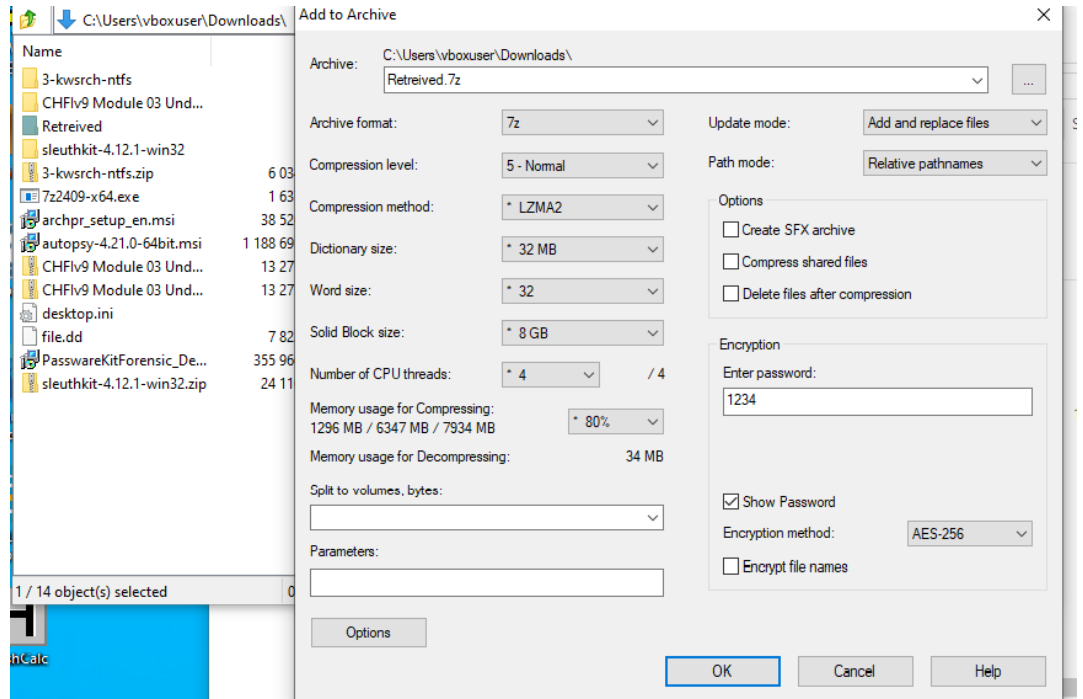


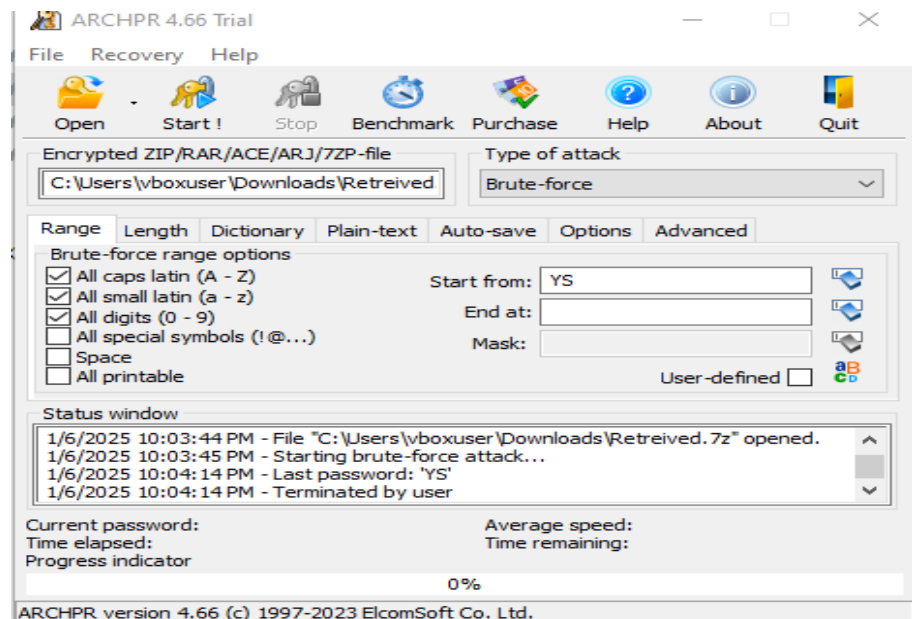
CRACKING APPLICATION PASSWORD

Advanced archive password recovery

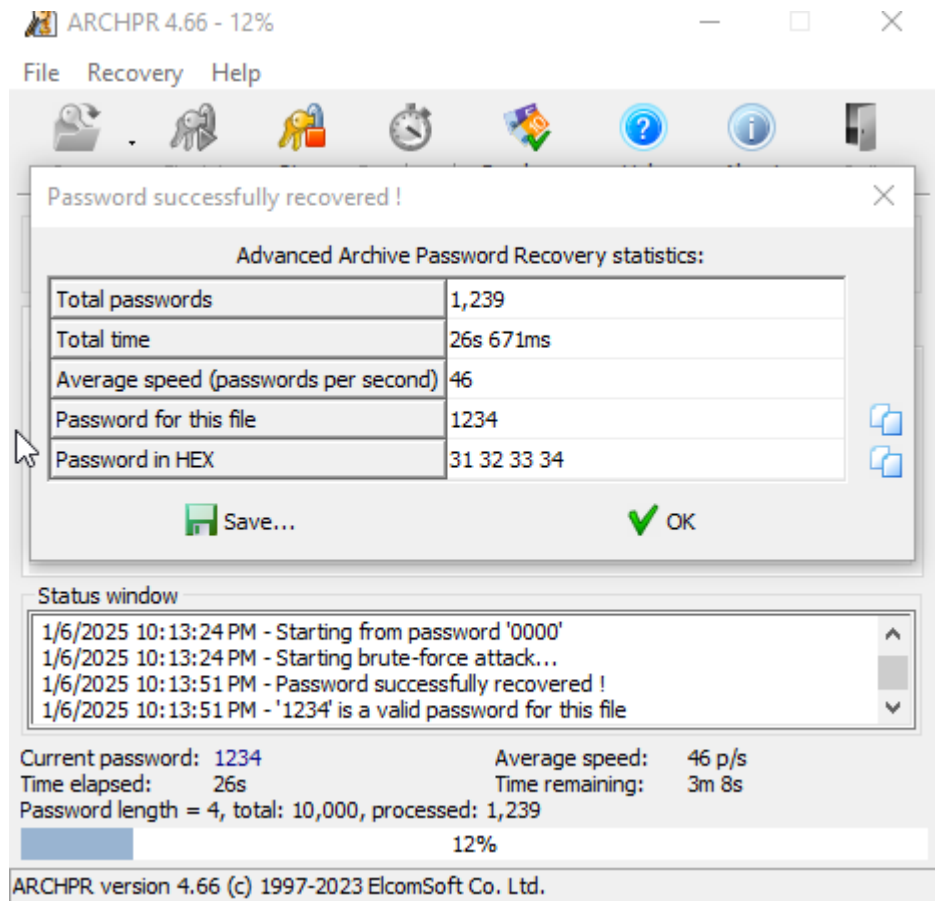
I crated my own evidence file of zip with the password of 1234



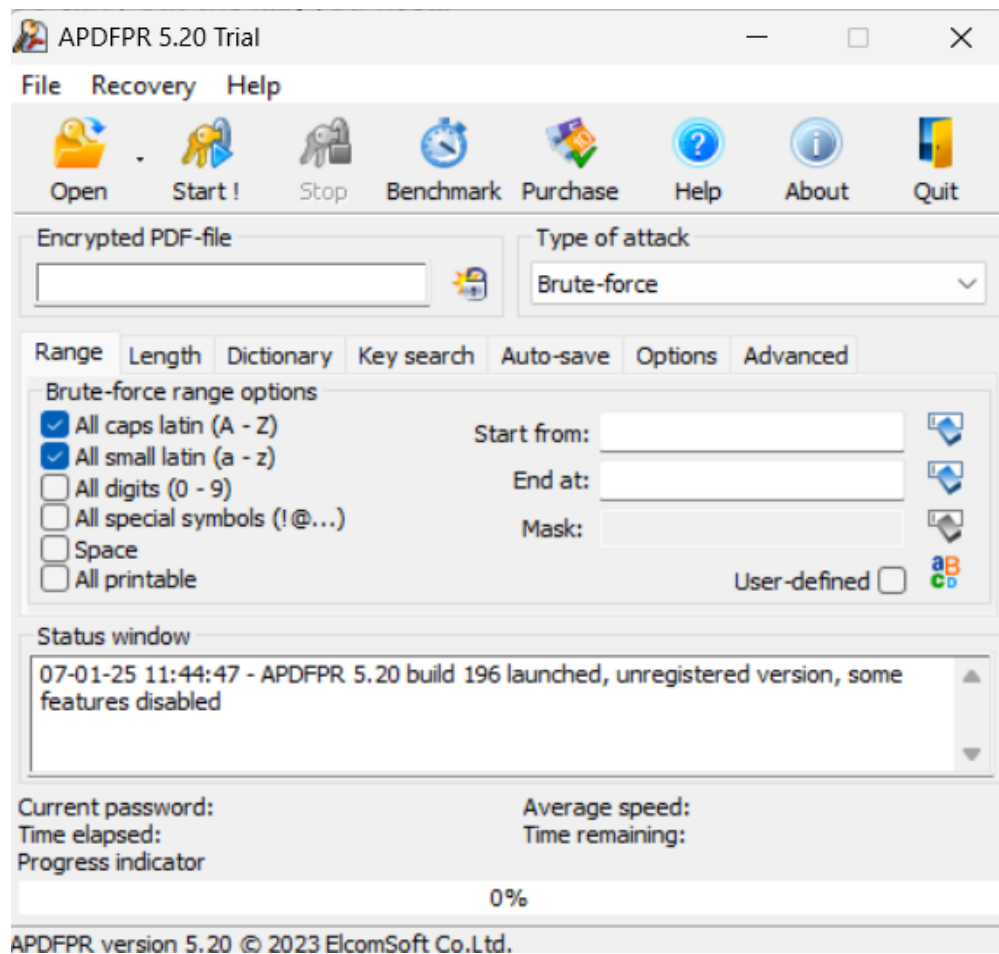
Now asking password I use recovery tool to crack password.



