Date- 16/09/2023

Roll No. - 25

Expt. No. - 7

K.M.S.P. Mandal’s

Sant Rawool Maharaj Mavidyalaya, Kudal

**Department of Computer Science**

Signature

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

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

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

Steganography is the practice of concealing information within another message or physical object to avoid detection. Steganography can be used to hide virtually any type of digital content, including text, image, video, or audio content. That hidden data is then extracted at its destination.

Content concealed through steganography is sometimes [encrypted](https://www.kaspersky.com/resource-center/definitions/encryption) before being hidden within another file format. If it isn’t encrypted, then it may be processed in some way to make it harder to detect.

As a form of covert communication, steganography is sometimes compared to [cryptography](https://www.kaspersky.com/resource-center/definitions/what-is-cryptography). However, the two are not the same since steganography does not involve scrambling data upon sending or using a key to decode it upon receipt.

The term ‘steganography’ comes from the Greek words ‘steganos’ (which means hidden or covered) and ‘graphein’ (which means writing). Steganography has been practiced in various forms for thousands of years to keep communications private. For example, in ancient Greece, people would carve messages on wood and then use wax to conceal them. Romans used various forms of invisible inks, which could be deciphered when heat or light were applied.

Steganography is relevant to cybersecurity because [ransomware](https://www.kaspersky.com/resource-center/threats/ransomware) gangs and other threat actors often hide information when attacking a target. For example, they might hide data, conceal a malicious tool, or send instructions for command-and-control servers. They could place all this information within innocuous-seeming image, video, sound, or text files.

## How steganography works

Steganography works by concealing information in a way that avoids suspicion. One of the most prevalent techniques is called ‘least significant bit’ (LSB) steganography. This involves embedding the secret information in the least significant bits of a media file. For example:

* In an image file, each pixel is made up of three bytes of data corresponding to the colors red, green, and blue. Some image formats allocate an additional fourth byte to transparency, or ‘alpha’.
* LSB steganography alters the last bit of each of those bytes to hide one bit of data. So, to hide one megabyte of data using this method, you would need an eight-megabyte image file.
* Modifying the last bit of the pixel value doesn’t result in a visually perceptible change to the picture, which means that anyone viewing the original and the steganographically-modified images won’t be able to tell the difference.

The same method can be applied to other digital media, such as audio and video, where data is hidden in parts of the file that result in the least change to the audible or visual output.

Another steganography technique is the use of word or letter substitution. This is where the sender of a secret message conceals the text by distributing it inside a much larger text, placing the words at specific intervals. While this substitution method is easy to use, it may also make the text look strange and out of place since the secret words might not fit logically within their target sentences.

Other steganography methods include hiding an entire partition on a hard drive or embedding data in the header section of files and network packets. The effectiveness of these methods depends on how much data they can hide and how easy they are to detect.

## Types of steganography

From a digital perspective, there are five main types of steganography. These are:

1. Text steganography
2. Image steganography
3. Video steganography
4. Audio steganography
5. Network steganography

Let’s look at each of these in more detail:

### Text steganography

Text steganography involves hiding information inside text files. This includes changing the format of existing text, changing words within a text, using context-free grammars to generate readable texts, or generating random character sequences.

### Image steganography

This involves hiding information within image files.  In digital steganography, images are often used to conceal information because there are a large number of elements within the digital representation of an image, and there are various ways to hide information inside an image.

### Audio steganography

Audio steganography involves secret messages being embedded into an audio signal which alters the binary sequence of the corresponding audio file. Hiding secret messages in digital sound is a more difficult process compared to others.

