Digital Forensic and Investigation

Course Code: 5207

Submitted By

Adri Saha

Department of CSE

ID: M240105050

Table of Contents

Introduction

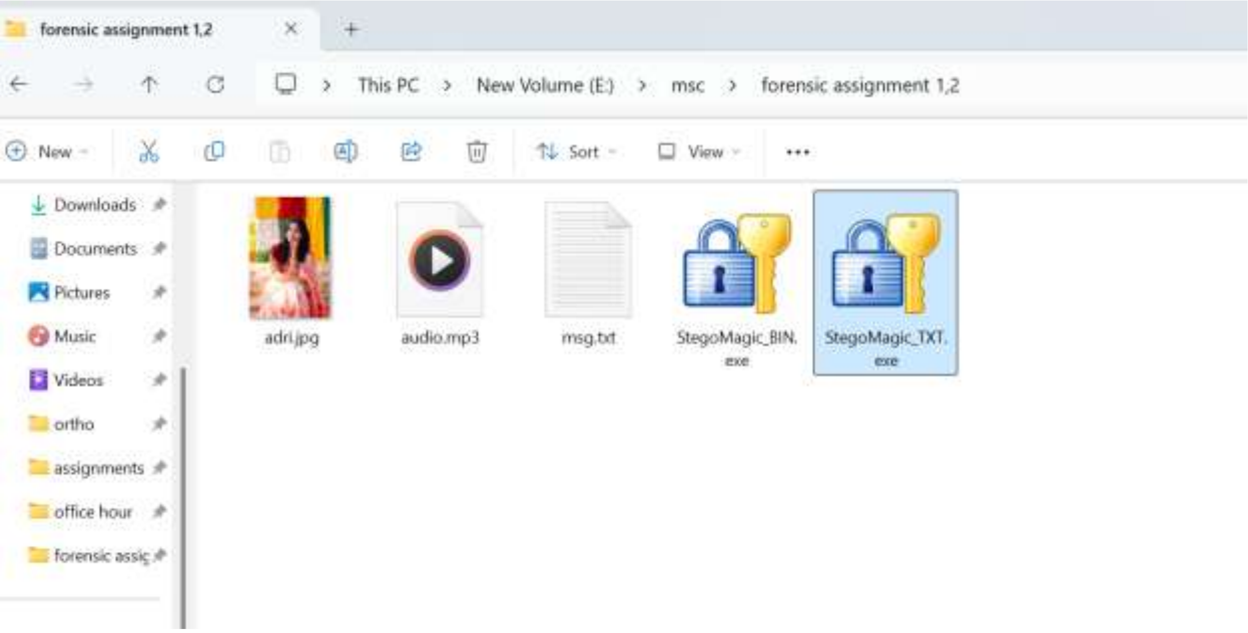
Digital forensics is the process of collecting, analyzing, and presenting digital evidence for legal or investigative purposes. It is used in civil, criminal and administrative cases to uncover and interpret data from devices like computers, smartphones and storage media.

The main goals of digital forensics are to preserve evidence, recover lost or deleted data, and analyze it to identify the facts. Digital forensics helps investigate cybercrimes, data breaches and fraud. It also assists in identifying security flaws and protecting sensitive information. By combining technology and investigation, digital forensics plays a key role in solving modern-day crimes.

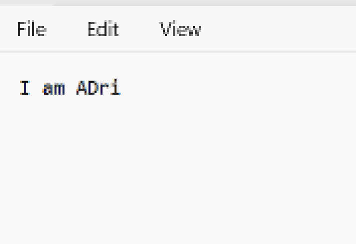
Tools such as EnCase, FTK (Forensic Toolkit) and Autopsy are commonly used to examine digital evidence and ensure its integrity. Here, I used some tools including: StegoMagic, HexWorkshop, lostmypass, EaseUS, IUWEshare.

Experiment-1: Hiding Text Data using StegoMagic Tool

Step 1: Download StegoMagic_Bin and StegoMagic_TXT tools. Open StegoMagic_TXT.exe to hide text data only.

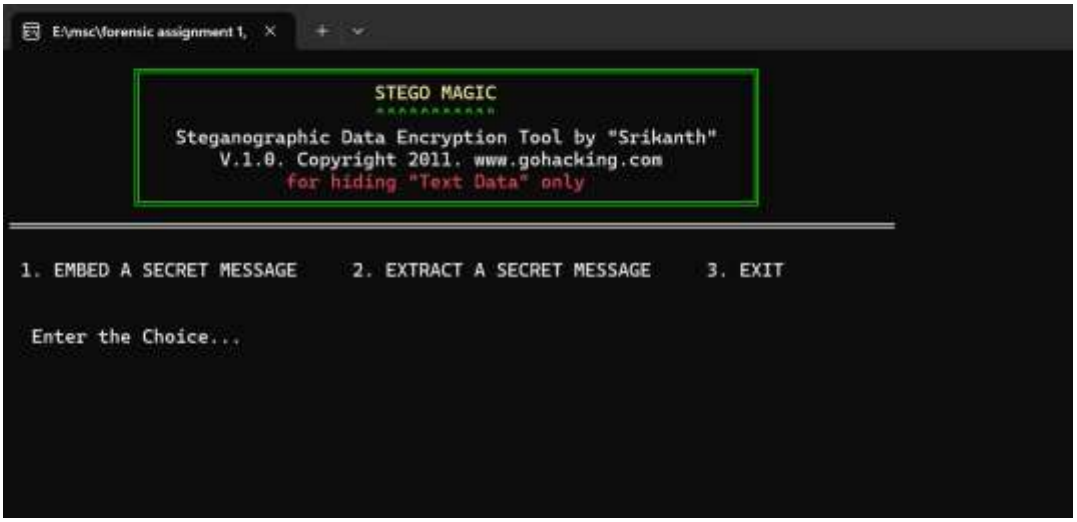


Step 2: This is a text file which I want to hide inside an image file.



```
I am ADri
```

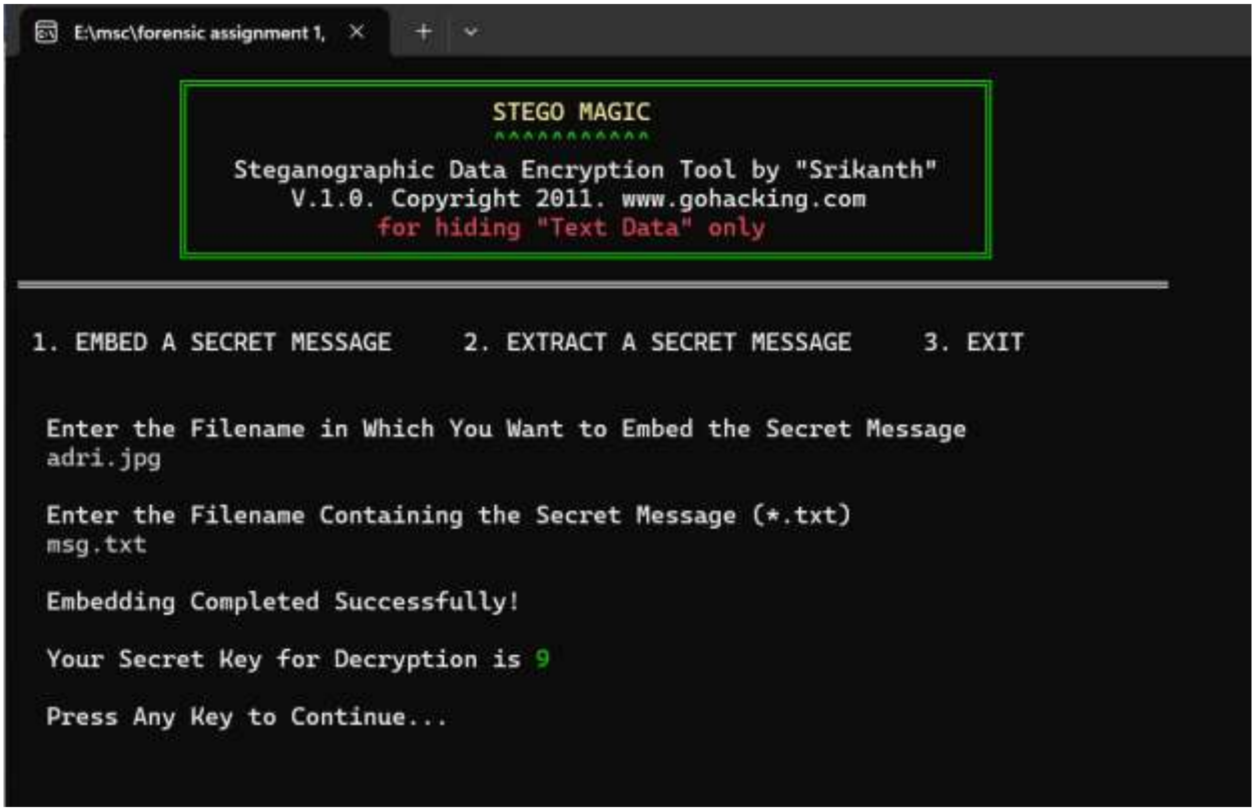
Step 3: Enter your choice that is 1.



```
                    STEGO MAGIC
                    ***********
  Steganographic Data Encryption Tool by "Srikanth"
      V.1.0. Copyright 2011. www.gohacking.com
           for hiding "Text Data" only

1. EMBED A SECRET MESSAGE    2. EXTRACT A SECRET MESSAGE    3. EXIT

 Enter the Choice...
```

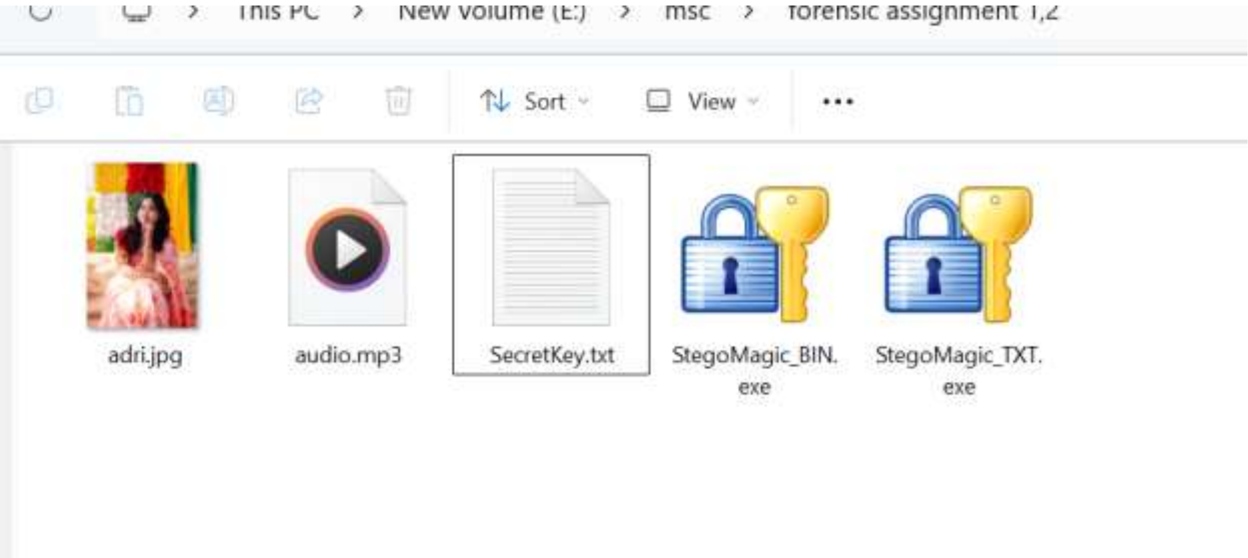
Step 4: Provide the file name first where I want to keep my secret message.

Step 5: Then enter the txt file which I want to hide. Embedding will be successfully complete and I’ll get a secret key for decryption.



```
                    STEGO MAGIC
                    ^^^^^^^^^^^
  Steganographic Data Encryption Tool by "Srikanth"
      V.1.0. Copyright 2011. www.gohacking.com
           for hiding "Text Data" only

1. EMBED A SECRET MESSAGE    2. EXTRACT A SECRET MESSAGE    3. EXIT

 Enter the Filename in Which You Want to Embed the Secret Message
 adri.jpg

 Enter the Filename Containing the Secret Message (*.txt)
 msg.txt

 Embedding Completed Successfully!

 Your Secret Key for Decryption is 9

 Press Any Key to Continue...
```

- This will generate a text file with the secret key.

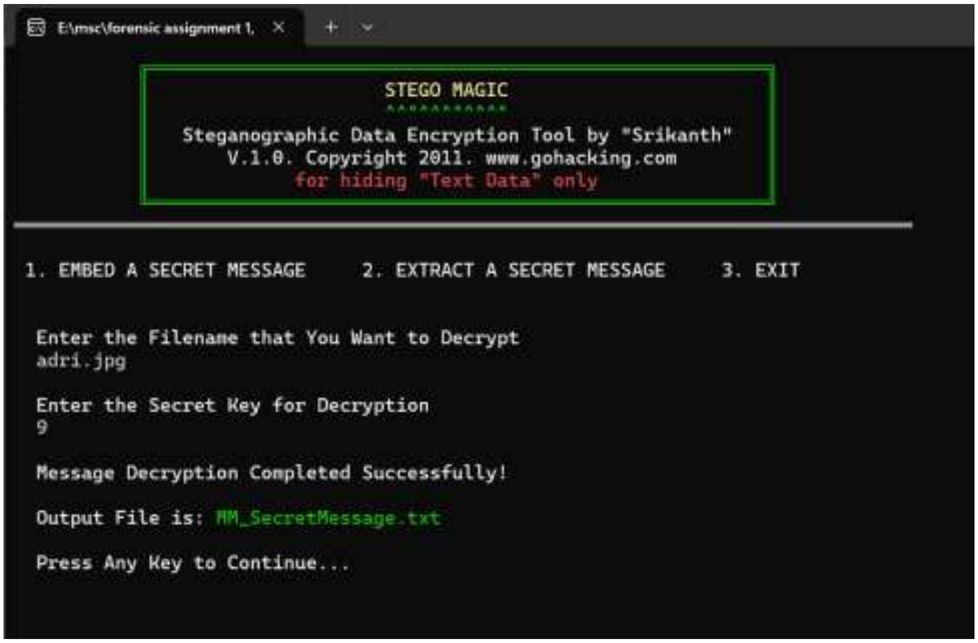


Step 6: Now delete the original text file.

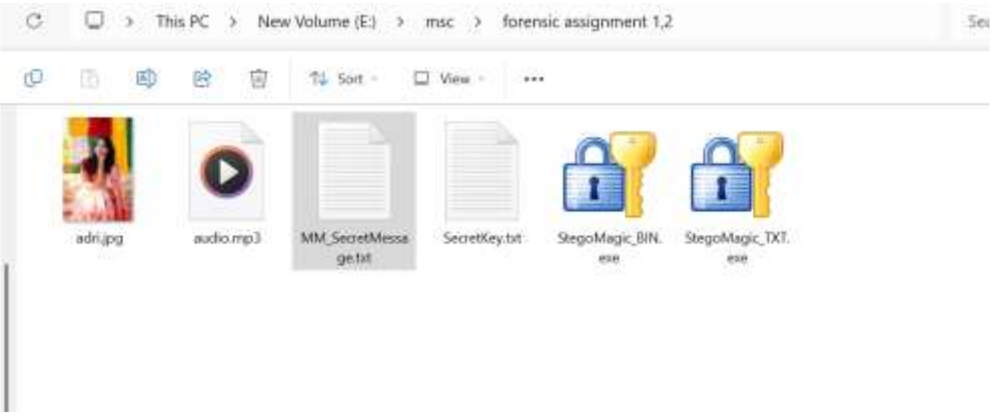
Step 7: To decrypt the message enter choice 2.

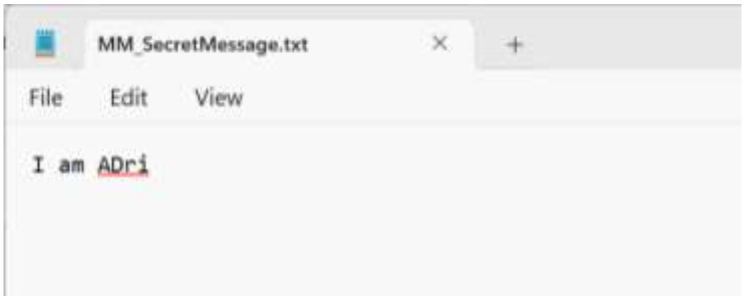
Step 8: Enter the file name from where I want to decrypt my text.