Select the file and select bruteforcing parameters and attack.

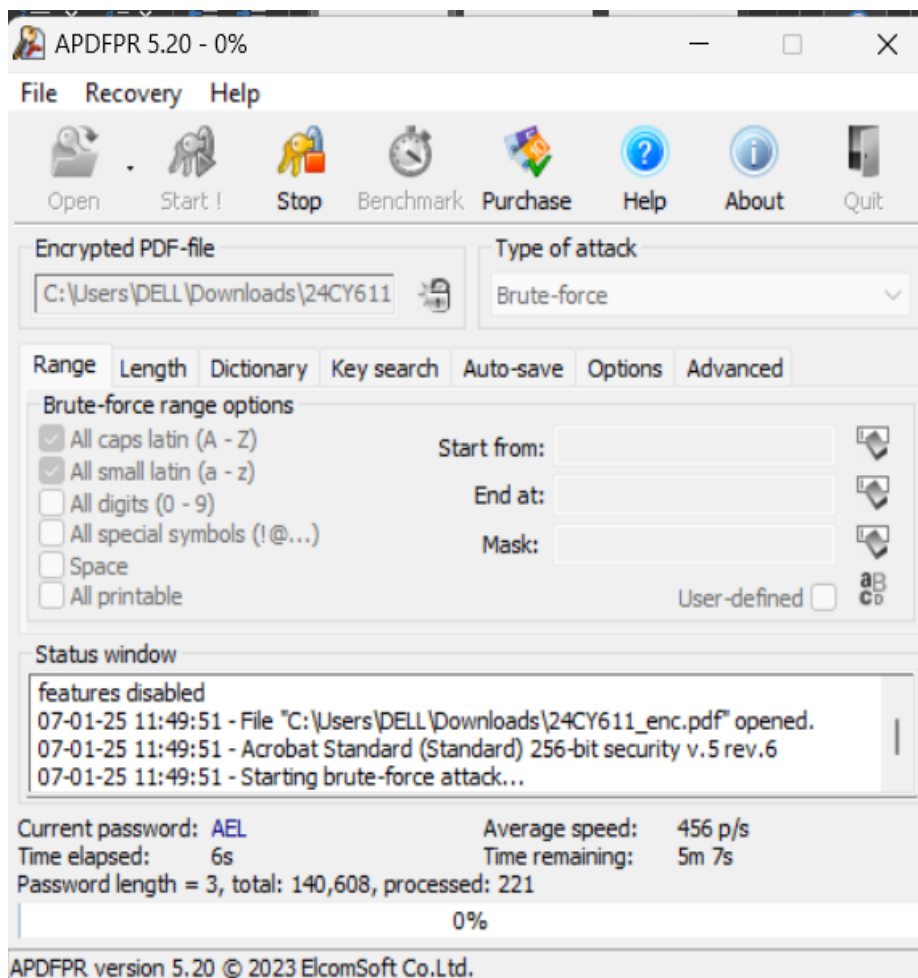
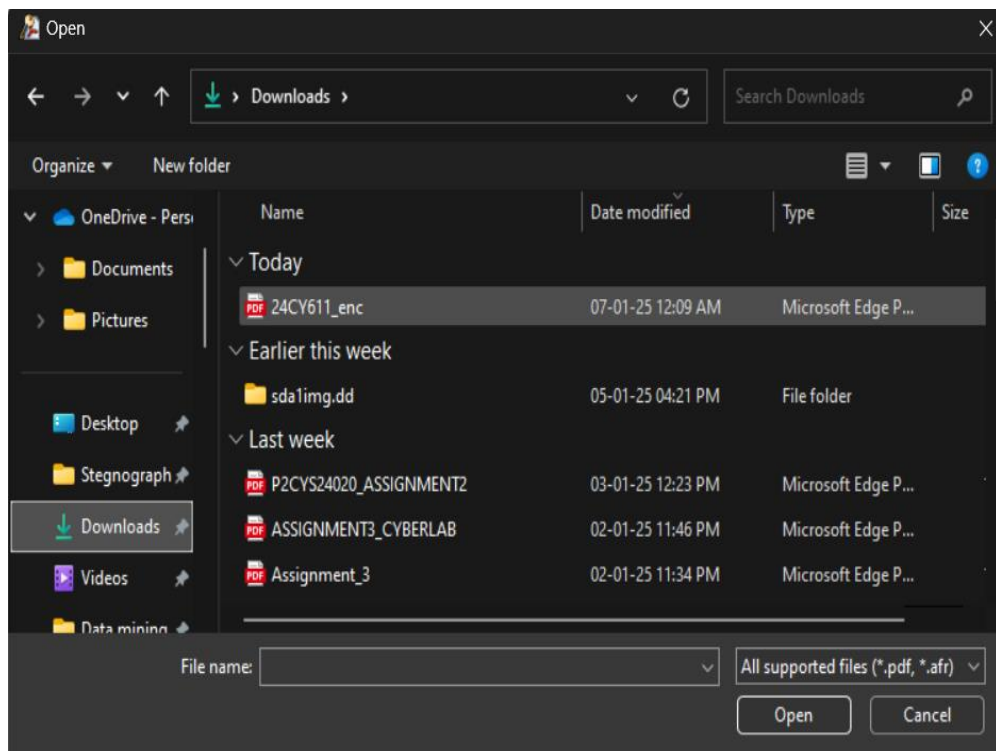


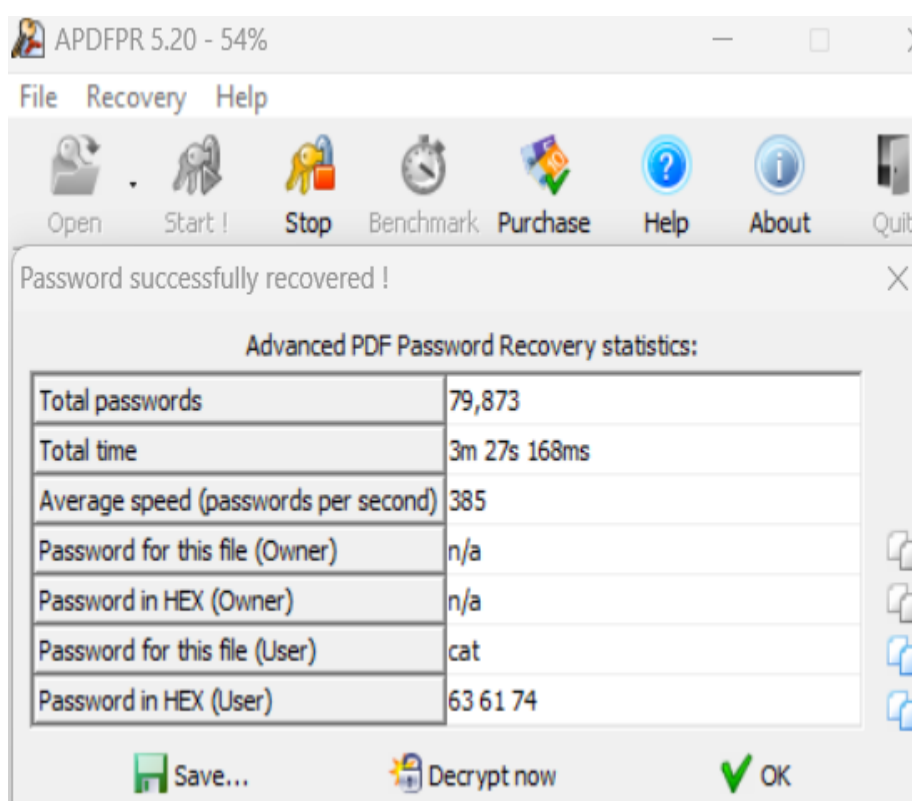
Advance pdf recovery tool



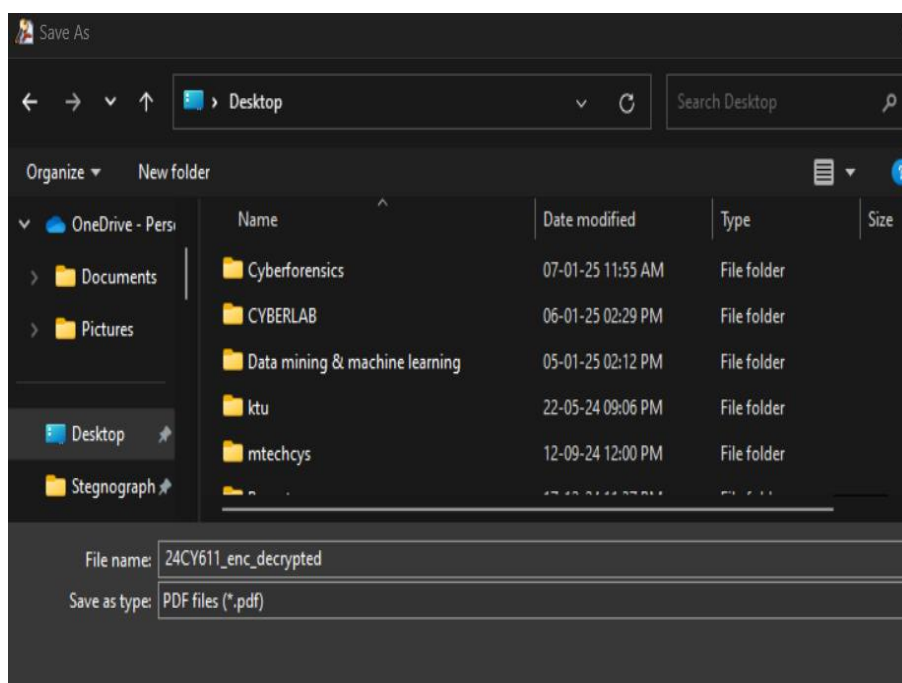
Encrypted pdf file with dictionary recovery method

Open the encrypted file





Here password 'cat' recovered.




