DIGITAL FORENSICS LAB

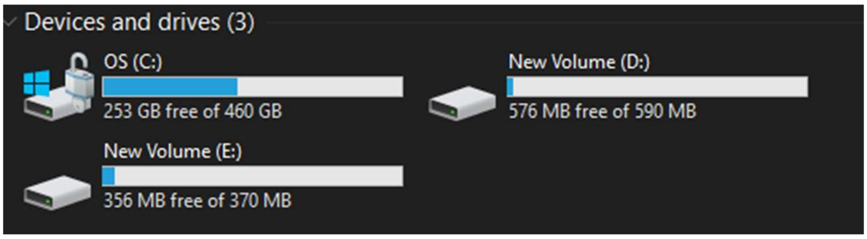
Exercise 13	
Name	S Shyam Sundaram
Registration Number	19BCE1560
Slot	L39+L40
Faculty	Dr. Seshu Babu Pulagara
Date	23rd November, 2021

AIM

Exploring various methods of data hiding.

Partition Hiding

The drive currently has partitions as shown below:



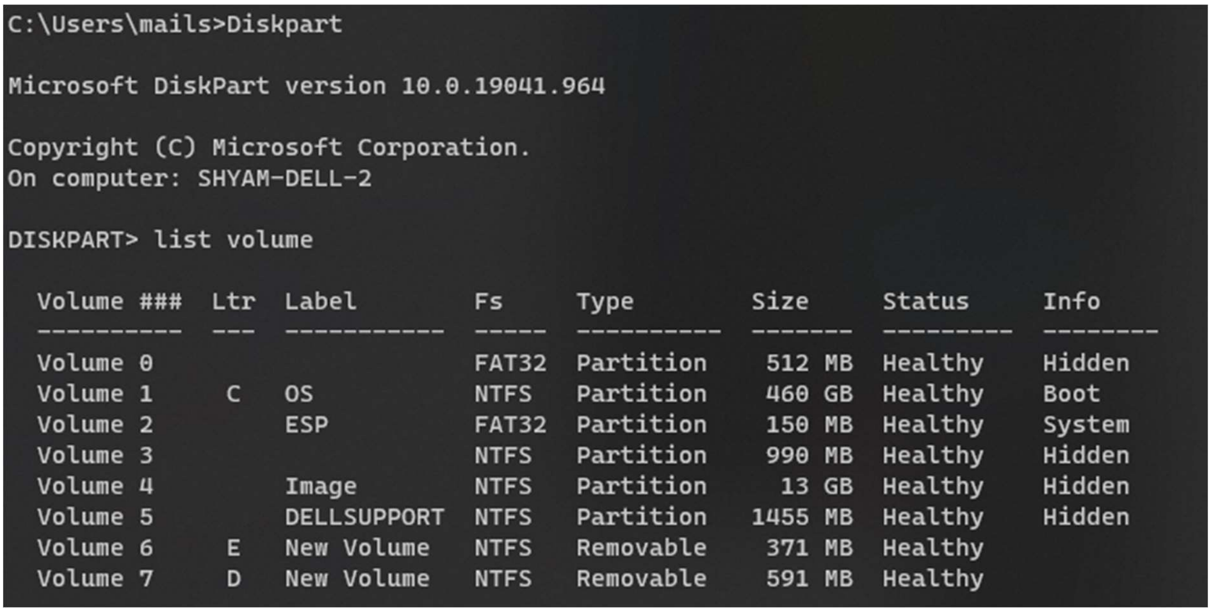
Devices and drives (3)

OS (C:)
253 GB free of 460 GB

New Volume (D:)
576 MB free of 590 MB

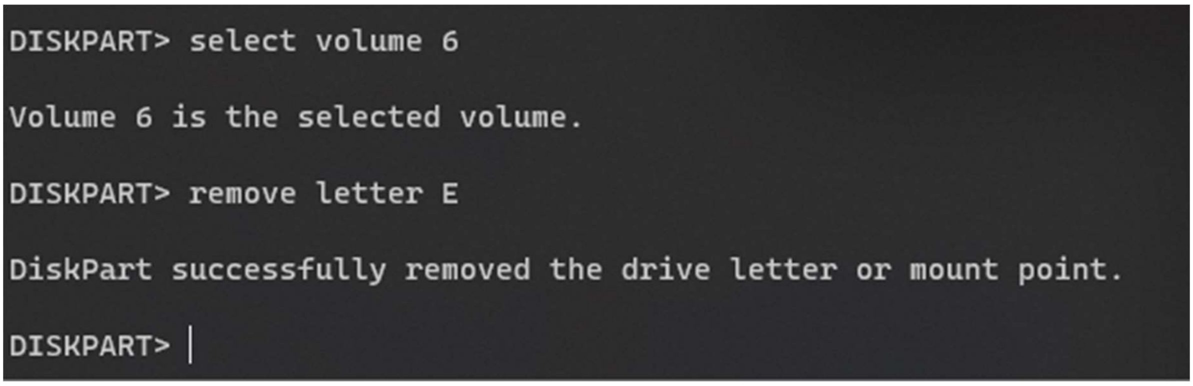
New Volume (E:)
356 MB free of 370 MB

To hide partition E:, open the terminal in Admin mode. Then type in 'Diskpart' and press enter. Then enter 'list volume' to list the volumes present.



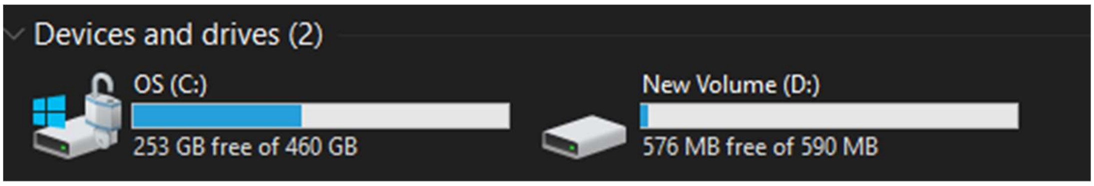
```
C:\Users\mails>Diskpart

Microsoft DiskPart version 10.0.19041.964

Copyright (C) Microsoft Corporation.
On computer: SHYAM-DELL-2

DISKPART> list volume

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0                      FAT32  Partition    512 MB  Healthy    Hidden
  Volume 1     C   OS           NTFS   Partition    460 GB  Healthy    Boot
  Volume 2         ESP          FAT32  Partition    150 MB  Healthy    System
  Volume 3                      NTFS   Partition    990 MB  Healthy    Hidden
  Volume 4         Image        NTFS   Partition     13 GB  Healthy    Hidden
  Volume 5         DELLSUPPORT  NTFS   Partition   1455 MB  Healthy    Hidden
  Volume 6     E   New Volume   NTFS   Removable    371 MB  Healthy
  Volume 7     D   New Volume   NTFS   Removable    591 MB  Healthy
```

Since we want to hide E:. enter 'select volume 6' and enter 'remove letter E'. The partition is now hidden.



```
DISKPART> select volume 6

Volume 6 is the selected volume.

DISKPART> remove letter E

DiskPart successfully removed the drive letter or mount point.

DISKPART> |
```

The partition and its contents are no longer visible.

