CSE 4004

Digital Forensics

Lab
Session 10

TOPIC: Recovering Deleted Partitions and Deleted Files

Name: Makesh Srinivasan
Registration number: 19BCE1717
Slot: L49 + L50
Date: 11-November-2021-Thursday
Faculty: Prof. Nagaraj

AIM: Recovering deleted partitions and deleted files

Cyber criminals often try to wipe clean a hard disk or other storage media such as Solid State Drives, USB flash drives, CDs, DVDs, magnetic tapes, RAID sub-systems etc. before they depart. They may do this by deleting everything on the storage media or reformatting it. In dealing with such cases, and to conduct a forensic investigation, an investigator needs to use many techniques and often proprietary forensic tools to examine a copy of the storage media and search hidden folders and unallocated disk space for copies of encrypted, deleted, or damaged files.
Partition recovery and file recovery allows you to recover important documents and files that have been lost perhaps by accidental deletion, intentional deletion to conceal evidence, an operating system crash, malfunction of a storage device, logical failure of a storage device, due to a virus, a software malfunction, or even sabotage. Forensic recovery of deleted partitions and files is achieved by using data recovery tools that identify the contents of these lost partitions or files on the storage media and allow for recovering and preserving the data forensically.
The following data recovery situations are some of the common possibilities:
Recovery of deleted or lost files emptied from the Recycle Bin
Disk recovery after a hard disk crash
Data recovery from a hard drive that has been reformatted or repartitioned
Recovery of important documents such as financial records
Recovery from a USB drive, memory card, memory stick, camera card, zip disk, floppy disk, or other storage media
Recovery of files with the original date and timestamp
Finding partitions automatically, even if the boot sector or FAT has been erased or damaged

INSTRUCTIONS:

Exercise 1 Identification of lost or deleted partitions
When a partition is deleted or if the partition table is corrupted, the file systems remain on the disk but their location is unknown and no data can be accessed. Many utilities allow search for partitions and can rewrite the partition table with the partitions chosen by the user. One such open source software for doing this is TestDisk. It was primarily designed to help recover lost partitions and/or make non-booting disks bootable again. It is available at
https://www.cgsecurity.org/wiki/TestDisk
It has many features. It can run under various OS including Windows and Linux.
Create a partition in your drive (may be a USB flash drive) using appropriate tools. Make and copy files of various file types (such as jpg, mp3 etc). Then delete the partition. Check if you are able to detect the files which were there earlier. Use a utility such as TestDisk to recover the partition and then the files.
Refer https://www.cgsecurity.org/wiki/TestDisk_Step_By_Step for step by step instructive examples

Exercise 2 Restoring Lost or Deleted Hard Disk Drive Partition
Download a trial version of EaseUS partition recovery software to restore lost or deleted hard drive partitions in Windows 10/8/7 from the link http://down.easeus.com/product/drw_trial