File is decrypted.



Document successfully decrypted.

OK

 24CY611_enc.pdf

24CY611_enc.pdf requires a password.

Enter password

Enter password to open
this PDF file



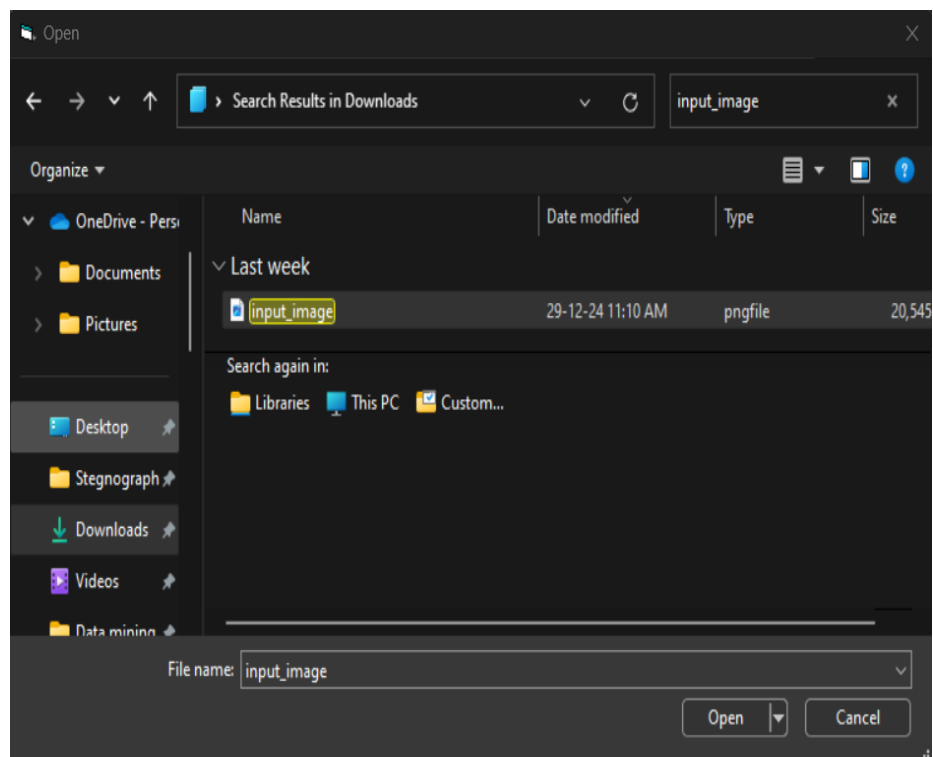
...

OK

Cancel

Lab-2 Detecting Stegnography

First try the tool stegspy to extract the hidden data




Form1

Choose a file to interrogate.
Run will allow you to choose
your file and identify a hidden
message.

Run

Steganography found at marker position
16554399
Hiderman program detected!



StegSpy V2.1 Copyright 2003, 2004
Logo Copyright 2003, 2004
By SpyHunter www.spy-hunter.com

Image Steganography

Encode

Image:
Drag-and-drop an image file here

Input Data:
☐ File Drag-and-drop a file to embed in the image here
☒ Text

Capacity: ...

Output Image: Choose...

Steganography Mode
☒ Embed
☐ Enlarge
☐ Difference

☒ Encode
☐ Decode
☐ Encrypt

Start

Idle

Image Steganography

Decode

Image:

Drag-and-drop an image with embedded data here

Image 2:

☐ Output to File

Choose...

