DIGITAL FORENSICS LAB

Exercise 10	
Name	S Shyam Sundaram
Registration Number	19BCE1560
Slot	L39+L40
Faculty	Dr. Seshu Babu Pulagara
Date	12th October, 2021

AIM

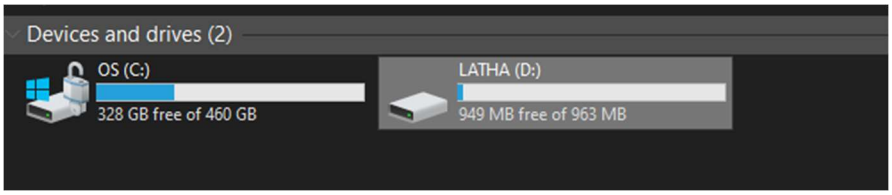
Working with TestDisk to recover deleted partitions and drives.

EXERCISE 1 - TestDisk

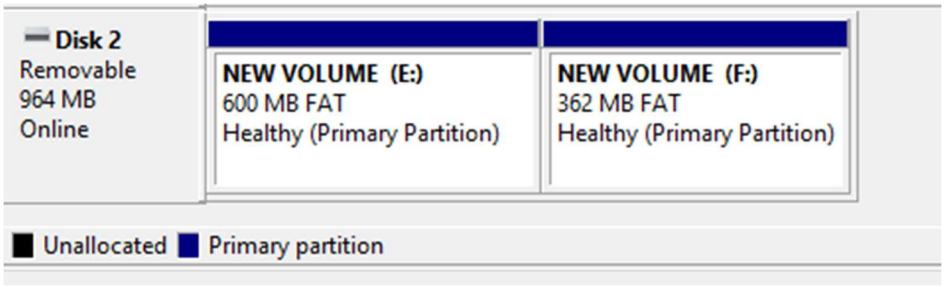
Identification of lost or deleted partitions.

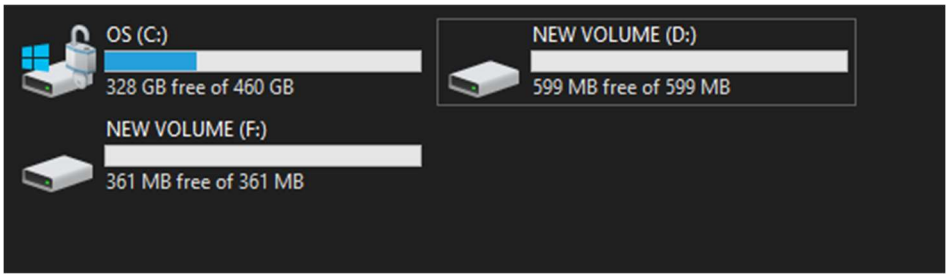
A

First, a partition is created in the USB shown below.

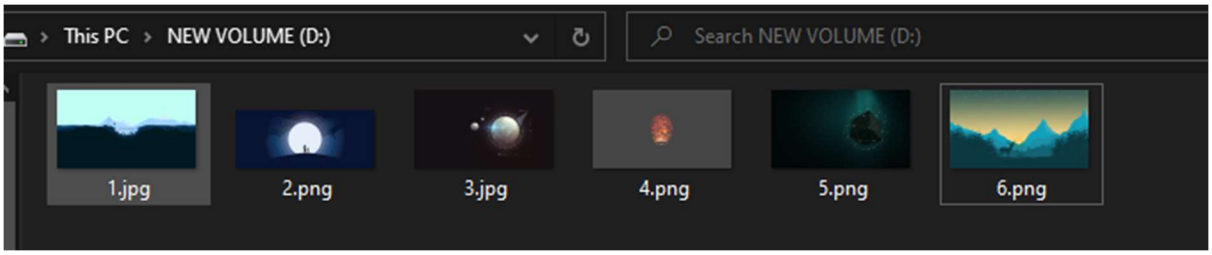


Next, two partitions were created on the USB drive. (Reference: https://www.windowscentral.com/how-set-usb-flash-drive-multiple-partitions-windows-10)

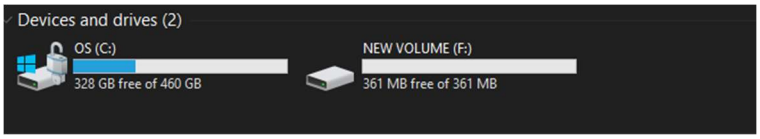




Partition D: was populated by a few JPG and PNG files.