Exercise 3 Recovering Files and Folders from Deleted Partitions

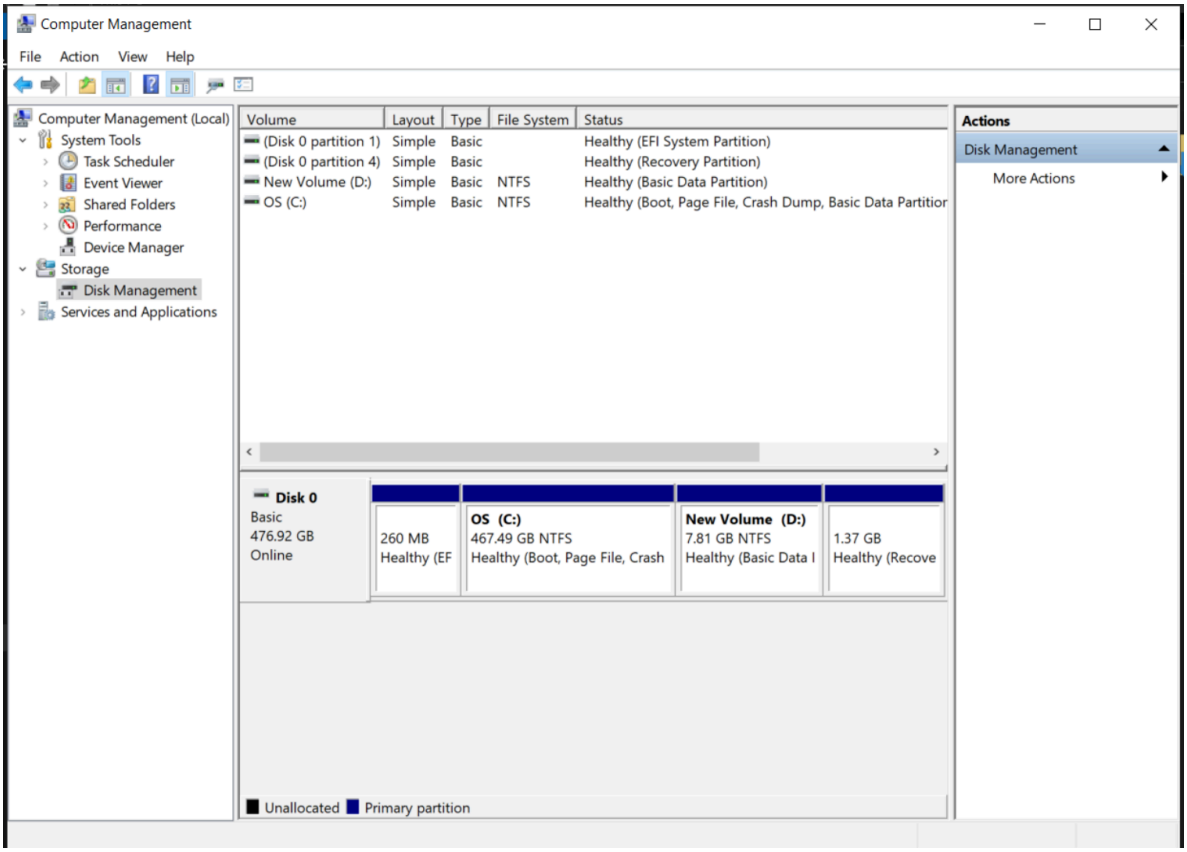
Use the software at http://www.active-undelete.com/undelete.htm and follow the instructions at
http://www.active-undelete.com/howto_recover_from_deleted.htm
For more data recovery tools look at
https://forensicswiki.xyz/wiki/index.php?title=Tools:Data_Recovery
If a particular tool does not work you may use alternative tools.
Include screenshots in your submission.

OBSERVATION:

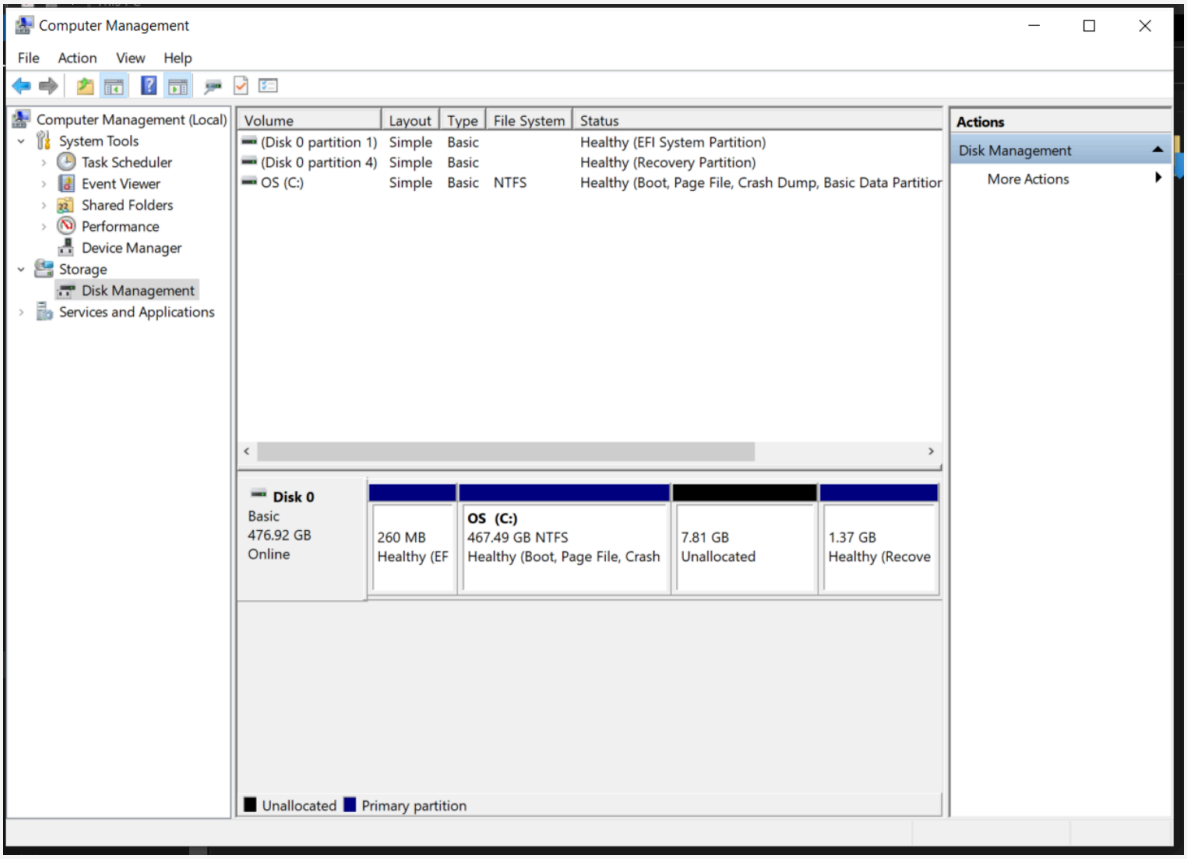
Exercise 1 Identification of lost or deleted partitions

