

EXPERIMENT--02

Aim:

To recover lost or deleted partitions/files using the TestDisk forensic tool.

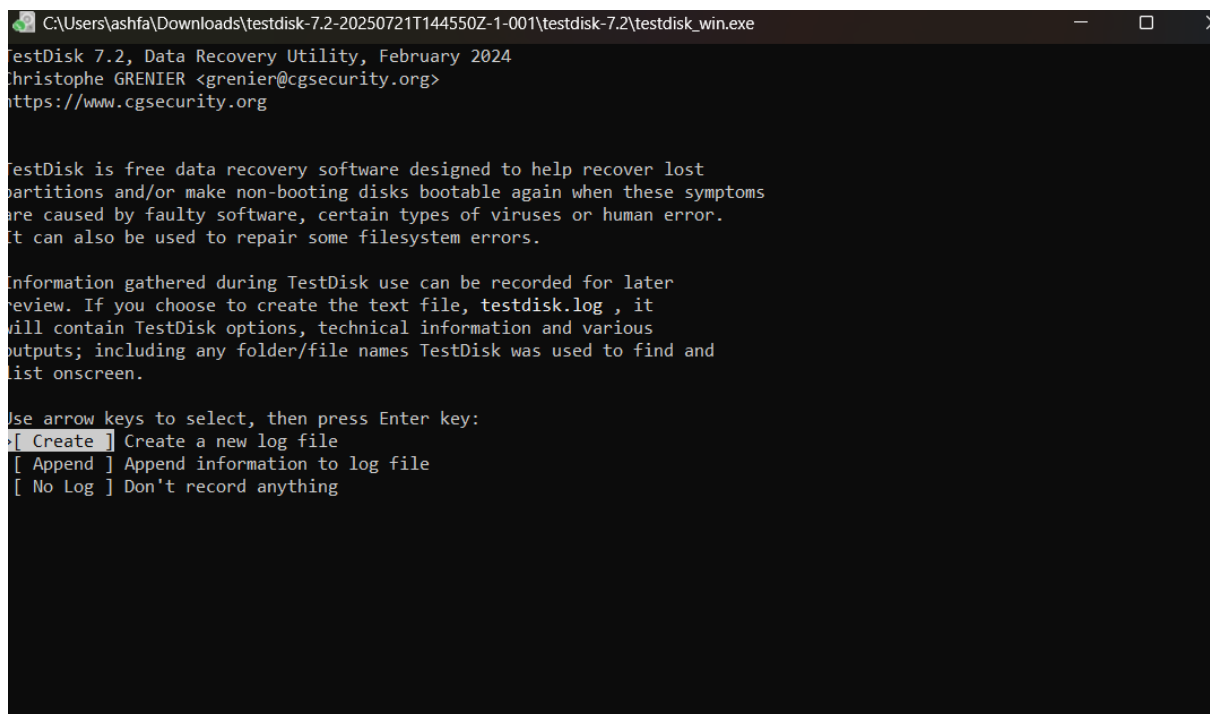
Tools Used:

- TestDisk
- Windows/Linux Operating System

Procedure:

1. Launch TestDisk from the command line.
2. Select the storage device to be analysed.
3. Choose Analyse to scan for lost or deleted partitions.
4. Navigate through the detected partitions and list the files.
5. Recover selected files or partitions to a safe location.

