**DIGITAL FORENSICS LAB**

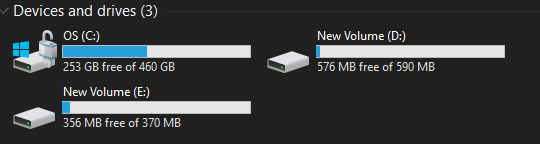
|  |  |
| --- | --- |
| Exercise 13 | |
| Name | S Shyam Sundaram |
| Registration Number | 19BCE1560 |
| Slot | L39+L40 |
| Faculty | Dr. Seshu Babu Pulagara |
| Date | 23rd November, 2021 |

**AIM**

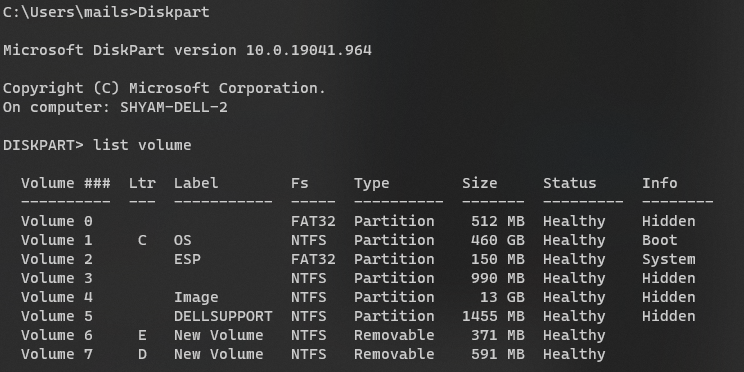
Exploring various methods of data hiding.

**Partition Hiding**

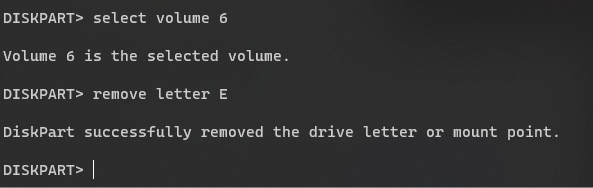
The drive currently has partitions as shown below:



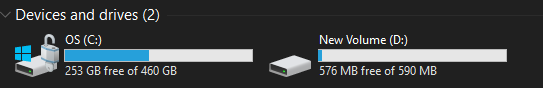
To hide partition E:, open the terminal in Admin mode. Then type in ‘Diskpart’ and press enter. Then enter ‘list volume’ to list the volumes present.



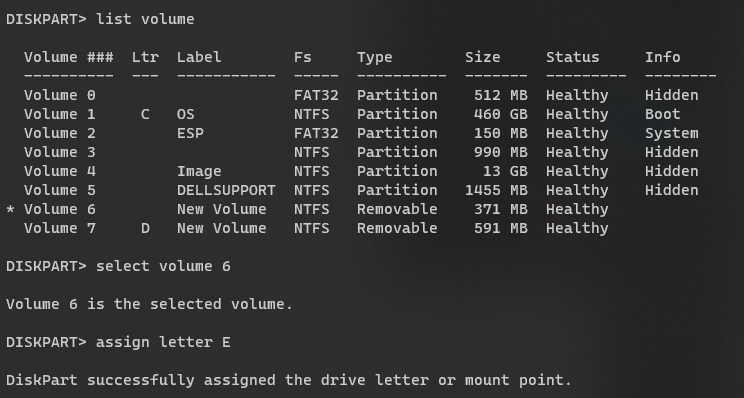
Since we want to hide E:. enter ‘select volume 6’ and enter ‘remove letter E’. The partition is now hidden.

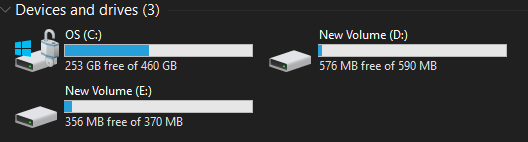


The partition and its contents are no longer visible.