☒ Output Text

Steganography Mode

☒ Embed

☐ Enlarge

☐ Difference

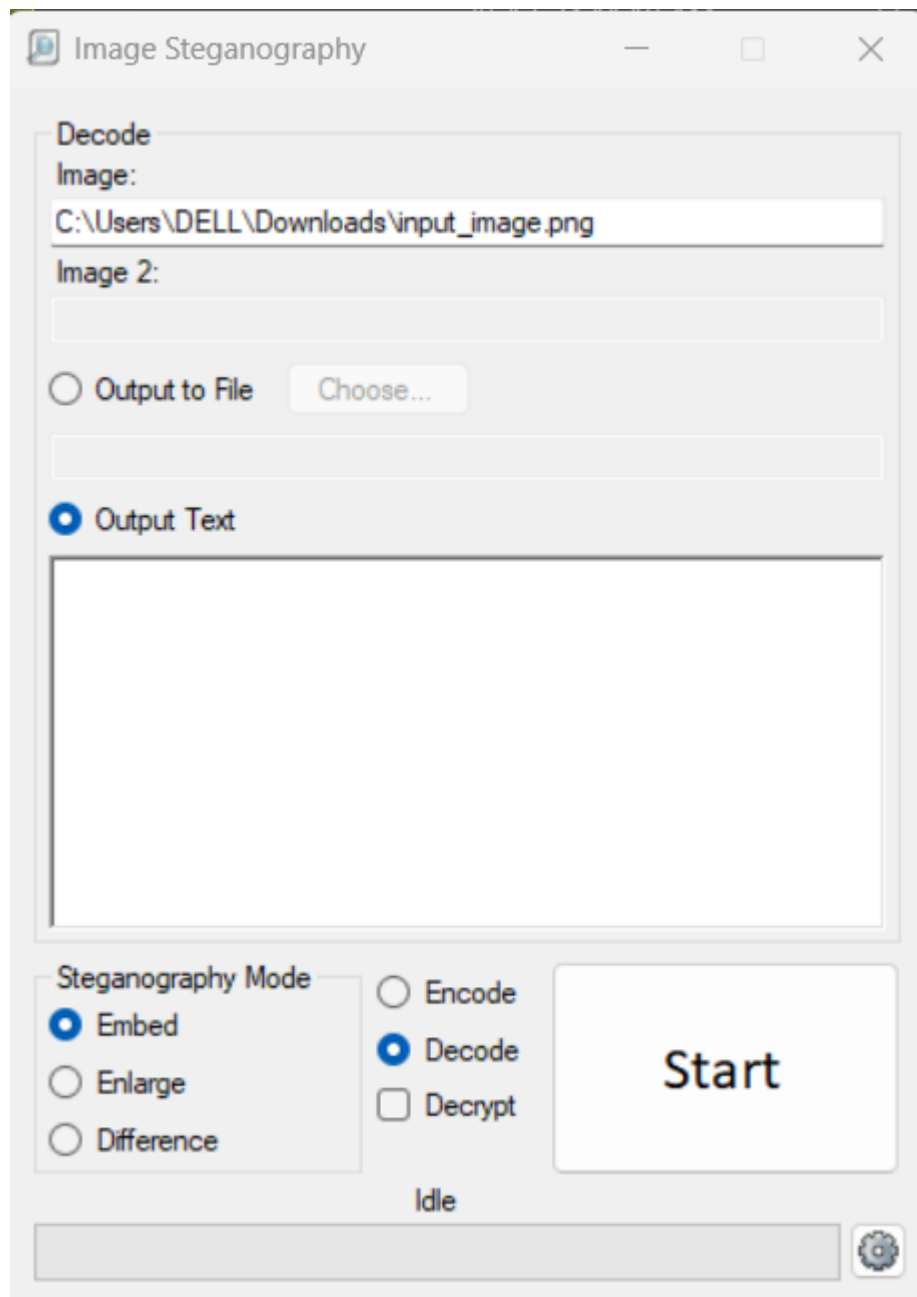
☐ Encode

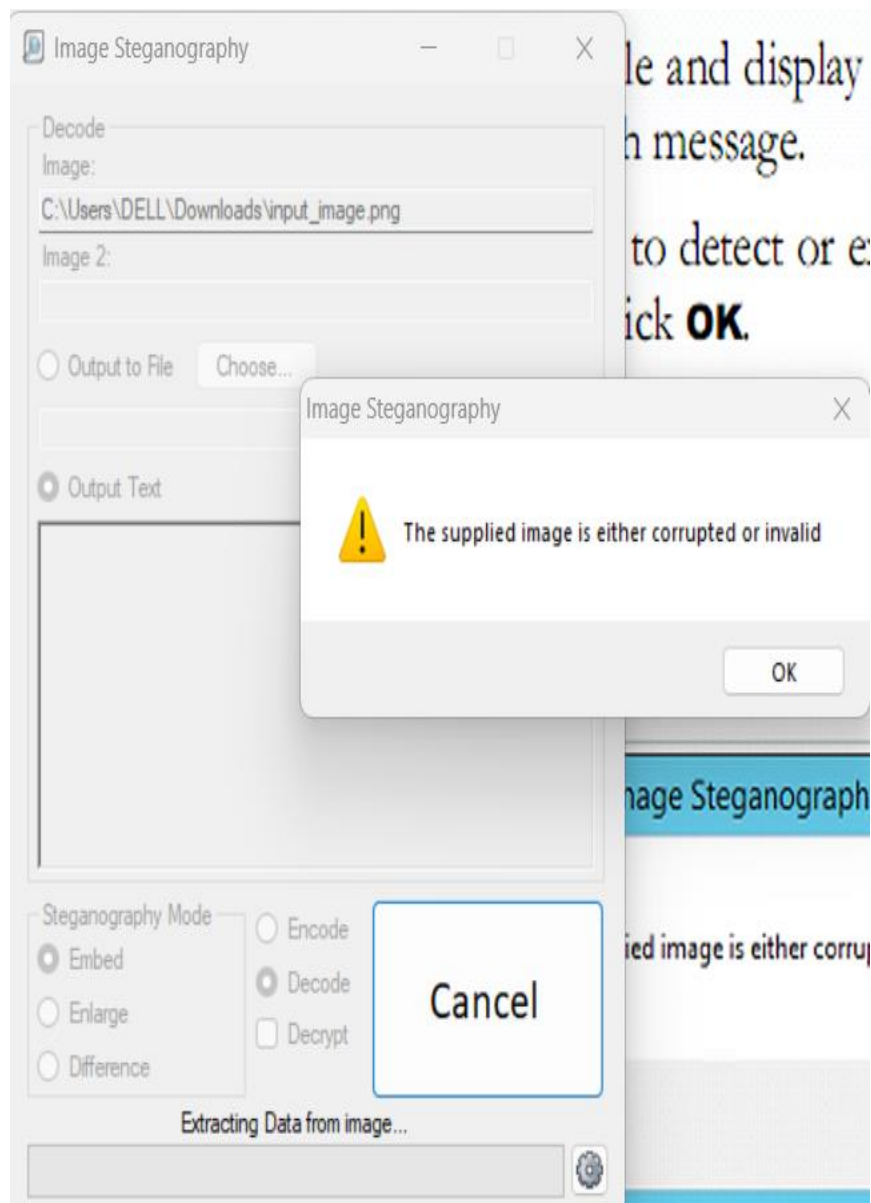
☒ Decode

☐ Decrypt

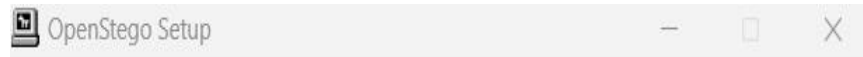
Start

Idle





Here failed.so use another tool openstego

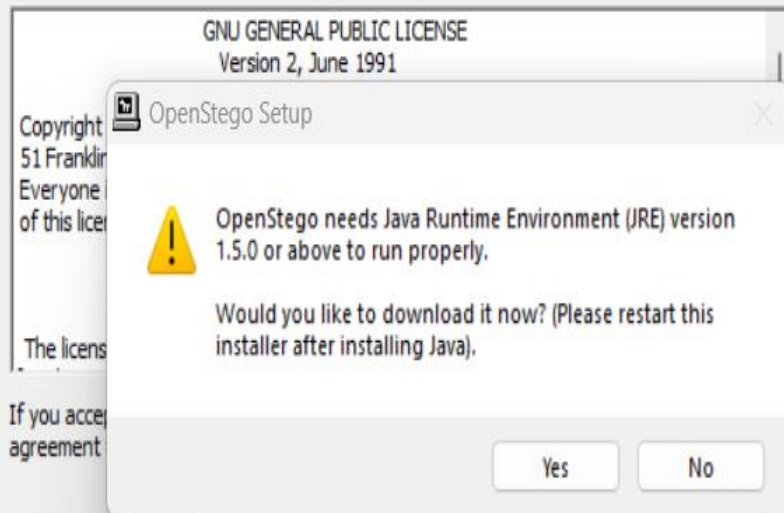


License Agreement

Please review the license terms before installing OpenStego.



Press Page Down to see the rest of the agreement.

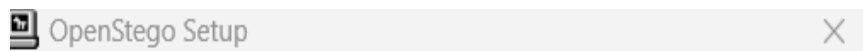


Nullsoft Install System v2.46

< Back

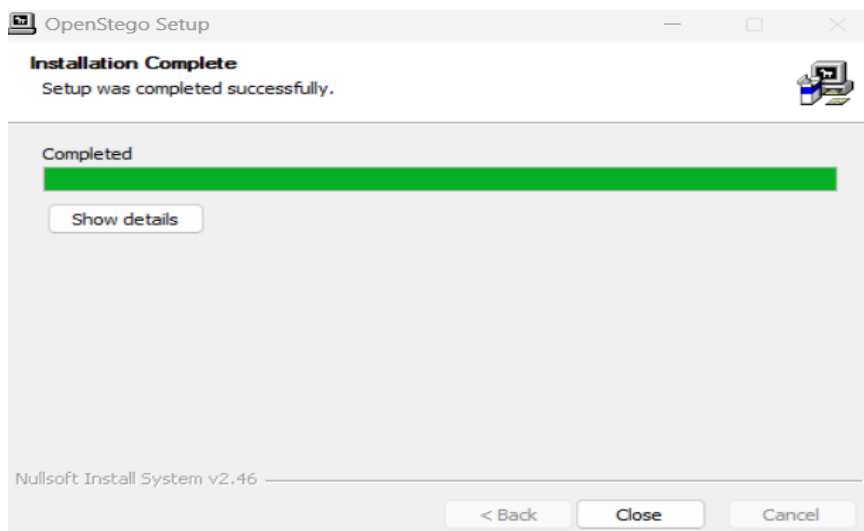
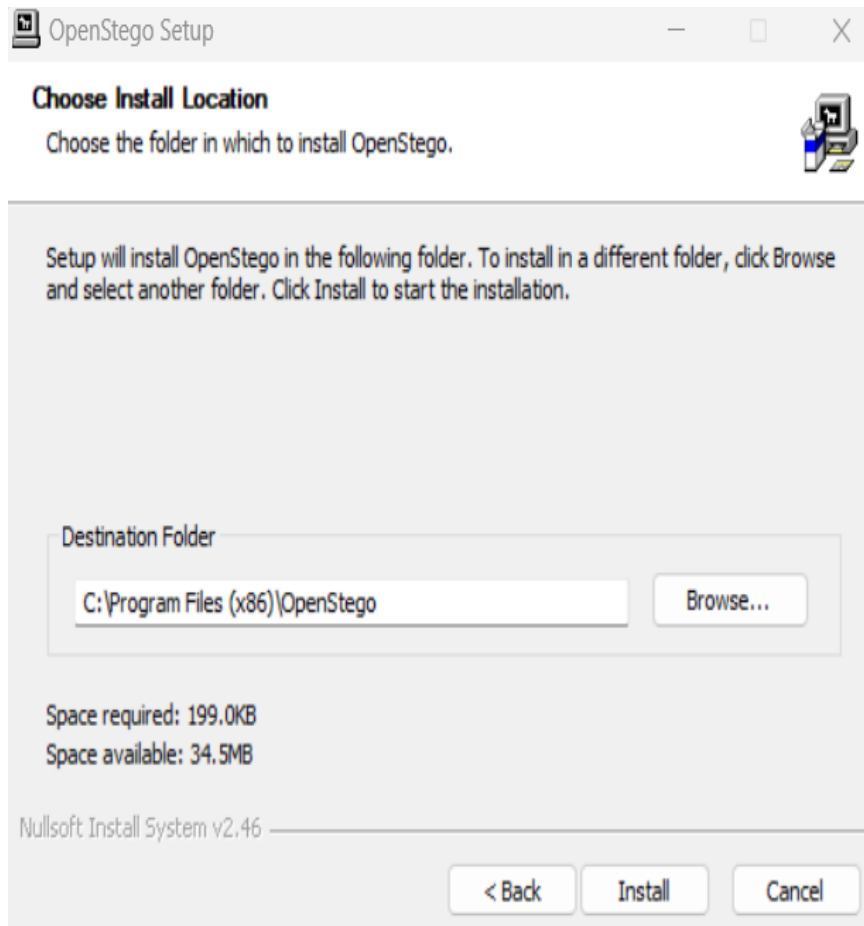
Next >