- Enter the secret key for decryption which I got.
- It will auto generate a output file named MMSecretMessage.txt
- Inside this file I'll get my old text which I deleted.



```
                    STEGO MAGIC
                    ***********
     Steganographic Data Encryption Tool by "Srikanth"
         V.1.0. Copyright 2011. www.gohacking.com
               for hiding "Text Data" only

1. EMBED A SECRET MESSAGE     2. EXTRACT A SECRET MESSAGE     3. EXIT

 Enter the Filename that You Want to Decrypt
 adri.jpg

 Enter the Secret Key for Decryption
 9

 Message Decryption Completed Successfully!

 Output File is: MM_SecretMessage.txt

 Press Any Key to Continue...
```

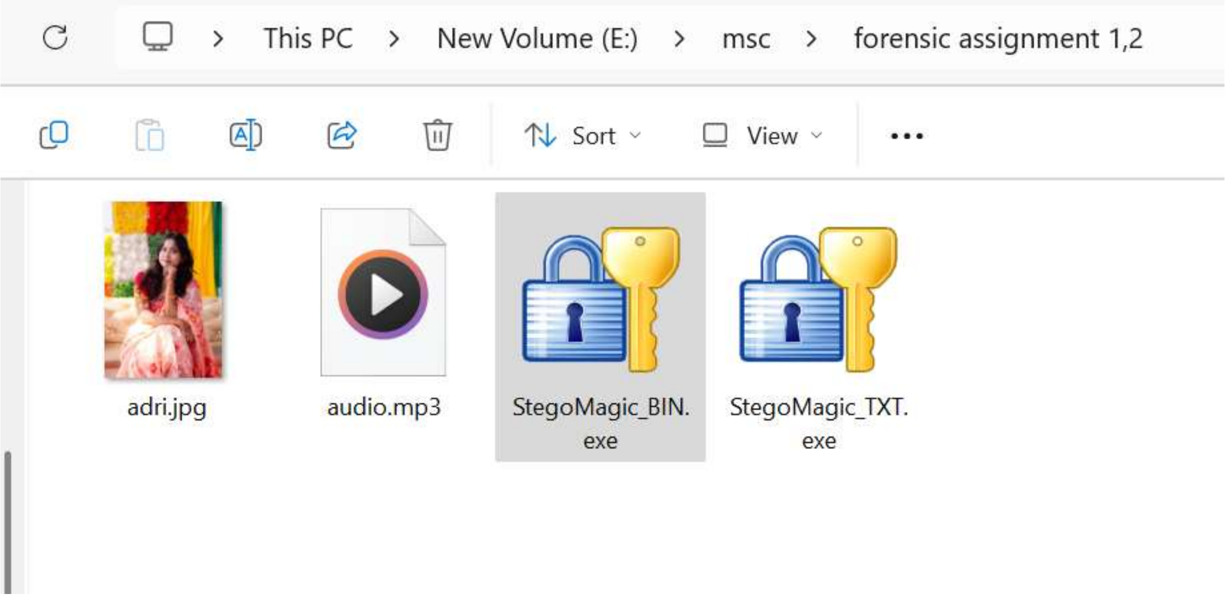




```
I am ADri
```

Experiment-2: Hiding “Binary Data”(Image, Audio/video & EXE) using StegoMagic Tool

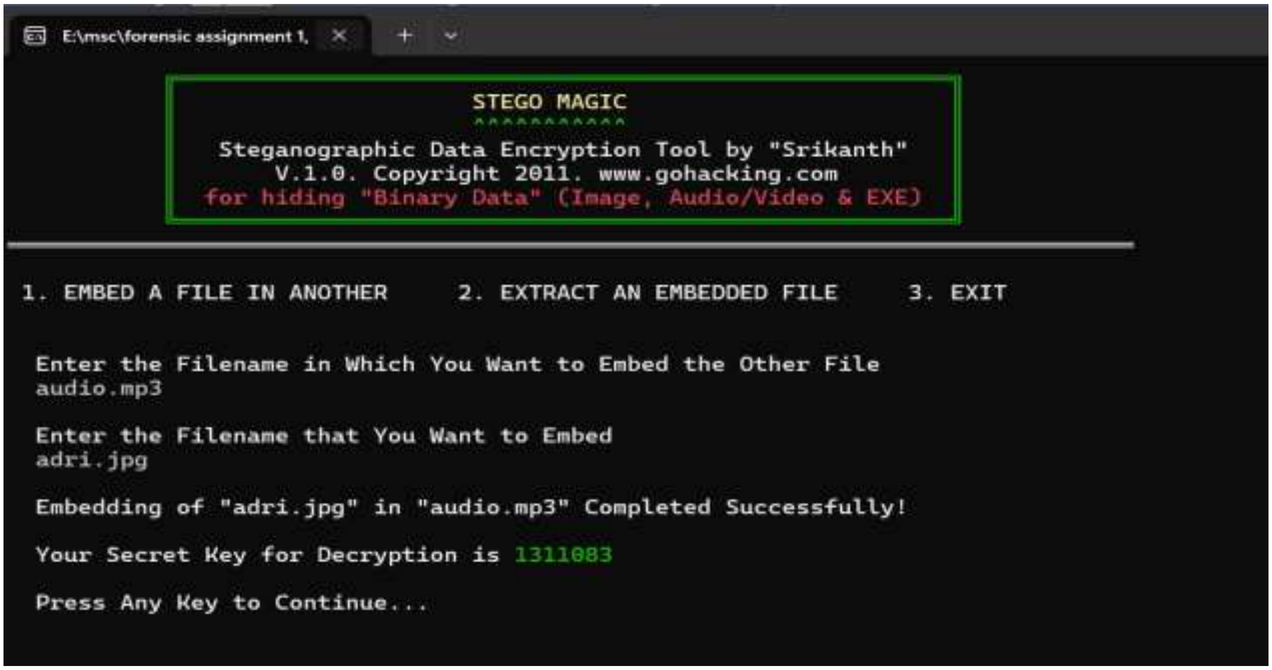
Step 1: Click on StegoMagic_BIN.exe tools to extract any data such as image, audio/video or exe.



Step 2: Enter your choice 1

Step 3: Enter the file name where I want to hide a file. Suppose, I want to hide my image file adri.jpg inside an audio file.

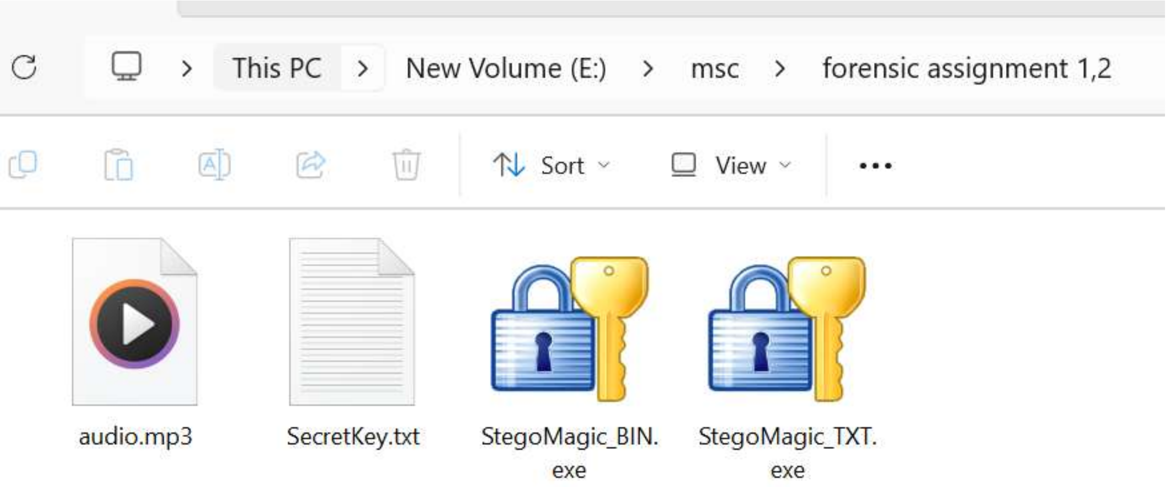
- Enter the file which I want to hide. Eg: adri.jpg.
- It will generate a secret key.



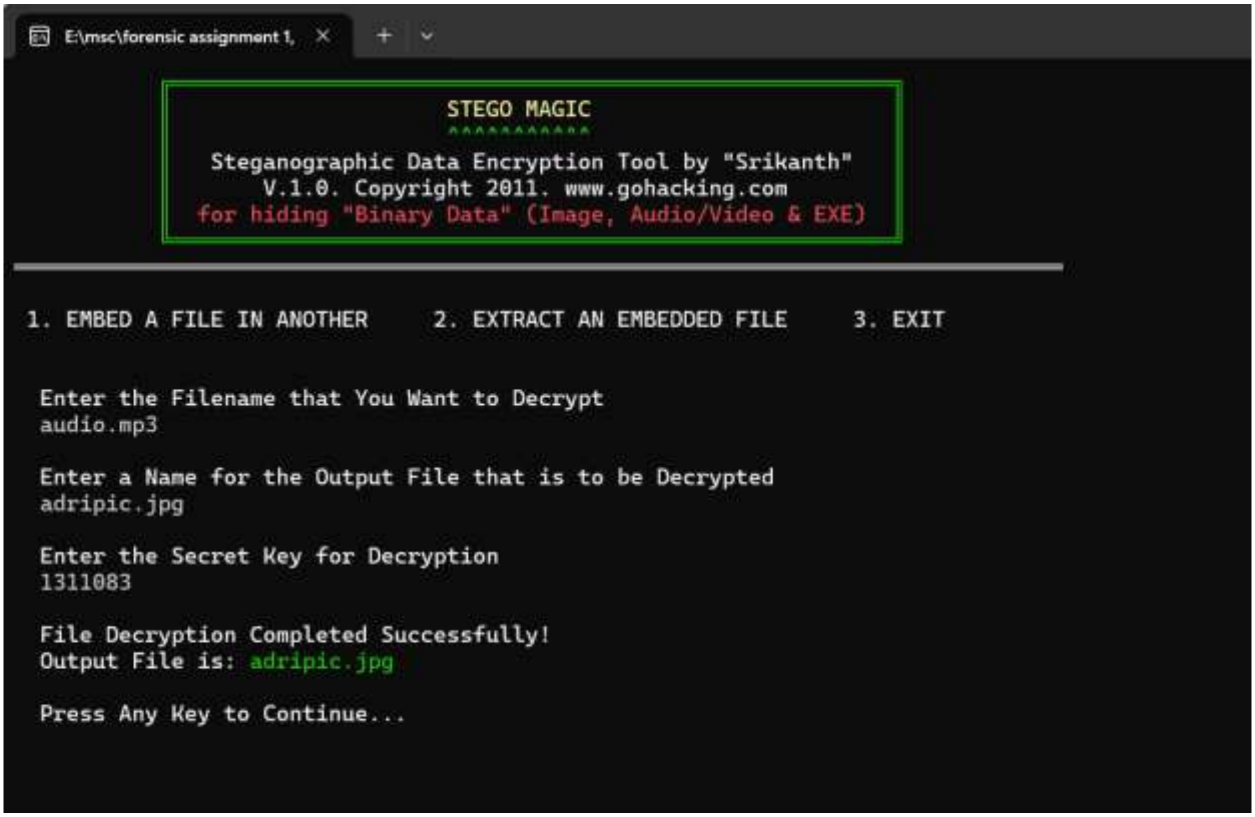
```
STEGO MAGIC
^^^^^^^^^^^

Steganographic Data Encryption Tool by "Srikanth"
V.1.0. Copyright 2011. www.gohacking.com
for hiding "Binary Data" (Image, Audio/Video & EXE)

1. EMBED A FILE IN ANOTHER     2. EXTRACT AN EMBEDDED FILE     3. EXIT

 Enter the Filename in Which You Want to Embed the Other File
 audio.mp3

 Enter the Filename that You Want to Embed
 adri.jpg

 Embedding of "adri.jpg" in "audio.mp3" Completed Successfully!

 Your Secret Key for Decryption is 1311083

 Press Any Key to Continue...
```

Step 4: Then I'll delete the original image file.

- Now I want to extract my image file from the audio.mp3.

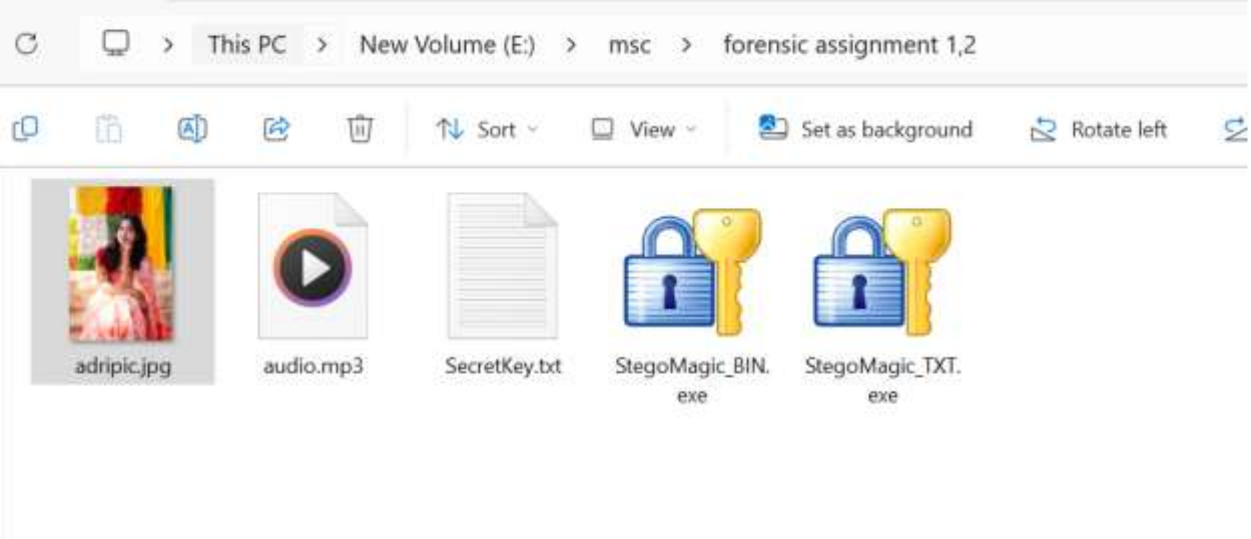


- Enter your choice 2.
- Enter the file name where the hidden image is. Eg: audio.mp3.
- Enter the output file name. Suppose: adripic.jpg.
- Enter the key for decryption.



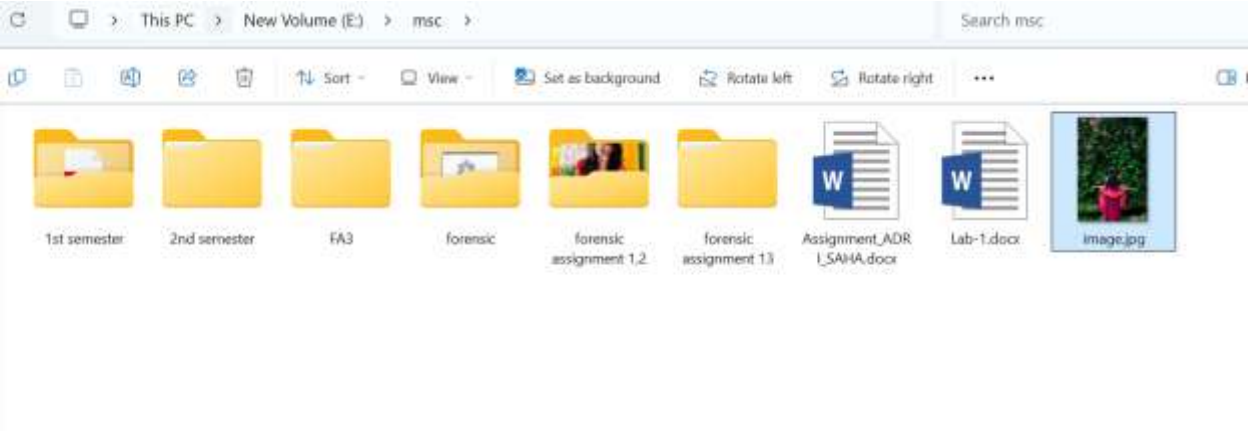
```
                              STEGO MAGIC
                              ^^^^^^^^^^^

          Steganographic Data Encryption Tool by "Srikanth"
              V.1.0. Copyright 2011. www.gohacking.com
         for hiding "Binary Data" (Image, Audio/Video & EXE)

1. EMBED A FILE IN ANOTHER     2. EXTRACT AN EMBEDDED FILE     3. EXIT

 Enter the Filename that You Want to Decrypt
 audio.mp3

 Enter a Name for the Output File that is to be Decrypted
 adripic.jpg

 Enter the Secret Key for Decryption
 1311083

 File Decryption Completed Successfully!
 Output File is: adripic.jpg

 Press Any Key to Continue...
```

- Go to the folder and see the picture is extracted from the audio file successfully.