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

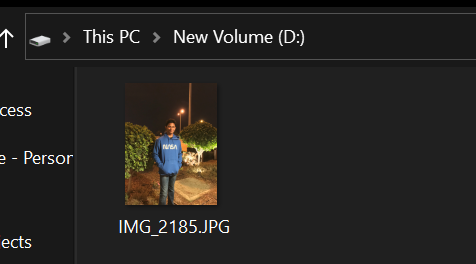




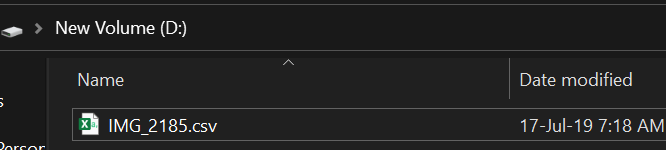
The partition is now unhidden.

**Changing file extensions**

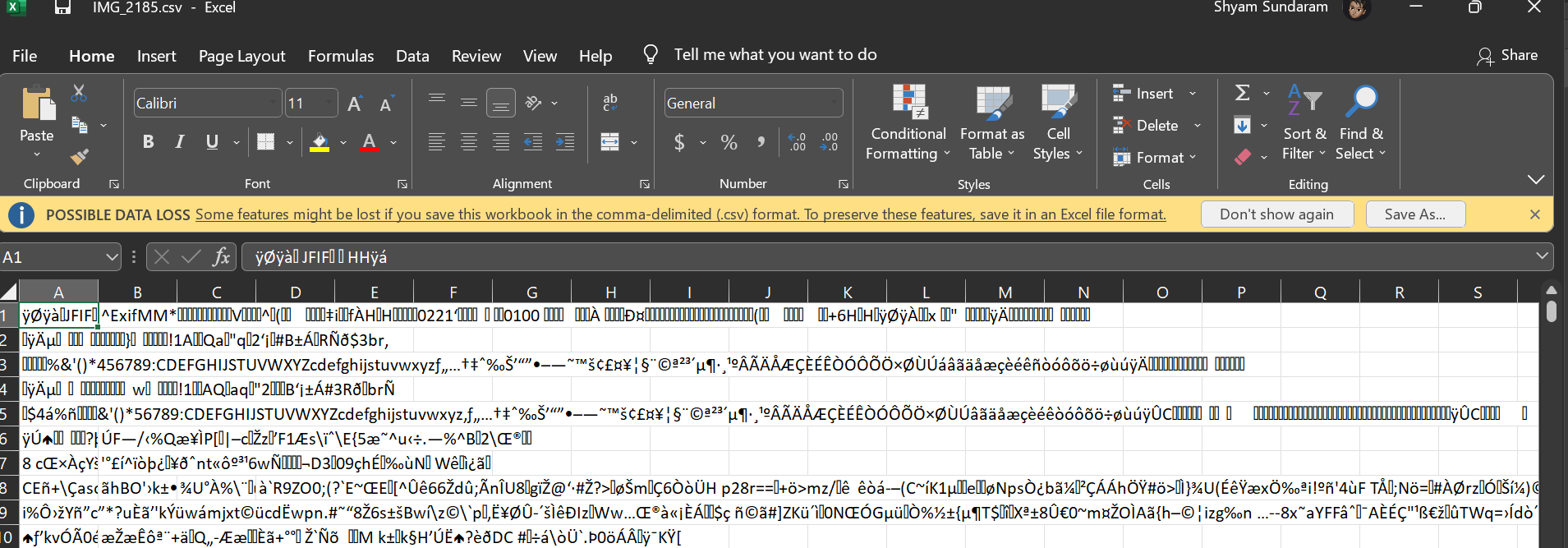
Here, we just change the extension of the file t be hidden. Say I wish to hide the JPG file below.