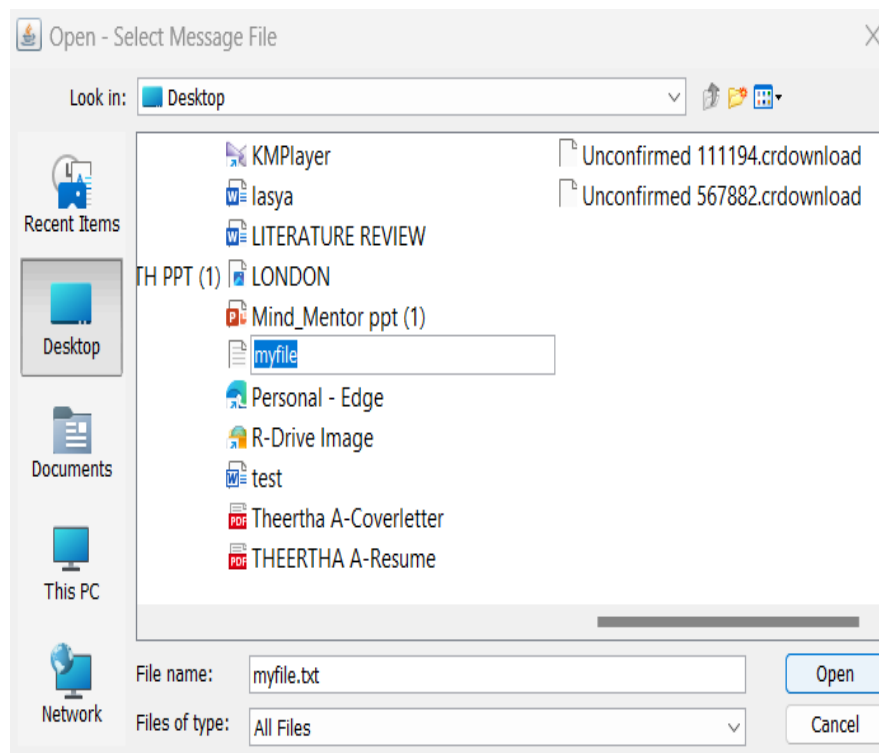
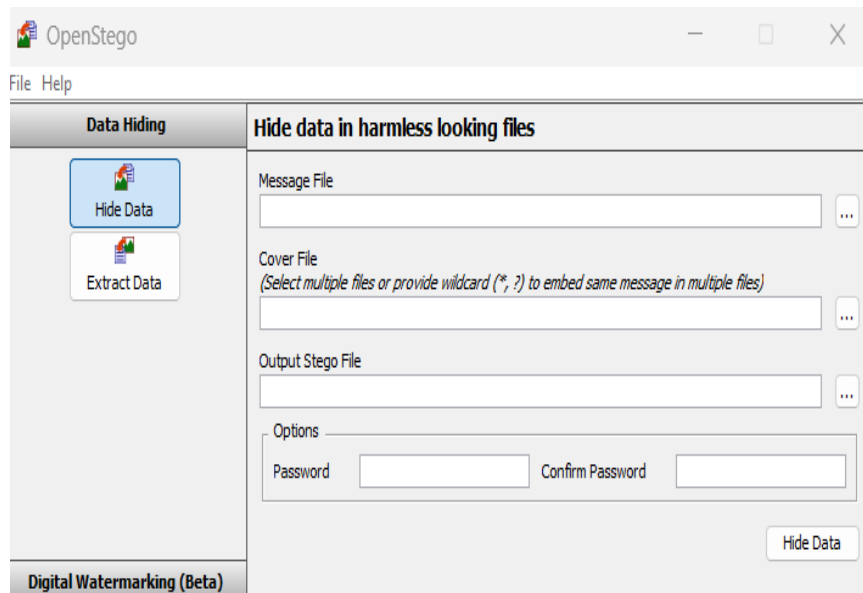
Cancel

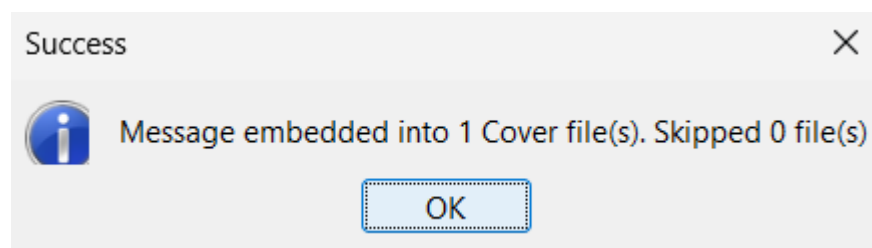
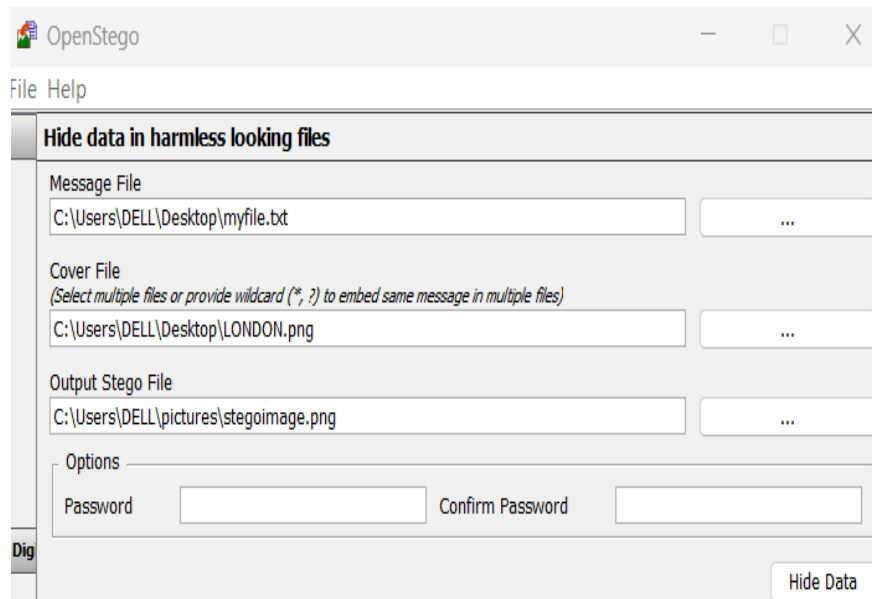


OpenStego will install even though you do not have required version of Java installed. Please don't complain later if it doesn't work.

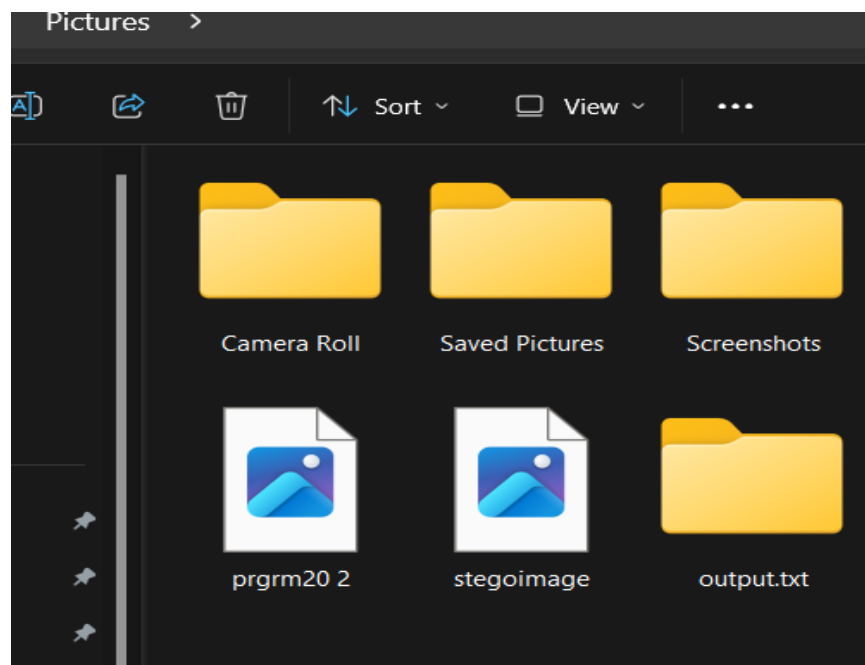
OK



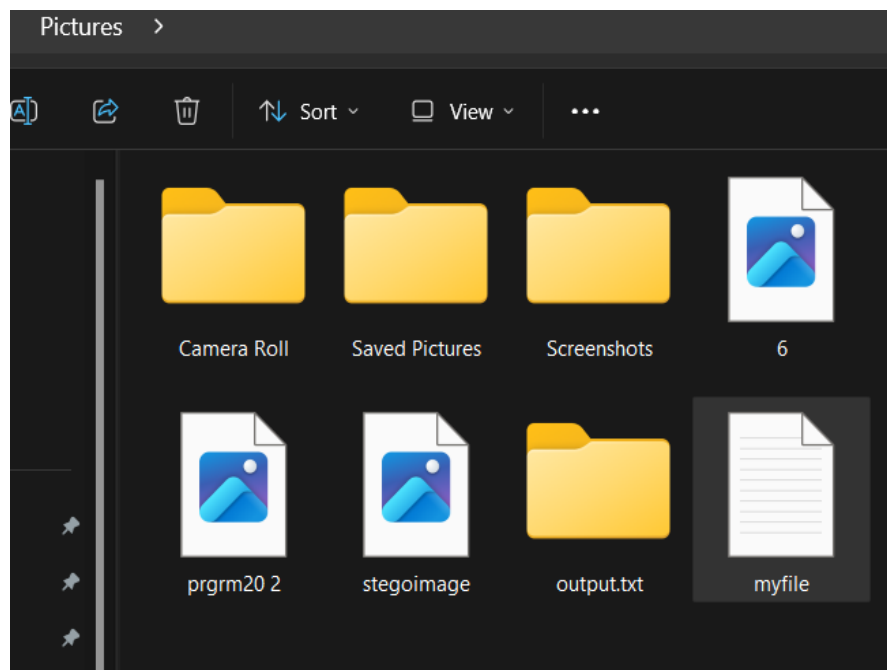
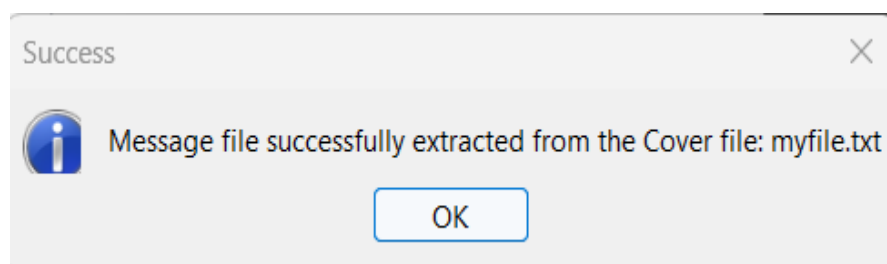
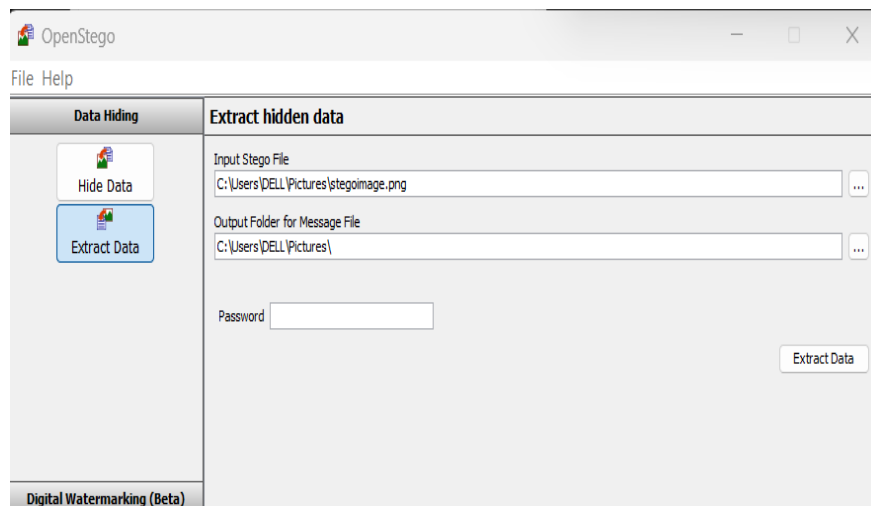