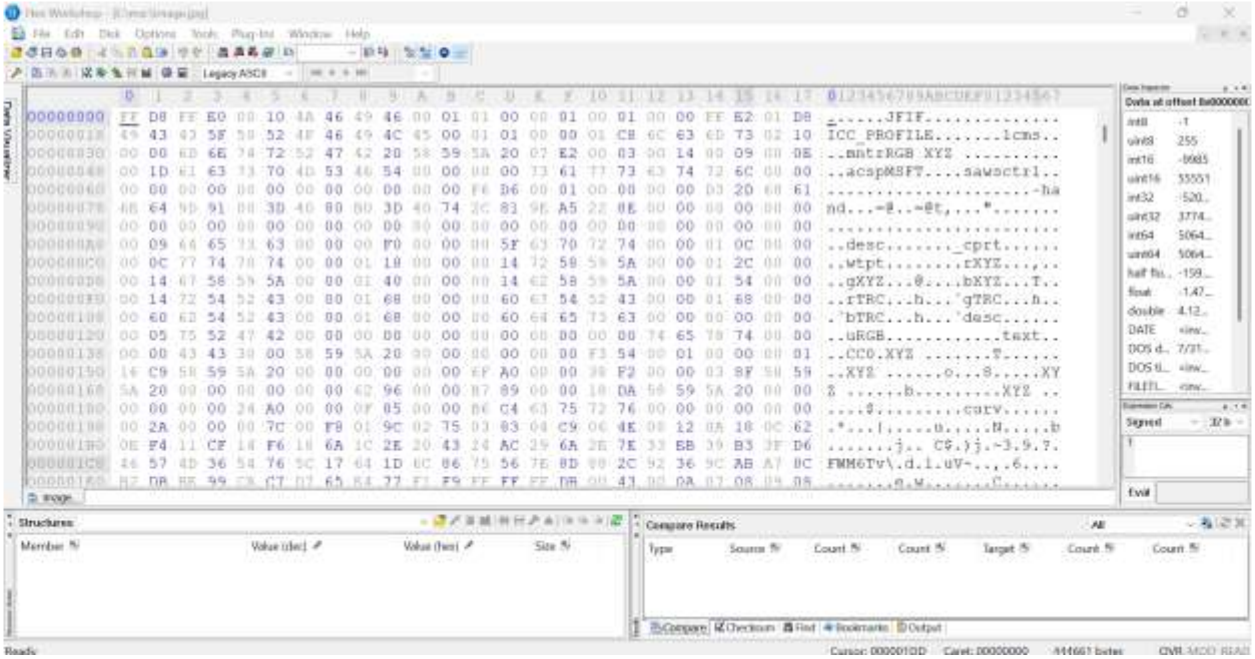


Experiment-3: File hiding using HexWorkshop:

Step-1: Let us consider we want to analyze an image file which is in format jpg as shown:



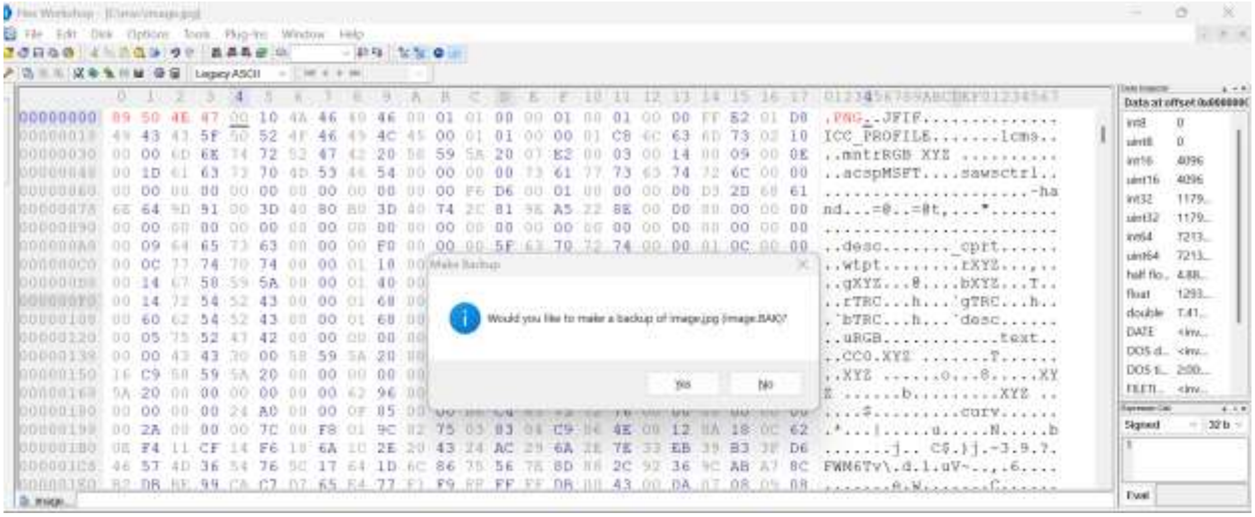
Step-2: Now if we open this file using HexWorkshop then following hex value will be appear:



```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  10 11 12 13 14 15 16 17  0123456789ABCDEF01234567
00000000  FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01 00 01 00 00 FF E2 01 D8  ......JFIF..............
00000018  49 43 43 5F 50 52 4F 46 49 4C 45 00 01 01 00 00 01 C8 6C 63 6D 73 02 10  ICC_PROFILE.......lcms..
00000030  00 00 6D 6E 74 72 52 47 42 20 58 59 5A 20 07 E2 00 03 00 14 00 09 00 0E  ..mntrRGB XYZ ..........
00000048  00 1D 61 63 73 70 4D 53 46 54 00 00 00 00 73 61 77 73 63 74 72 6C 00 00  ..acspMSFT....sawsctrl..
00000060  00 00 00 00 00 00 00 00 00 00 00 00 F6 D6 00 01 00 00 00 00 D3 2D 68 61  ......................-ha
00000078  6E 64 9D 91 00 3D 40 80 B0 3D 40 74 2C 81 9E A5 22 8E 00 00 00 00 00 00  nd...=@..=@t,...".......
00000090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
000000A8  00 09 64 65 73 63 00 00 00 F0 00 00 00 5F 63 70 72 74 00 00 01 0C 00 00  ..desc......._cprt......
000000C0  00 0C 77 74 70 74 00 00 01 18 00 00 00 14 72 58 59 5A 00 00 01 2C 00 00  ..wtpt........rXYZ...,..
000000D8  00 14 67 58 59 5A 00 00 01 40 00 00 00 14 62 58 59 5A 00 00 01 54 00 00  ..gXYZ...@....bXYZ...T..
000000F0  00 14 72 54 52 43 00 00 01 68 00 00 00 60 67 54 52 43 00 00 01 68 00 00  ..rTRC...h...`gTRC...h..
00000108  00 60 62 54 52 43 00 00 01 68 00 00 00 60 64 65 73 63 00 00 00 00 00 00  .`bTRC...h...`desc......
00000120  00 05 75 52 47 42 00 00 00 00 00 00 00 00 00 00 00 00 74 65 78 74 00 00  ..uRGB............text..
00000138  00 00 43 43 30 00 58 59 5A 20 00 00 00 00 00 00 F3 54 00 01 00 00 00 01  ..CC0.XYZ .......T......
00000150  16 C9 58 59 5A 20 00 00 00 00 00 00 6F A0 00 00 38 F2 00 00 03 8F 58 59  ..XYZ ......o...8.....XY
00000168  5A 20 00 00 00 00 00 00 62 96 00 00 B7 89 00 00 18 DA 58 59 5A 20 00 00  Z ......b.........XYZ ..
00000180  00 00 00 00 24 A0 00 00 0F 85 00 00 B6 C4 63 75 72 76 00 00 00 00 00 00  ....$.........curv......
00000198  00 2A 00 00 00 7C 00 F8 01 9C 02 75 03 83 04 C9 06 4E 08 12 0A 18 0C 62  .*...|.....u.....N.....b
000001B0  0E F4 11 CF 14 F6 18 6A 1C 2E 20 43 24 AC 29 6A 2E 7E 33 EB 39 B3 3F D6  .......j.. C$.)j.~3.9.?.
000001C8  46 57 4D 36 54 76 5C 17 64 1D 6C 86 75 56 7E 8D 88 2C 92 36 9C AB A7 8C  FWM6Tv\.d.l.uV~..,.6....
000001E0  B2 DB BE 99 CA C7 D7 65 E4 77 F1 F9 FF FF FF DB 00 43 00 0A 07 08 09 08  .......e.w.......C......
```

Here at the top of the Hex Workshop window, note that the hexadecimal values starting of original image is FF D8 FF E0 from offset 0 and the label name JFIF starting at offset 6. For different files this first 8 characters are define their file extension or type. For analyzing a file we have to know all possible formats.

Step-3: Now replace the first 8 number with 89 50 4E 47 which is the header for png image file and then save the original file.



Hex Workshop - [E:\msc\image.jpg]

```
           0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  10 11 12 13 14 15 16 17  0123456789ABCDEF01234567
00000000  89 50 4E 47 00 10 4A 46 49 46 00 01 01 00 00 01 00 01 00 00 FF E2 01 D0  .PNG_..JFIF.............
00000018  49 43 43 5F 50 52 4F 46 49 4C 45 00 01 01 00 00 01 C8 6C 63 6D 73 02 10  ICC_PROFILE.......lcms..
00000030  00 00 6D 6E 74 72 52 47 42 20 58 59 5A 20 07 E2 00 03 00 14 00 09 00 0E  ..mntrRGB XYZ ..........
00000048  00 1D 61 63 73 70 4D 53 46 54 00 00 00 00 73 61 77 73 63 74 72 6C 00 00  ..acspMSFT....sawsctrl..
00000060  00 00 00 00 00 00 00 00 00 00 00 00 F6 D6 00 01 00 00 00 00 D3 2D 68 61  ......................-ha
00000078  6E 64 9D 91 00 3D 40 80 B0 3D 40 74 2C 81 9E A5 22 8E 00 00 00 00 00 00  nd...=@..=@t,...".......
00000090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
000000A8  00 09 64 65 73 63 00 00 00 F0 00 00 00 5F 63 70 72 74 00 00 01 0C 00 00  ..desc......._cprt......
000000C0  00 0C 77 74 70 74 00 00 01 18 00                                         ..wtpt........rXYZ......
000000D8  00 14 67 58 59 5A 00 00 01 40 00                                         ..gXYZ...@....bXYZ...T..
000000F0  00 14 72 54 52 43 00 00 01 68 00                                         ..rTRC...h...'gTRC...h..
00000108  00 60 62 54 52 43 00 00 01 68 00                                         .`bTRC...h...`desc......
00000120  00 05 75 52 47 42 00 00 00 00 00                                         ..uRGB..............text..
00000138  00 00 43 43 30 00 58 59 5A 20 00                                         ..CC0.XYZ .......T......
00000150  16 C9 58 59 5A 20 00 00 00 00 00                                         ..XYZ ......o...8.....XY
00000168  5A 20 00 00 00 00 00 00 62 96 00                                         Z ......b.........XYZ ..
00000180  00 00 00 00 24 A0 00 00 0F 85 00                                         ....$.........curv......
00000198  00 2A 00 00 00 7C 00 F8 01 9C 02 75 03 83 04 C9 06 4E 00 12 0A 18 0C 62  .*...|.....u.....N.....b
000001B0  0E F4 11 CF 14 F6 18 6A 1C 2E 20 43 24 AC 29 6A 2E 7E 33 EB 39 B3 3F D6  .......j.. C$.)j.~3.9.?.
000001C8  46 57 4D 36 54 76 5C 17 64 1D 6C 86 75 56 7E 8D 88 2C 92 36 9C AB A7 8C  FWM6Tv\.d.l.uV~..,.6....
000001E0  B2 DB BE 99 CA C7 D7 65 E4 77 F1 F9 FF FF FF DB 00 43 00 DA 07 08 05 08  .......e.w.......C......
```

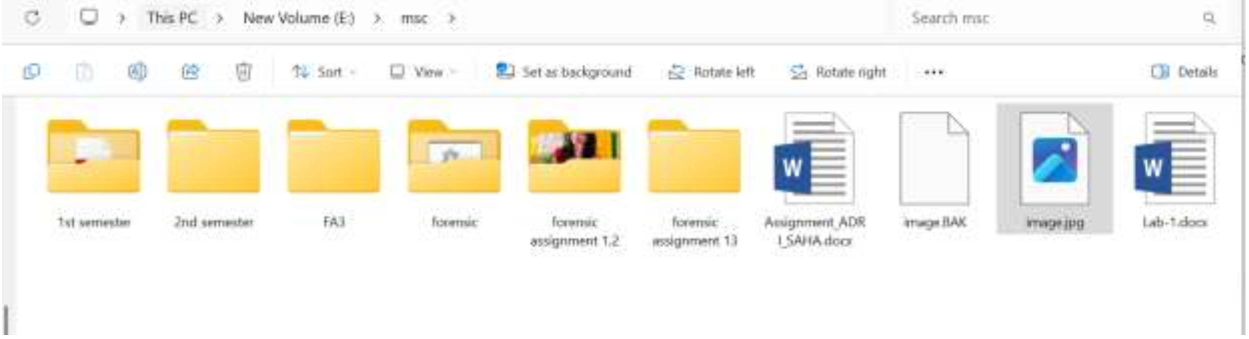
Make Backup

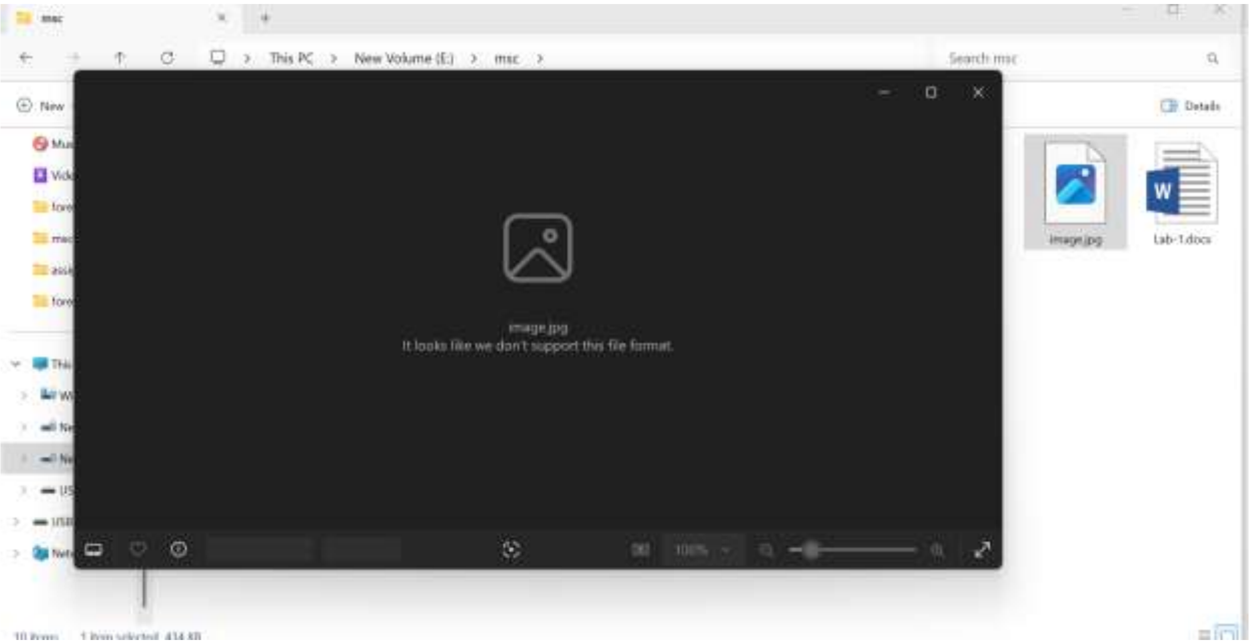
Would you like to make a backup of image.jpg (image.BAK)?