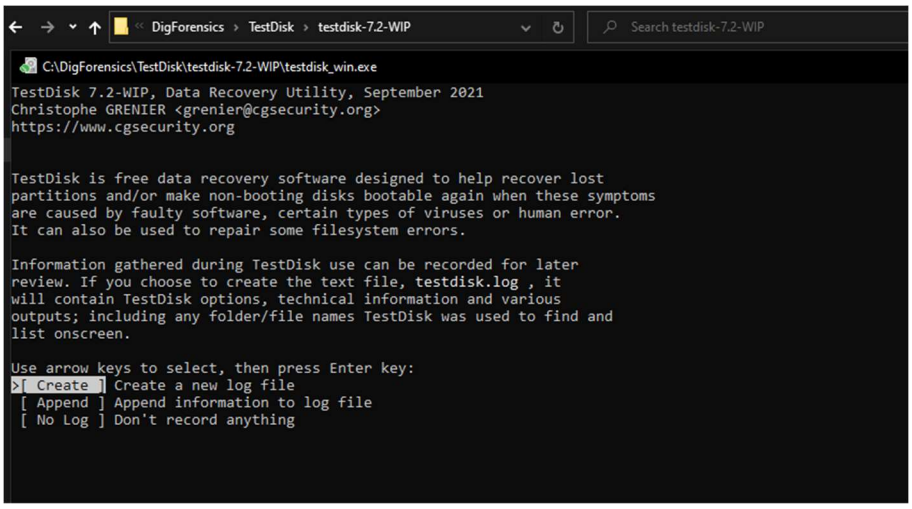
Now, that partition is deleted.



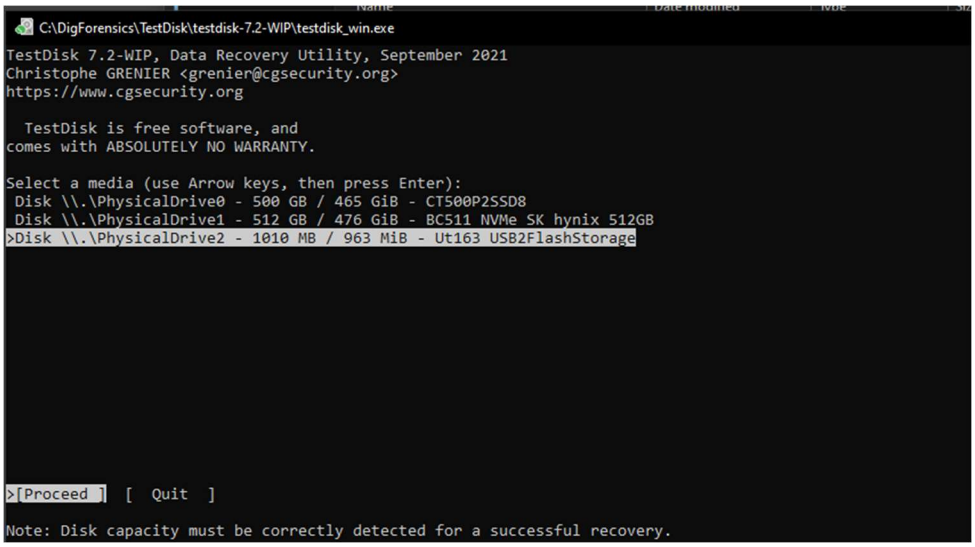
We now use TestDisk to see if we can identify the deleted partition.