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



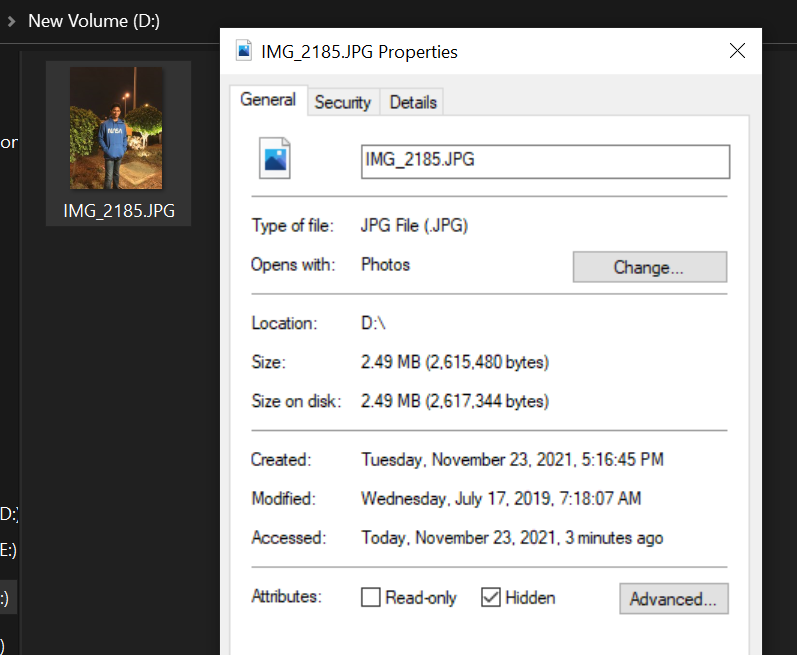
But the file would appear to be gibberish:

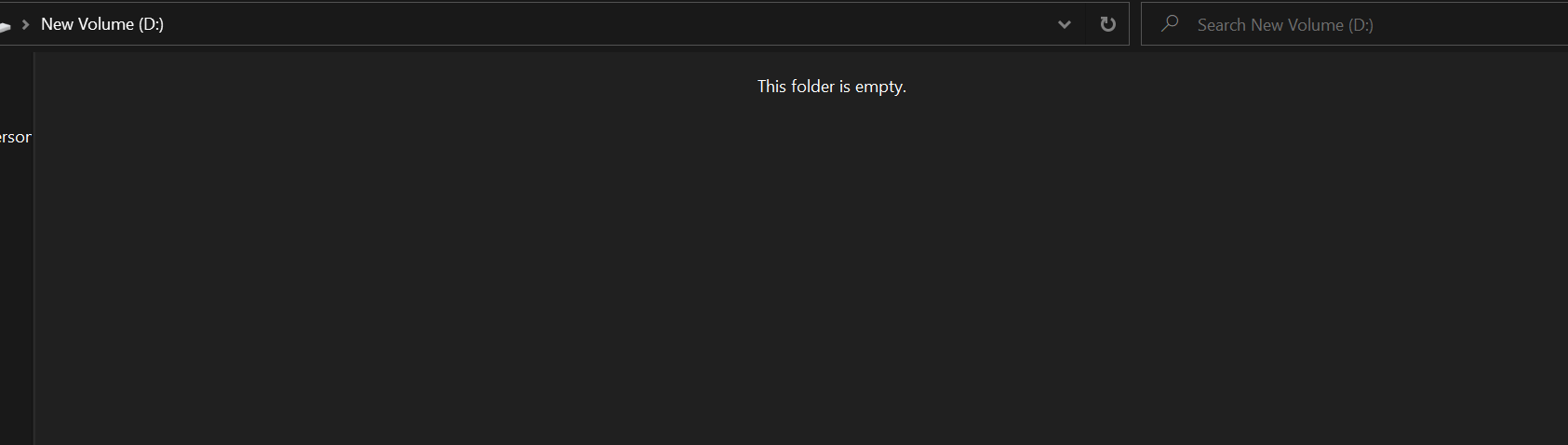


We can obtain it back by changing the extension back to JPG.

**Setting File attributes to Hidden**

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





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.