Data at offset 0x00000000

int8	0
uint8	0
int16	4096
uint16	4096
int32	1179...
uint32	1179...
int64	7213...
uint64	7213...
half flo...	4.88...
float	1293...
double	7.41...
DATE	<inv...
DOS d...	<inv...
DOS t...	2:00...
FILETI...	<inv...

Step-4: After saving the file our main image will be damaged and it will not open any program for image file preview, as follows:



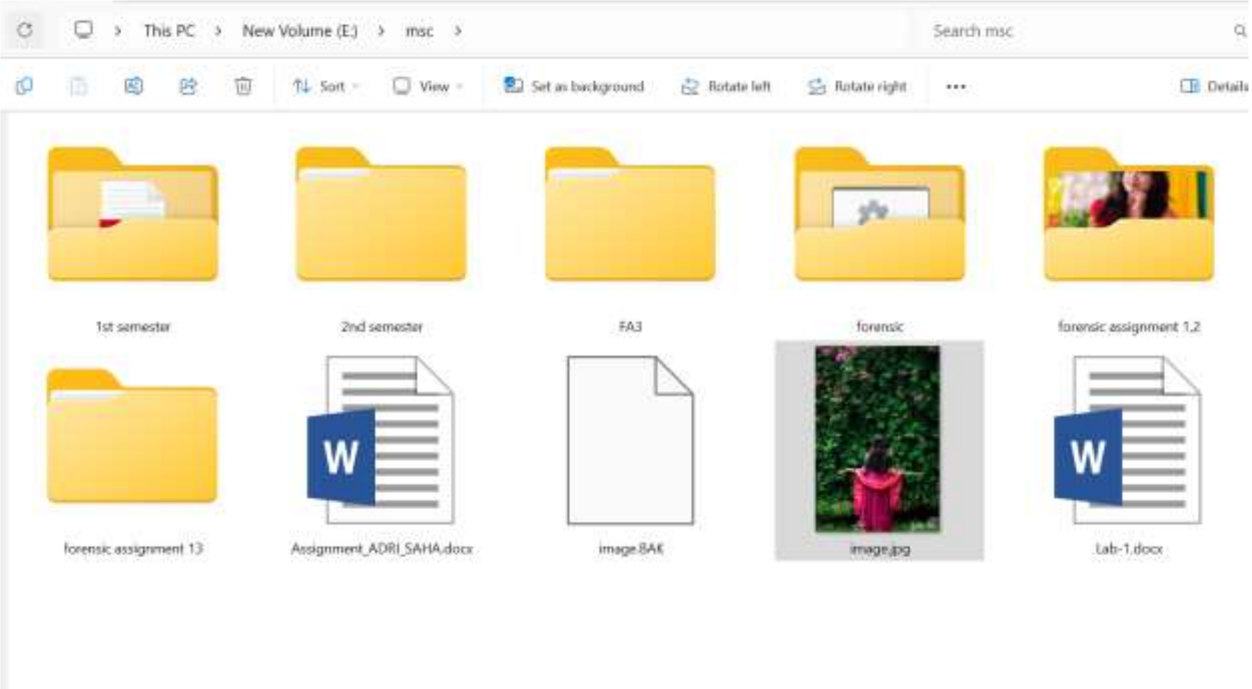


msc
This PC > New Volume (E:) > msc >
Search msc
New
Details
image.jpg
Lab-1.docx
100%
10 items 1 item selected 434 KB

image.jpg

It looks like we don't support this file format.

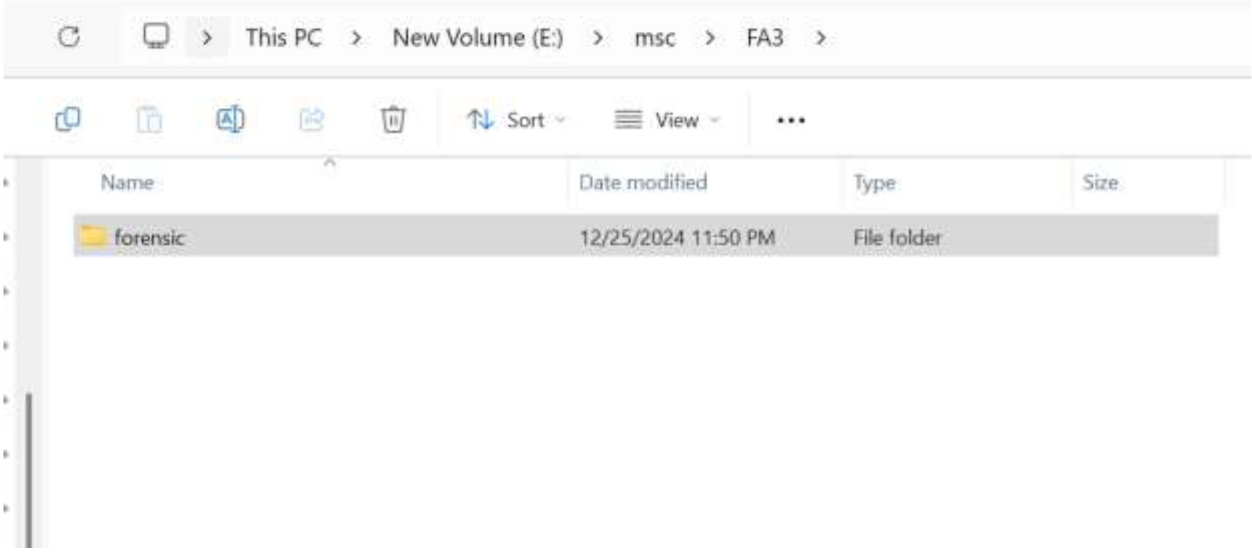
Step-5: For reconstruct the damaged file again we have to replace the first 8 values with FF D8 FF E0 which is the jpg header, then it will be visible and can open with image viewer:



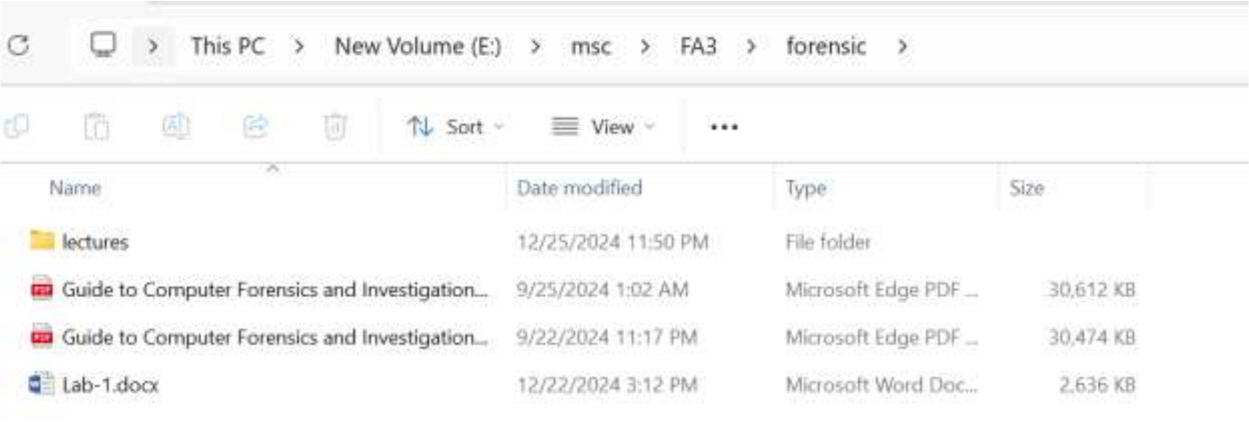
In this way we can hide a file and then reconstract it again. Thus we can maintain privacy of our confidential files.

Experment-4: Folder Lock and Unlock Using Command Prompt

Step 1: Create a folder named forensic. Inside this folder there are some files.

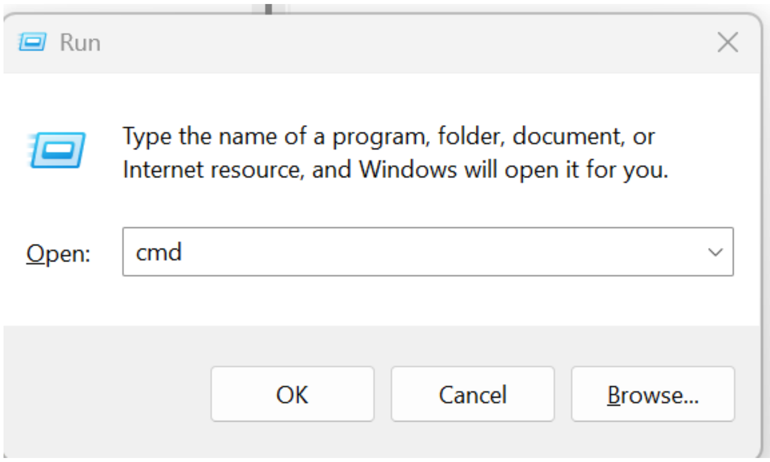


Name	Date modified	Type	Size
forensic	12/25/2024 11:50 PM	File folder	



Name	Date modified	Type	Size
lectures	12/25/2024 11:50 PM	File folder	
Guide to Computer Forensics and Investigation...	9/25/2024 1:02 AM	Microsoft Edge PDF ...	30,612 KB
Guide to Computer Forensics and Investigation...	9/22/2024 11:17 PM	Microsoft Edge PDF ...	30,474 KB
Lab-1.docx	12/22/2024 3:12 PM	Microsoft Word Doc...	2,636 KB

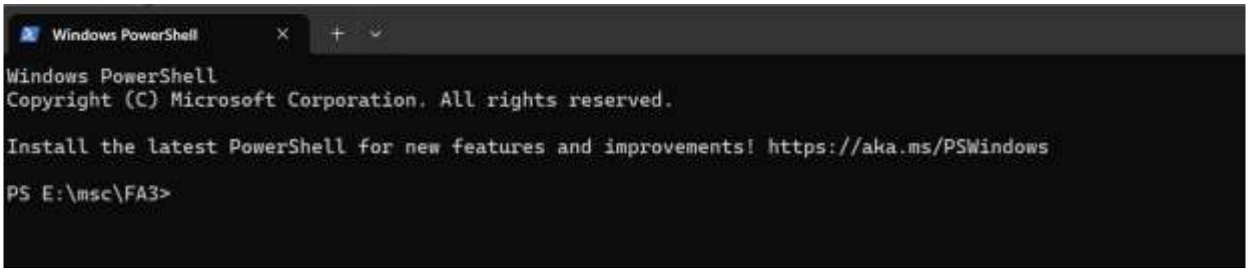
Step 2: Type win+R and write command cmd. Or,



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

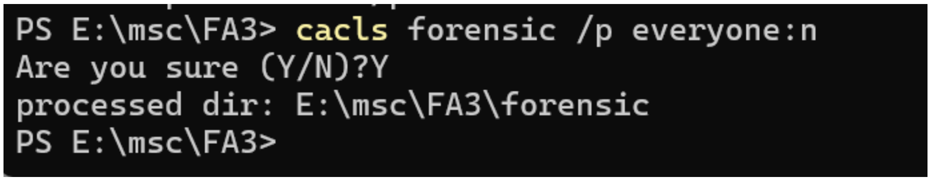
Step 3: Open the terminal from this folder.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS E:\msc\FA3>
```

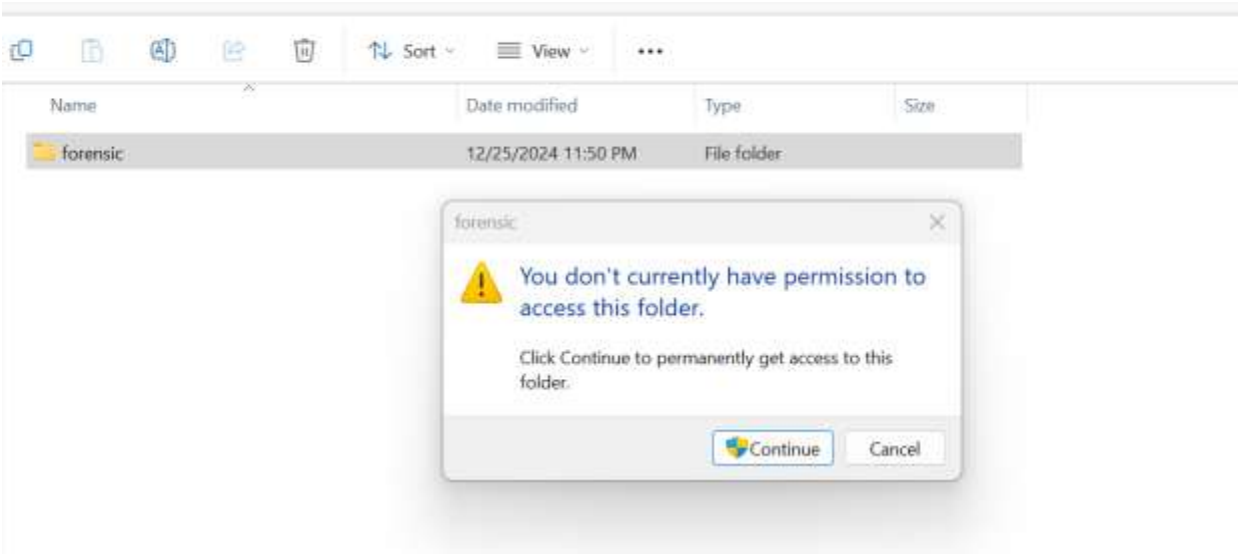
Step 4: Write **cacls file_name /p everyone: n**

Here: **cacls forensic /p everyone:n**



```
PS E:\msc\FA3> cacls forensic /p everyone:n
Are you sure (Y/N)?Y
processed dir: E:\msc\FA3\forensic
PS E:\msc\FA3>
```

Step 5: Now the folder is locked. If I want to excess this folder it will show this error.



Name	Date modified	Type	Size
forensic	12/25/2024 11:50 PM	File folder	

forensic

You don't currently have permission to access this folder.

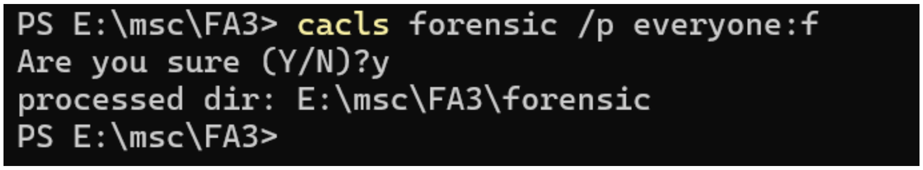
Click Continue to permanently get access to this folder.

Step 6: To unlock this folder again,

- Go to cmd prompt.
- Type

cacls forensic /p everyone:f

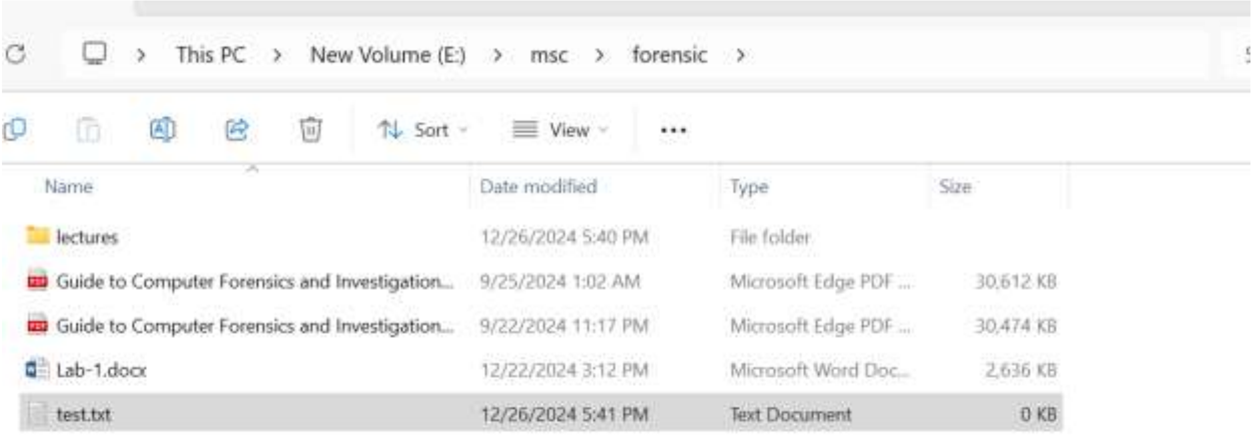
- Click Y for Yes.