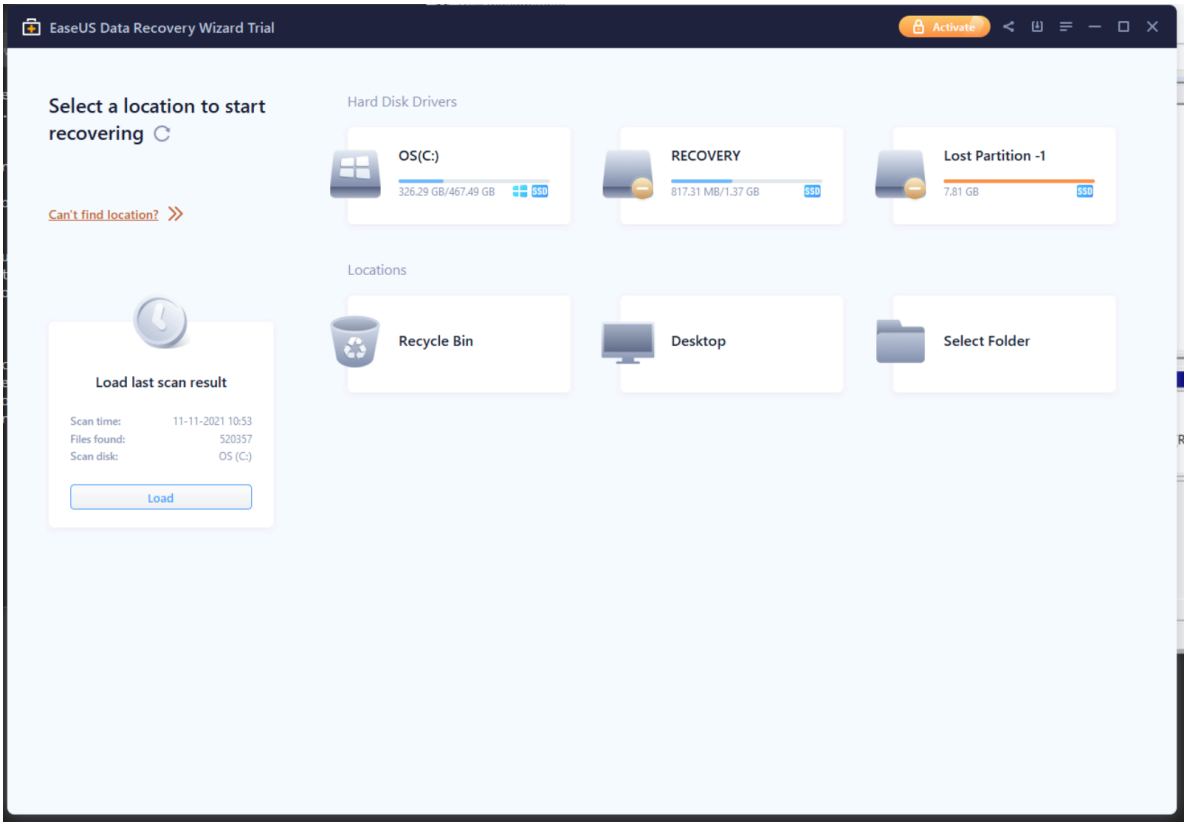
A partition volume D was created, and deleted. With the help of EaseUS, the lost partition is found. The deleted fie is also found by clicking on the lost partition.