STEPS

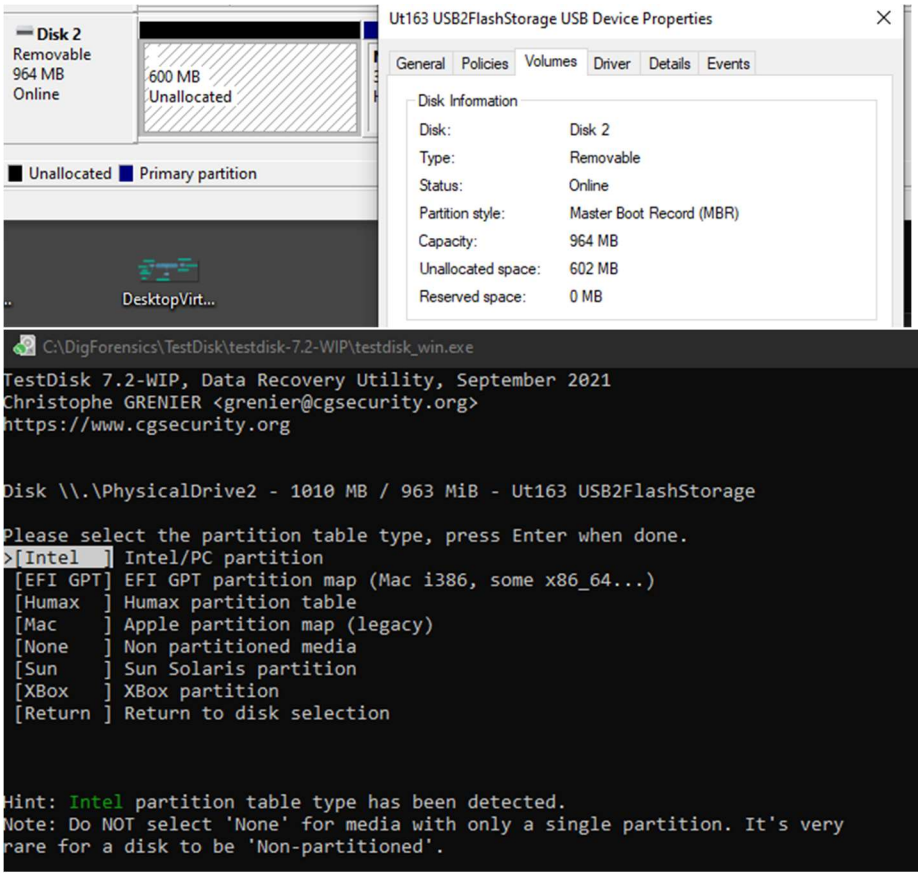
1. Open testdisk_win.exe in the test-disk-7.2-WIP folder.
2. Select 'Create'



3. Select the disk of interest. Here, we choose the USB of 1 GB we had partitioned above.

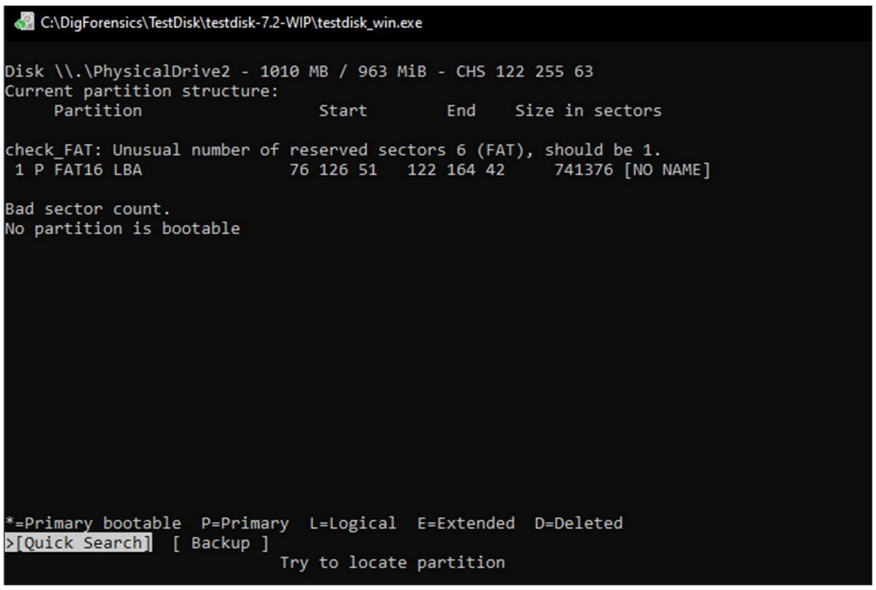


4. Now, select the partition table type. We can see this by checking out the partition properties in the Disk Management program under Volumes tab. We see that this USB partition style is MBR. This means we select ‘Intel/PC partition’ option.