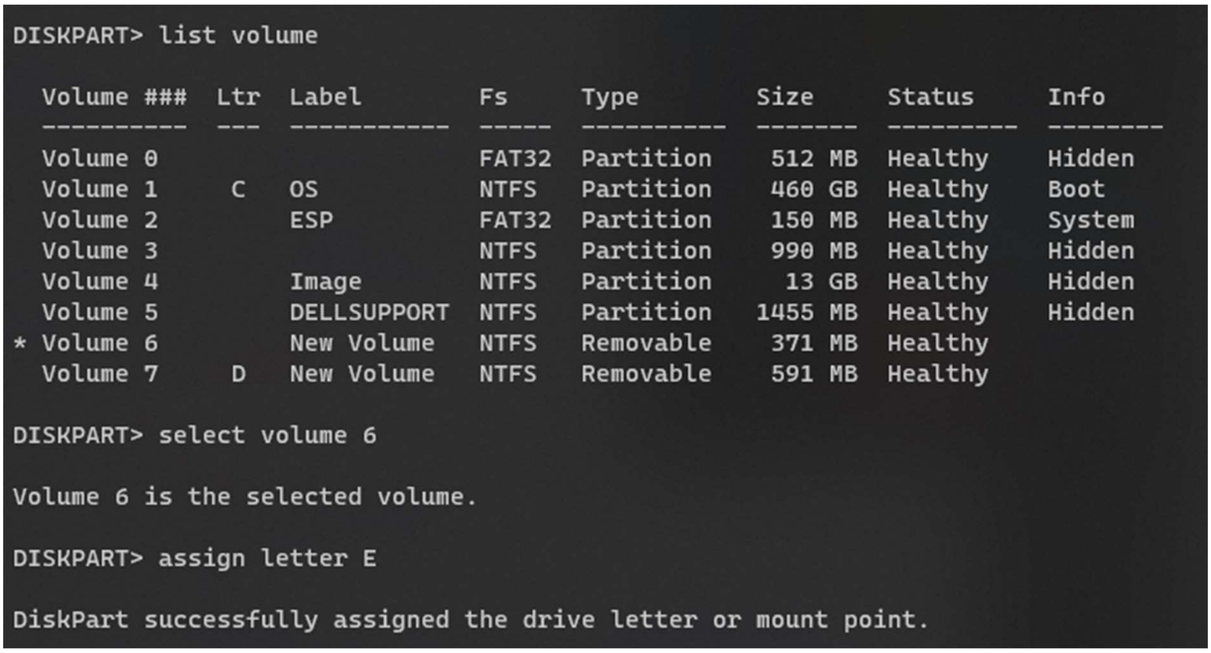


Devices and drives (2)

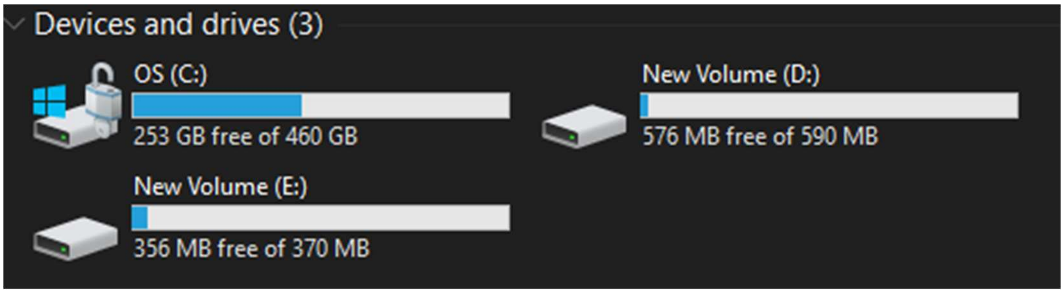
OS (C:)
253 GB free of 460 GB

New Volume (D:)
576 MB free of 590 MB

To unhide it and assign it the letter E, select the volume again and assign letter E as shown below.



```
DISKPART> list volume

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0                      FAT32  Partition    512 MB  Healthy    Hidden
  Volume 1     C   OS           NTFS   Partition    460 GB  Healthy    Boot
  Volume 2         ESP          FAT32  Partition    150 MB  Healthy    System
  Volume 3                      NTFS   Partition    990 MB  Healthy    Hidden
  Volume 4         Image        NTFS   Partition     13 GB  Healthy    Hidden
  Volume 5         DELLSUPPORT  NTFS   Partition   1455 MB  Healthy    Hidden
* Volume 6         New Volume   NTFS   Removable    371 MB  Healthy
  Volume 7     D   New Volume   NTFS   Removable    591 MB  Healthy

DISKPART> select volume 6

Volume 6 is the selected volume.

DISKPART> assign letter E

DiskPart successfully assigned the drive letter or mount point.
```



Devices and drives (3)

