# Digital Forensics Assignment

**Assignment: 01**
**Submission Day: Monday**
**Instructor: Sir Sohaib**
**Submission By Muhsin Ali Shah**

## Practical Exploration of Steganography with OpenStego:

### Objective:

This assignment aims to introduce me to the basics of steganography, focusing on data embedding and extraction using the OpenStego tool. I will understand how steganography can be applied and explore its security implications.

## Assignment Details

### Part 1: Understanding Steganography and OpenStego

*1.1 - Write a brief overview of steganography, including its purpose and typical applications:*

Steganography is the technique of hiding data in a way to track that file or data. It can be used for different purposes depends on the user how he wants to use steganography and in what type of file he wants to inject. it is used to convey a secret code or message can be in any file such as text or image formats.

*1.2 - Explain the difference between steganography and cryptography.*

There is a very thin difference between them as steganography hides the message it self and no one can read or detect it except with a proper method while cryptography messages or code can be readable by the right key to decipher it, so in short steganography conceals the secret message itself while cryptography masks it.

*1.3 Summarize the primary functionalities of OpenStego.*

To summarize in short, the functions of OpenStego are two main functions as Data hiding and watermarking.

*1.4 Explain two scenarios where steganography could be misused in a cybersecurity context.*

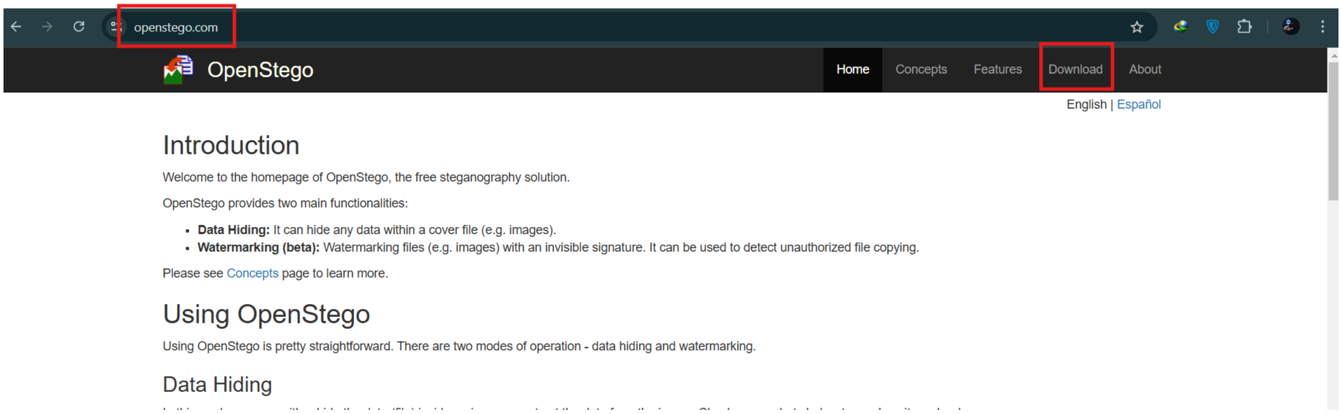
Well, it can be used in different scenarios such as malware distribution, data exfiltration, command and control communications, Evasion of Censorship, Financial frauds or a corporate espionage.

Example: A new campaign conducted by the TA558 hacking group is concealing malicious code inside images using steganography to deliver various malware tools onto targeted systems
Example2 : Busted Alleged Russian Spies Used Steganography To Conceal Communications.

# Part 2: Installation and Configuration.

**1:** It's very easy to Download OpenStego as search in google **Download OpenStego** or simply by visiting ***https://www.openstego.com/*** it will redirect you to GitHub repository and simply download exe file for windows. Secondly it Needs java in environmental path so for that we will have to download java se development kit if it is giving any error in launching after installing.

**Screenshot Note: Capture screenshots of:**



## Introduction

Welcome to the homepage of OpenStego, the free steganography solution.