Output stegofile is saved in
C:\Users\DELL\pictures\stegoimage.png



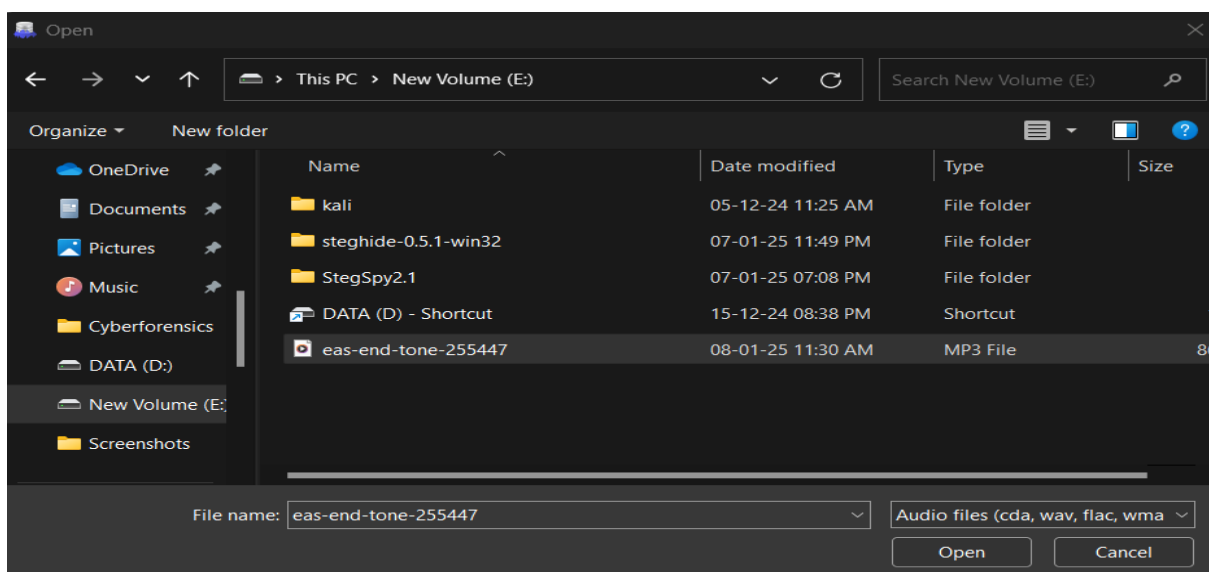
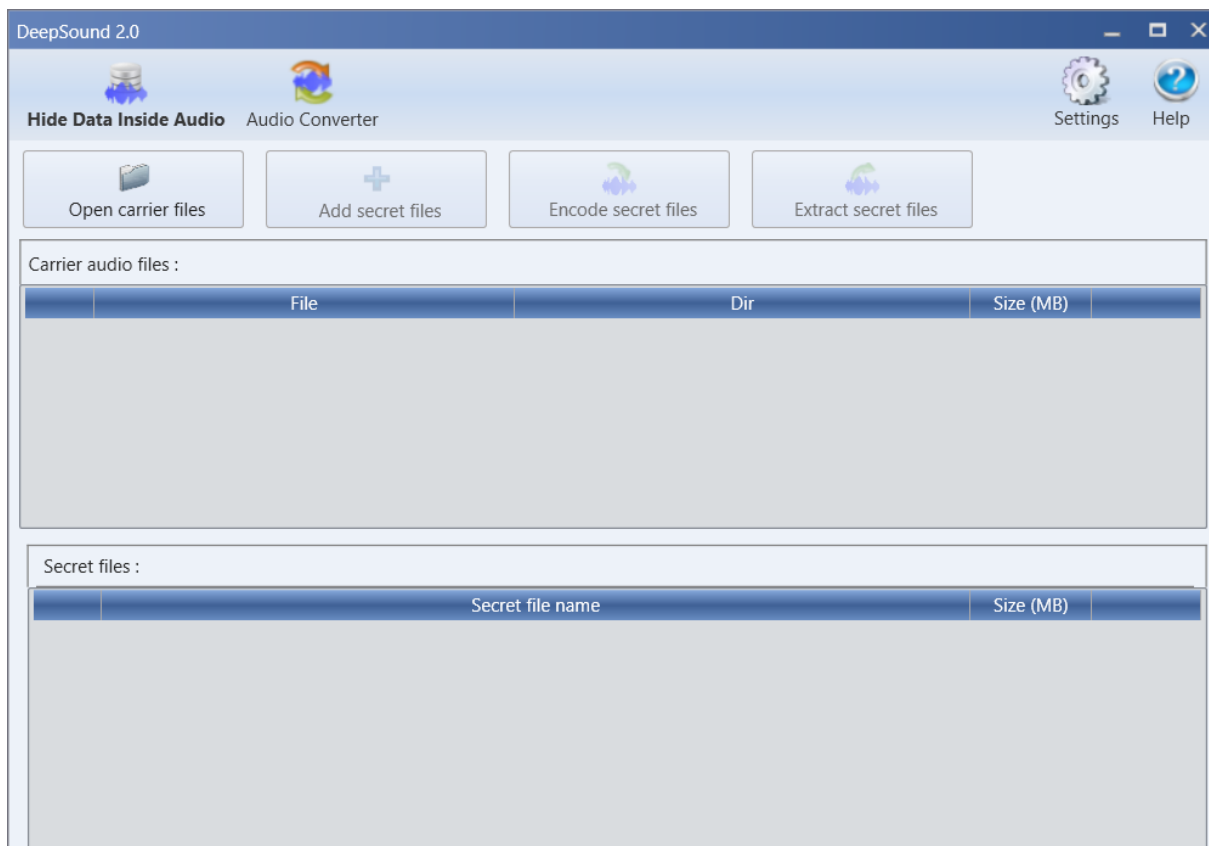
Then extract the hidden data

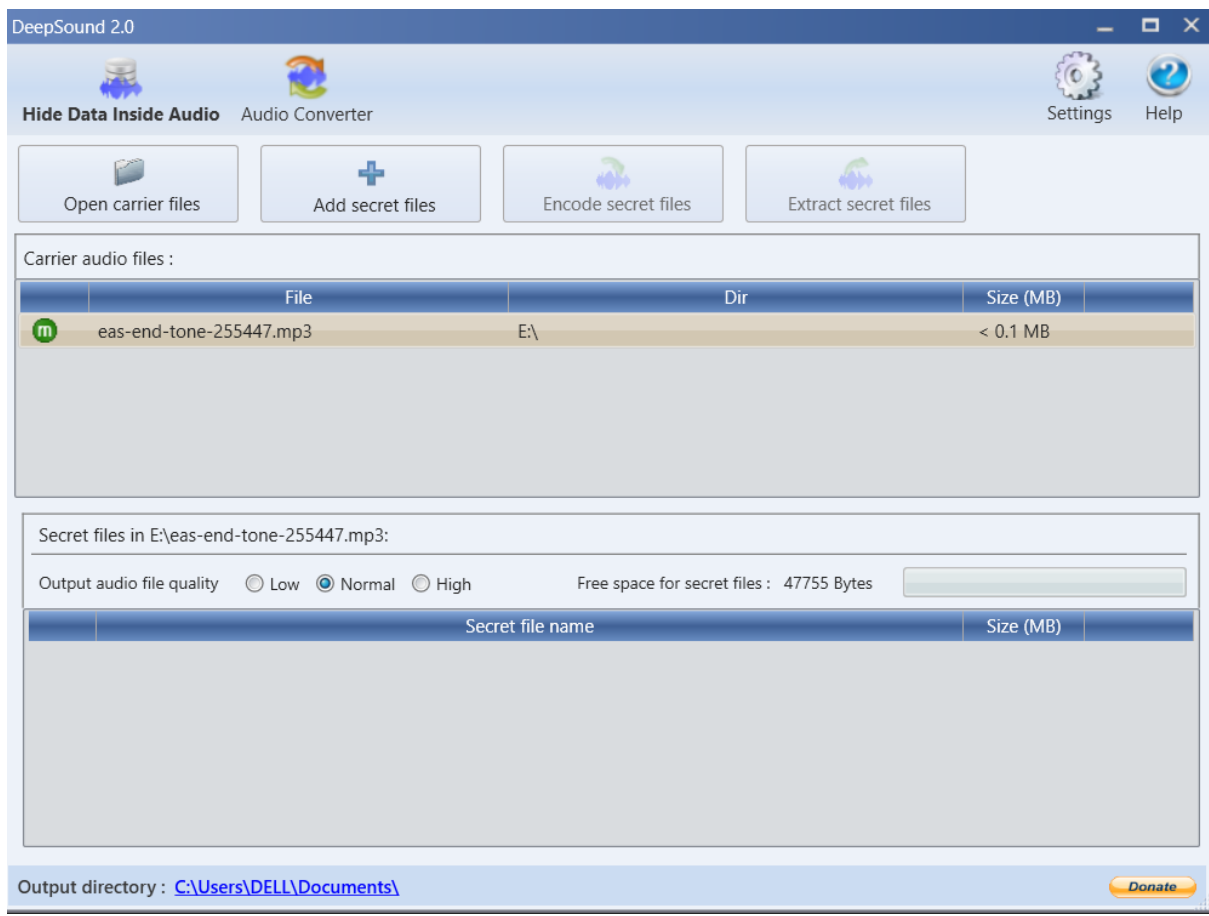


Here myfile.txt is the hidden file. Now successfully extracted that file and save in this directory.

