Ex.No.2 Recover Deleted or Damaged Files using TestDisk

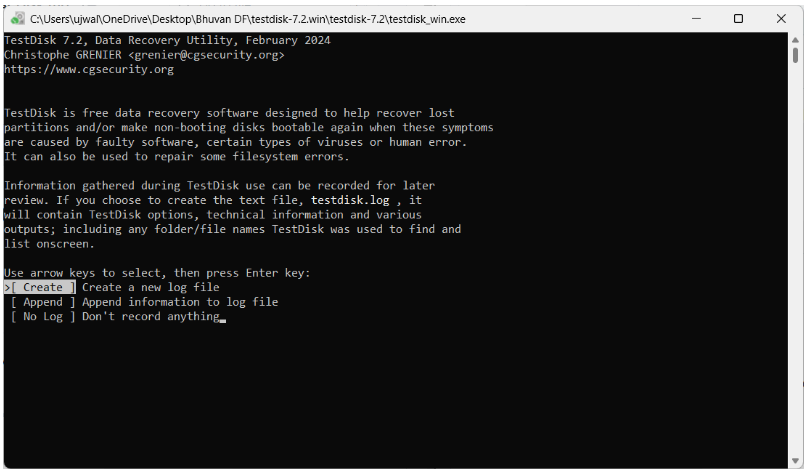
Aim

To use **TestDisk** step-by-step to recover a missing partition, repair a corrupted partition, and restore access to lost files.

Step 1: Log Creation & Disk Detection

Log Creation

- When TestDisk starts, Select the [Create] option to generate a log file of the recovery session. This is helpful for future reference or troubleshooting.


C:\Users\ujwal\OneDrive\Desktop\Bhuvan DF\testdisk-7.2.win\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
```

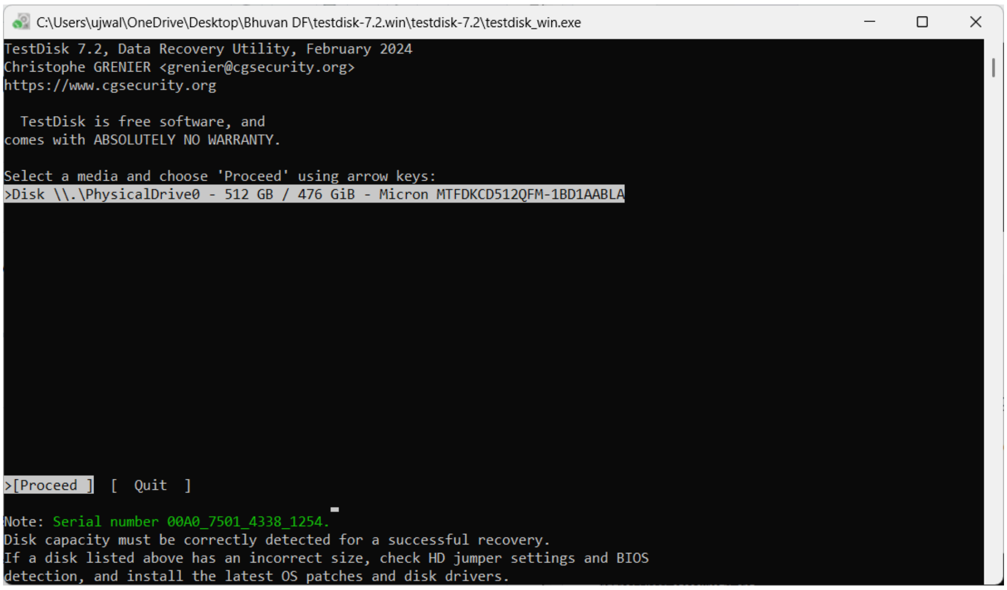
Disk Detection

- All hard drives will be listed with their correct sizes.

Use the **Up/Down arrow keys** to select the target disk.

> If available, prefer `/dev/rdisk*` (raw device) over `/dev/disk*` for faster performance

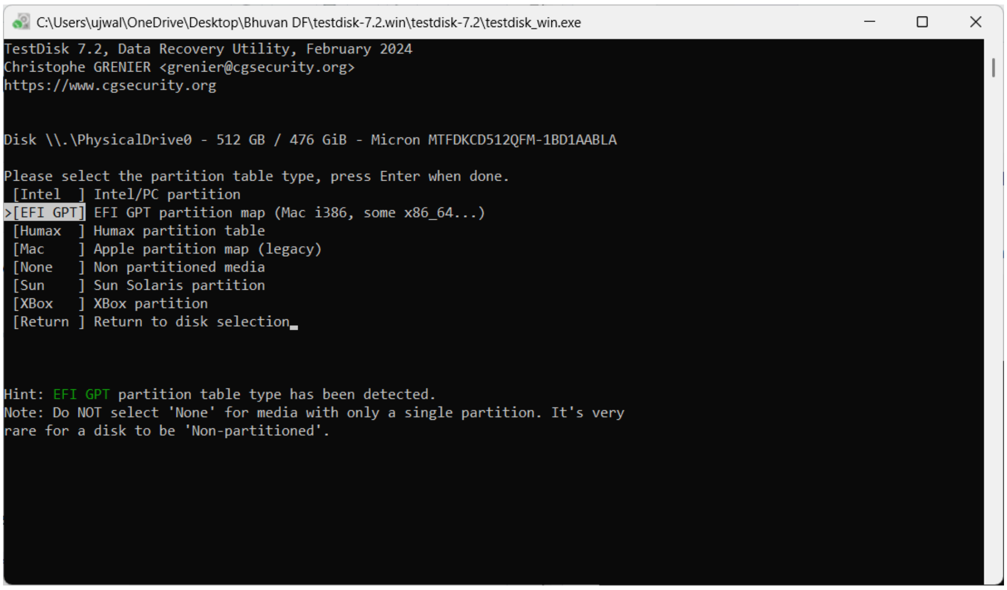
- Select [Proceed] to move to the next step.


C:\Users\ujwal\OneDrive\Desktop\Bhuvan DF\testdisk-7.2.win\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 - Micron MTFDKCD512QFM-1BD1AABLA



>[Proceed ]  [  Quit  ]

Note: Serial number 00A0_7501_4338_1254.
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.
```