OpenStego provides two main functionalities:

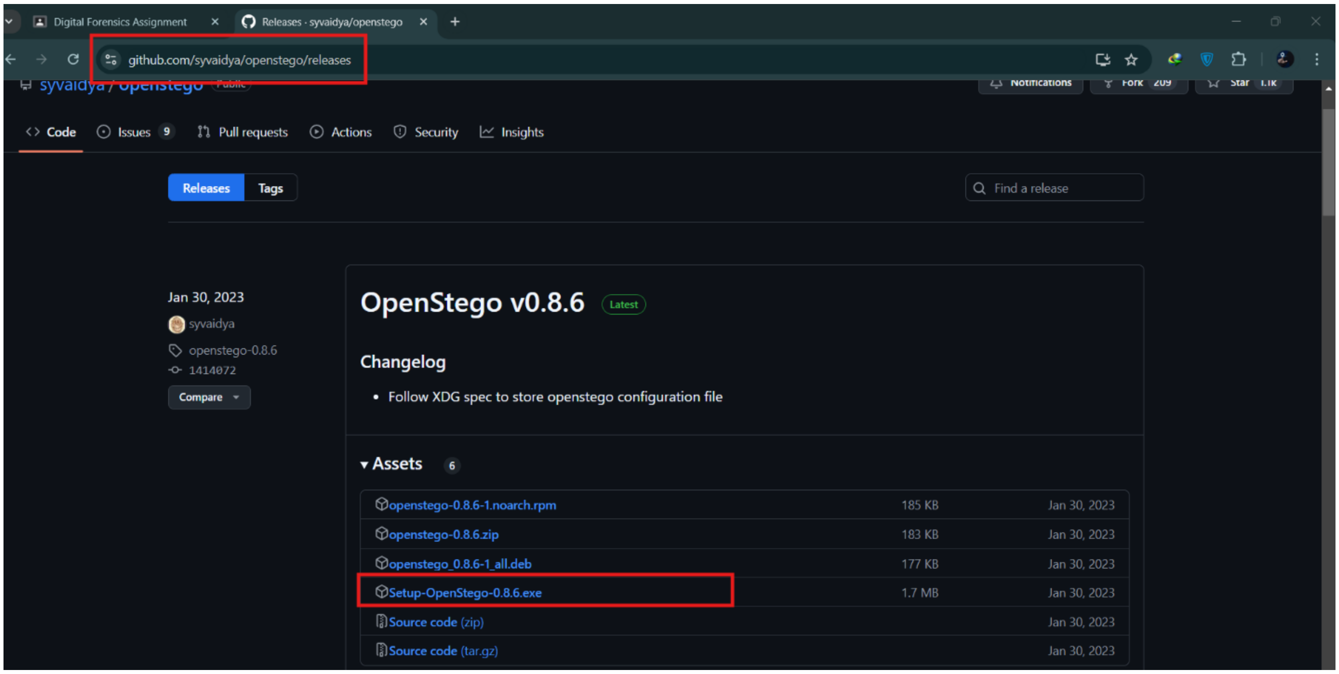
- **Data Hiding:** It can hide any data within a cover file (e.g. images).
- **Watermarking (beta):** Watermarking files (e.g. images) with an invisible signature. It can be used to detect unauthorized file copying.

Please see Concepts page to learn more.

## Using OpenStego

Using OpenStego is pretty straightforward. There are two modes of operation - data hiding and watermarking.