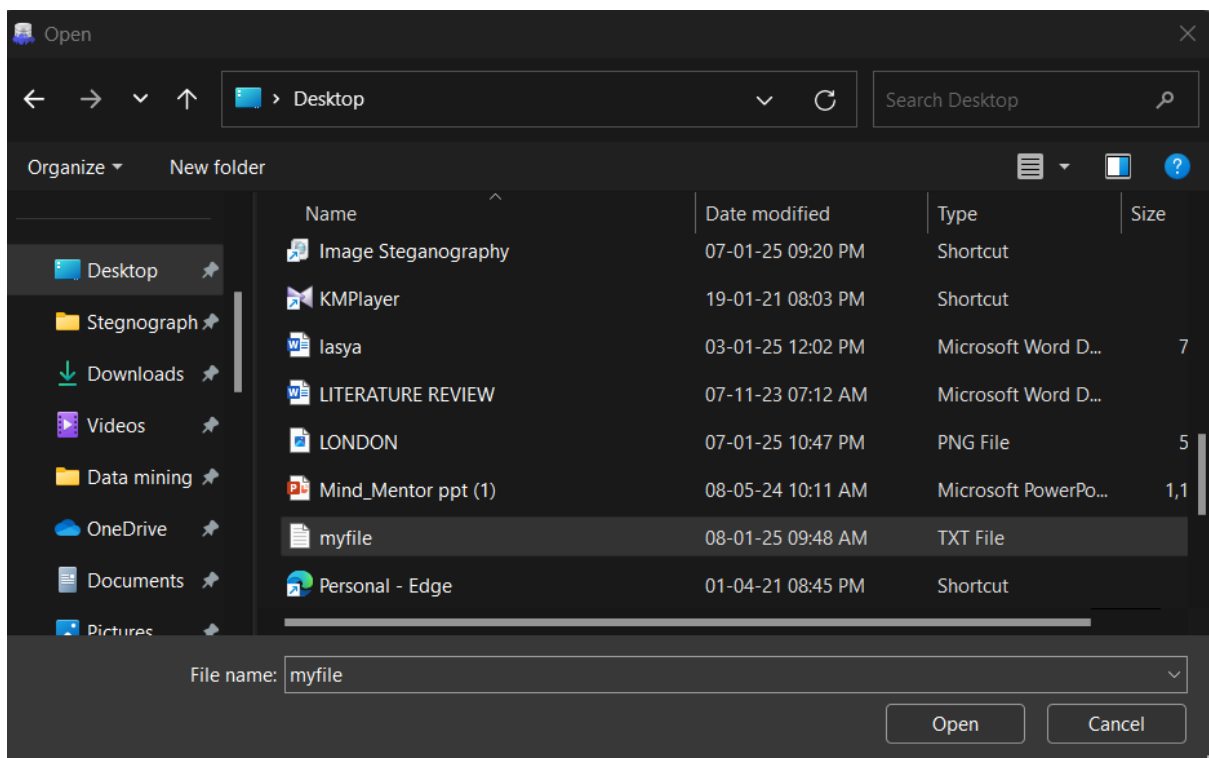
Extracting hidden data from audio file

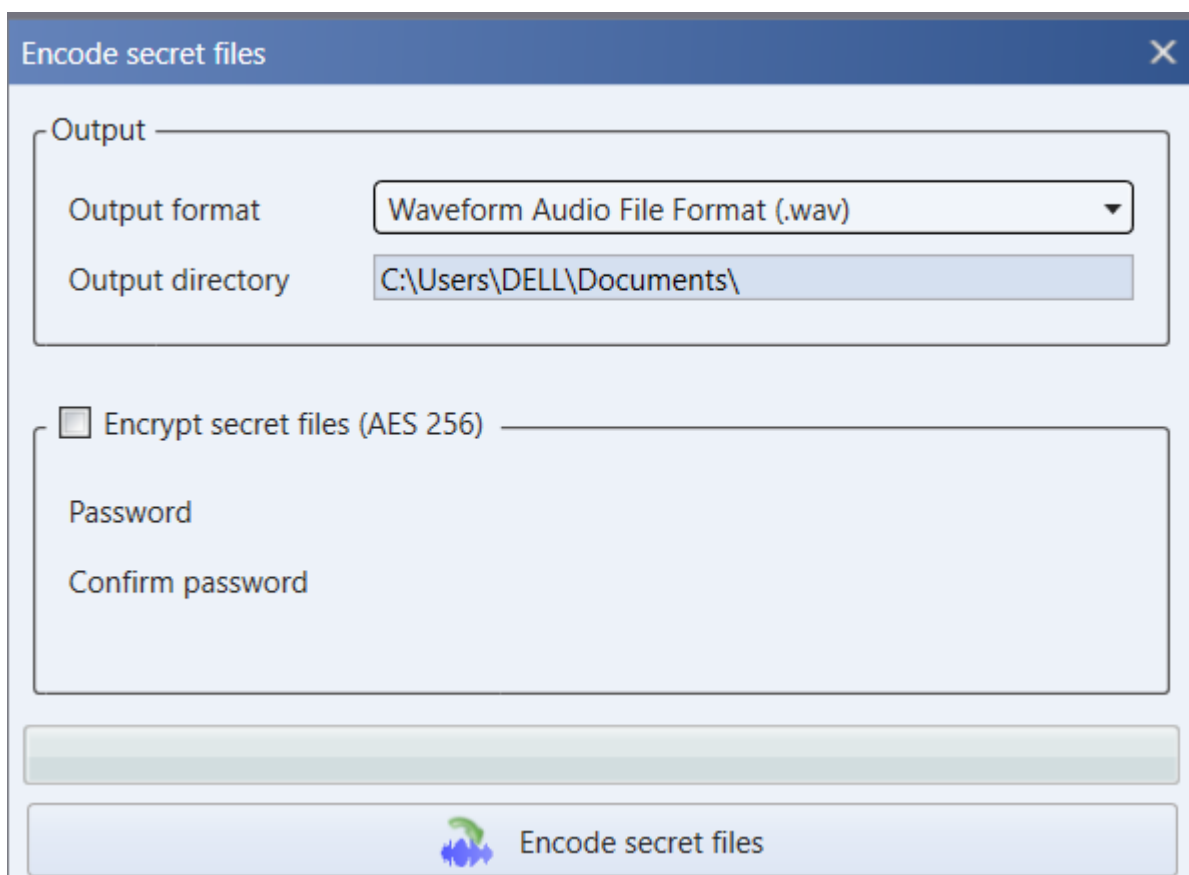
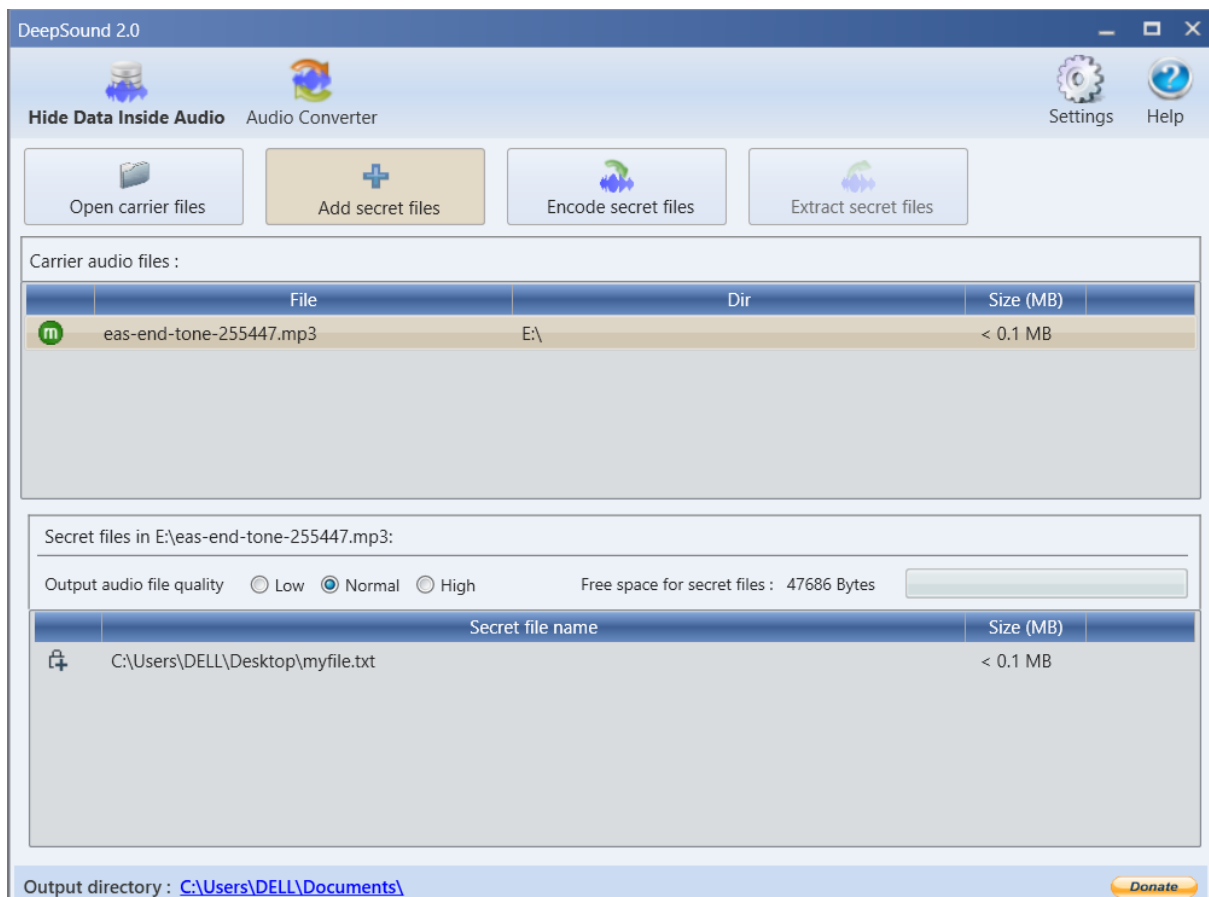
The attackers may use audio file to hide data. So in this lab learn the process of extracting hidden data from audio file by using DeepSound tool.