Step 2: Partition Table Type Selection

- TestDisk auto-detects the partition table type.
- Usually, the **default value is correct**.
- Press **Enter** to proceed.


C:\Users\ujwal\OneDrive\Desktop\Bhuvan DF\testdisk-7.2.win\testdisk-7.2\testdisk_win.exe

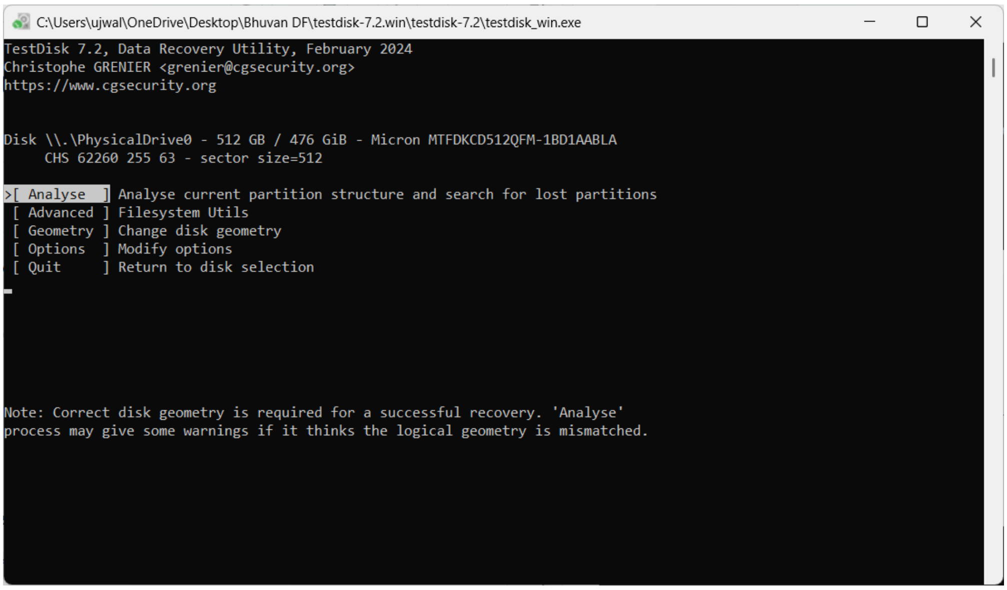
```
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org


Disk \\.\PhysicalDrive0 - 512 GB / 476 GiB - Micron MTFDKCD512QFM-1BD1AABLA

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'.
```

Step 3: Analyse Partition Structure

- Select **Analyse** from the menu to view the current partition structure.
- Missing or corrupted partitions will be shown here.