### Data Hiding



Jan 30, 2023
syvaidya
openstego-0.8.6
1414072

## OpenStego v0.8.6 Latest

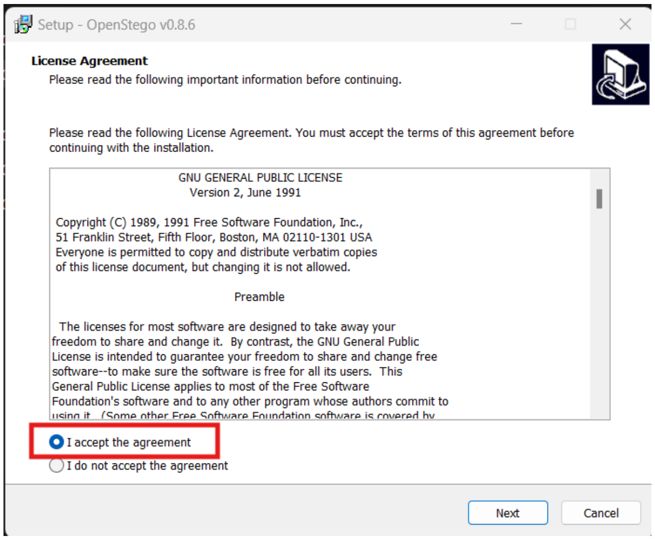
### Changelog

- Follow XDG spec to store openstego configuration file

### Assets 6

| | | |
|---|---|---|
| openstego-0.8.6-1.noarch.rpm | 185 KB | Jan 30, 2023 |
| openstego-0.8.6.zip | 183 KB | Jan 30, 2023 |
| openstego_0.8.6-1_all.deb | 177 KB | Jan 30, 2023 |
| Setup-OpenStego-0.8.6.exe | 1.7 MB | Jan 30, 2023 |
| Source code (zip) | | Jan 30, 2023 |
| Source code (tar.gz) | | Jan 30, 2023 |

**The installation wizard steps.**



Setup - OpenStego v0.8.6

**License Agreement**

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

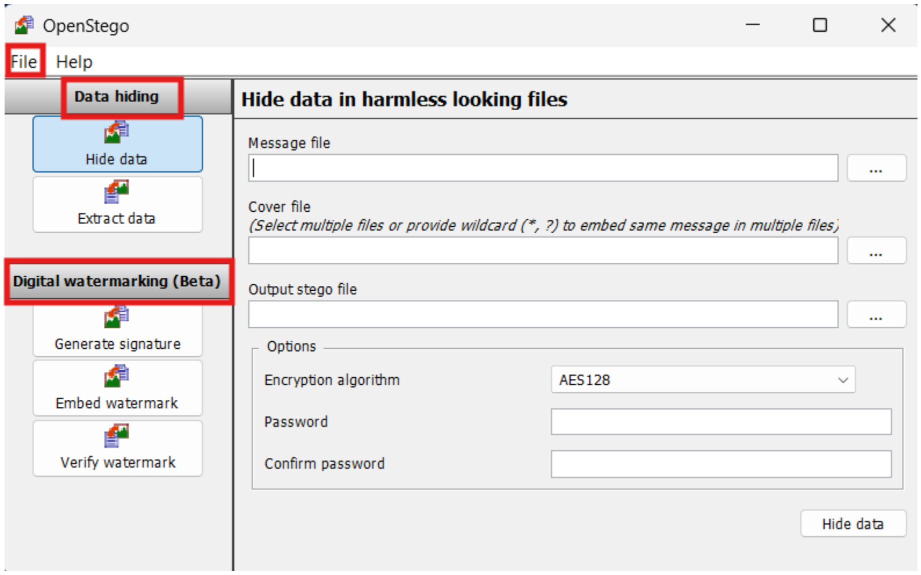
The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by

● I accept the agreement

○ I do not accept the agreement

*After this next and finish.*

## 2. Interface Overview.



**Hide data in harmless looking files**

Message file

Cover file
*(Select multiple files or provide wildcard (*, ?) to embed same message in multiple files)*