### Video steganography

This is where data is concealed within digital video formats. Video steganography allows large amounts of data to be hidden within a moving stream of images and sounds. Two types of video steganography are:

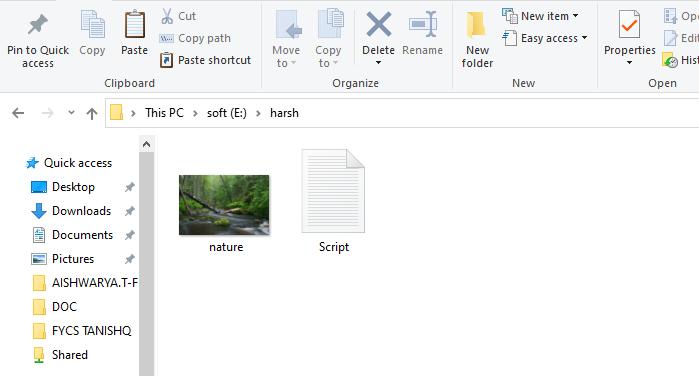
* Embedding data in uncompressed raw video and then compressing it later
* Embedding data directly into the compressed data stream

### Network steganography

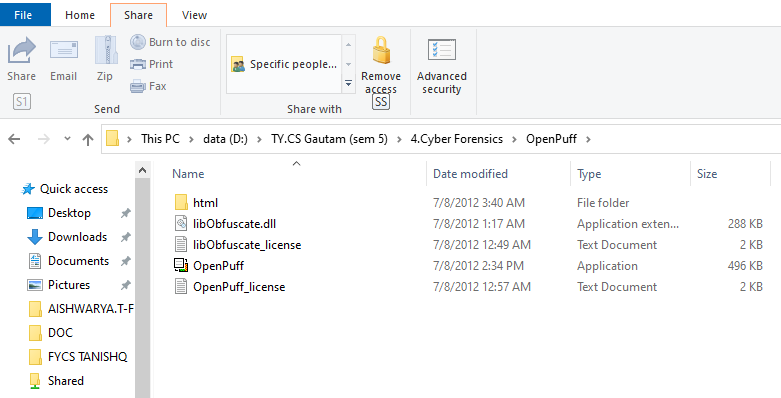
Network steganography, sometimes known as protocol steganography, is the technique of embedding information within network control protocols used in data transmission such TCP, UDP, ICMP, etc.

**Method 1**

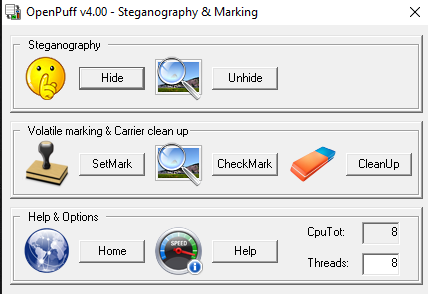
**Create a folder and with one image and script file**