```
PS E:\msc\FA3> cacls forensic /p everyone:f
Are you sure (Y/N)?y
processed dir: E:\msc\FA3\forensic
PS E:\msc\FA3>
```

Experiment-5: Protect a folder with Password using batch file:

Step 1: 1st we choose a folder. Then we create a Text file into that folder.



This PC > New Volume (E:) > msc > forensic >

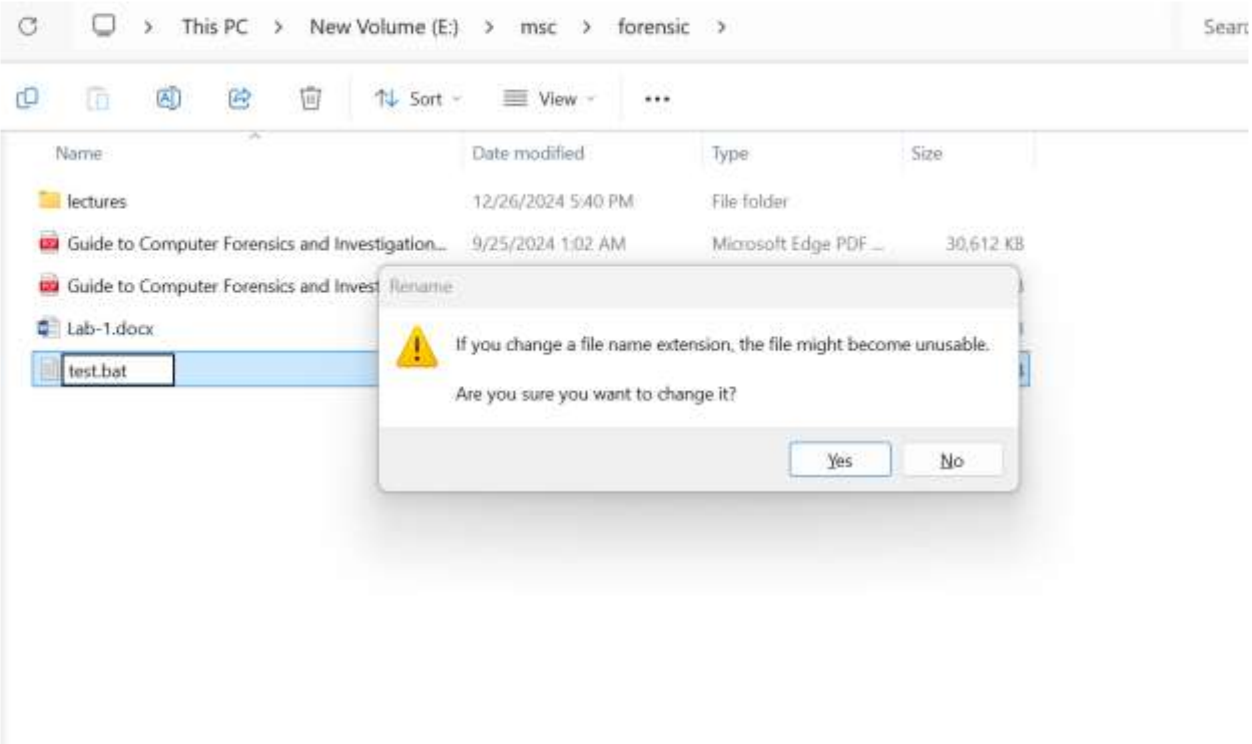
Name	Date modified	Type	Size
lectures	12/26/2024 5:40 PM	File folder	
Guide to Computer Forensics and Investigation...	9/25/2024 1:02 AM	Microsoft Edge PDF ...	30,612 KB
Guide to Computer Forensics and Investigation...	9/22/2024 11:17 PM	Microsoft Edge PDF ...	30,474 KB
Lab-1.docx	12/22/2024 3:12 PM	Microsoft Word Doc...	2,636 KB
test.txt	12/26/2024 5:41 PM	Text Document	0 KB

Step 2: Then we write down a script on that Txt file and Set a Password & save it.

```
@ECHO OFF
if EXIST "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}" goto UNLOCK
if NOT EXIST Private goto MDPrivate
:CONFIRM
echo Are you sure to lock this folder? (Y/N)
set/p "cho=>"
if %cho%==Y goto LOCK
if %cho%==y goto LOCK
if %cho%==n goto END
if %cho%==N goto END
echo Invalid choice.
goto CONFIRM
:LOCK
ren Private "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
attrib +h +s "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
echo Folder locked
goto End
:UNLOCK
```

```
        echo Enter password to Unlock Your Secure Folder
        set/p "pass=>"
        if NOT %pass%== 1234 goto FAIL
        attrib -h -s "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
        ren "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}" Private
        echo Folder Unlocked successfully
        goto End
        :FAIL
        echo Invalid password
        goto end
        :MDPrivate
        md Private
        echo Private created successfully
        goto End
:End
```

Step 3: Now we change the text file extension from .txt to .bat. when it changes, it will give us permission. And it creates a private Folder. Then we move all files & data into that private folder.



lectures 12/26/2024 5:40 PM File folder

Guide to Computer Forensics and Investigation... 9/25/2024 1:02 AM Microsoft Edge PDF ... 30,612 KB

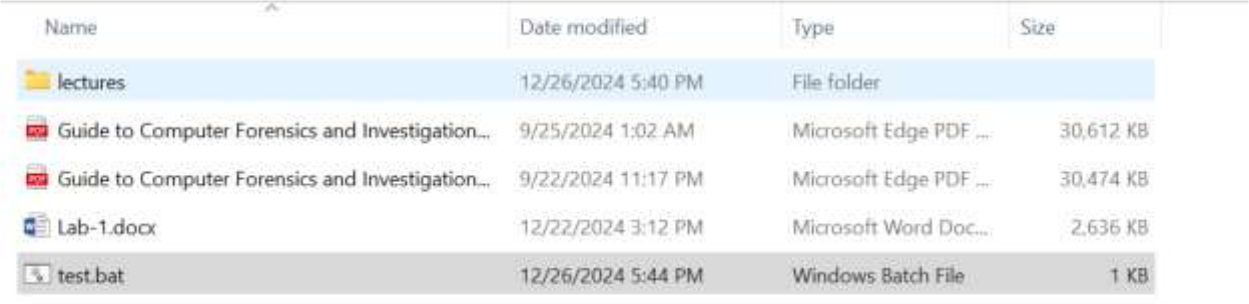
Guide to Computer Forensics and Invest

Lab-1.docx

test.bat

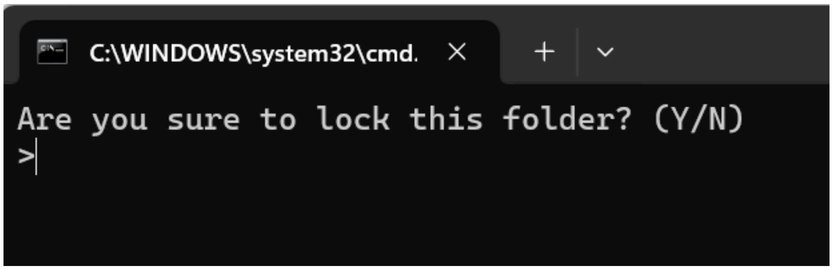
If you change a file name extension, the file might become unusable.

Are you sure you want to change it?

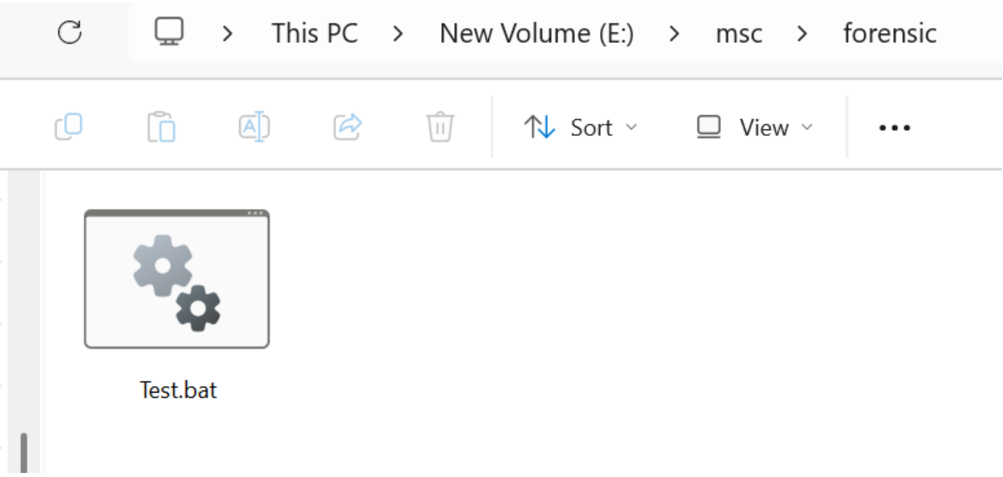


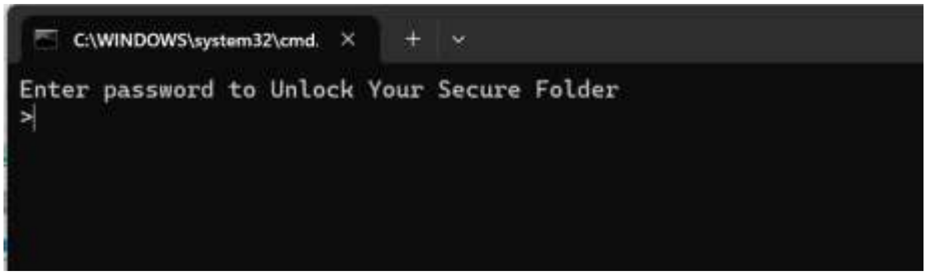
Name	Date modified	Type	Size
lectures	12/26/2024 5:40 PM	File folder	
Guide to Computer Forensics and Investigation...	9/25/2024 1:02 AM	Microsoft Edge PDF ...	30,612 KB
Guide to Computer Forensics and Investigation...	9/22/2024 11:17 PM	Microsoft Edge PDF ...	30,474 KB
Lab-1.docx	12/22/2024 3:12 PM	Microsoft Word Doc...	2,636 KB
test.bat	12/26/2024 5:44 PM	Windows Batch File	1 KB

Step 4: Now we click the .bat file, then open a Command port & it takes permission from the user. When we select yes. The folder becomes locked and files are hidden. Again, when we click the .bat file, Command ports are open again and it wants a password. When the password match the folder will be open otherwise it will be encrypted.

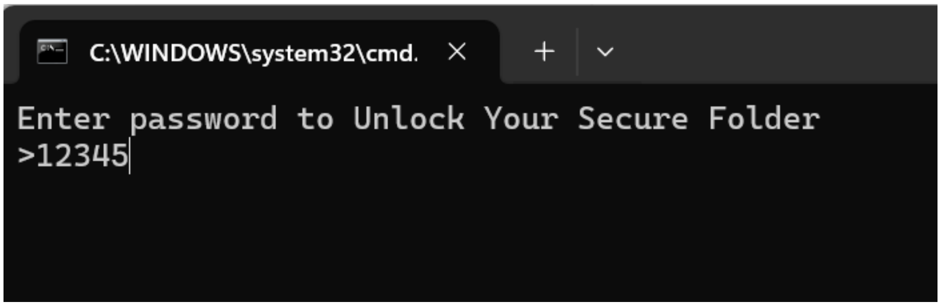


```
Are you sure to lock this folder? (Y/N)
>
```

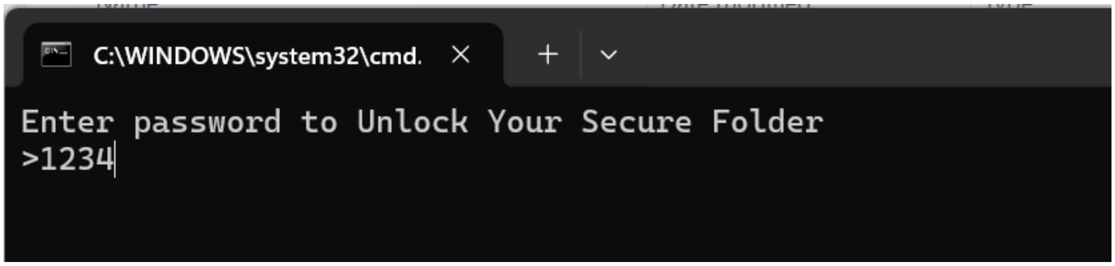




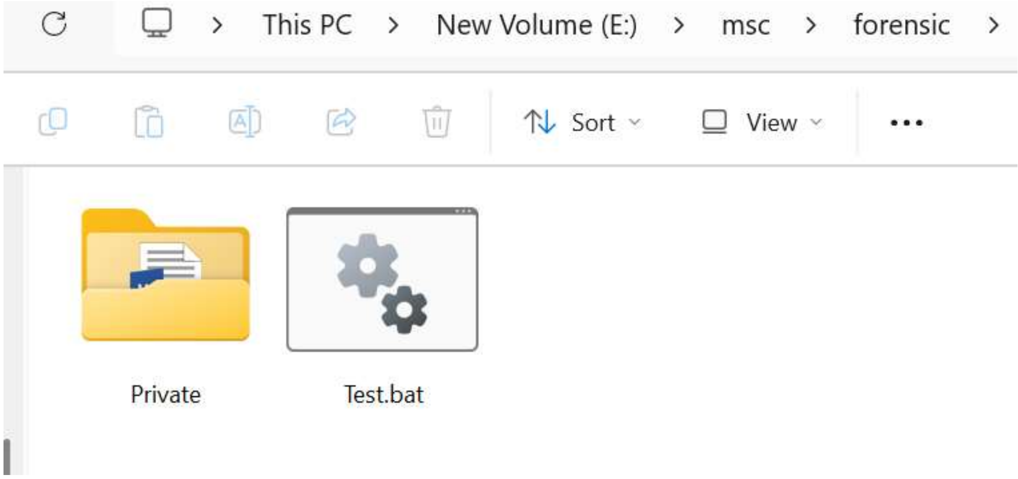
```
Enter password to Unlock Your Secure Folder
>
```