Output stego file

Options

Encryption algorithm: AES128

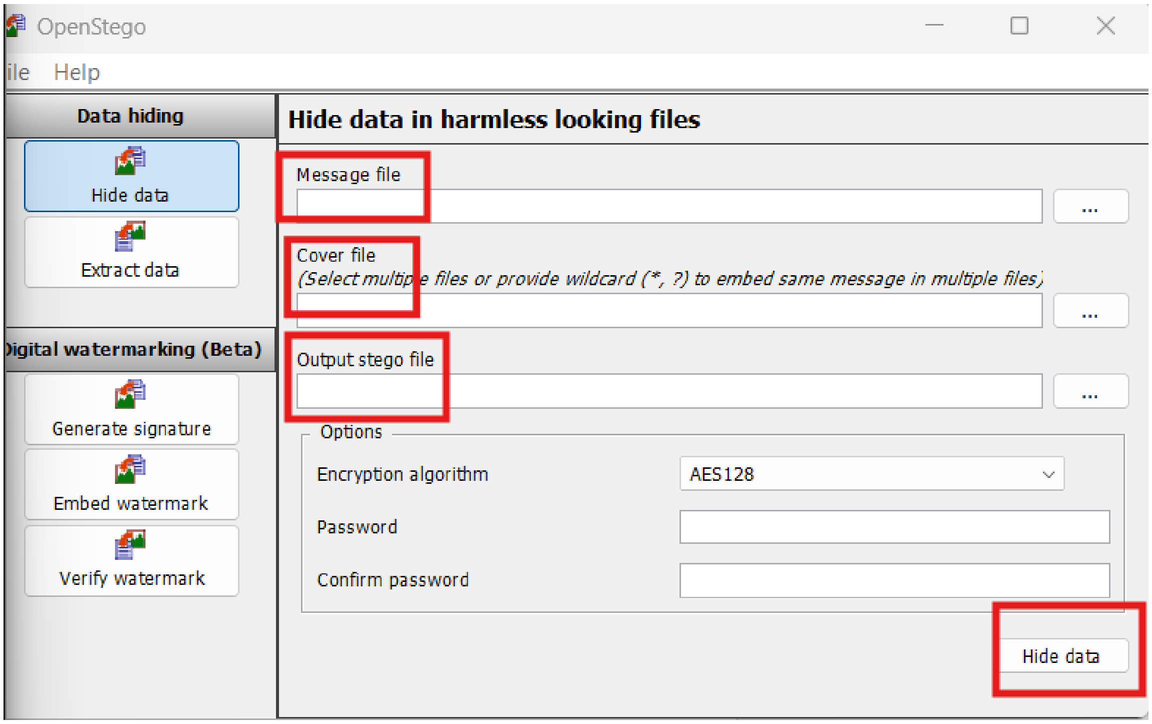
Password

Confirm password

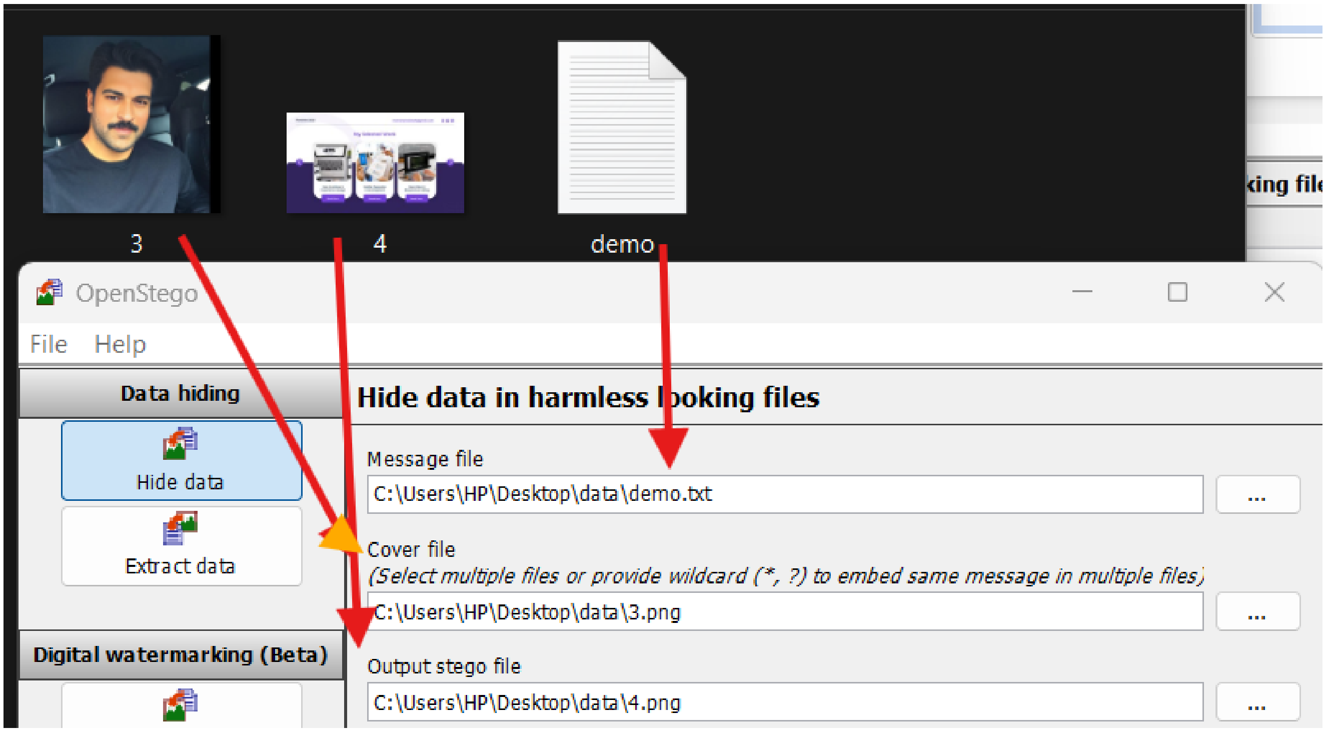
In this image we can see two  option of data hiding and digital watermarking and then its different functions in them .