OS (C:)
253 GB free of 460 GB

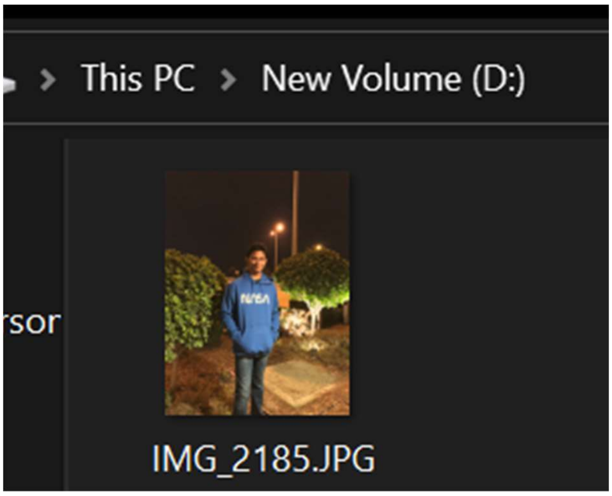
New Volume (D:)
576 MB free of 590 MB

New Volume (E:)
356 MB free of 370 MB

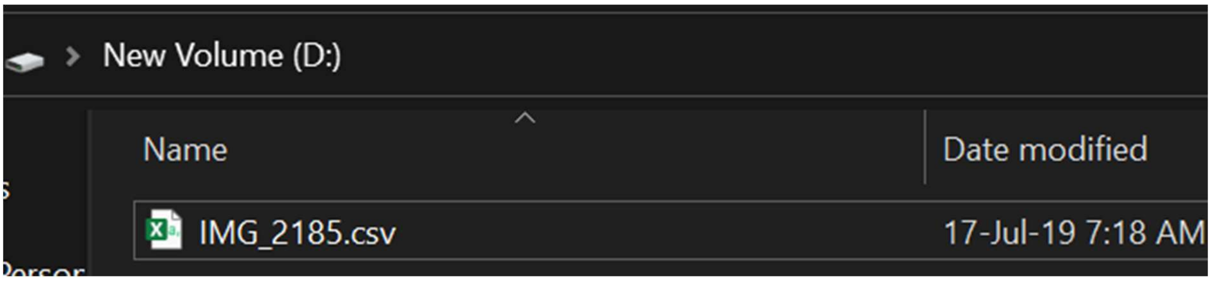
The partition is now unhidden.

Changing file extensions

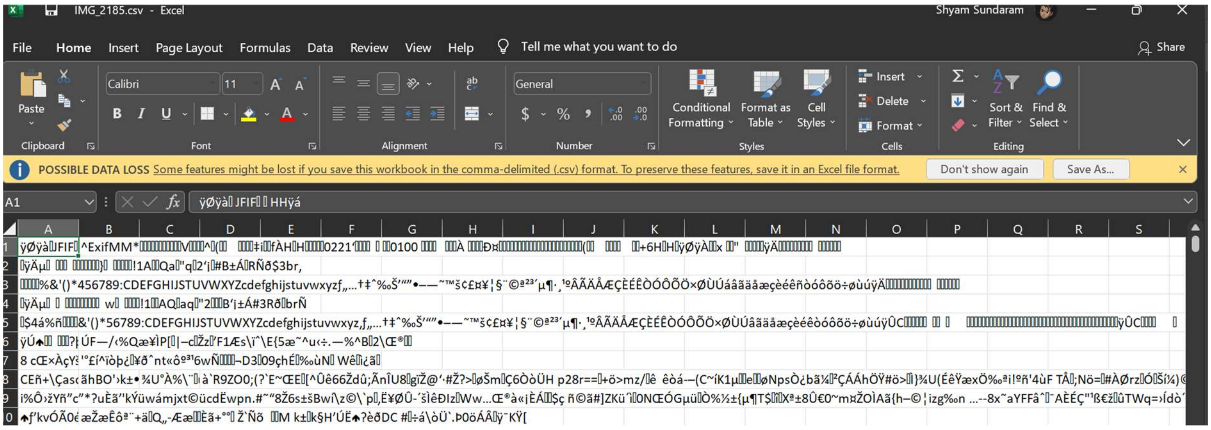
Here, we just change the extension of the file t be hidden. Say I wish to hide the JPG file below.



The extension, JPG, can be changed to something else.



But the file would appear to be gibberish:



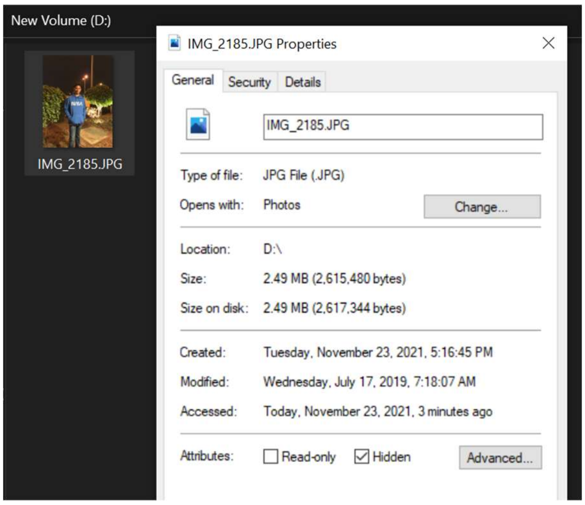
POSSIBLE DATA LOSS Some features might be lost if you save this workbook in the comma-delimited (.csv) format. To preserve these features, save it in an Excel file format.

A1: ÿØÿà JFIF HHÿá

We can obtain it back by changing the extension back to JPG.

Setting File attributes to Hidden

This is done by selecting the file’s ‘Hidden’ attribute in properties.



IMG_2185.JPG

Type of file: JPG File (.JPG)

Opens with: Photos

Location: D:\

Size: 2.49 MB (2,615,480 bytes)

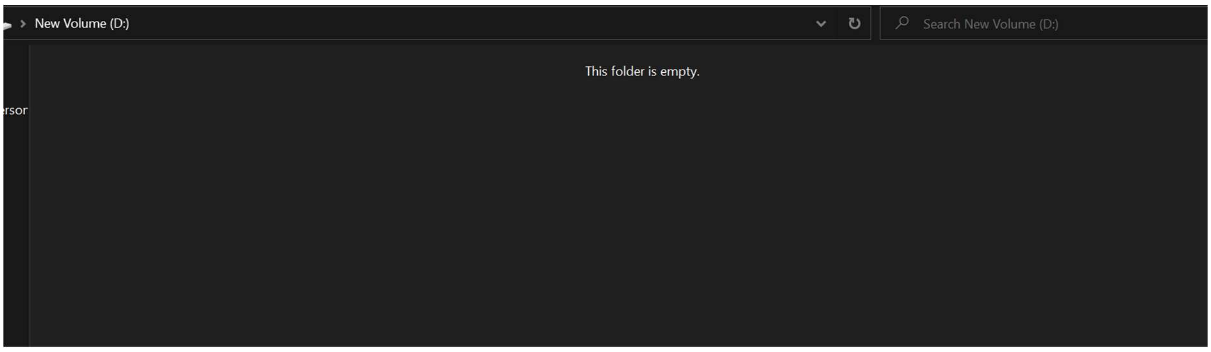
Size on disk: 2.49 MB (2,617,344 bytes)