```
Enter password to Unlock Your Secure Folder
>12345
```



```
Enter password to Unlock Your Secure Folder
>1234
```



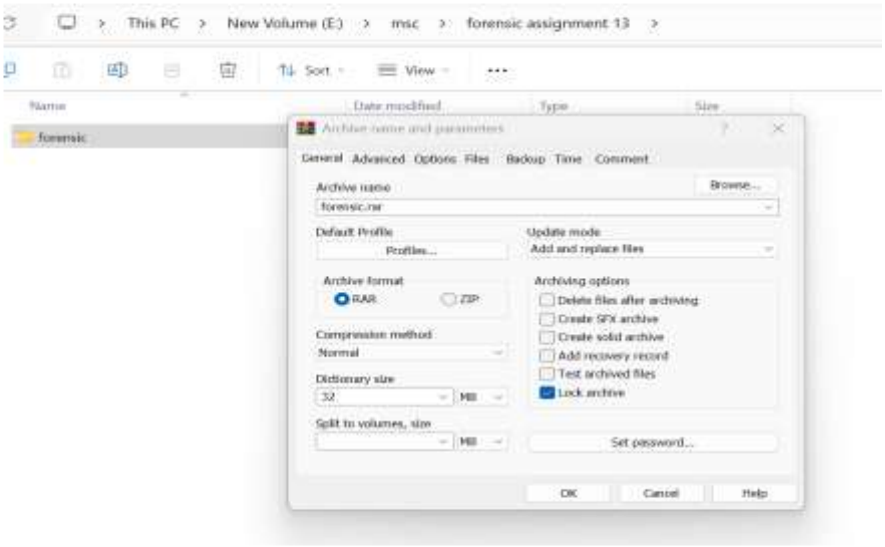
Experiment-6: Protect Archive File Using Password:

Step 1: Right click on the folder.

Step 2: Click on WinRar--- add to archive.

Step 3: Archive format RAR, advanced option: mark on lock archive.

Step 4: Click on set password.



This PC > New Volume (E:) > msc > forensic assignment 13 >

Archive name and parameters

Archive name: forensic.rar

Update mode: Add and replace files

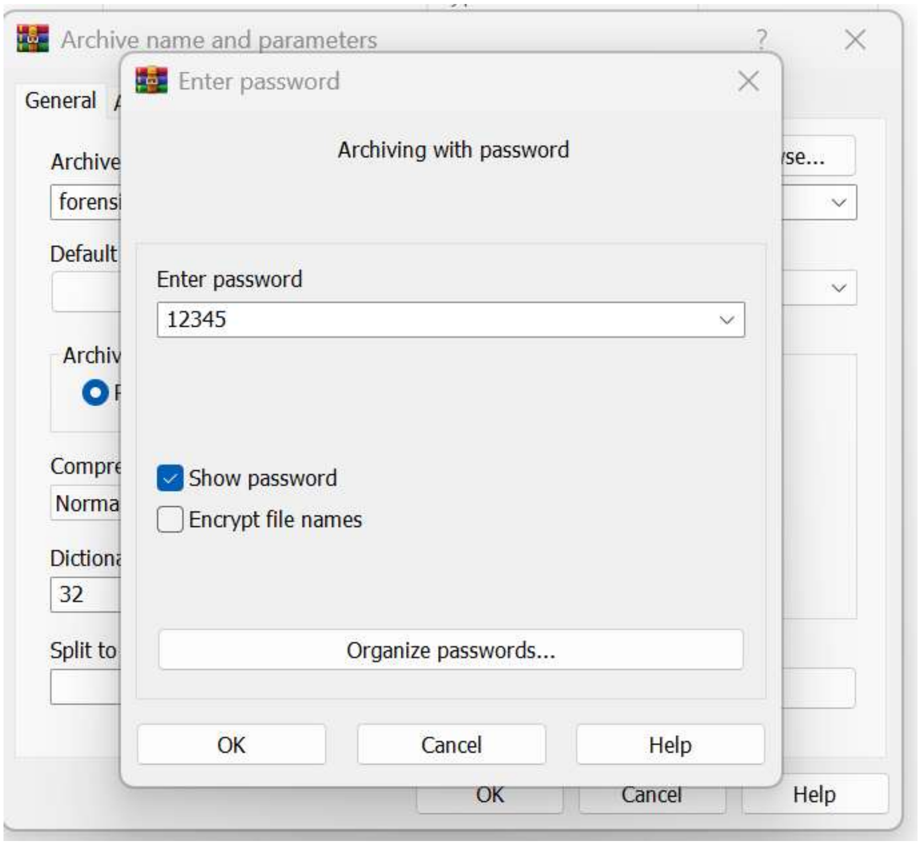
Archive format: ● RAR ○ ZIP

Compression method: Normal

Dictionary size: 32 MB

Archiving options:
- □ Delete files after archiving
- □ Create SFX archive
- □ Create solid archive
- □ Add recovery record
- □ Test archived files
- ☑ Lock archive

Step 5: Write your password. Suppose: 12345. Click on ok.



Enter password

Archiving with password

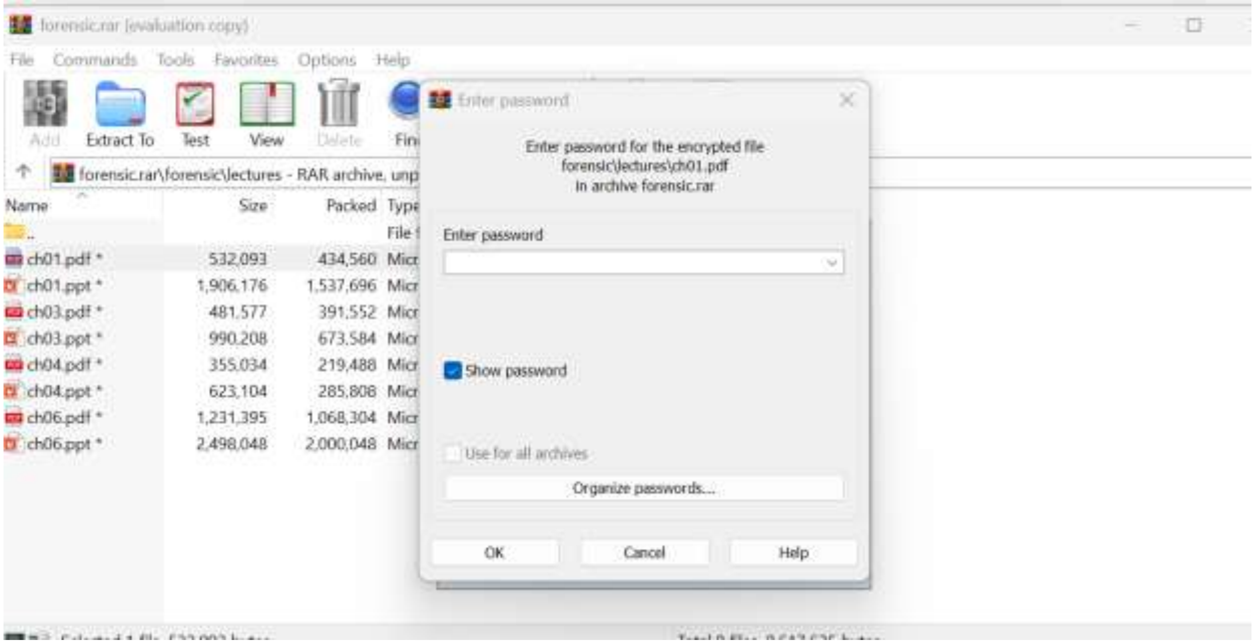
Enter password: 12345

☑ Show password

□ Encrypt file names

Step 6: Now, to open the files it will ask to enter your password.

Step 7: If you will type the wrong password it will be restricted.



forensic.rar\forensic\lectures - RAR archive, unp

Name	Size	Packed	Type
..			File f
ch01.pdf *	532,093	434,560	Micr
ch01.ppt *	1,906,176	1,537,696	Micr
ch03.pdf *	481,577	391,552	Micr
ch03.ppt *	990,208	673,584	Micr
ch04.pdf *	355,034	219,488	Micr
ch04.ppt *	623,104	285,808	Micr
ch06.pdf *	1,231,395	1,068,304	Micr
ch06.ppt *	2,498,048	2,000,048	Micr

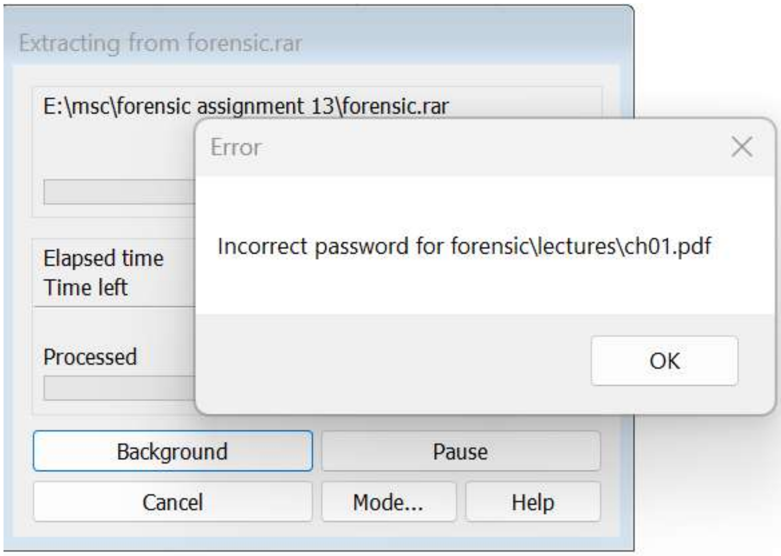
Enter password

Enter password for the encrypted file
forensic\lectures\ch01.pdf
in archive forensic.rar

Enter password

☑ Show password

☐ Use for all archives



Extracting from forensic.rar

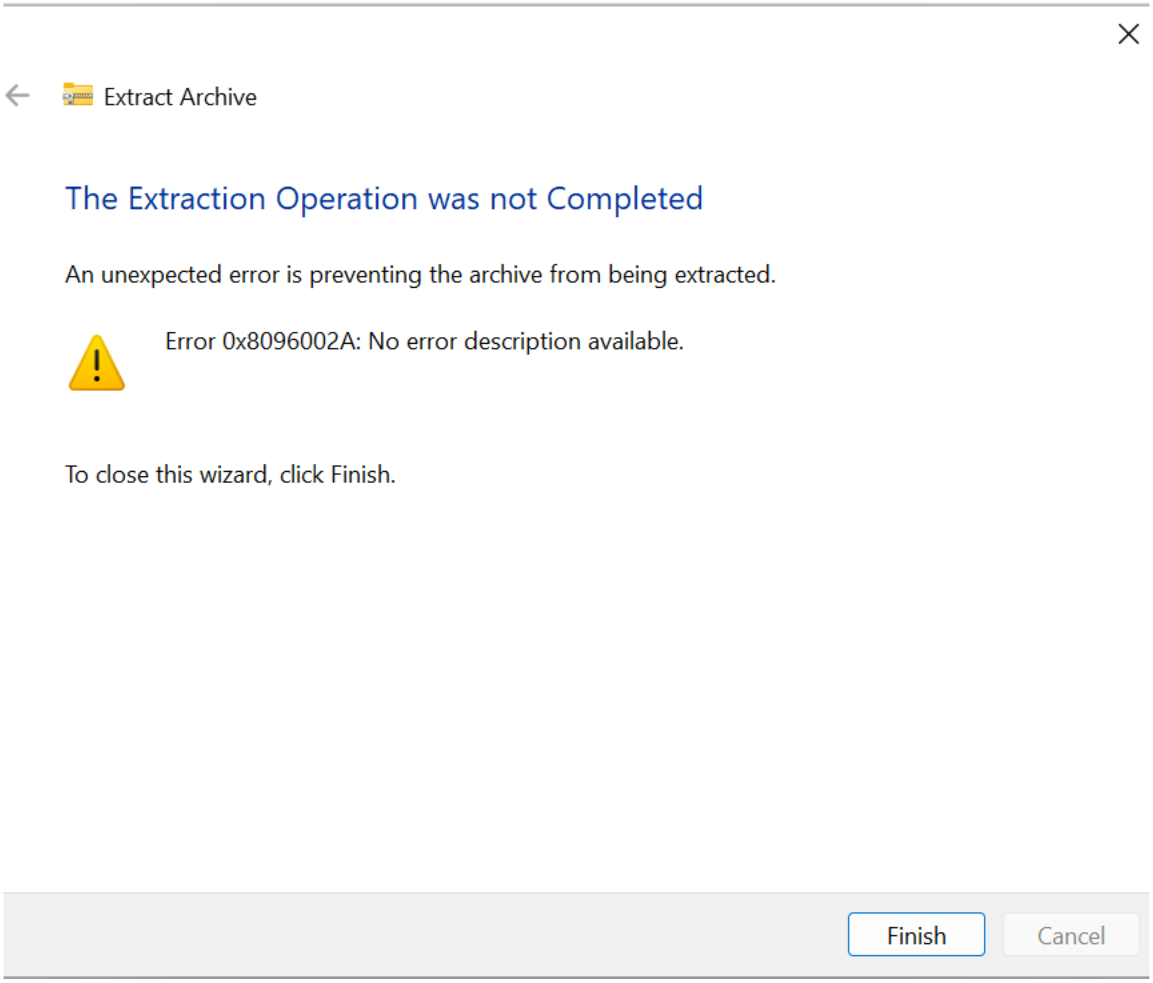
E:\msc\forensic assignment 13\forensic.rar

Elapsed time
Time left

Processed

Error

Incorrect password for forensic\lectures\ch01.pdf



The Extraction Operation was not Completed

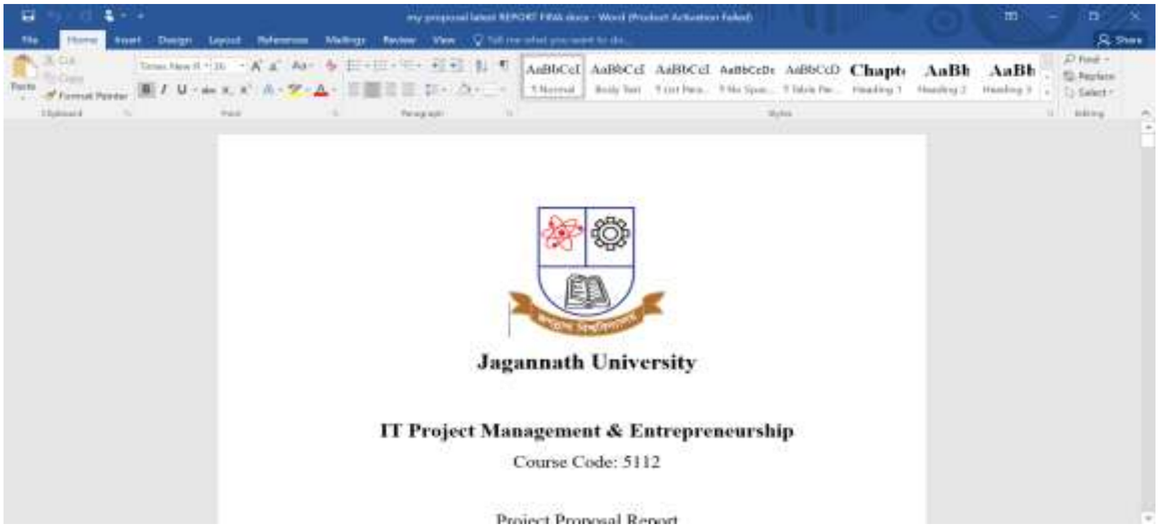
An unexpected error is preventing the archive from being extracted.

Error 0x8096002A: No error description available.

To close this wizard, click Finish.

Experiment-7: Protect any document File with Password:

Step 1: Create a document file and go to file option.

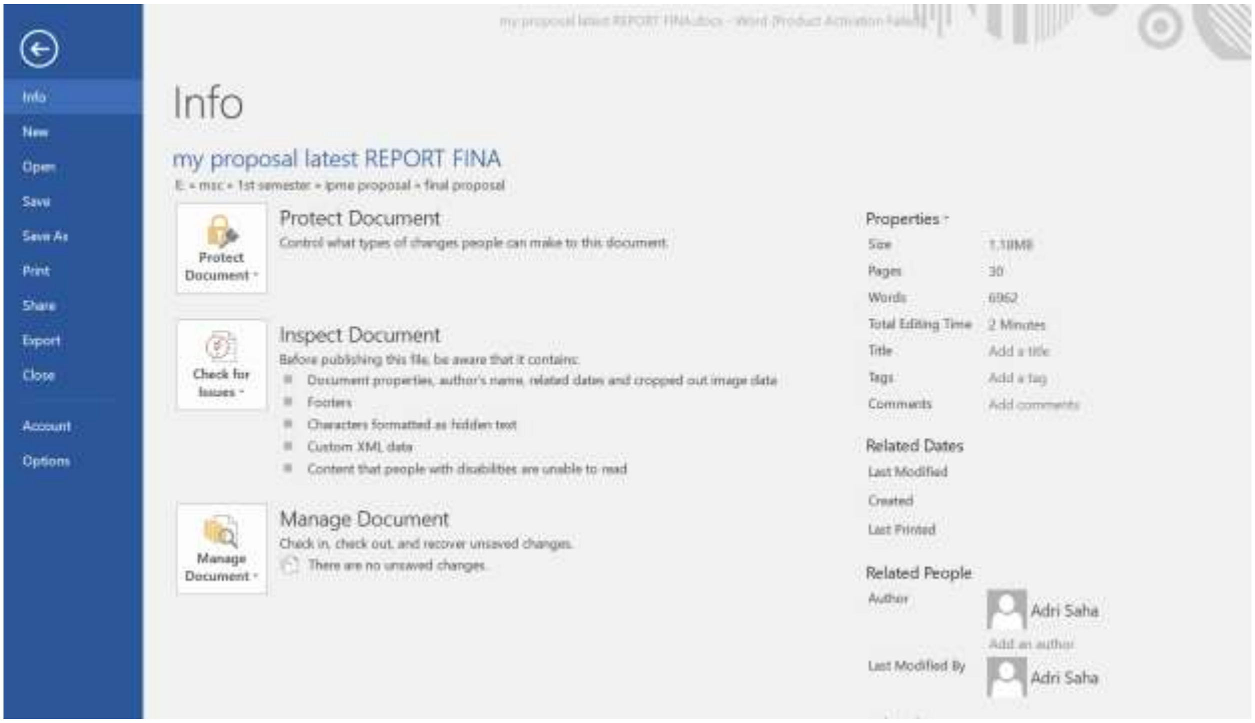


Jagannath University

IT Project Management & Entrepreneurship

Course Code: 5112

Project Proposal Report



Info

my proposal latest REPORT FINA

E: » msc » 1st semester » ipme proposal » final proposal

Protect Document

Control what types of changes people can make to this document.

Inspect Document

Before publishing this file, be aware that it contains:

- Document properties, author's name, related dates and cropped out image data
- Footers
- Characters formatted as hidden text
- Custom XML data
- Content that people with disabilities are unable to read

Manage Document

Check in, check out, and recover unsaved changes.

There are no unsaved changes.