## Part 3: Practical Data Embedding and Extraction.

We Will create a message in text file and the n open it in message file area then we will like to add any cover or wild card to hide and then we will like to add any output stego for our final user that how it would like for example.



*As we can see in this image if I select some files.*

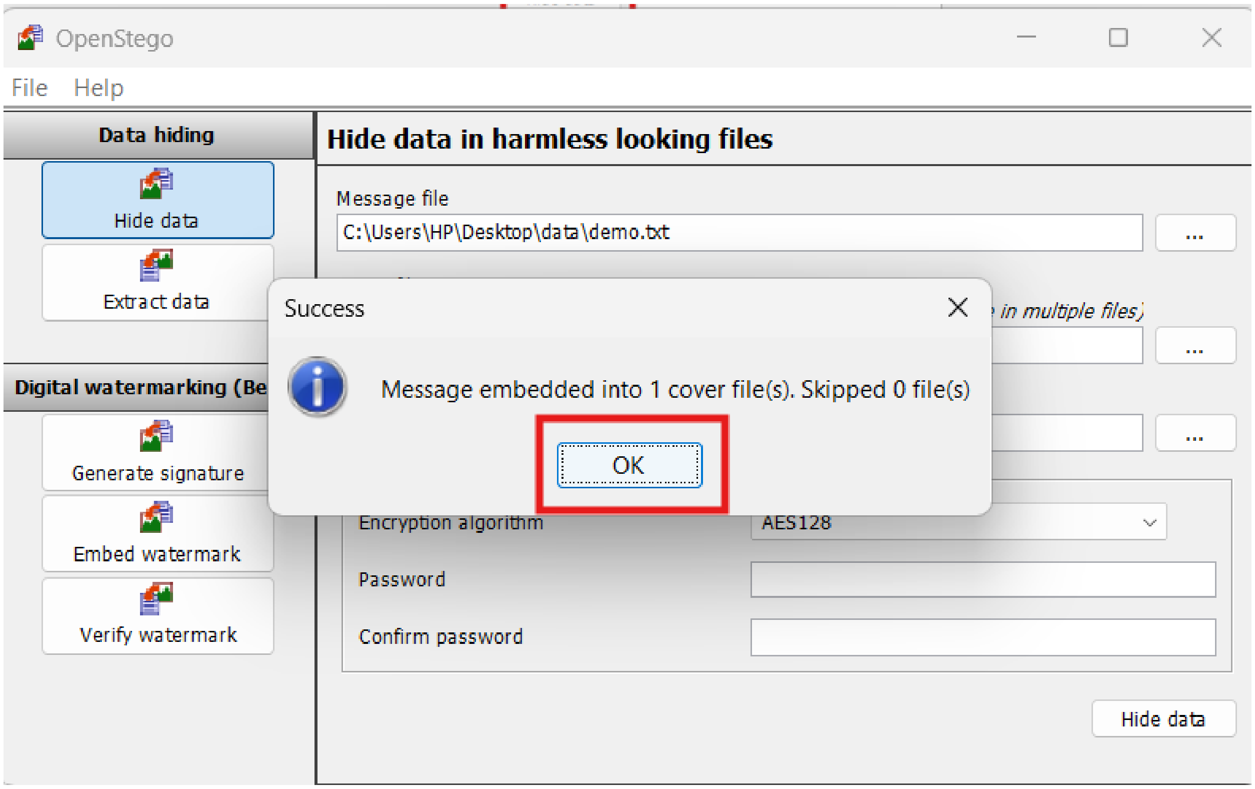

3
4
demo
OpenStego
File
Help
Data hiding
Hide data
Extract data
Digital watermarking (Beta)
Hide data in harmless looking files
Cover file
(Select multiple files or provide wildcard (*, ?) to embed same message in multiple files)
...

Message file: C:\Users\HP\Desktop\data\demo.txt