Exercise 1

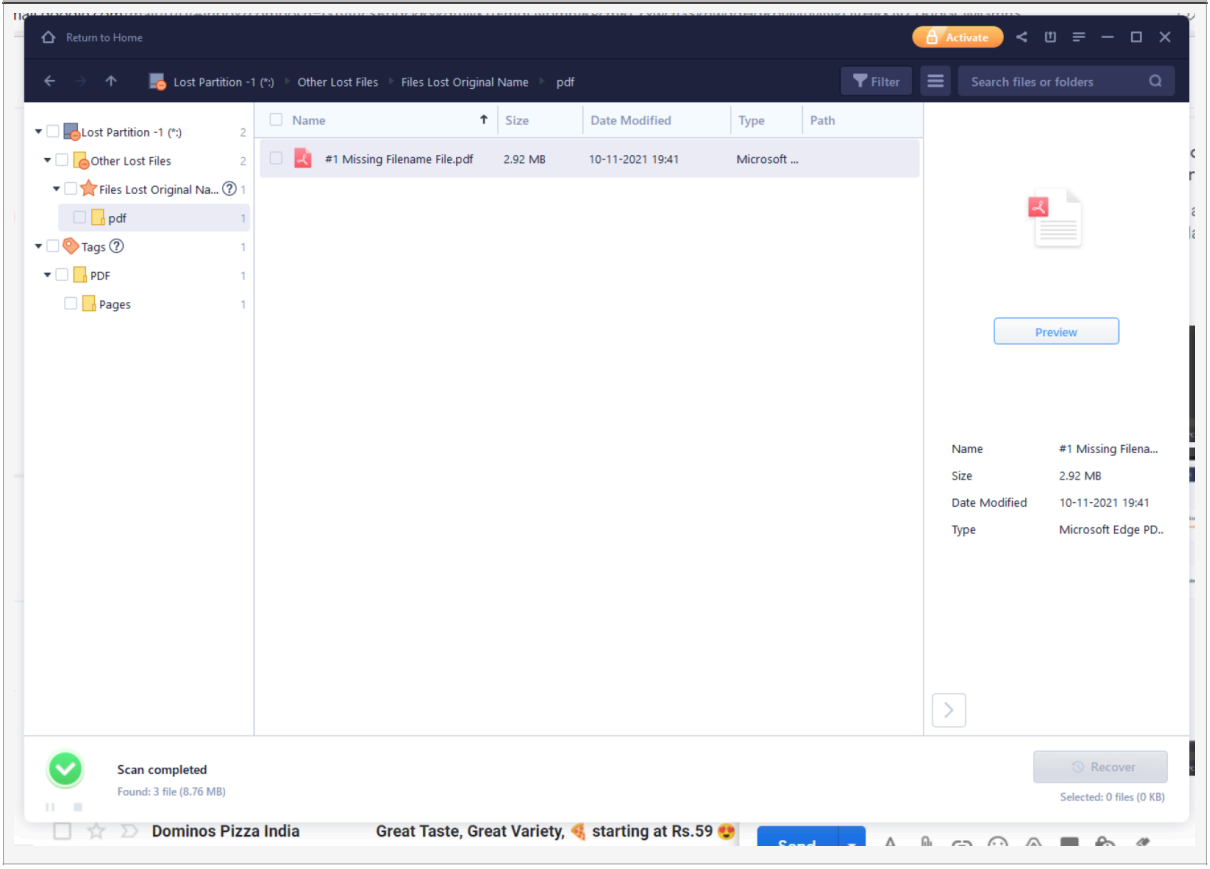


Exercise 1


Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Performance
Device Manager
Storage
Disk Management
Services and Applications
Volume Layout Type File System Status
(Disk 0 partition 1) Simple Basic Healthy (EFI System Partition)
(Disk 0 partition 4) Simple Basic Healthy (Recovery Partition)
OS (C:) Simple Basic NTFS Healthy (Boot, Page File, Crash Dump, Basic Data Partitior
Actions
Disk Management
More Actions
Disk 0
Basic
476.92 GB
Online
260 MB
Healthy (EF
OS (C:)
467.49 GB NTFS
Healthy (Boot, Page File, Crash
7.81 GB
Unallocated
1.37 GB
Healthy (Recove
Unallocated
Primary partition


EaseUS Data Recovery Wizard Trial
Activate
Select a location to start recovering
Can't find location?
Hard Disk Drivers
OS(C:)
326.29 GB/467.49 GB
SSD
RECOVERY
817.31 MB/1.37 GB
SSD
Lost Partition -1
7.81 GB
SSD
Locations
Recycle Bin
Desktop
Select Folder
Load last scan result
Scan time: 11-11-2021 10:53
Files found: 520357
Scan disk: OS (C:)
Load