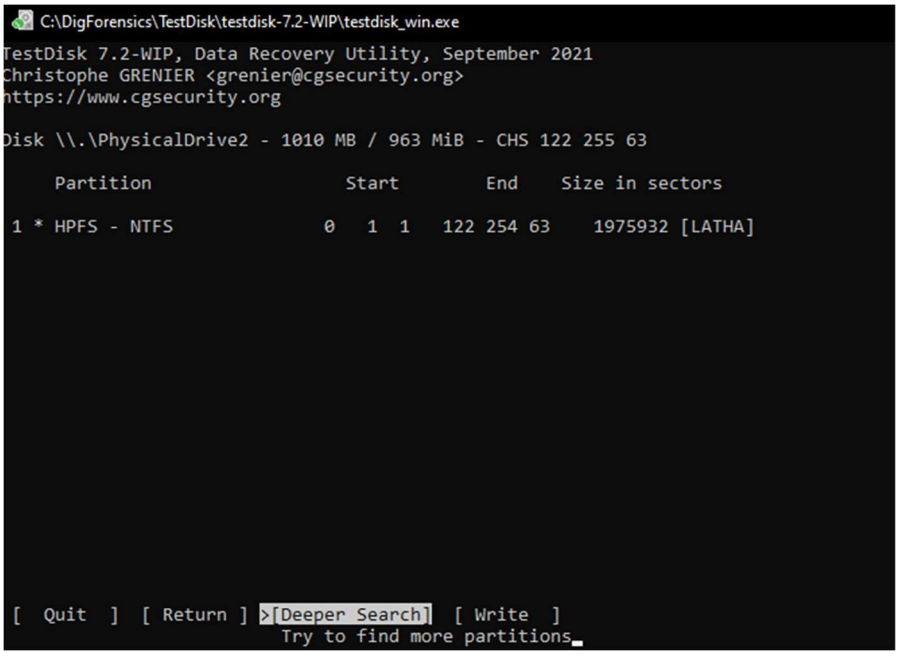


5. Select ‘Analyse’

6. Select ‘Quick Search’.



7. Select ‘Deeper Search’.



8. Upon deeper Search, the deleted partition is not visible.

Note: As this tool did not detect deleted Partition and Undelete requires registration with payment to be used. For this exercise, the third suggested tool, EaseUs is used.