Created: Tuesday, November 23, 2021, 5:16:45 PM

Modified: Wednesday, July 17, 2019, 7:18:07 AM

Accessed: Today, November 23, 2021, 3 minutes ago

Attributes: □ Read-only ☑ Hidden



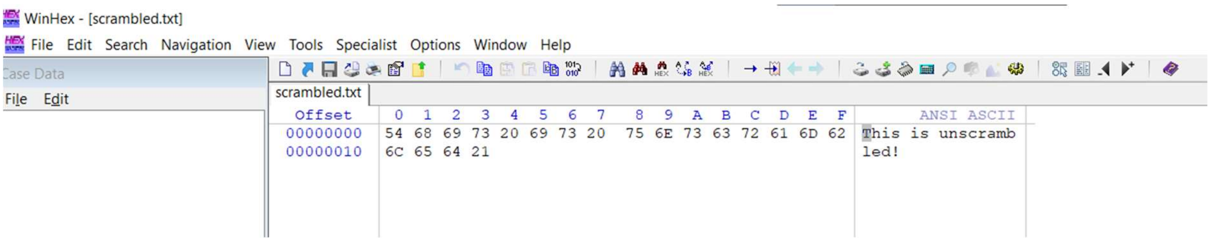
This folder is empty.

To unhide, click on View in file explorer, then select ‘Hidden Item’ in ‘Show/Hide’ group. The file will be visible and then the ‘Hidden’ attribute can be unchecked.

Bit Shifting

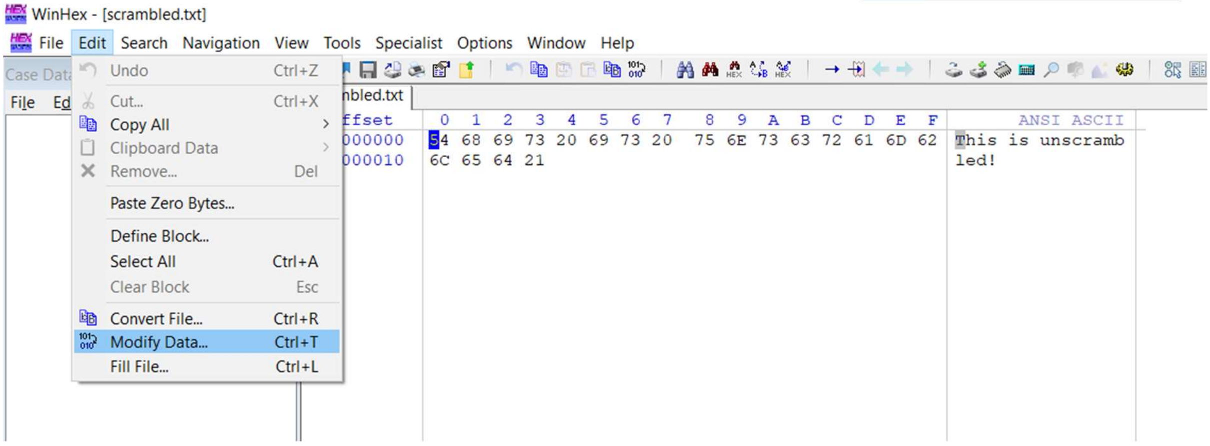
WinHex can be used for this.

First, open a file in WinHex. Here, a text file is opened as shown.


WinHex - [scrambled.txt]
File Edit Search Navigation View Tools Specialist Options Window Help
Case Data
File Edit
scrambled.txt

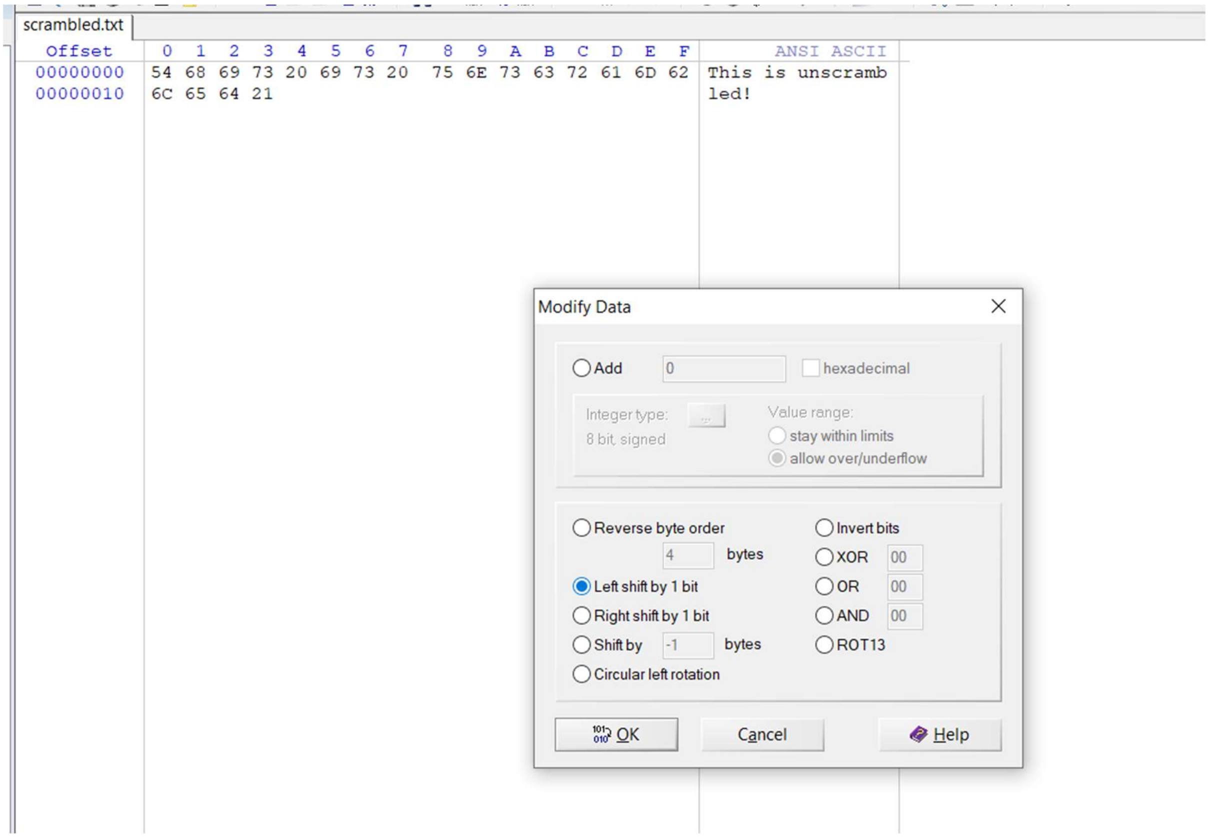
```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F     ANSI ASCII
 00000000  54 68 69 73 20 69 73 20  75 6E 73 63 72 61 6D 62  This is unscramb
 00000010  6C 65 64 21                                       led!
```