Cover file: C:\Users\HP\Desktop\data\3.png

Output stego file: C:\Users\HP\Desktop\data\4.png

*We can clearly see our file has been embed with a secret.*



OpenStego

File Help

Data hiding

Hide data

Extract data

Digital watermarking (Be

Generate signature

Embed watermark

Verify watermark

Hide data in harmless looking files

Message file

C:\Users\HP\Desktop\data\demo.txt

Success

Message embedded into 1 cover file(s). Skipped 0 file(s)

OK

Encryption algorithm: AES128

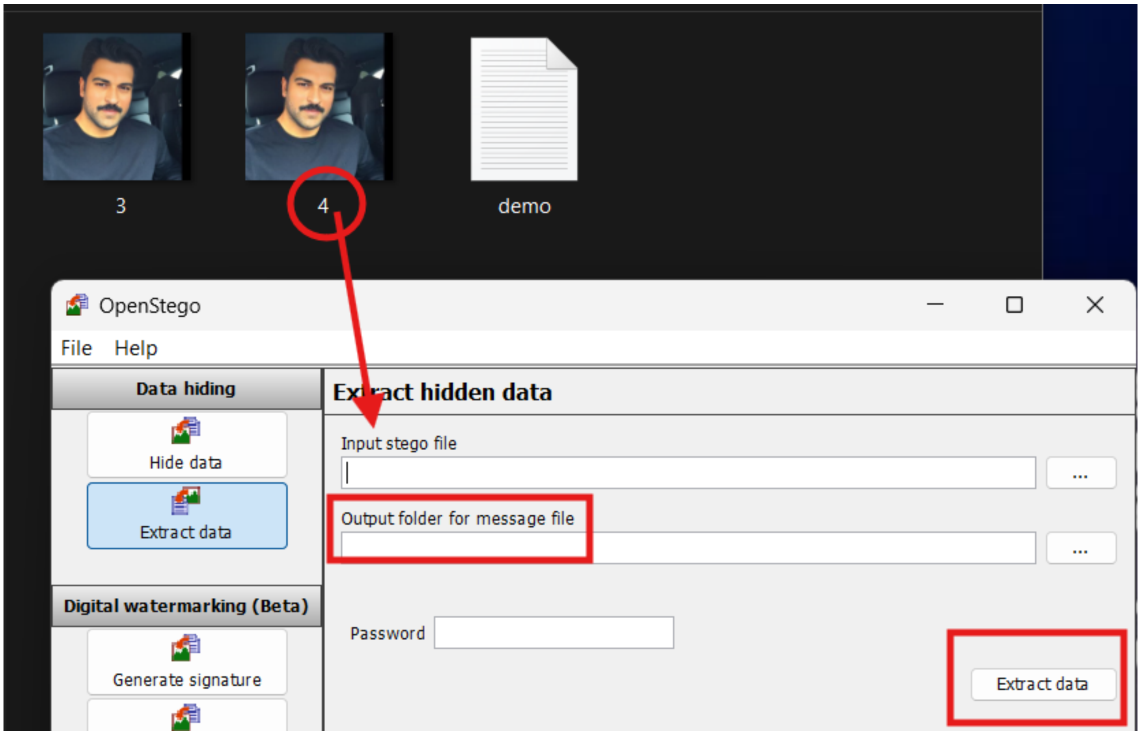
Password

Confirm password

Hide data

## Now we will try to extract Data:

We can clearly see the file that was created with stego no we will extract data as :