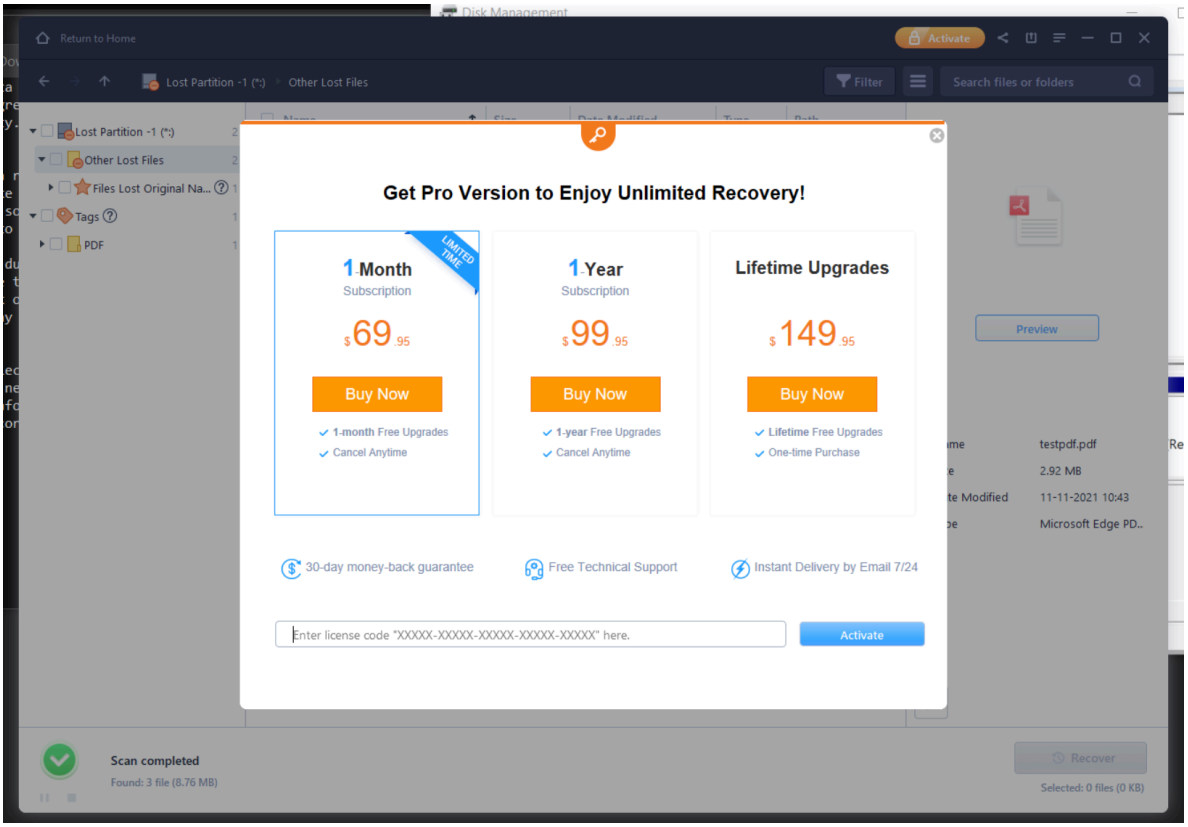
Exercise 1



The files and the lost partition is found

Exercise 2 Restoring Lost or Deleted Hard Disk Drive Partition

Exercise 2

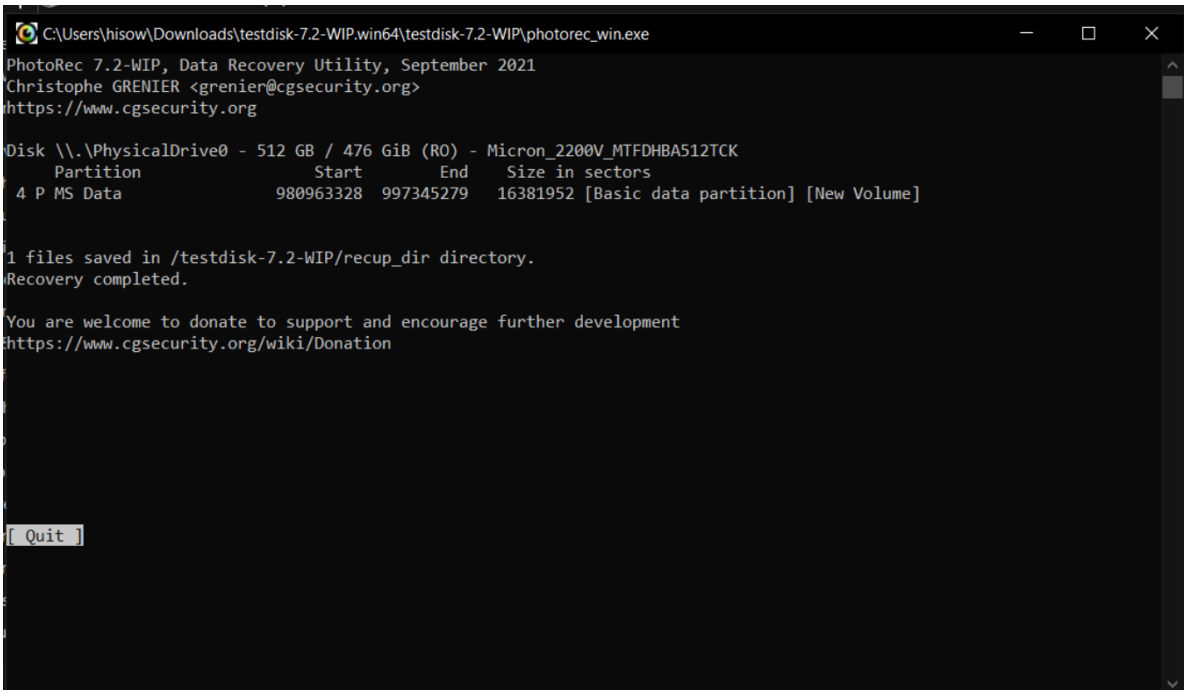