> Example issues:

- A partition listed twice → indicates corruption.
- "Invalid NTFS boot" → damaged NTFS boot sector.
- Missing logical partition(s).
- Press **Enter** to proceed to **Quick Search**.



C:\Users\ujwal\OneDrive\Desktop\Bhuvan DF\testdisk-7.2.win\testdisk-7.2\testdisk_win.exe

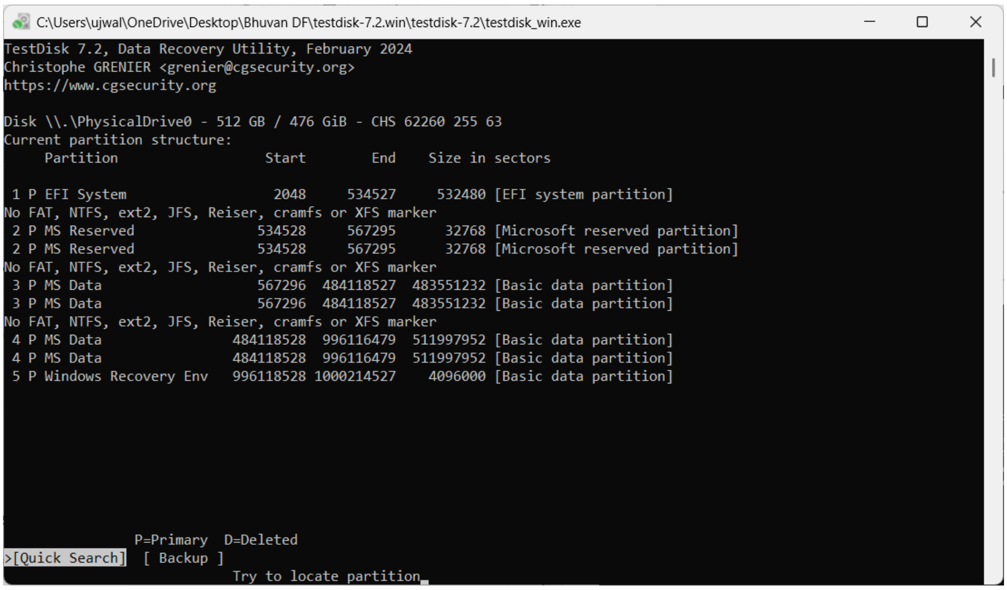
```
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org


Disk \\.\PhysicalDrive0 - 512 GB / 476 GiB - Micron MTFDKCD512QFM-1BD1AABLA
     CHS 62260 255 63 - sector size=512

>[ Analyse  ] Analyse 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. 'Analyse'
process may give some warnings if it thinks the logical geometry is mismatched.
```

Step 4: Quick Search for Partitions

- TestDisk performs a **Quick Search** and lists found partitions in real-time.
- Highlight the missing partition and press **p** to list its files.

> Files in **red** are deleted entries. Use **q** to go back.