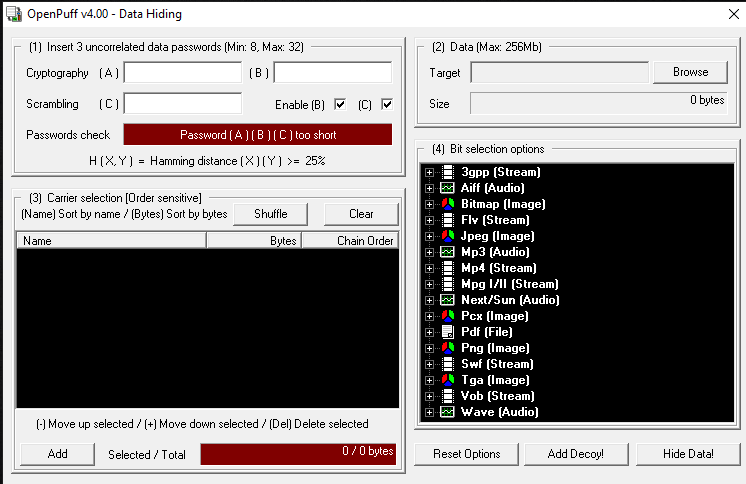
****

**Open OpenPuff Software**

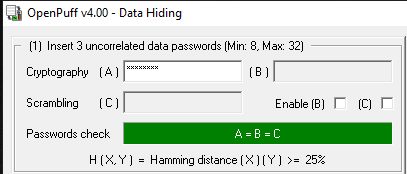
****

**Choose Hide**

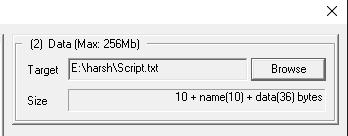
****

**Data Hiding**

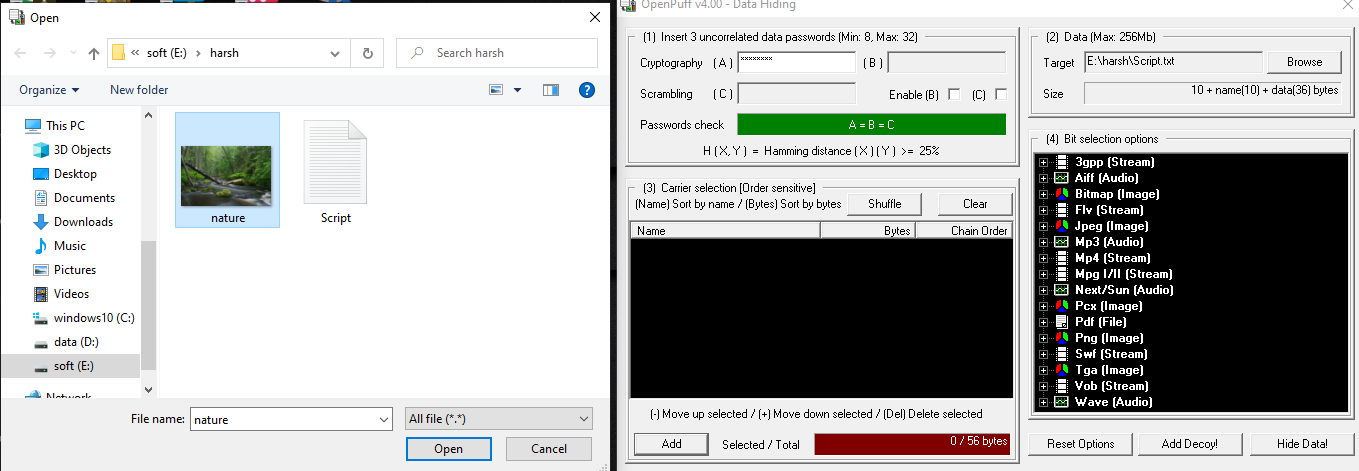
**Set Password**



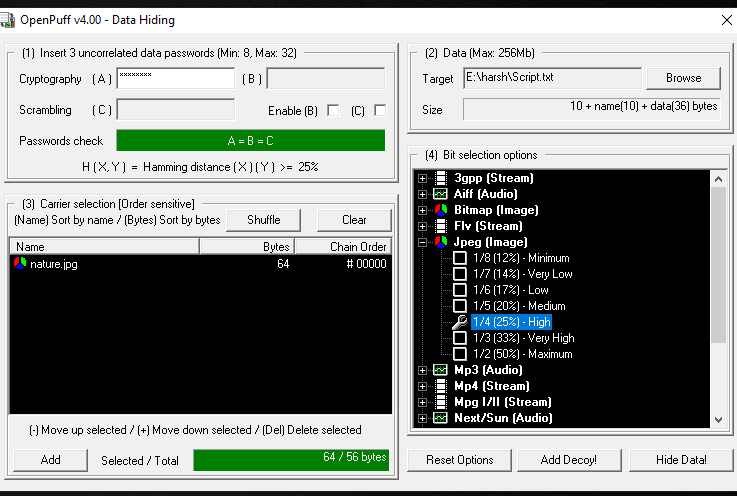