Properties

Size	1.18MB
Pages	30
Words	6962
Total Editing Time	2 Minutes
Title	Add a title
Tags	Add a tag
Comments	Add comments

Related Dates

Last Modified

Created

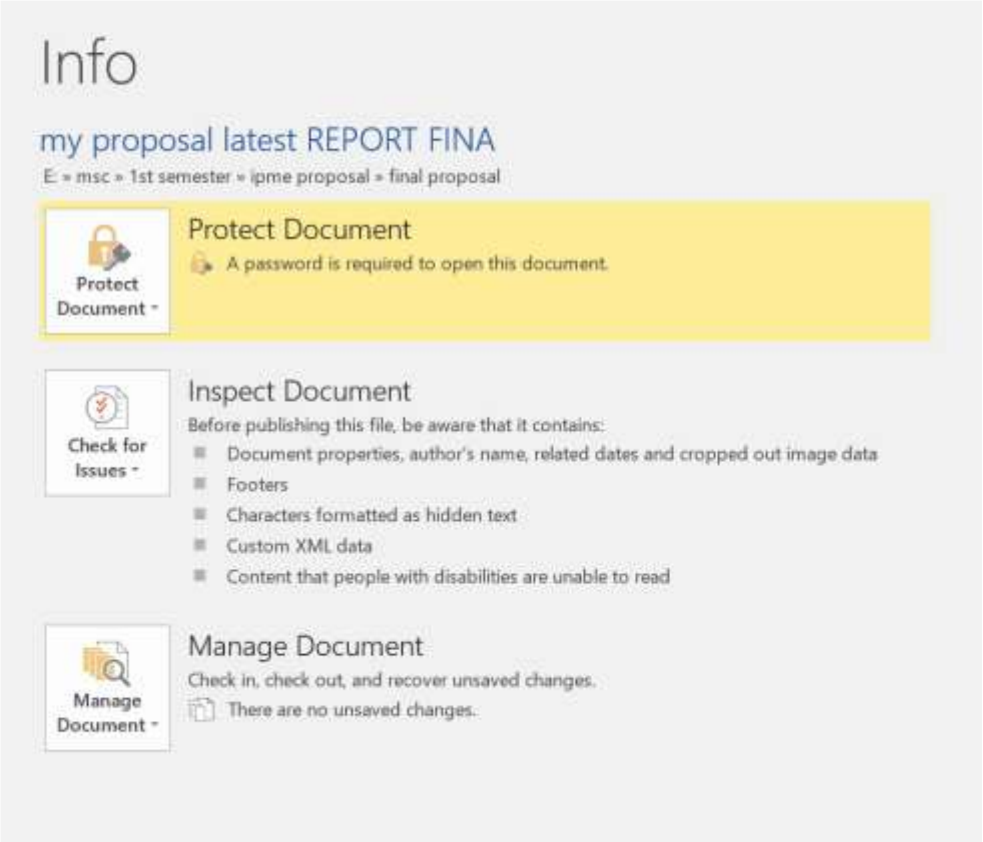
Last Printed

Related People

Author	Adri Saha Add an author
Last Modified By	Adri Saha

Step 2: Click on protect document and click on encrypt with password.

Step 3: Reenter the password.



Info

my proposal latest REPORT FINA

E » msc » 1st semester » ipme proposal » final proposal

Protect Document

A password is required to open this document.

Inspect Document

Before publishing this file, be aware that it contains:

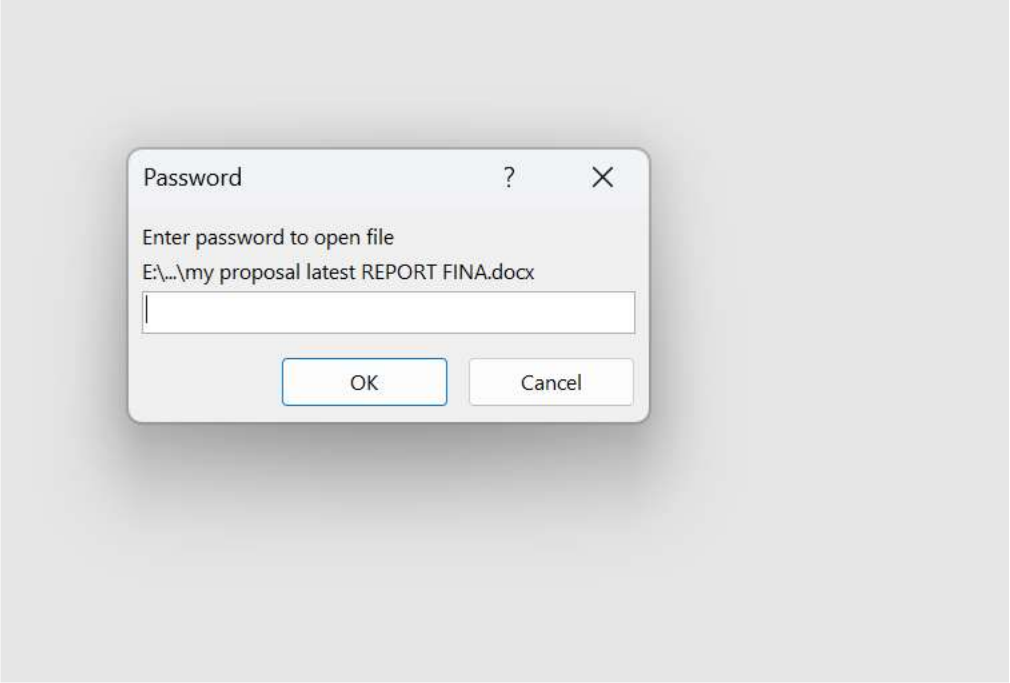
- Document properties, author's name, related dates and cropped out image data
- Footers
- Characters formatted as hidden text
- Custom XML data
- Content that people with disabilities are unable to read

Manage Document

Check in, check out, and recover unsaved changes.

There are no unsaved changes.

Step 4: Now the file is password protected.

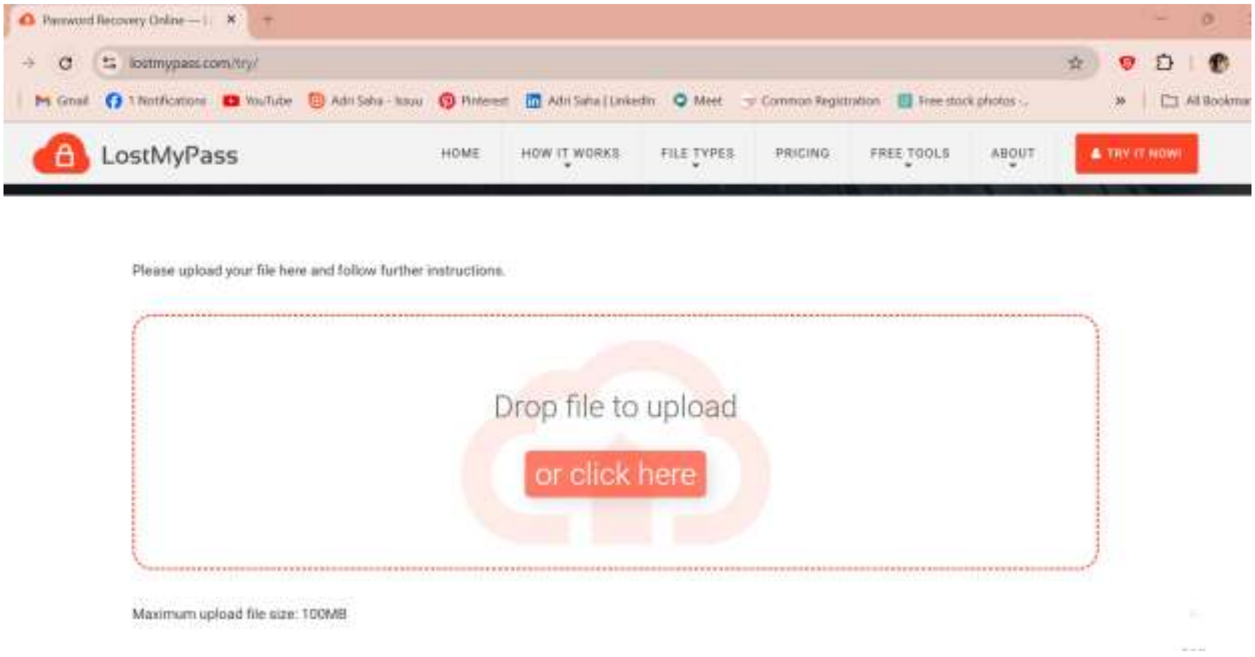


Password

Enter password to open file

E:\...\my proposal latest REPORT FINA.docx

Step 5: To break the password there is a online tool: Go to LostMyPass url.

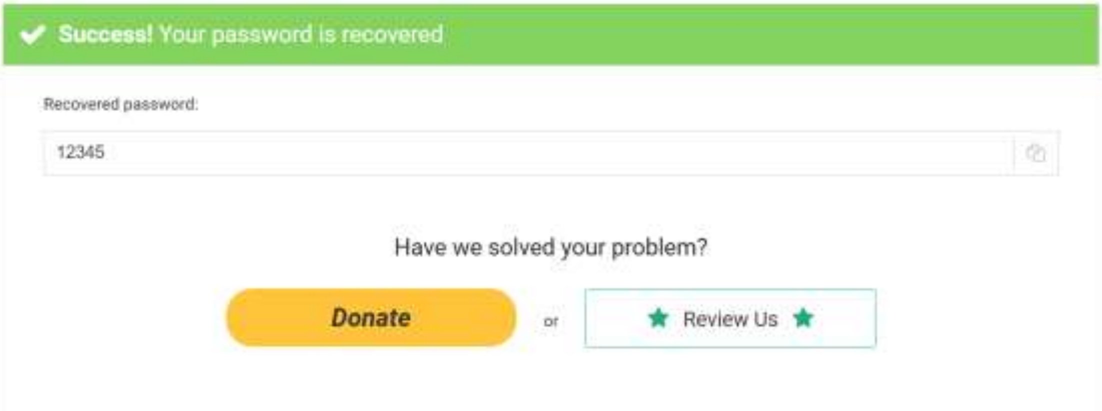


Please upload your file here and follow further instructions.

Drop file to upload

or click here

Maximum upload file size: 100MB



✓ Success! Your password is recovered

Recovered password:

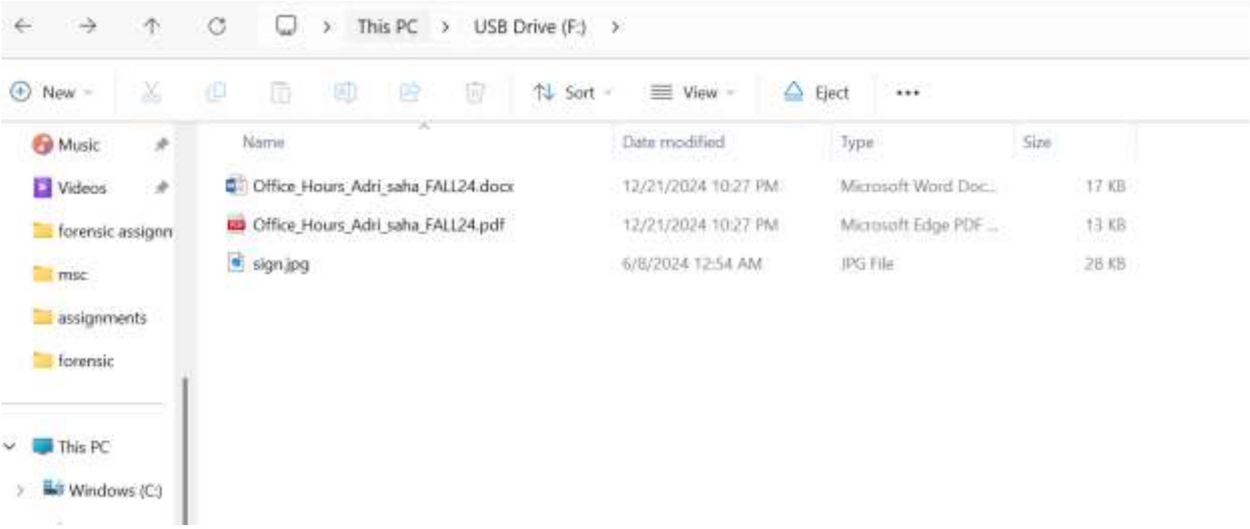
12345

Have we solved your problem?

- Password recovered successfully.

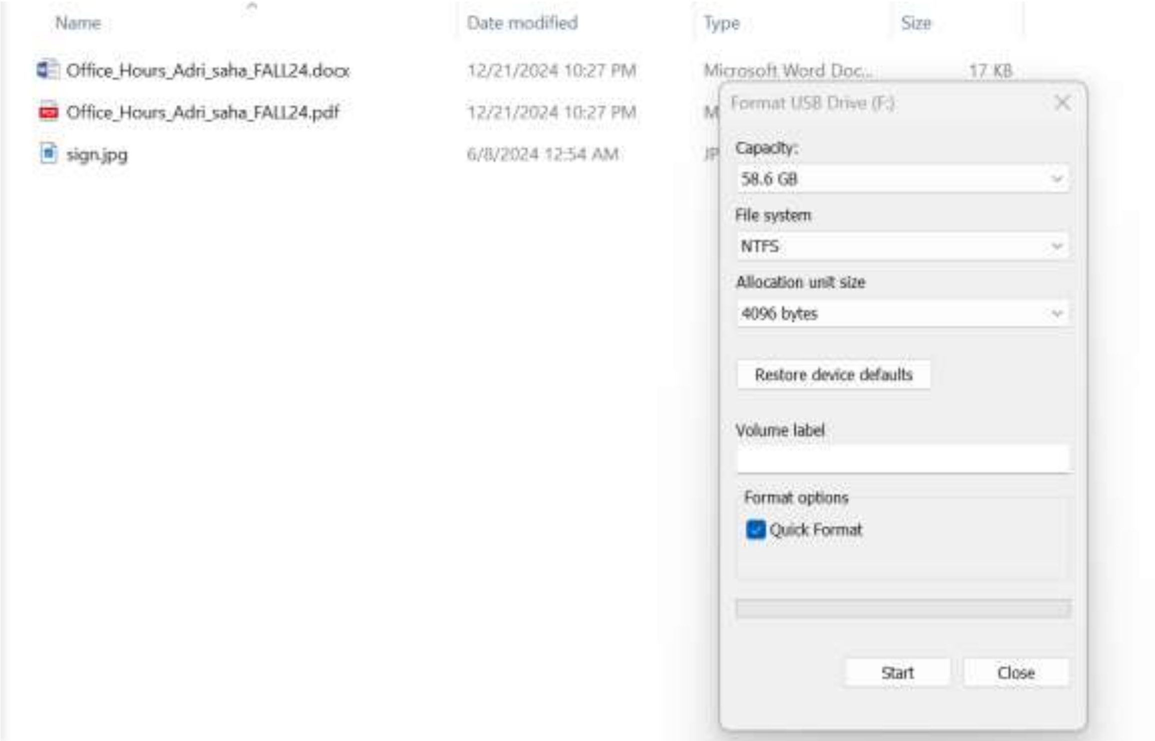
Experiment-8: Recovering files from a formatted hard drive using EaseUS:

How to recover files from a formatted hard drive?
EaseUS Data Recovery Wizard is your best choice. It allows you to complete the recovery job with a few simple clicks. You can download the software and follow the below guide to recover your lost data.
STEP 1: At first, I have kept a file in my pen Drive.



Name	Date modified	Type	Size
Office_Hours_Adri_saha_FALL24.docx	12/21/2024 10:27 PM	Microsoft Word Doc...	17 KB
Office_Hours_Adri_saha_FALL24.pdf	12/21/2024 10:27 PM	Microsoft Edge PDF ...	13 KB
sign.jpg	6/8/2024 12:54 AM	JPG File	28 KB

STEP 2: Then I format it and try to recover my File.



Name	Date modified	Type	Size
Office_Hours_Adri_saha_FALL24.docx	12/21/2024 10:27 PM	Microsoft Word Doc...	17 KB
Office_Hours_Adri_saha_FALL24.pdf	12/21/2024 10:27 PM	M	
sign.jpg	6/8/2024 12:54 AM	JP	

Format USB Drive (F:)

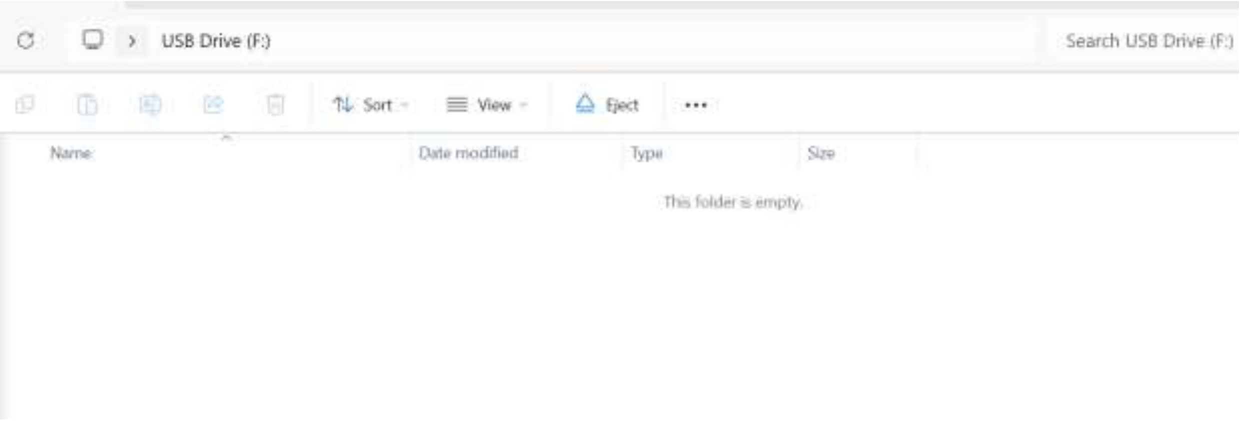
Capacity:
58.6 GB

File system
NTFS

Allocation unit size
4096 bytes

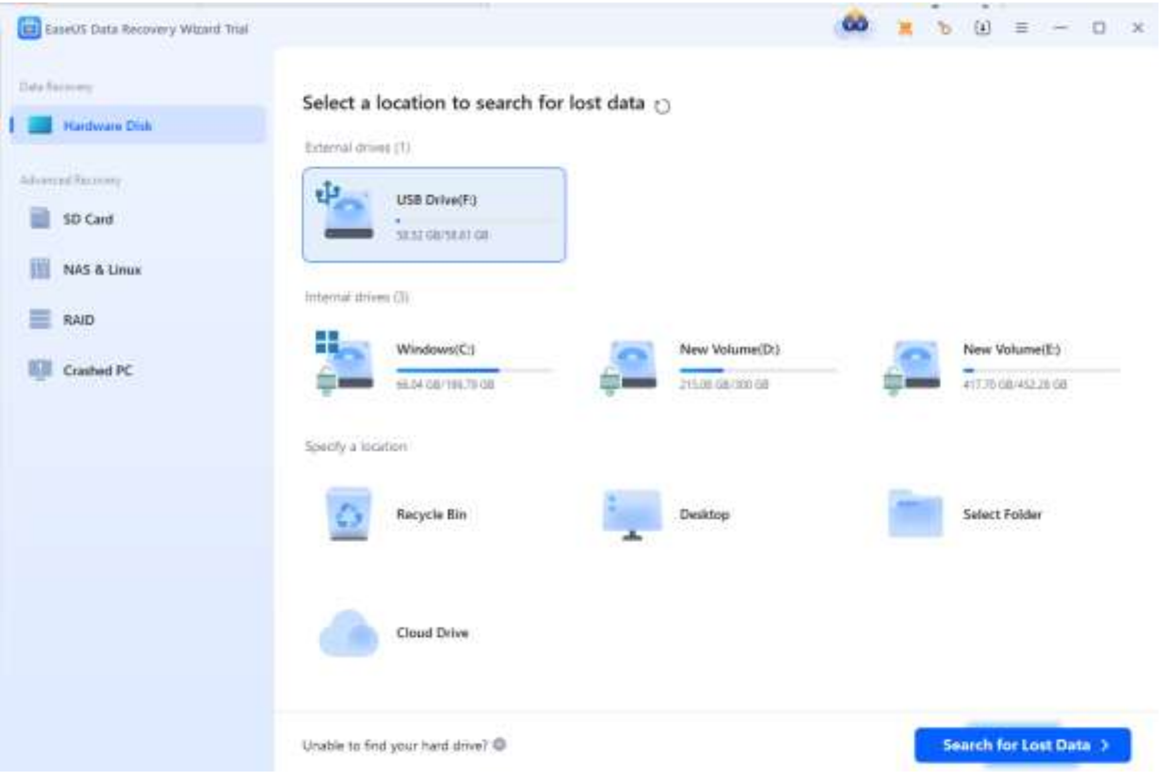
Volume label

Format options
☑ Quick Format



This folder is empty.

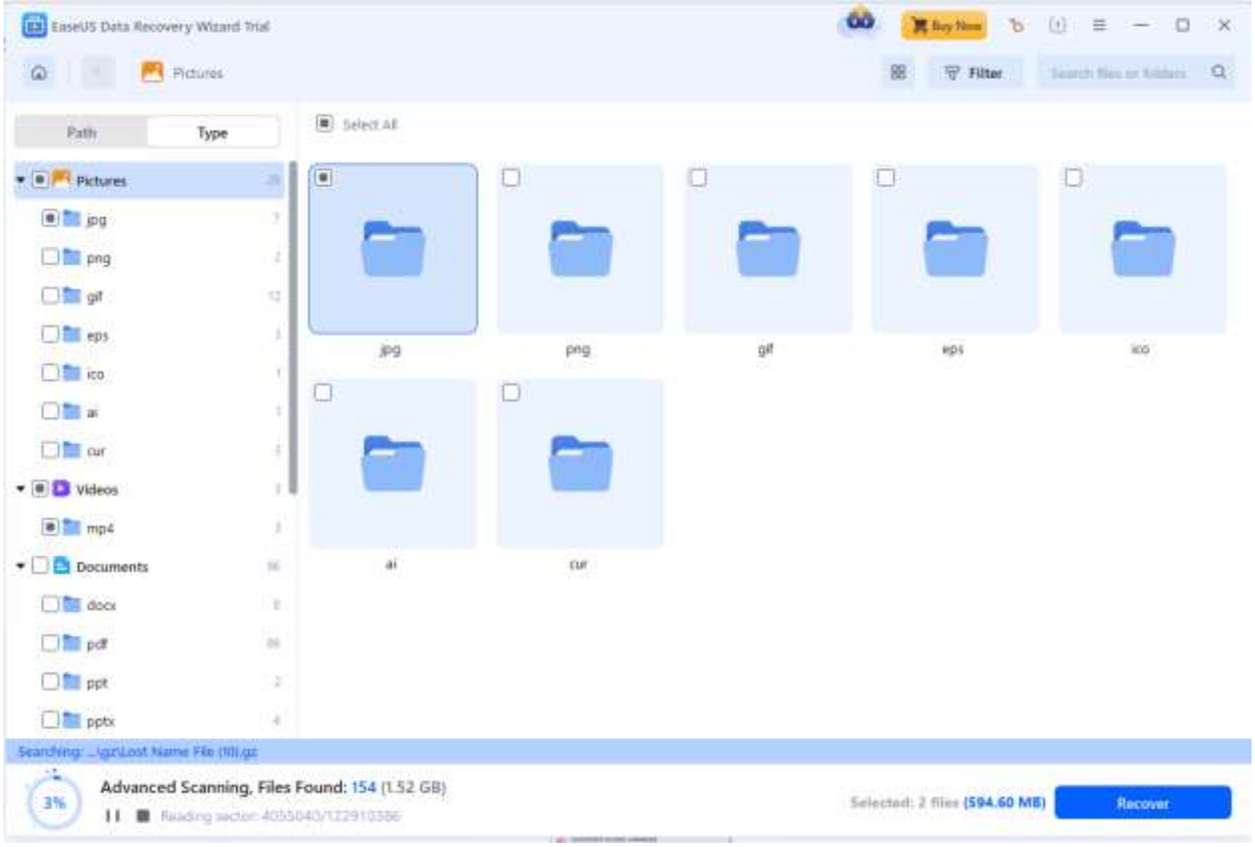
STEP 3: Launch EaseUS formatted data recovery software after the installation.



Select a location to search for lost data

Unable to find your hard drive?