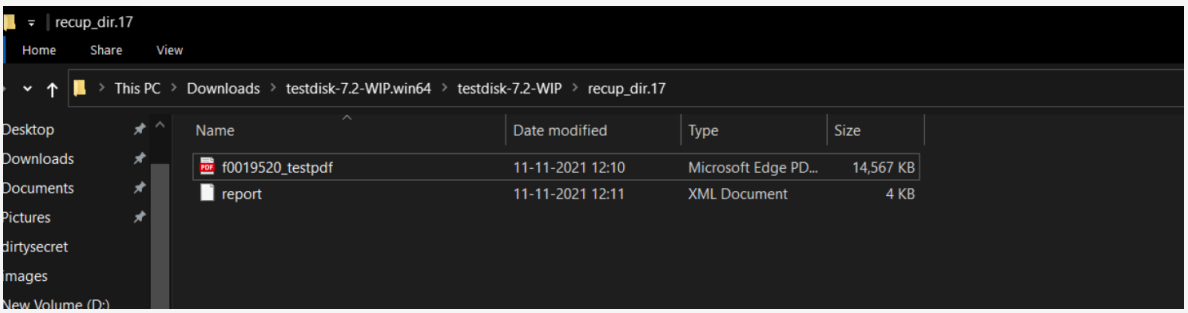
The lost partition is found using EaseUS but an active paid plan is necessary to restore the lost partition along with the lost files.