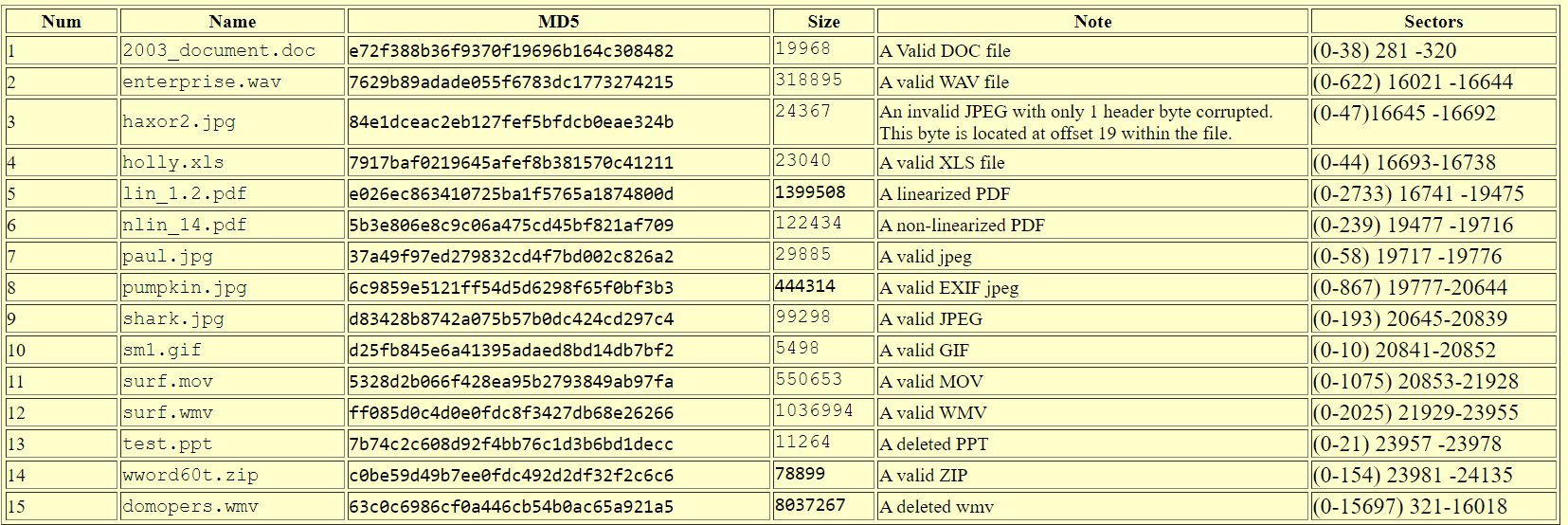
**Bit Shifting**

WinHex can be used for this.

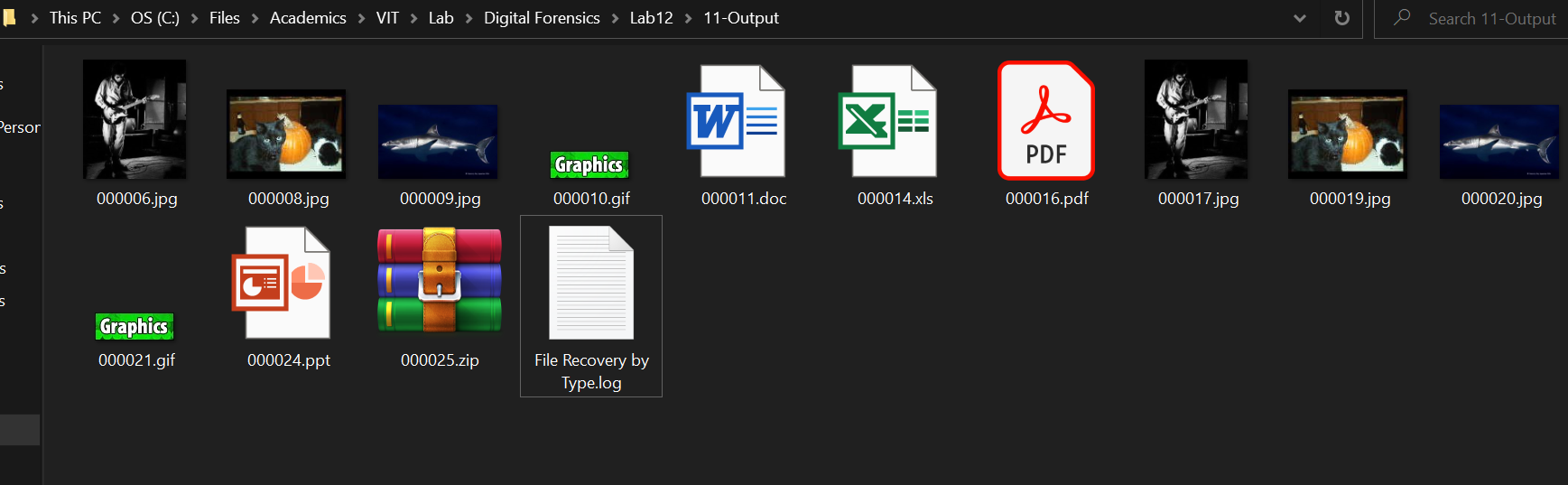
**OBSERVATIONS**

**Image 1 – Image of a FAT disk**

The image used here is that of a FAT disk. It had the following list of files which were then deleted:

