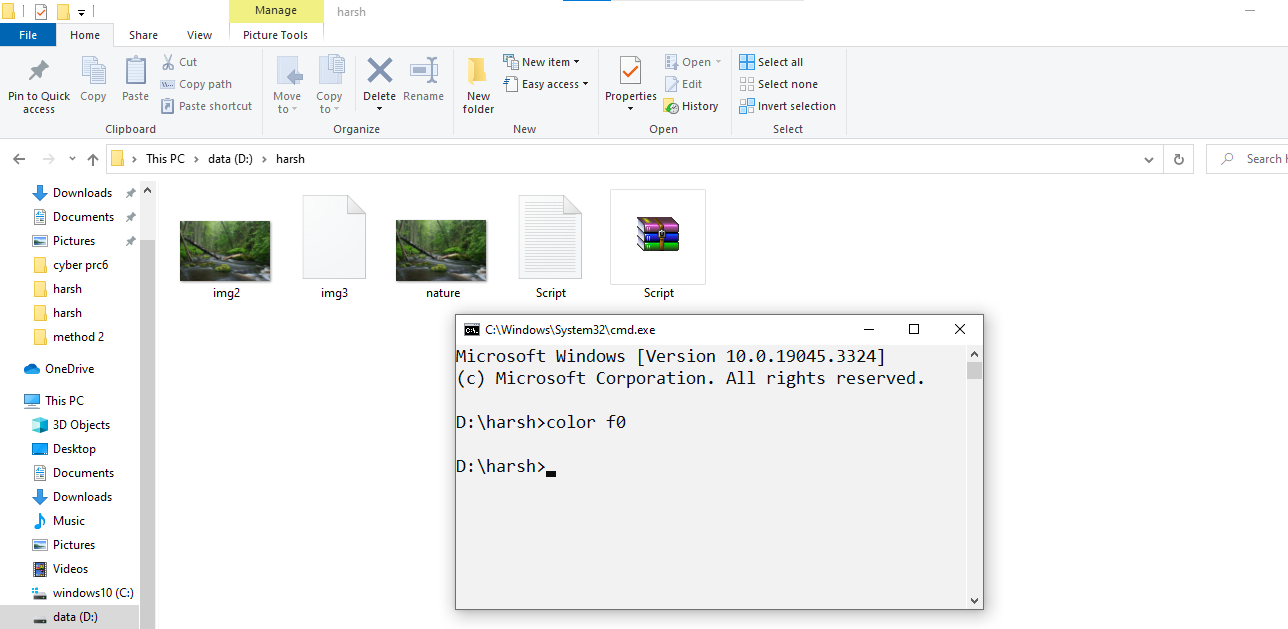


**Summary**

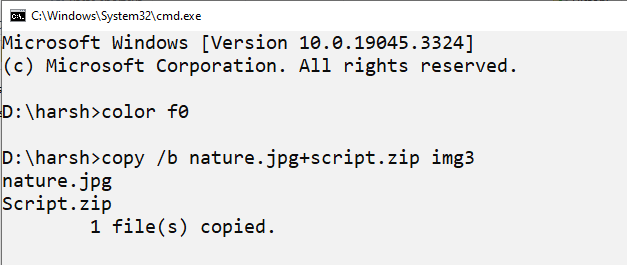
 

**Method 2**

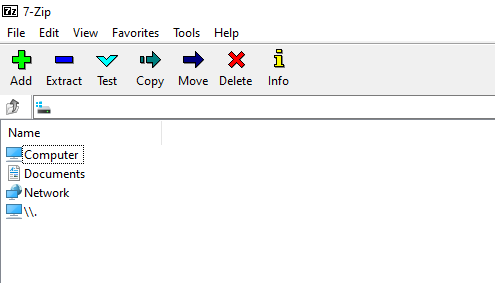
**Open CMD**



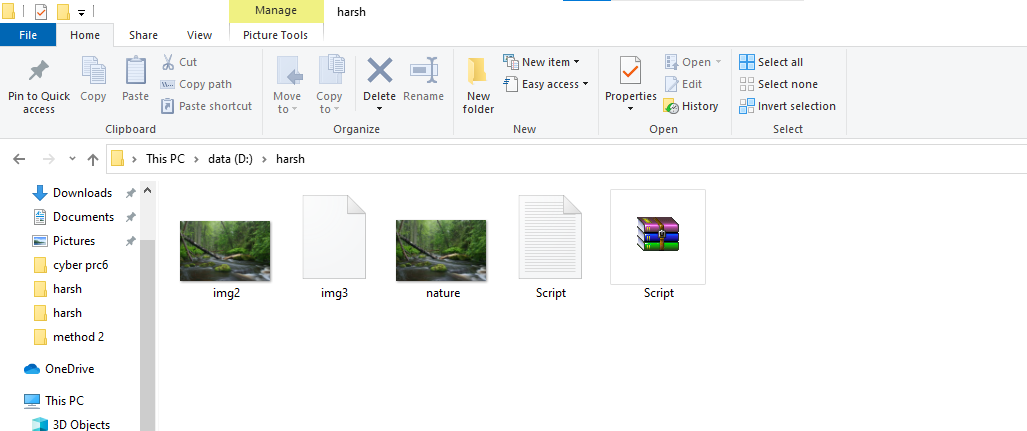
**Type Command**

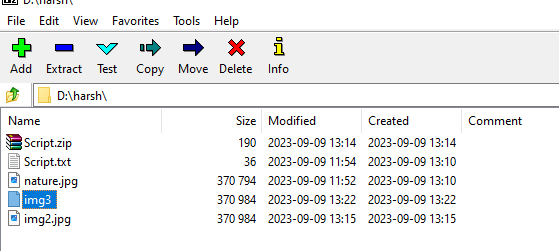


**Open 7-zip**



**Img 3 created**





**Open Img3**