Exercise 3: Recovering Files and Folders from Deleted Partitions

The deleted files can be restored or recovered using TextDisk and the steps are shown below.

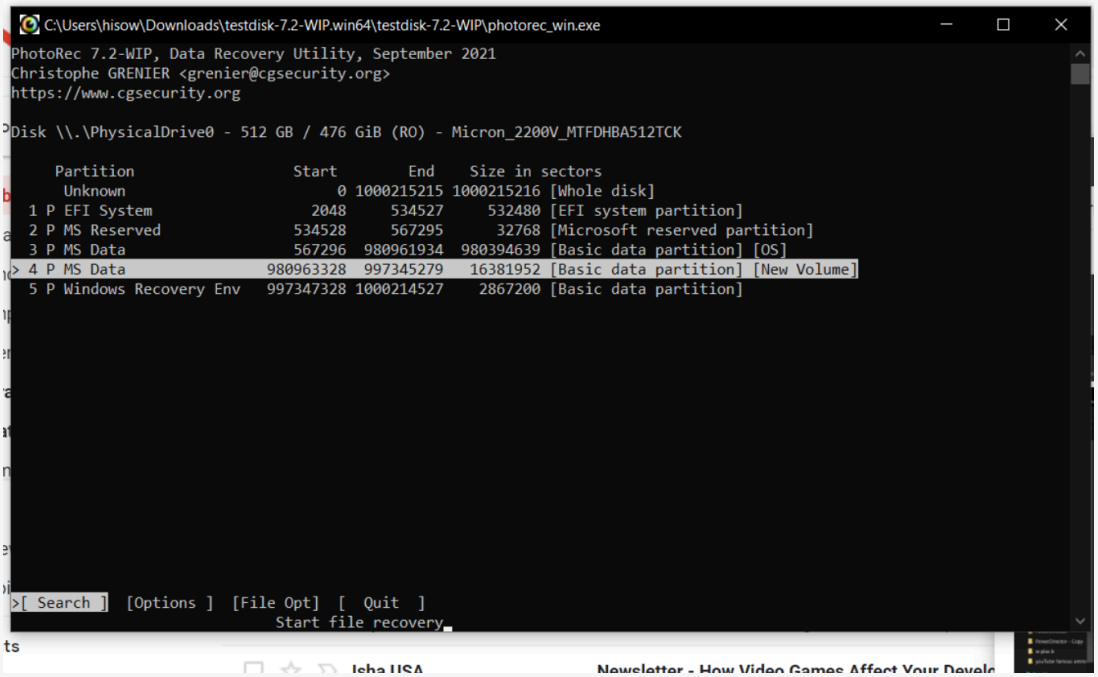
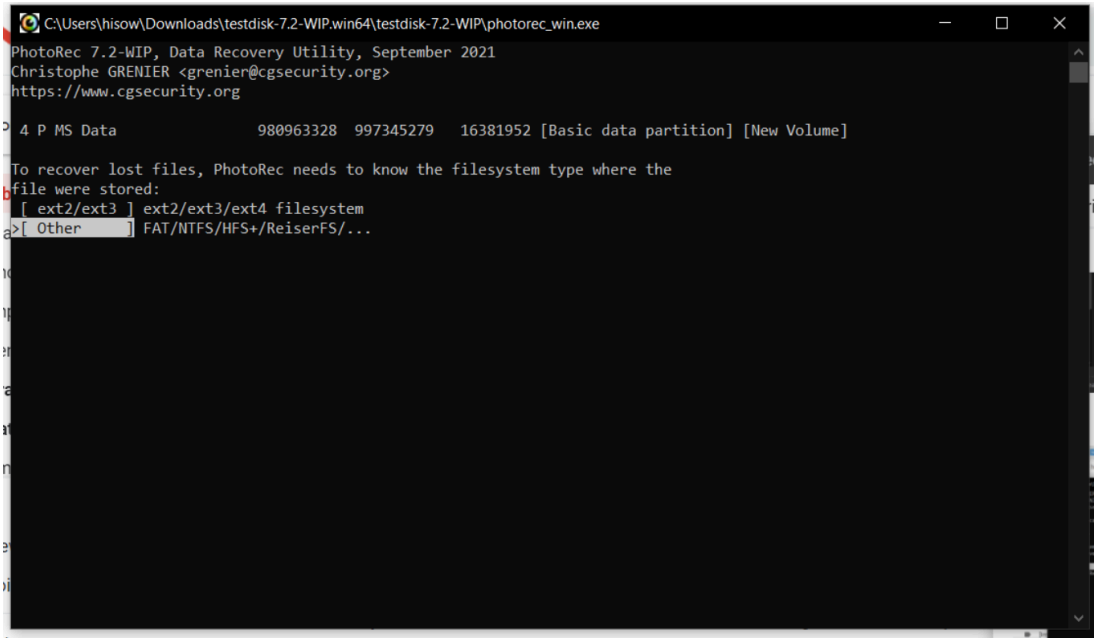
Exercise 3