**Set Target**



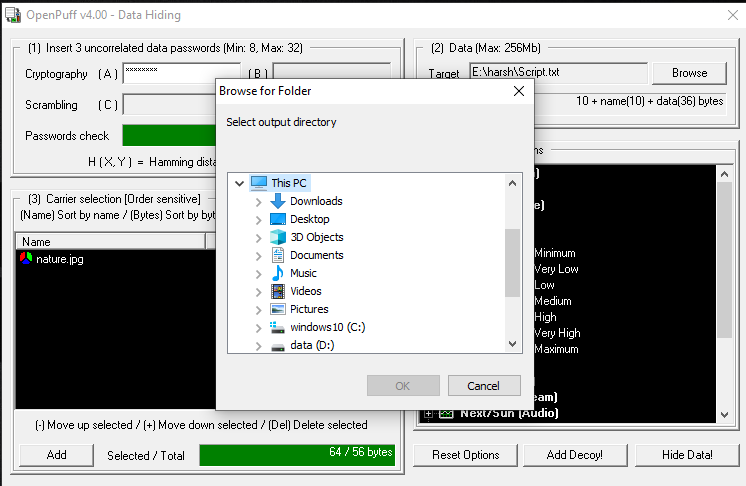
**Add Image**



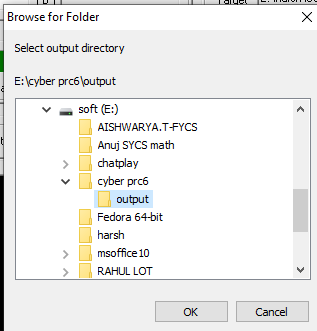
**Data hiding**



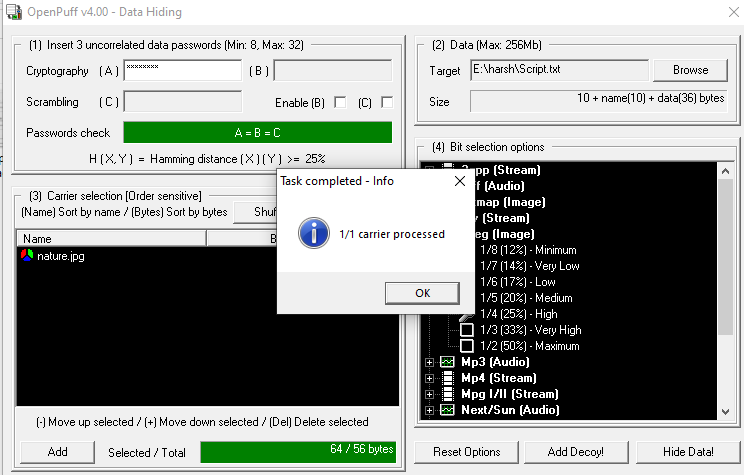
**Select Output directory**

****

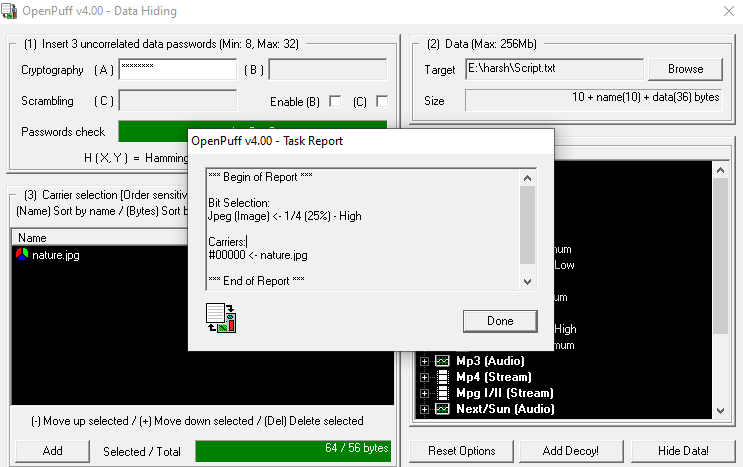