Now, go to Edit->Modify data.



```
ffset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
000000   54 68 69 73 20 69 73 20  75 6E 73 63 72 61 6D 62  This is unscramb
000010   6C 65 64 21                                       led!
```

Now, select how you wish to shift the bits. Here I shift bits to the left once.



```
Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000  54 68 69 73 20 69 73 20  75 6E 73 63 72 61 6D 62  This is unscramb
00000010  6C 65 64 21                                       led!
```

○ Add 0 □ hexadecimal

Integer type: 8 bit, signed

Value range: ○ stay within limits ● allow over/underflow

○ Reverse byte order 4 bytes

● Left shift by 1 bit

○ Right shift by 1 bit

○ Shift by -1 bytes

○ Circular left rotation

○ Invert bits

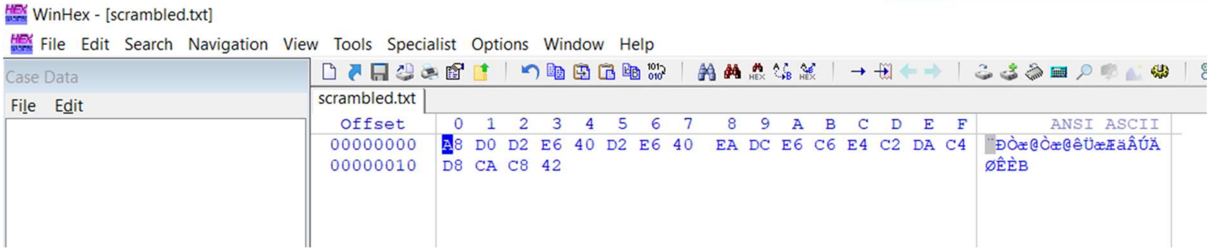
○ XOR 00

○ OR 00

○ AND 00

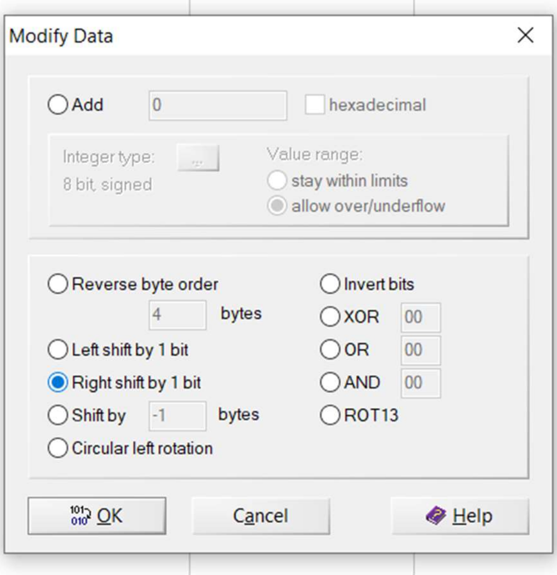
○ ROT13

The file is now scrambled and unreadable.


WinHex - [scrambled.txt]
File Edit Search Navigation View Tools Specialist Options Window Help
Case Data
File Edit
scrambled.txt

```
Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000  A8 D0 D2 E6 40 D2 E6 40  EA DC E6 C6 E4 C2 DA C4  ¨ÐÒæ@Òæ@êÜæÆäÂÚÄ
00000010  D8 CA C8 42                                       ØÊÈB
```

To unscramble, shift the file bits in the other direction. Since we shifted it to the left by one place, we now shift the bits to the right by one place to unscramble.



Modify Data

○ Add 0 □ hexadecimal

Integer type: 8 bit, signed

Value range: ○ stay within limits ● allow over/underflow

○ Reverse byte order 4 bytes

○ Left shift by 1 bit

● Right shift by 1 bit

○ Shift by -1 bytes

○ Circular left rotation

○ Invert bits

○ XOR 00

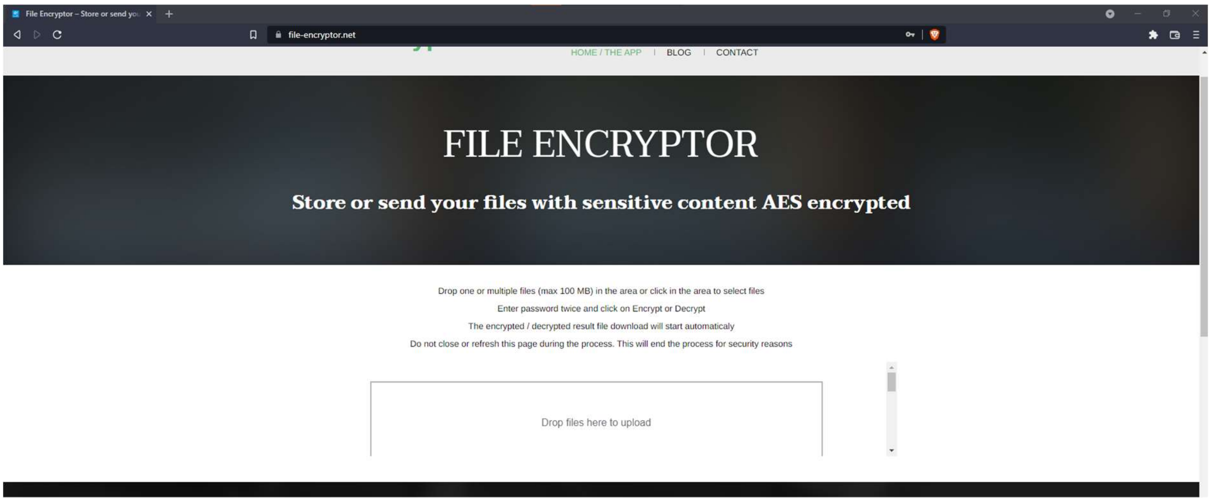
○ OR 00

○ AND 00

○ ROT13

Encryption

Visit any online website that does this. Here, file-encryptor.net was used as shown in image.