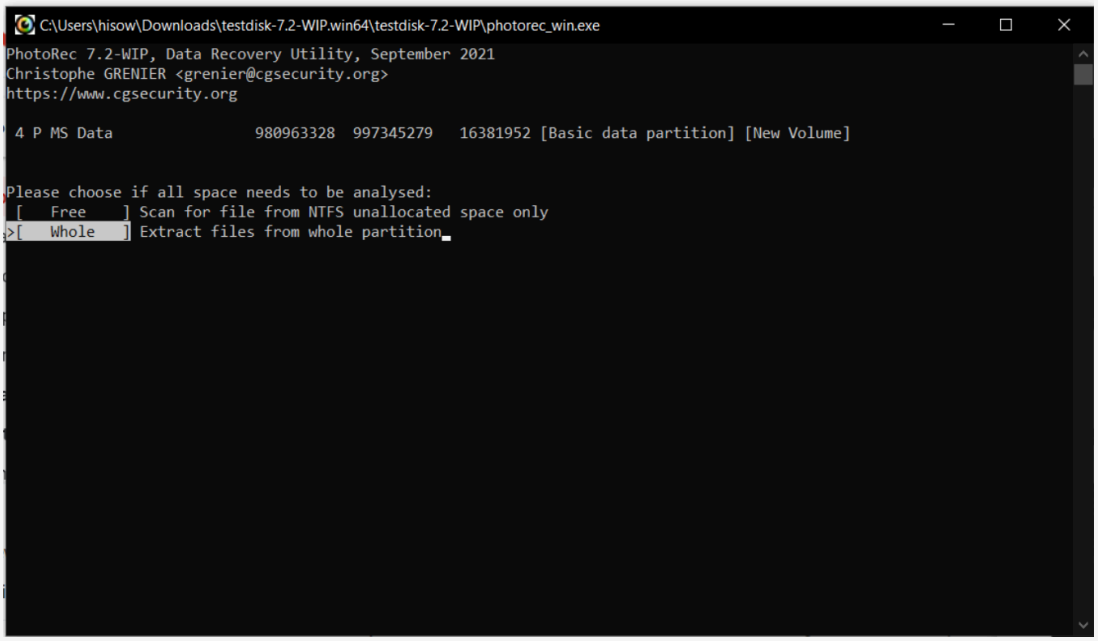




As shown above, the files are recovered and stored in the recup_dir

The following screenshots show the process to recover the files.

1	Open the TestDisk application and choose log create option
2	Choose the partition to recover files in 
3	Choose other: 

4	Search the whole partition to recover the file: 
5	Recovered the file: 

Conclusion

The three exercises were done using EaseUS and TestDisk application on the Windows 10 operating system environment.