**Choose Folder**

****

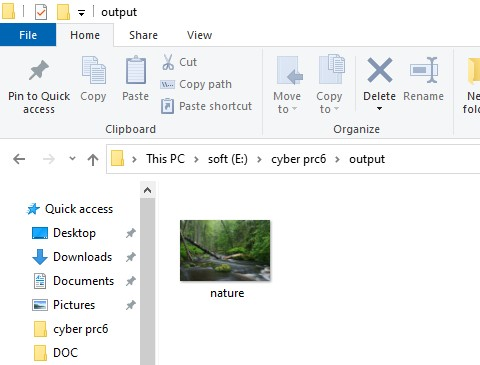
**Data Hiding process**

****

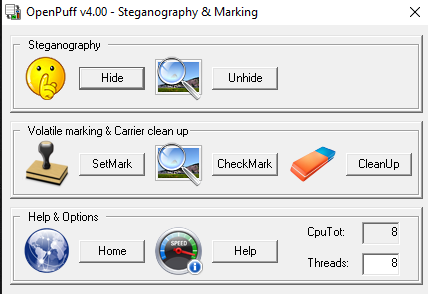
**Task Report**

****

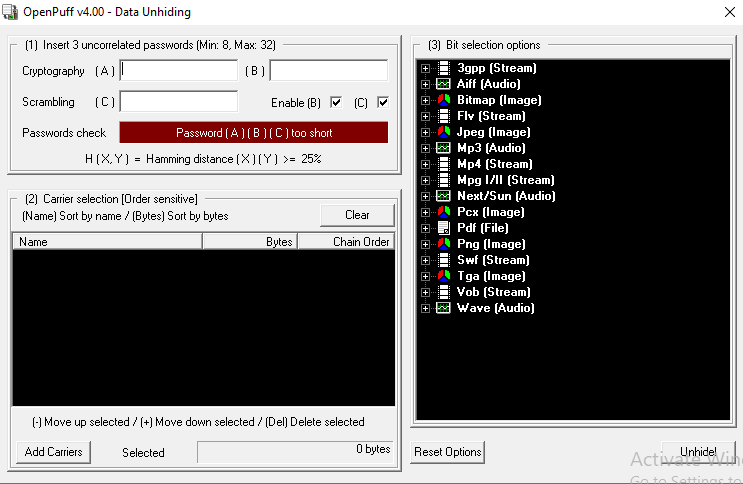
**Output**



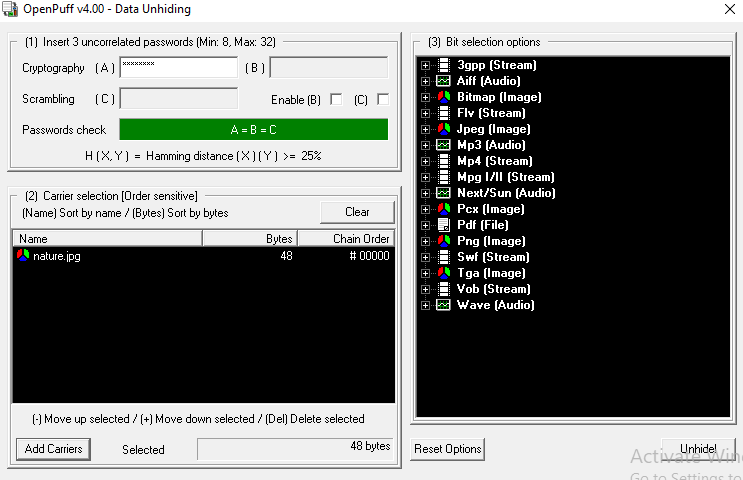