OpenStego

File Help

Data hiding

Hide data

Extract data

Digital watermarking (Beta)

Generate signature

Extract hidden data

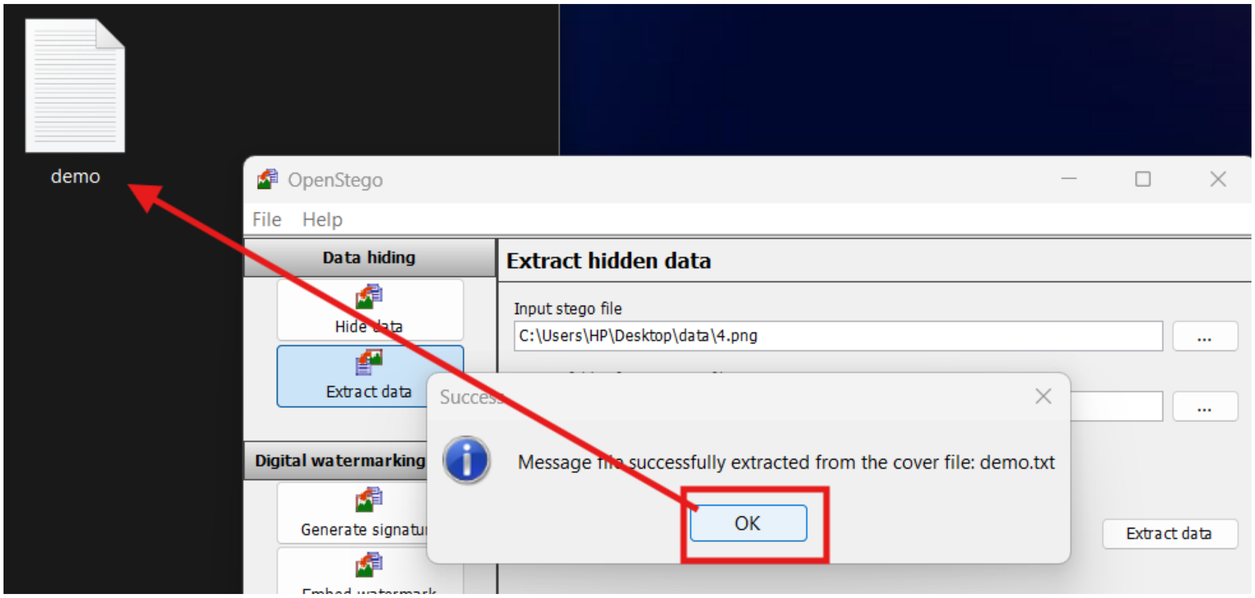
Input stego file

Output folder for message file

Password

Extract data

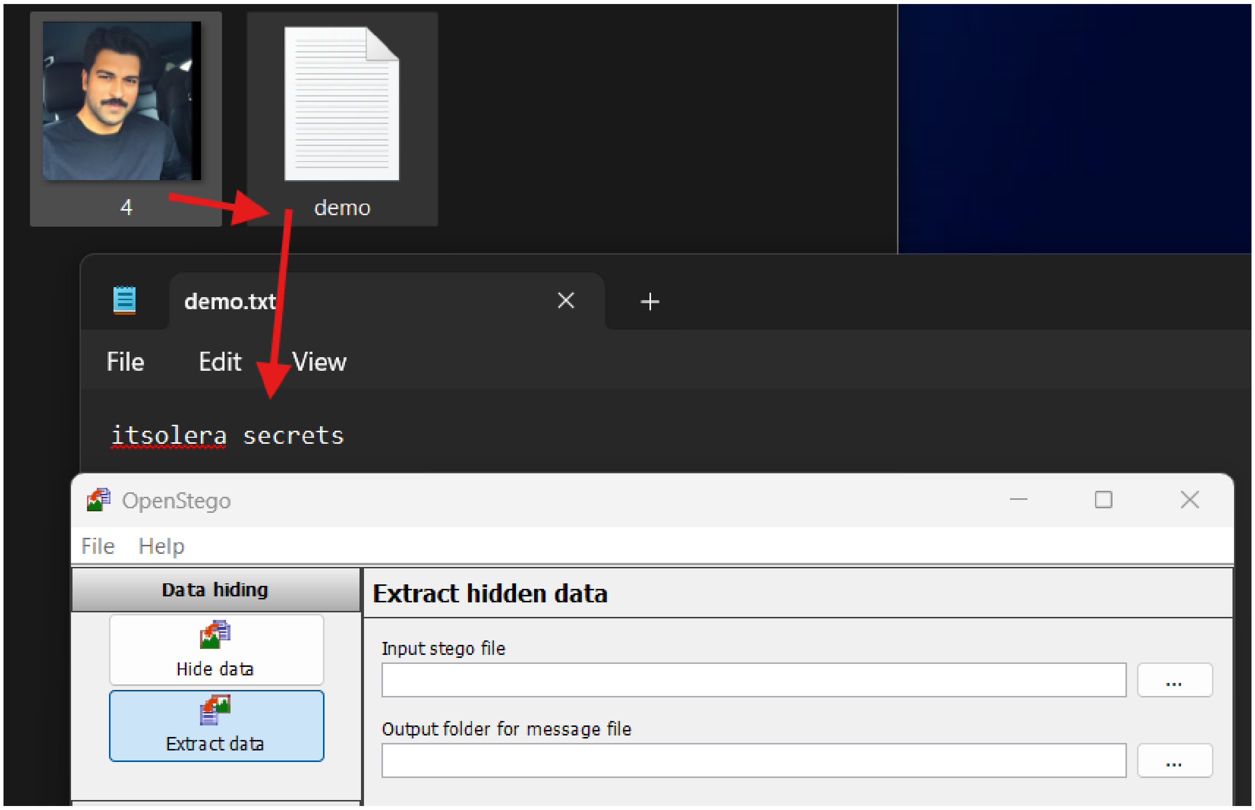
As we know that our file name was 4 that we created with OpenStego and we will like to extract data from it so we open it in extract data and we can see the result.



Input stego file: C:\Users\HP\Desktop\data\4.png

Message file successfully extracted from the cover file: demo.txt

Now we will like to see what was the secret that was embed in picture.



```
itsolera secrets
```

This is the final text secret that was earlier embed in the image which we have extracted Now.

## Part 4: Analysis of Steganography Security Implications:

### 1. Detection Challenges:

Steganography, as I use it in OpenStego, is hard for security tools to detect because it hides data without significantly altering the cover file's appearance or stats. Another reason is that it Changes the least important bits in an image or audio file

### 2 Discuss why steganography, as used in OpenStego, is difficult for security tools to detect.

It is difficult for security tools to detect because it operates on the principle of "security through obscurity" which means that steganography relies on the fact that hidden data is embedded so well that it blends in with normal data. By not altering the appearance or structure of the file in an obvious way, it avoids detection. It's like hiding a needle in a haystack: if the needle looks just like a piece of straw, it’s tough to find.

### 3 Briefly describe one steganalysis technique that could potentially detect hidden data in images.

One steganalysis technique is **visual analysis**. This involves examining the image closely for any inconsistencies that might suggest hidden data. Likewise, if image seem oddly pixelated or have unexpected color variations, it could indicate that data has been embedded there.

***Example:*** Imagine you have a simple black-and-white image. If you notice some areas with unexpected gray pixels, it might be a clue that hidden information is embedded using techniques like LSB substitution. This approach relies on our ability to spot what doesn’t quite fit naturally in the image’s context….