FILE ENCRYPTOR

Store or send your files with sensitive content AES encrypted

Drop one or multiple files (max 100 MB) in the area or click in the area to select files

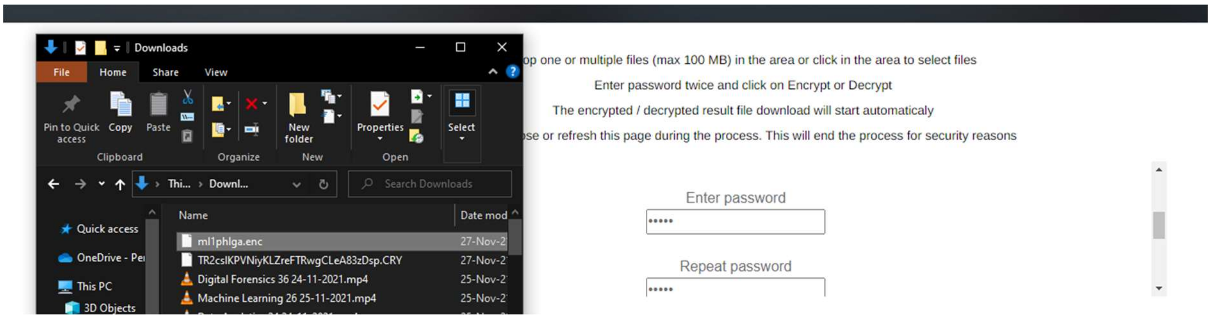
Enter password twice and click on Encrypt or Decrypt

The encrypted / decrypted result file download will start automaticaly

Do not close or refresh this page during the process. This will end the process for security reasons

Drop files here to upload

Drop the file here then scroll down in the iframe to provide password for encryption. Then click Encrypt. A file of extension enc is created. To decrypt this, drop the enc file, enter the password used while encrypting then click Decrypt. The original image is gotten back.



ml1phlga.enc 27-Nov-2

TR2csIKPVNiyKLZreFTRwgCLeA83zDsp.CRY 27-Nov-2

Digital Forensics 36 24-11-2021.mp4 25-Nov-2

Machine Learning 26 25-11-2021.mp4 25-Nov-2

op one or multiple files (max 100 MB) in the area or click in the area to select files

Enter password twice and click on Encrypt or Decrypt

The encrypted / decrypted result file download will start automaticaly

se or refresh this page during the process. This will end the process for security reasons

Enter password

•••••

Repeat password

•••••

Password protection

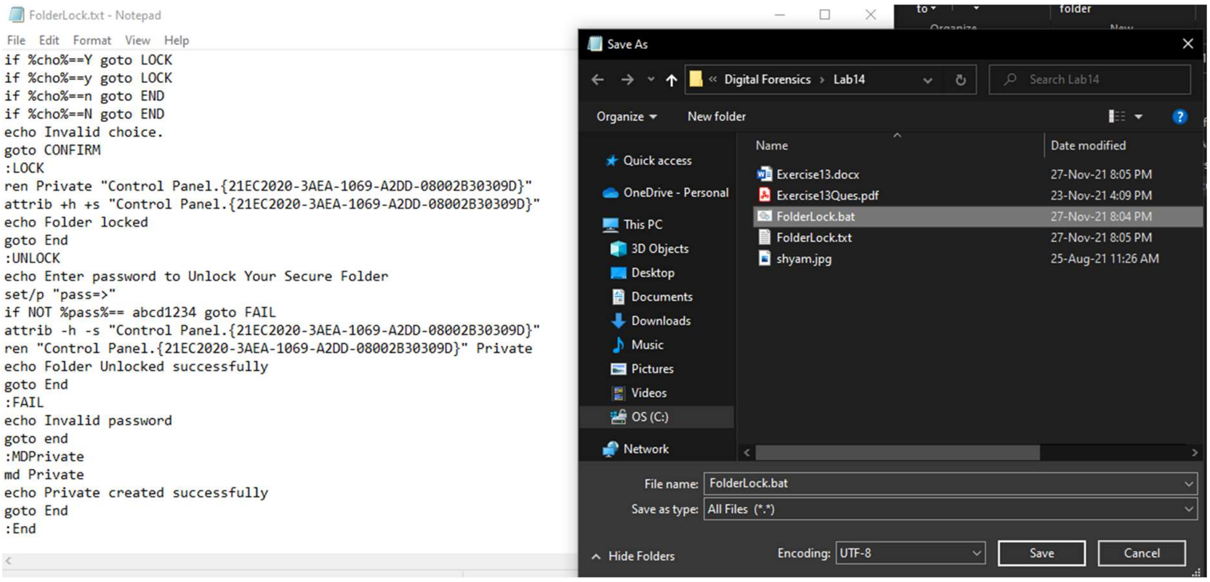
Windows Home editions do not have this feature available for use. So, we will have to rely on third party tools or find some other way as follows:

1. Create a txt file and paste the following code:

```
@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%== YOUR-PASSWORD 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
```

2. In the code above, replace ‘YOUR PASSWORD’ with the password you wish to use.
3. Then save the txt file as a .bat file.