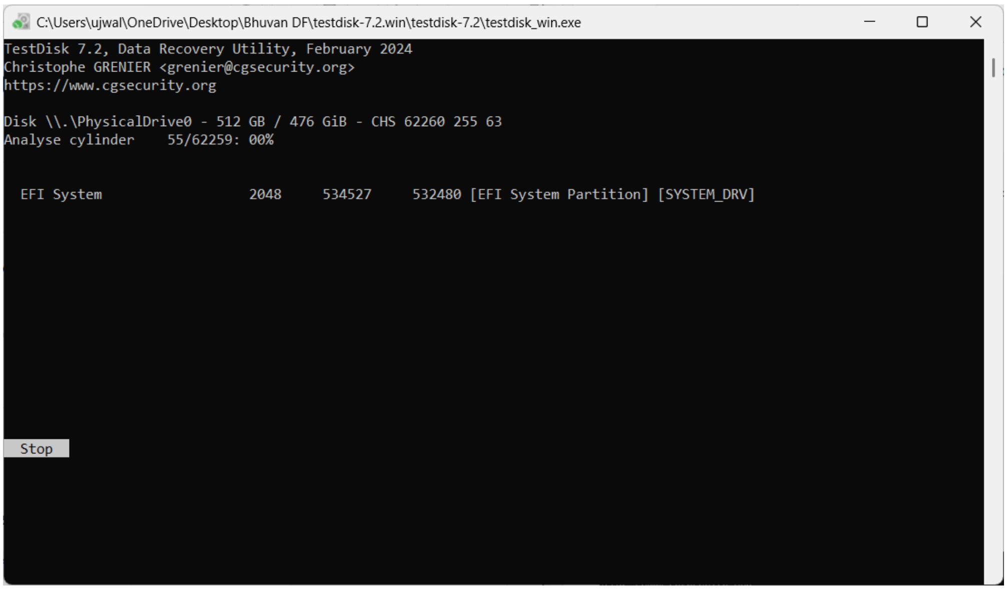
- If all looks correct, press **Enter** to continue.



```
C:\Users\ujwal\OneDrive\Desktop\Bhuvan DF\testdisk-7.2.win\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  484118527  483551232 [Basic data partition]
 3 P MS Data                   567296  484118527  483551232 [Basic data partition]
No FAT, NTFS, ext2, JFS, Reiser, cramfs or XFS marker
 4 P MS Data                484118528  996116479  511997952 [Basic data partition]
 4 P MS Data                484118528  996116479  511997952 [Basic data partition]
 5 P Windows Recovery Env   996118528 1000214527    4096000 [Basic data partition]






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

Step 5: Save Partition Table / Deeper Search

- If not all partitions are visible, select **Deeper Search**.
- This scans for backup boot sectors (FAT32, NTFS, ext2/ext3) cylinder by cylinder.
- This process can take a long time, as it scans the entire drive, block by block, to find remnants of partition structures.
- Again, use p to preview files and confirm if a found partition is the one you are looking for.

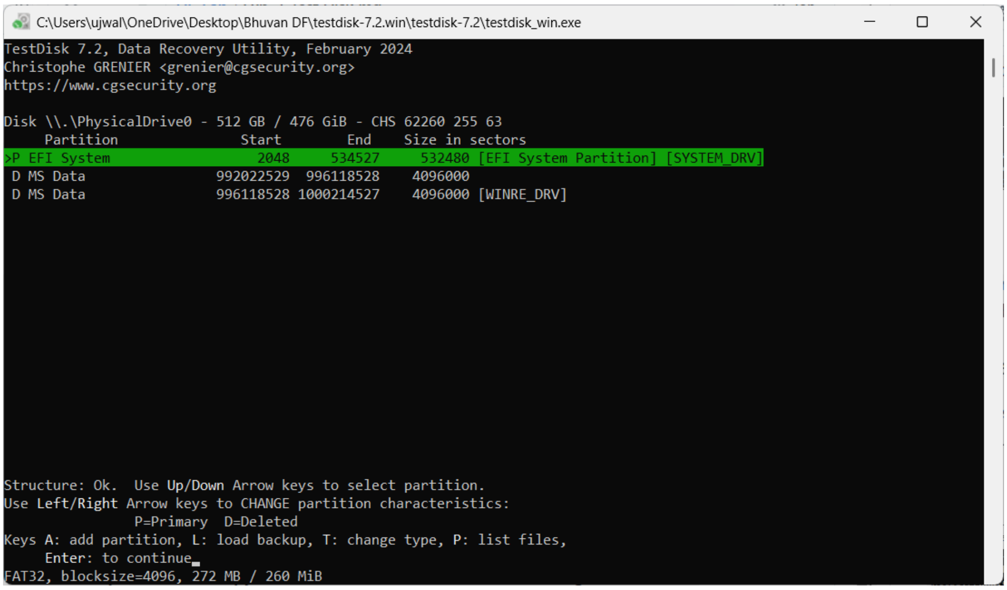


```
C:\Users\ujwal\OneDrive\Desktop\Bhuvan DF\testdisk-7.2.win\testdisk-7.2\testdisk_win.exe
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk \\.\PhysicalDrive0 - 512 GB / 476 GiB - CHS 62260 255 63
Analyse cylinder    55/62259: 00%