Outputs:



```
C:\Users\ashfa\Downloads\testdisk-7.2-20250721T144550Z-1-001\testdisk-7.2\testdisk_win.exe
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

TestDisk is free data recovery software designed to help recover lost
partitions and/or make non-booting disks bootable again when these symptoms
are caused by faulty software, certain types of viruses or human error.
It can also be used to repair some filesystem errors.

Information gathered during TestDisk use can be recorded for later
review. If you choose to create the text file, testdisk.log , it
will contain TestDisk options, technical information and various
outputs; including any folder/file names TestDisk was used to find and
list onscreen.

Use arrow keys to select, then press Enter key:
[ Create ] Create a new log file
[ Append ] Append information to log file
[ No Log ] Don't record anything
```

```
C:\Users\ashfa\Downloads\testdisk-7.2-20250721T144550Z-1-001\testdisk-7.2\testdisk_win.exe
testDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

TestDisk is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media and choose 'Proceed' using arrow keys:
Disk \\.\PhysicalDrive0 - 512 GB / 476 GiB - NVMe Micron_2450_MTFDKBA512TFK

[Proceed] [Quit]

Note: Serial number 0000_0000_0000_0001_00A0_7522_3823_189F.
Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has an incorrect size, check HD jumper settings and BIOS
detection, and install the latest OS patches and disk drivers.
```

```
C:\Users\ashfa\Downloads\testdisk-7.2-20250721T144550Z-1-001\testdisk-7.2\testdisk_win.exe
testDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk \\.\PhysicalDrive0 - 512 GB / 476 GiB - NVMe Micron_2450_MTFDKBA512TFK

Please select the partition table type, press Enter when done.
[Intel] Intel/PC partition
[EFI GPT] EFI GPT partition map (Mac i386, some x86_64...)
[Humax] Humax partition table
[Mac] Apple partition map (legacy)
[None] Non partitioned media
[Sun] Sun Solaris partition
[XBox] Xbox partition
[Return] Return to disk selection

Hint: EFI GPT partition table type has been detected.
Note: Do NOT select 'None' for media with only a single partition. It's very
rare for a disk to be 'Non-partitioned'.
```

```
C:\Users\ashfa\Downloads\testdisk-7.2-20250721T144550Z-1-001\testdisk-7.2\testdisk_win.exe
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk \\.\PhysicalDrive0 - 512 GB / 476 GiB - NVMe Micron_2450_MTFDKBA512TFK
CHS 62260 255 63 - sector size=512

> [ Analyze ] Analyze current partition structure and search for lost partitions
[ Advanced ] Filesystem Utils
[ Geometry ] Change disk geometry
[ Options ] Modify options
[ Quit ] Return to disk selection

Note: Correct disk geometry is required for a successful recovery. 'Analyze'
process may give some warnings if it thinks the logical geometry is mismatched.
```

```
C:\Users\ashfa\Downloads\testdisk-7.2-20250721T144550Z-1-001\testdisk-7.2\testdisk_win.exe
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk \\.\PhysicalDrive0 - 512 GB / 476 GiB - CHS 62260 255 63
Current partition structure:
  Partition          Start          End      Size in sectors
1 P EFI System       2048          534527    532480 [EFI system partition]
No FAT, NTFS, ext2, JFS, Reiser, cramfs or XFS marker
2 P MS Reserved     534528         567295     32768 [Microsoft reserved partition]
2 P MS Reserved     534528         567295     32768 [Microsoft reserved partition]
No FAT, NTFS, ext2, JFS, Reiser, cramfs or XFS marker
3 P MS Data         567296     997495438    996928143 [Basic data partition]
3 P MS Data         567296     997495438    996928143 [Basic data partition]
4 P Windows Recovery Env 997496832    999682047     2185216
5 P Windows Recovery Env 999682048   1000214527    532480 [Basic data partition]

P=Primary D=Deleted
> [Quick Search] [ Backup ]
Try to locate partition
```

```
C:\Users\ashfa\Downloads\testdisk-7.2-20250721T144550Z-1-001\testdisk-7.2\testdisk_win.exe
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk \\.\PhysicalDrive0 - 512 GB / 476 GiB - CHS 62260 255 63
Analyze cylinder 39/62259: 00%

EFI System                2048      534527      532480 [EFI System Partition] [SYSTEM]

Stop
```

```
TestDisk 7.3-WIP, Data Recovery Utility, April 2025
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Write partition table, confirm ? (Y/N)
```

Result:

Lost or deleted files/partitions were successfully identified and recovered using TestDisk.