**Unhide Process – Choose Unhide**



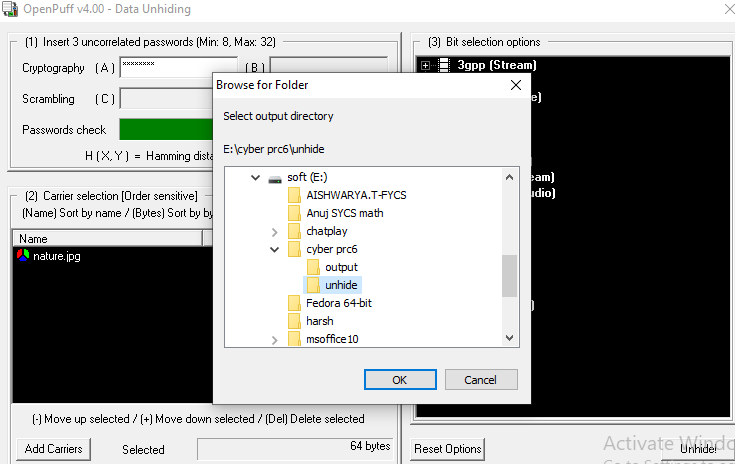
**Data Unhiding**



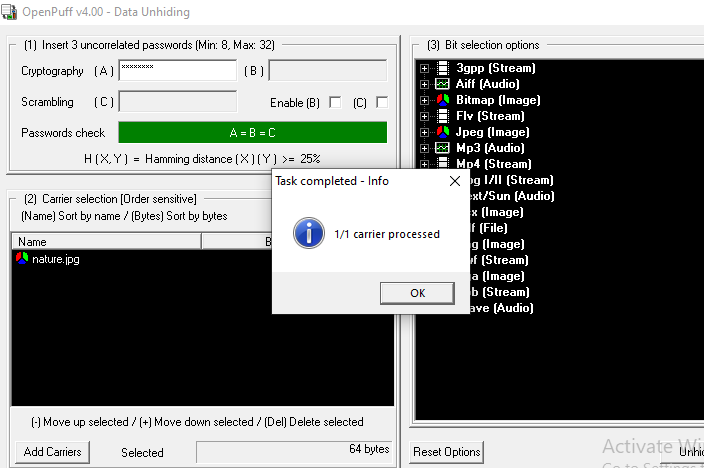
**Set Password and Add Carrier**



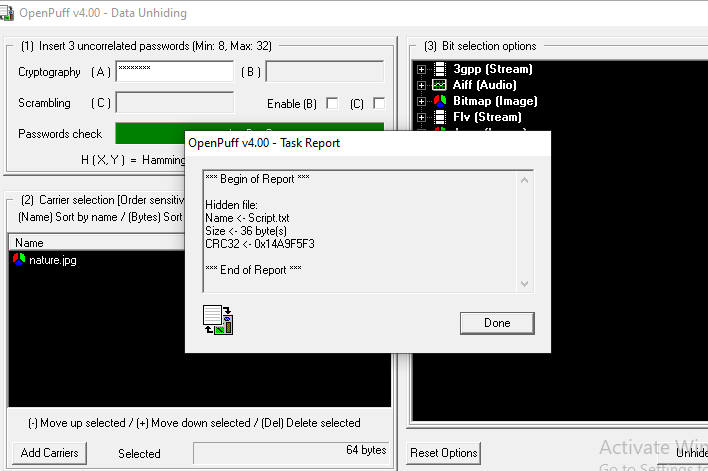
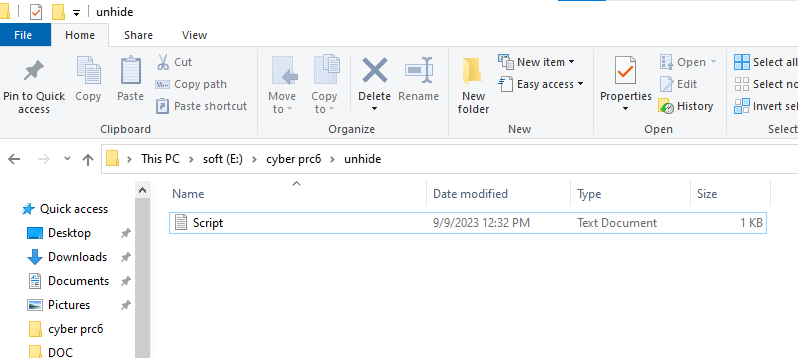
**Choose Output directory For Unhide**