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













  Stop
```

After the deeper scan:

- Partitions found using backup boot sectors are listed.
- Overlapping or corrupted entries will appear as **D (Deleted)**.
- Highlight the correct partition and press **p** to verify its files.

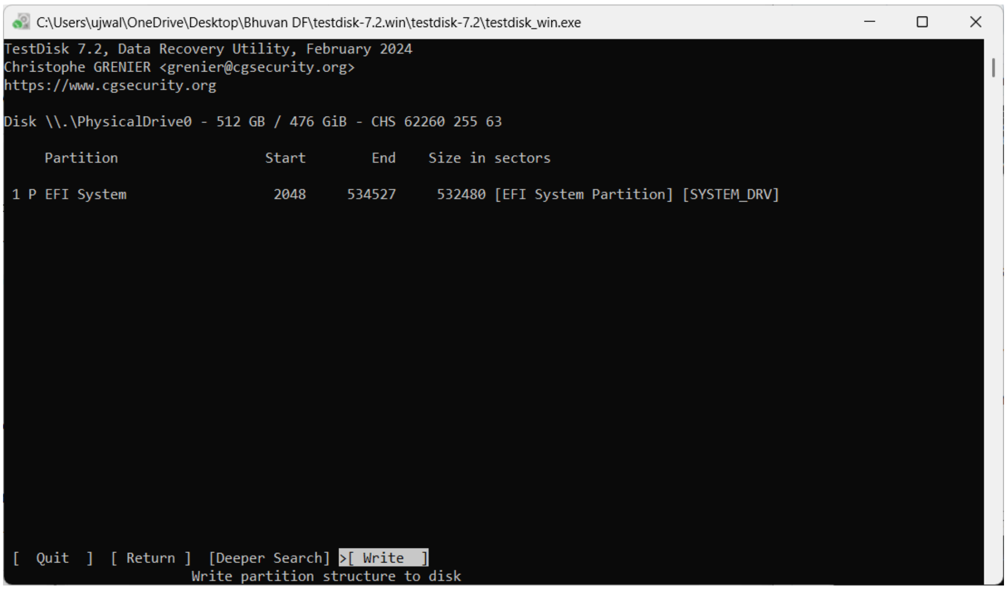
- Use **Left/Right arrow keys** to change partition status:
  - `P` → Primary
  - `*` → Bootable
  - `L` → Logical
  - `D` → Deleted


C:\Users\ujwal\OneDrive\Desktop\Bhuvan DF\testdisk-7.2.win\testdisk-7.2\testdisk_win.exe

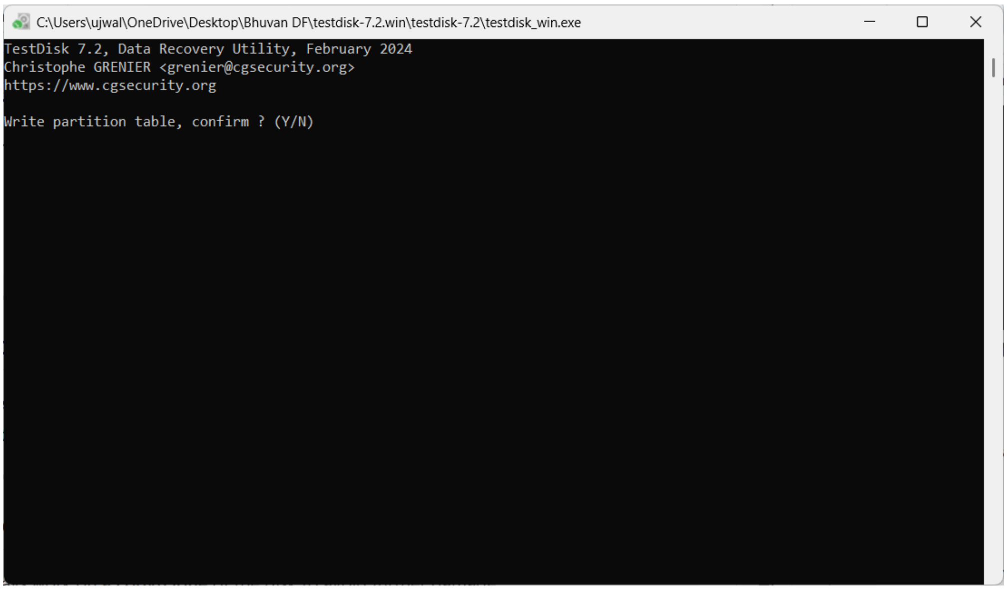
```
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk \\.\PhysicalDrive0 - 512 GB / 476 GiB - CHS 62260 255 63
     Partition               Start        End    Size in sectors
>P EFI System                 2048     534527     532480 [EFI System Partition] [SYSTEM_DRV]
 D MS Data               992022529  996118528    4096000
 D MS Data               996118528 1000214527    4096000 [WINRE_DRV]