STEP 4: Choose the hard drive which you've accidentally formatted. - - Click "Scan". Start scanning lost data all over the hard drive.
STEP 5: After the scan, browse data in each section, especially in "Lost Partition". It's a highlighted feature of EaseUS Data Recovery Wizard for retrieving data from a formatted hard drive partition. - Select the data files you wish to recover.
STEP 6: Click "Recover".



Searching: ...\gz\Lost Name File (10).gz

Advanced Scanning, Files Found: 154 (1.52 GB)

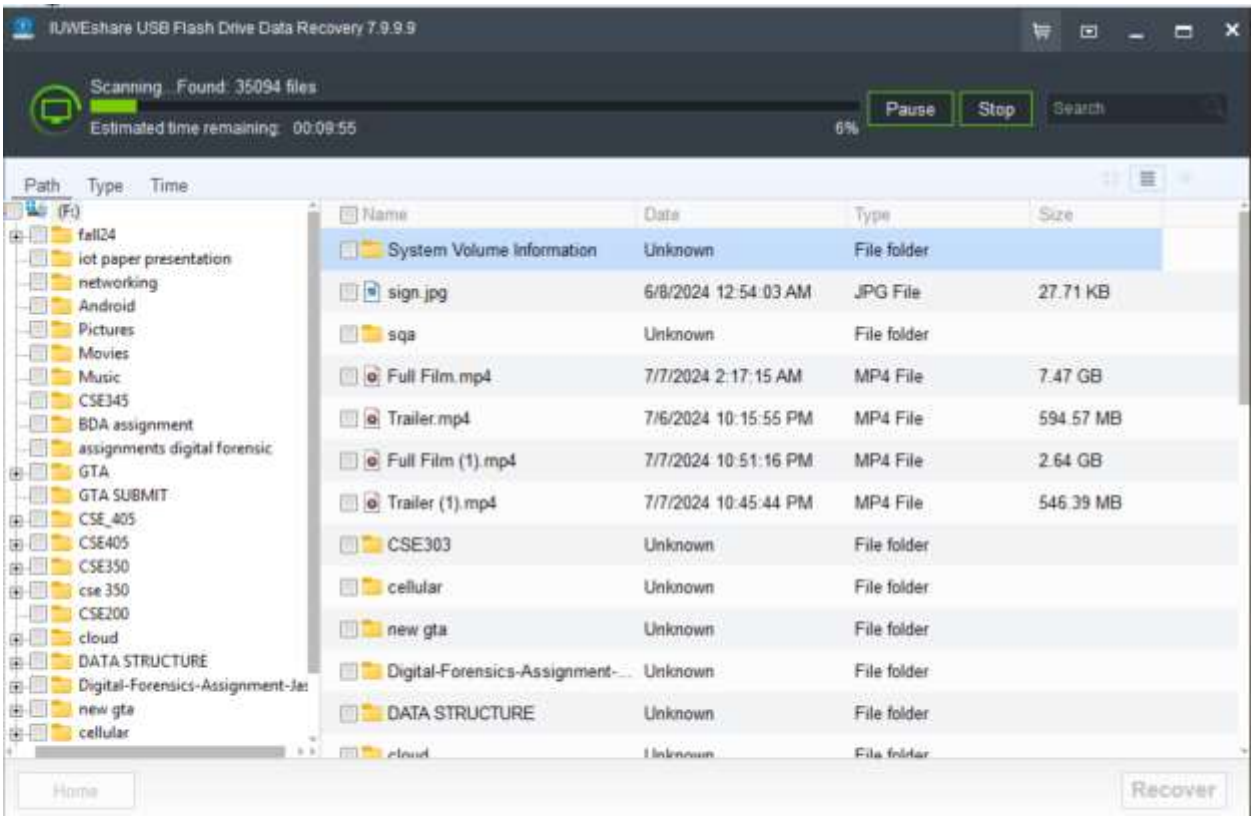
Reading sector: 4055040/122910386

Selected: 2 files (594.60 MB)

Experiment-9: Removal Disk Recovery Using IUWEshare:

Download IUWEshare from https://www.iuweshare.com/usb-flash-drive-data-recovery.html

Step-1: Run the software and click recover all or you can select the specific files you want to recover.
Step-2: After click start the list of removal disk will show. Select the suspect drive and click scan:
Step-3: After complete the scanning, the list of present and deleted files will be shown in a table:
Step-4: Now you can select the desired file and then can preview or recover:
Step-5: Currently you just see the deleted and present files in the usb drive but if you want to recover those files before format the drive, then you have to click "Deep Scan". After that it will scan the drive again and show the list of all those files which are stored in this drive upto 1000 format:



Scanning...Found: 35094 files

Estimated time remaining: 00:09:55 6%

(F:)
- fall24
- iot paper presentation
- networking
- Android
- Pictures
- Movies
- Music
- CSE345
- BDA assignment
- assignments digital forensic
- GTA
- GTA SUBMIT
- CSE_405
- CSE405
- CSE350
- cse 350
- CSE200
- cloud
- DATA STRUCTURE
- Digital-Forensics-Assignment-Ja
- new gta
- cellular

Name	Date	Type	Size
System Volume Information	Unknown	File folder	
sign.jpg	6/8/2024 12:54:03 AM	JPG File	27.71 KB
sqa	Unknown	File folder	
Full Film.mp4	7/7/2024 2:17:15 AM	MP4 File	7.47 GB
Trailer.mp4	7/6/2024 10:15:55 PM	MP4 File	594.57 MB
Full Film (1).mp4	7/7/2024 10:51:16 PM	MP4 File	2.64 GB
Trailer (1).mp4	7/7/2024 10:45:44 PM	MP4 File	546.39 MB
CSE303	Unknown	File folder	
cellular	Unknown	File folder	
new gta	Unknown	File folder	
Digital-Forensics-Assignment-...	Unknown	File folder	
DATA STRUCTURE	Unknown	File folder	
cloud	Unknown	File folder	

Conclusion:

With the growing reliance on the internet and information technology, digital crimes (e-crimes) have become a significant challenge, requiring advanced prevention, detection, investigation, and prosecution methods. Computer forensics, an emerging field, combines information technology, forensic science, and law to address these challenges by detecting crimes and gathering evidence admissible in court.

In this assignment, I have explored key forensic techniques such as data recovery, data hiding, validation, protection, and reconstruction. Through this effort, I believe I have successfully demonstrated the fundamental concepts and importance of computer forensics.