FolderLock.txt - Notepad

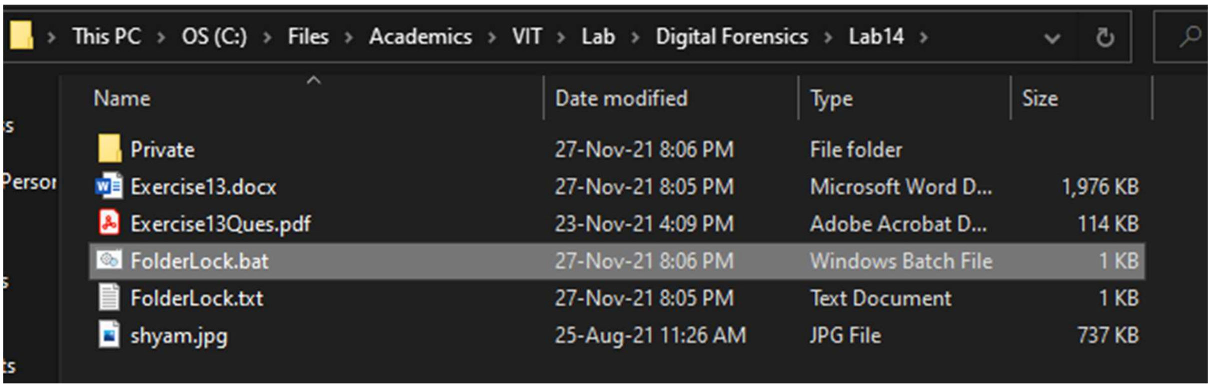
```
if %cho%==Y goto LOCK
if %cho%==y goto LOCK
if %cho%==n goto END
if %cho%==N goto END
echo Invalid choice.
goto CONFIRM
:LOCK
ren Private "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
attrib +h +s "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
echo Folder locked
goto End
:UNLOCK
echo Enter password to Unlock Your Secure Folder
set/p "pass=>"
if NOT %pass%== abcd1234 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
```

Save As

Name	Date modified
Exercise13.docx	27-Nov-21 8:05 PM
Exercise13Ques.pdf	23-Nov-21 4:09 PM
FolderLock.bat	27-Nov-21 8:04 PM
FolderLock.txt	27-Nov-21 8:05 PM
shyam.jpg	25-Aug-21 11:26 AM

File name: FolderLock.bat
Save as type: All Files (*.*)
Encoding: UTF-8

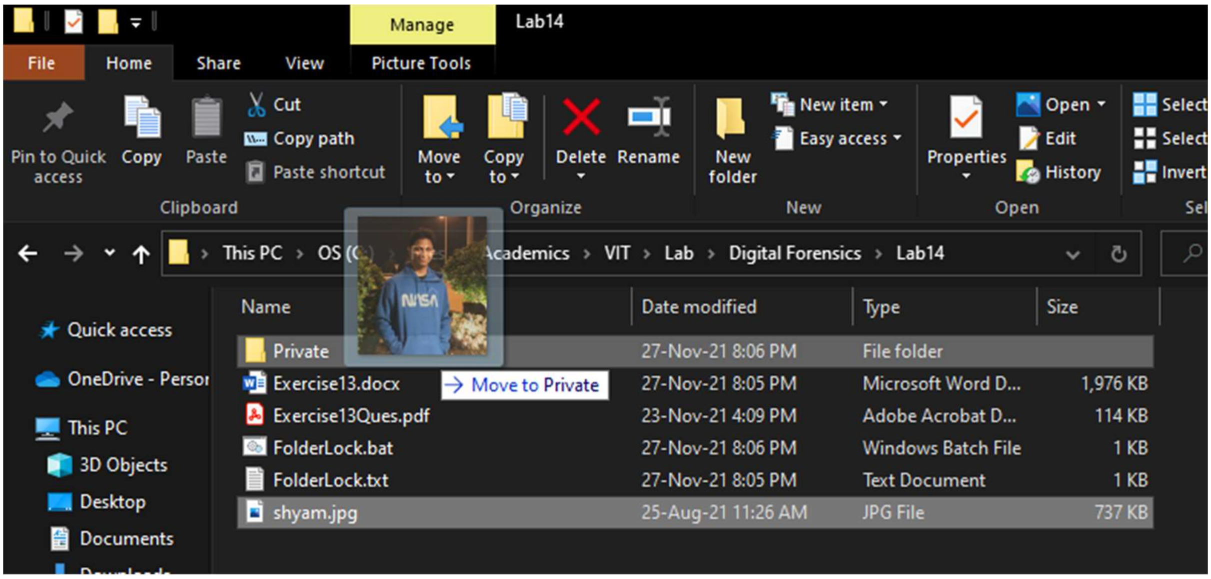
4. Now, double click on the bat file. A folder called ‘Private’ will be created.



This PC › OS (C:) › Files › Academics › VIT › Lab › Digital Forensics › Lab14 ›

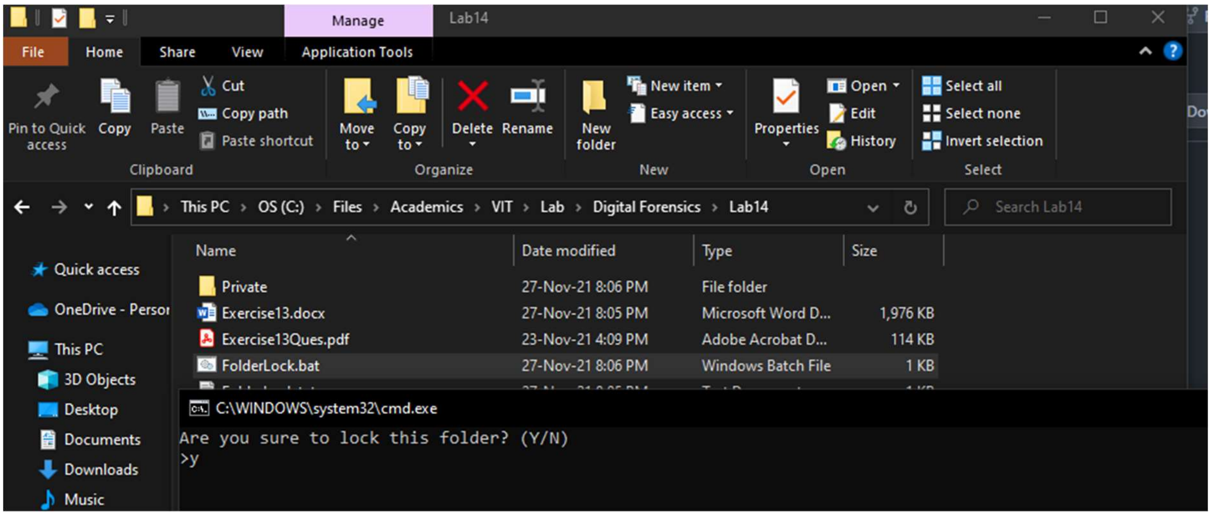
Name	Date modified	Type	Size
Private	27-Nov-21 8:06 PM	File folder	
Exercise13.docx	27-Nov-21 8:05 PM	Microsoft Word D...	1,976 KB
Exercise13Ques.pdf	23-Nov-21 4:09 PM	Adobe Acrobat D...	114 KB
FolderLock.bat	27-Nov-21 8:06 PM	Windows Batch File	1 KB
FolderLock.txt	27-Nov-21 8:05 PM	Text Document	1 KB
shyam.jpg	25-Aug-21 11:26 AM	JPG File	737 KB