Structure: Ok.  Use Up/Down Arrow keys to select partition.
Use Left/Right Arrow keys to CHANGE partition characteristics:
                P=Primary  D=Deleted
Keys A: add partition, L: load backup, T: change type, P: list files,
     Enter: to continue
FAT32, blocksize=4096, 272 MB / 260 MiB
```

Step 6: Partition Table Recovery

- Once correct partitions are marked:
  - Confirm with **Write** → press **Enter**, then `y`, then **OK**.
- TestDisk updates the partition table automatically.


C:\Users\ujwal\OneDrive\Desktop\Bhuvan DF\testdisk-7.2.win\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

     Partition                  Start        End    Size in sectors

 1 P EFI System                  2048     534527     532480 [EFI System Partition] [SYSTEM_DRV]






 [  Quit  ]  [ Return ]  [Deeper Search] >[ Write  ]
                       Write partition structure to disk
```



C:\Users\ujwal\OneDrive\Desktop\Bhuvan DF\testdisk-7.2.win\testdisk-7.2\testdisk_win.exe

```
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

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

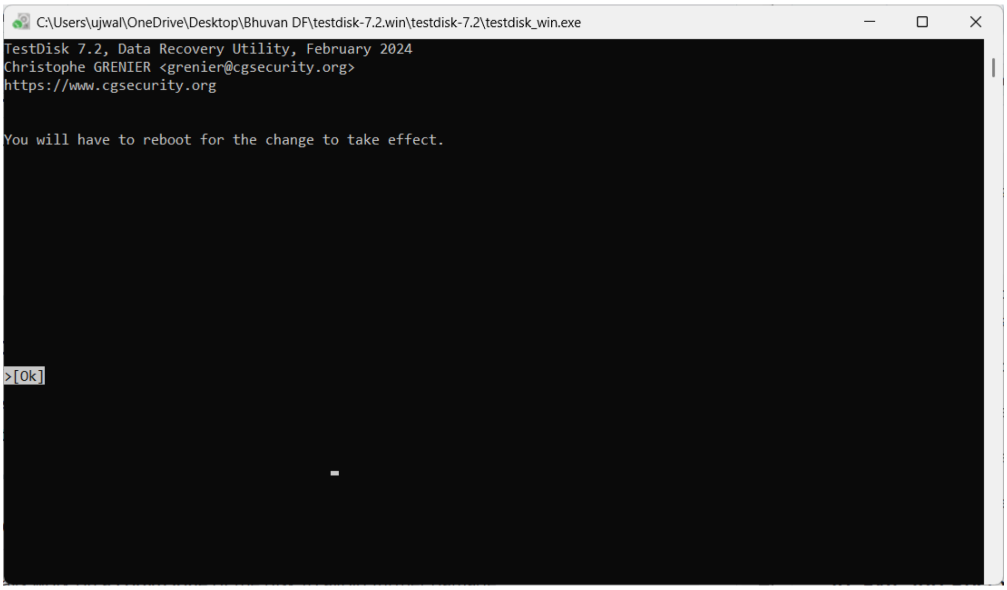
Step 7: NTFS Boot Sector Recovery

- If NTFS boot sector is damaged:
  - Select **Backup BS** to copy the backup boot sector over the bad one.
  - Confirm with **y** → then **OK**.

Now the boot sector and backup are identical, meaning recovery succeeded.

Step 8: Restart System

- After successful recovery, TestDisk prompts you to **reboot the computer**.
- Restart and check if your partitions and files are accessible again.



C:\Users\ujwal\OneDrive\Desktop\Bhuvan DF\testdisk-7.2.win\testdisk-7.2\testdisk_win.exe

```
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org


You will have to reboot for the change to take effect.










>[Ok]
```

Rubrics

Criteria	Mark Allotted	Mark Awarded
1. GitHub Activity & Submission Regularity	3	
2. Application of Forensic Tools & Practical Execution	3	
3. Documentation & Reporting	2	
4. Engagement, Problem-Solving & Team Collaboration	2	
Total	10	

Result

Successfully acquired the **RAM dump (.mem)** and **disk image (.E01)** of the target system using **FTK Imager**.
The **MD5/SHA1 hash values** of the acquired images were verified, confirming that the evidence was collected without alteration and is **forensically sound**.