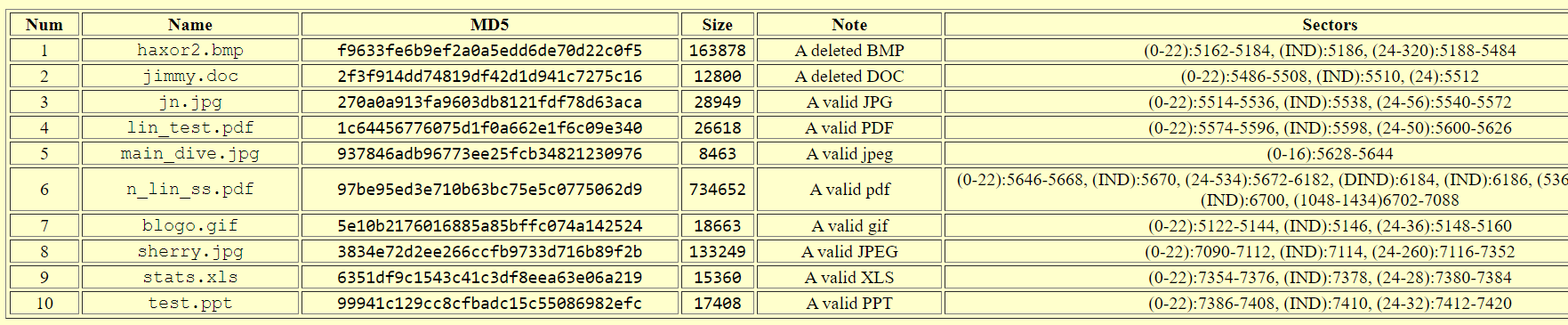


Using WinHex, we try and recover the deleted files by following the process above.



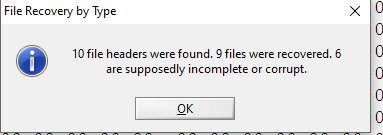
**Image 2 – Image of a EXT2 disk**

The image used here is that of a EXT2 disk. It had the following list of files which were then deleted:

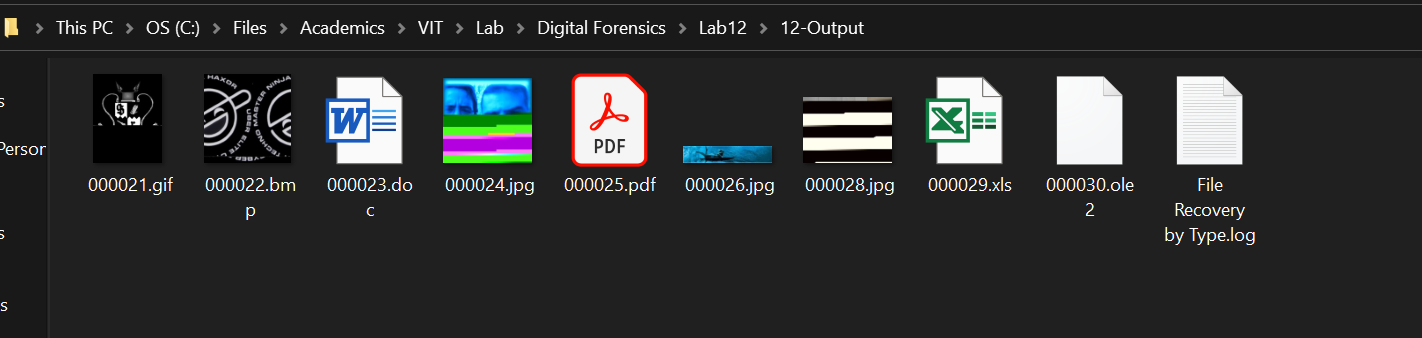


Using WinHex, we try and recover the deleted files by following the process above.

Deleted files which were supported by WinHex could be recovered. However, due to the limits the lack of licensing poses, we extract only files that are smaller than 200 KB. Out of the 10 files detected, 9 were recovered. 6 of them appear to be incomplete or corrupt according to WinHex.



All files recovered from the second image are the following:



**CONCLUSION**

The deleted files were recovered using file/data carving with the aid of WinHex.