5. Drag and drop the files you want to lock into this ‘Private’ folder.



Name	Date modified	Type	Size
Private	27-Nov-21 8:06 PM	File folder	
Exercise13.docx	27-Nov-21 8:05 PM	Microsoft Word D...	1,976 KB
Exercise13Ques.pdf	23-Nov-21 4:09 PM	Adobe Acrobat D...	114 KB
FolderLock.bat	27-Nov-21 8:06 PM	Windows Batch File	1 KB
FolderLock.txt	27-Nov-21 8:05 PM	Text Document	1 KB
shyam.jpg	25-Aug-21 11:26 AM	JPG File	737 KB

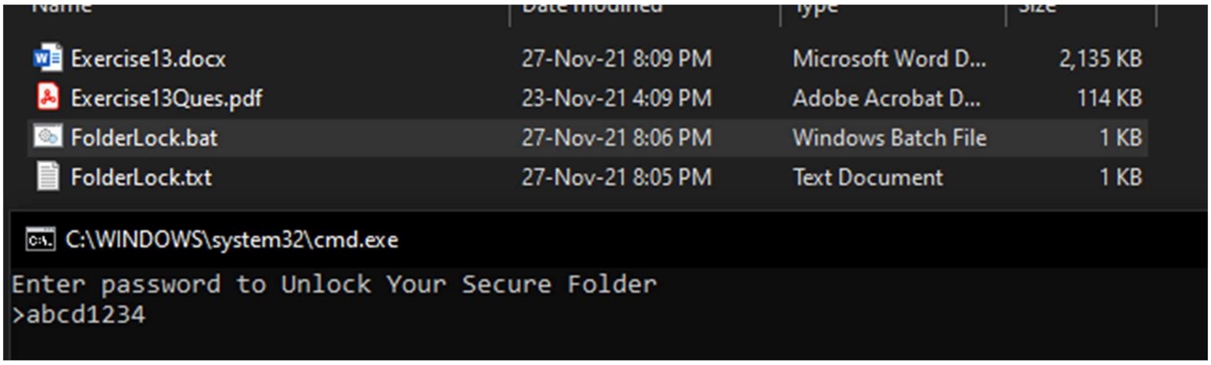
6. Then, again double click on the bat file. A prompt likthis will be presented. Press ‘y’ and Enter.



Name	Date modified	Type	Size
Private	27-Nov-21 8:06 PM	File folder	
Exercise13.docx	27-Nov-21 8:05 PM	Microsoft Word D...	1,976 KB
Exercise13Ques.pdf	23-Nov-21 4:09 PM	Adobe Acrobat D...	114 KB
FolderLock.bat	27-Nov-21 8:06 PM	Windows Batch File	1 KB

```
C:\WINDOWS\system32\cmd.exe
Are you sure to lock this folder? (Y/N)
>y
```

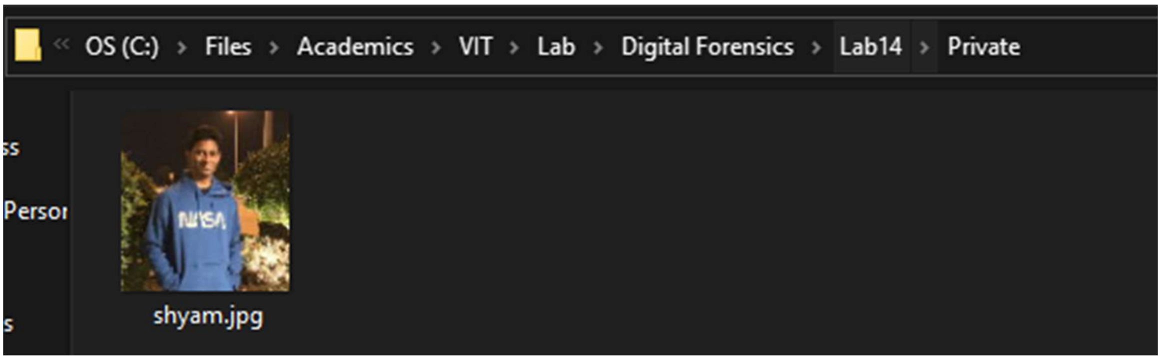
7. The Private folder now disappears. To view the folder and it’s contents again, double click on the bat file and enter the password.



Name	Date modified	Type	Size
Exercise13.docx	27-Nov-21 8:09 PM	Microsoft Word D...	2,135 KB
Exercise13Ques.pdf	23-Nov-21 4:09 PM	Adobe Acrobat D...	114 KB
FolderLock.bat	27-Nov-21 8:06 PM	Windows Batch File	1 KB
FolderLock.txt	27-Nov-21 8:05 PM	Text Document	1 KB

```
C:\WINDOWS\system32\cmd.exe
Enter password to Unlock Your Secure Folder
>abcd1234
```

8. The folder and its contents are now visible again.


OS (C:) › Files › Academics › VIT › Lab › Digital Forensics › Lab14 › Private
ss
Persor
s
shyam.jpg

OBSERVATIONS

In the methods used above, files are either completely hidden from view or were transformed into a form or file type that is not their own, rendering them unreadable. In some methods, the data within the file is scrambled to render them as nonsense to anyone else.

CONCLUSION

Thus, we have explored the various ways to hide files.