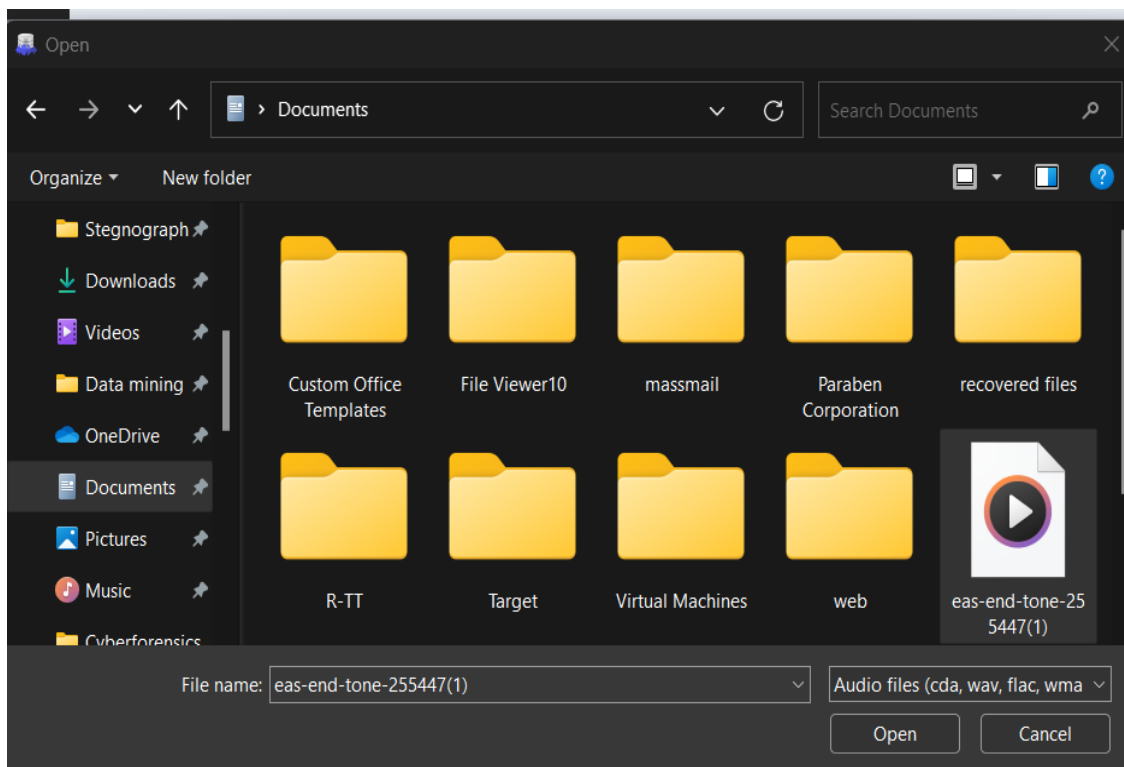
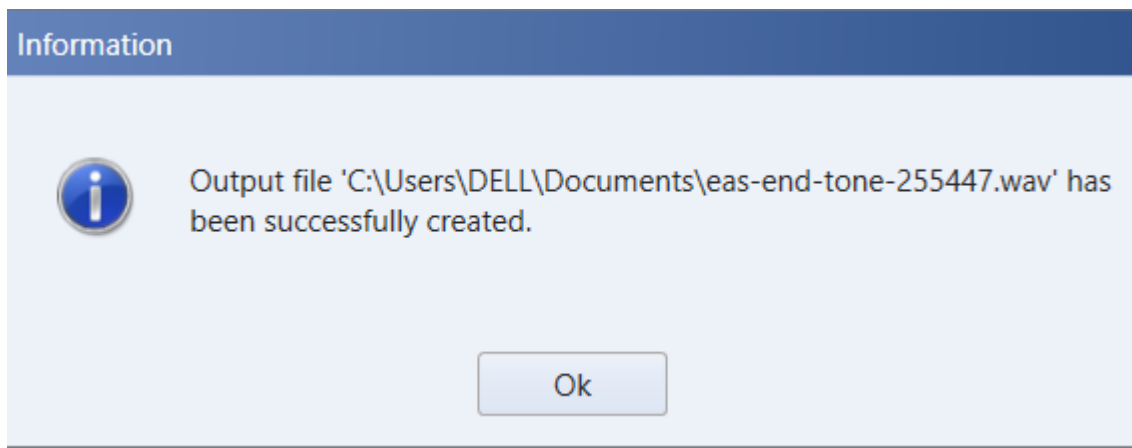




add secret file







Select the stegnography file and extract secret files.

DeepSound 2.0

Hide Data Inside Audio

Audio Converter

Settings

Help

Open carrier files

Add secret files

Encode secret files

Extract secret files

Carrier audio files :

	File	Dir	Size (MB)
	eas-end-tone-255447(1).wav	C:\Users\DELL\Documents	0.2 MB

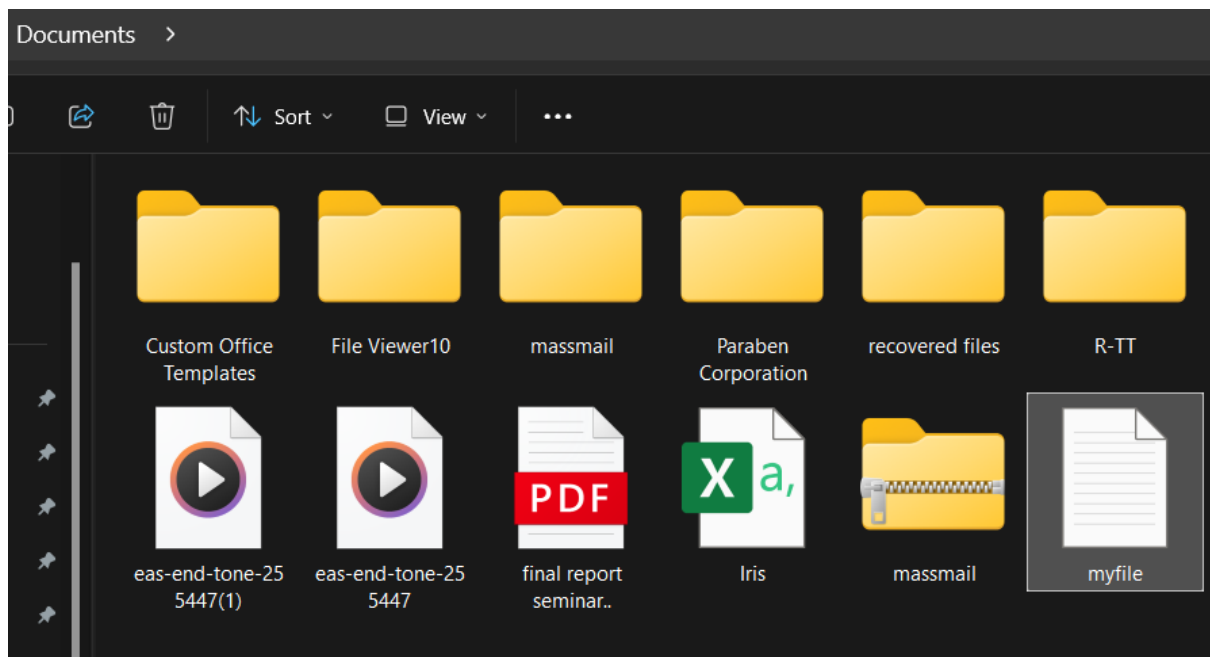
Secret files in C:\Users\DELL\Documents\eas-end-tone-255447(1).wav:

	Secret file name	Size (MB)
	myfile.txt	< 0.1 MB

Information

1 files decoded to C:\Users\DELL\Documents\

Ok



Here the extracted file is saved.