**Data Unhide**

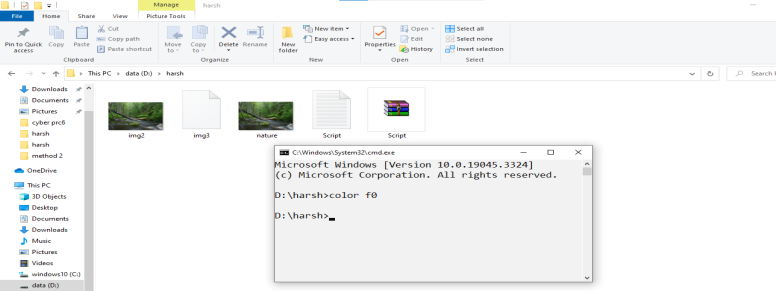


**Summary**

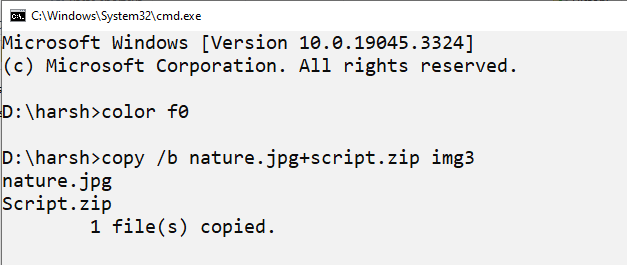
 

**Method 2**

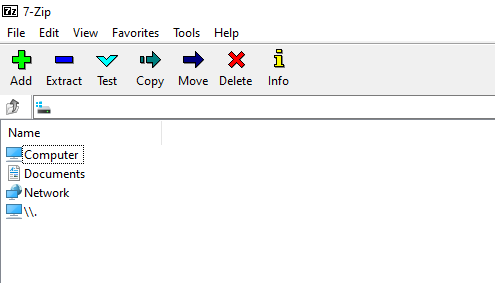
**Open CMD**



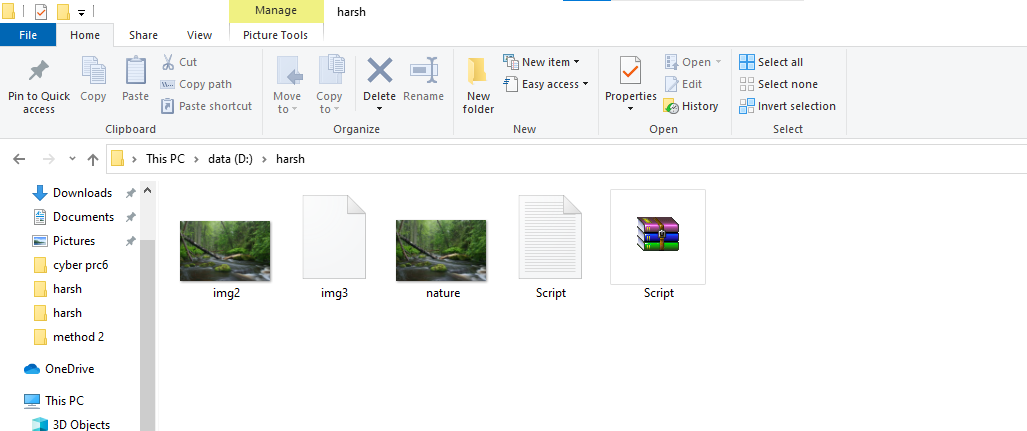
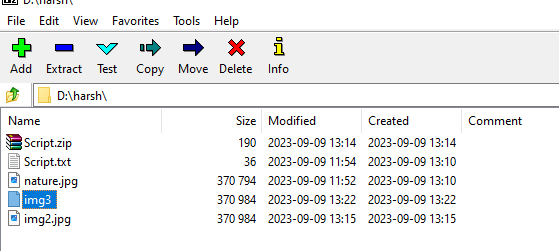
**Type Command**



**Open 7-zip**



**Img 3 created**



**Open Img3**