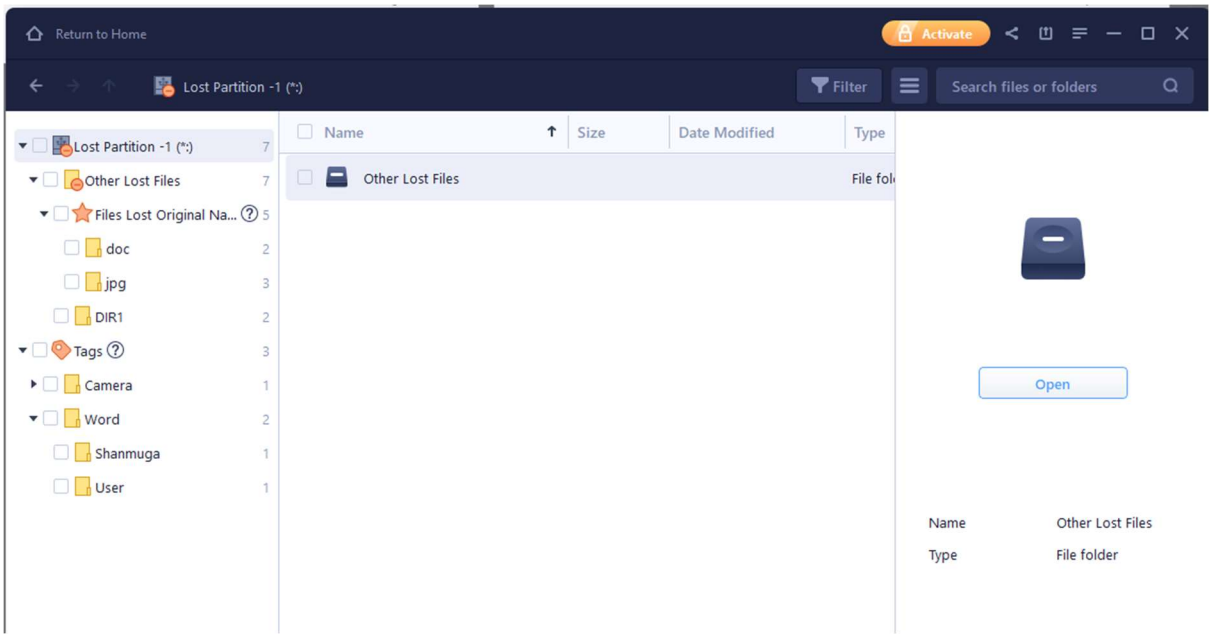
EXERCISE 2 and 3 - EaseUS

Q Identification and recovery of deleted/lost partitions and files.

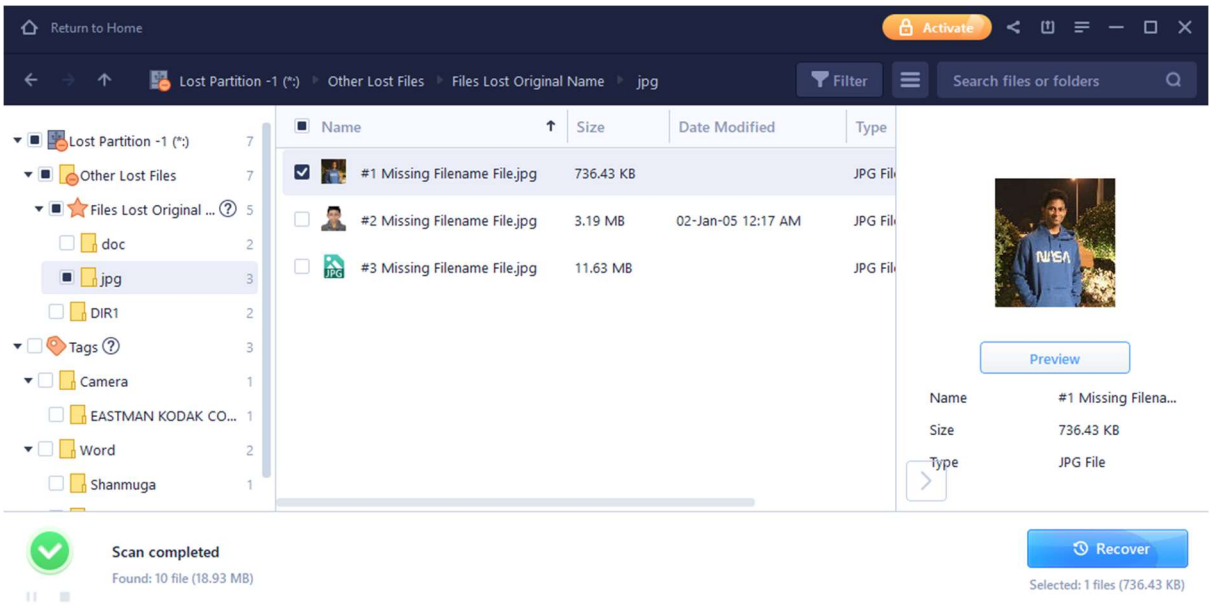
A

For this exercise, the same USB is used and is populated with a JPG file. Then, the whole partition is deleted as seen below.

Next, we open EaseUS and scan the drive. Upon scanning, we see the following:



All the files from the deleted partition are found. Even certain older files are discovered.



The images from the deleted partition are also discovered! To recover, we click ‘Recover’. This recovery will happen only after payment to use the software is done.

OBSERVATIONS

We see that partitions and files deleted can indeed be recovered. These need not be recent files necessarily. Even much older data deleted from drives can be recovered with tools. Some tools are more effective than others (as seen, EaseUS was able to detect and recover partitions and files, whereas TestDisk could not discover the deleted partition itself) but may be proprietary and require purchase of license.

CONCLUSION

Data and partitions deleted can be recovered from drives.