

Ex No-2: Recover deleted or damaged files from a storage device using Test Disk

AIM:

To recover lost partitions and deleted files using TestDisk.

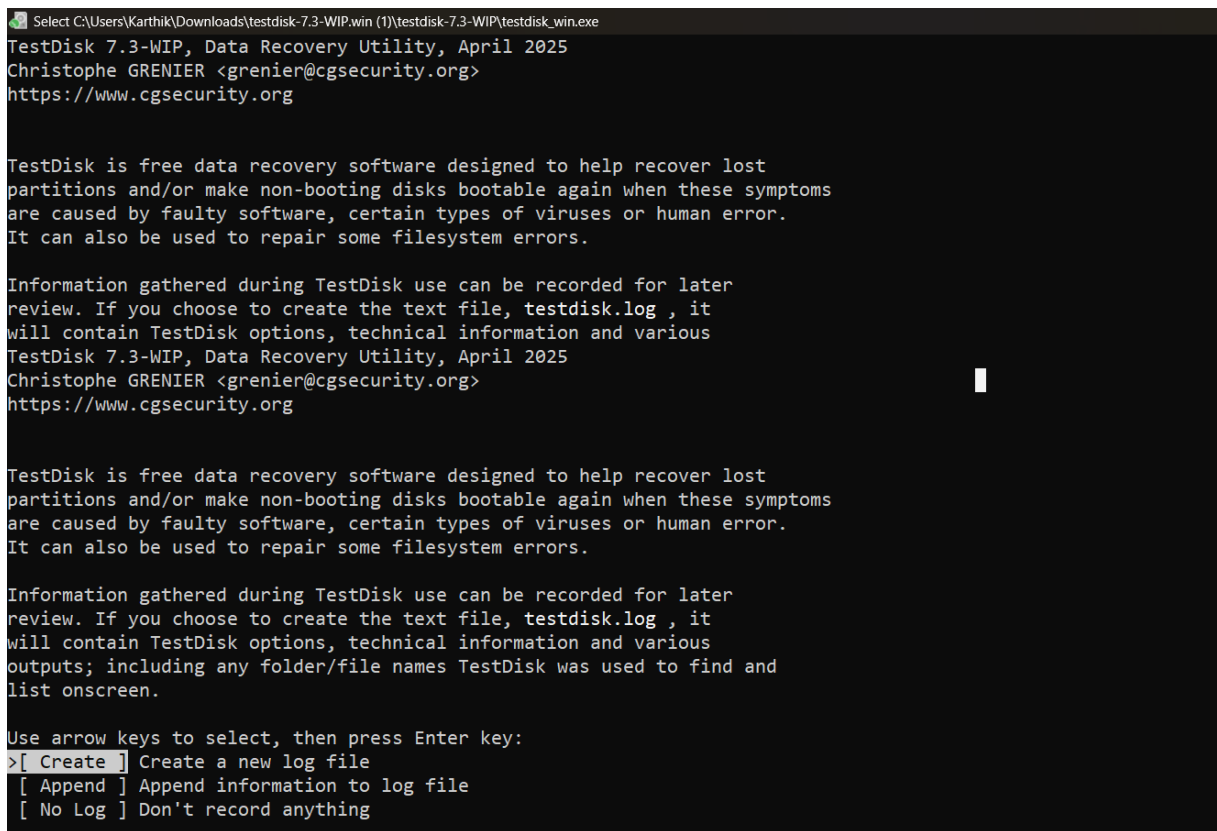
Requirements:

- TestDisk
- Windows

Description:

- TestDisk is an open-source forensic tool used for recovering lost partitions and repairing damaged boot sectors.
- It can restore accidentally deleted files from FAT, NTFS, ext2/ext3 file systems.
- Investigators use it to quickly recover inaccessible data and make disks bootable again.

Step-1: Launch the TestDisk tool and in the terminal window, select “Create” to make a new log file and press Enter



```
Select C:\Users\Karthik\Downloads\testdisk-7.3-WIP.win (1)\testdisk-7.3-WIP\testdisk_win.exe
TestDisk 7.3-WIP, Data Recovery Utility, April 2025
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
TestDisk 7.3-WIP, Data Recovery Utility, April 2025
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
```

Step-2: TestDisk will list available disks (HDDs, SSDs, USB drives). Use the arrow keys to highlight the disk you want to analyze and Press Enter

```
C:\Users\Karthik\Downloads\testdisk-7.3-WIP.win (1)\testdisk-7.3-WIP\testdisk_win.exe

TestDisk 7.3-WIP, Data Recovery Utility, April 2025
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
```

Step-3: TestDisk usually auto-detects the partition table (Intel/PC, EFI GPT, Mac, etc.). Verify and press Enter.

```
C:\Users\Karthik\Downloads\testdisk-7.3-WIP.win (1)\testdisk-7.3-WIP\testdisk_win.exe

TestDisk 7.3-WIP, Data Recovery Utility, April 2025
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-4: Analyze the current partition structure, from the terminal select Analyse and press enter.

```
C:\Users\Karthik\Downloads\testdisk-7.3-WIP.win (1)\testdisk-7.3-WIP\testdisk_win.exe

TestDisk 7.3-WIP, Data Recovery Utility, April 2025
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-5: After analysis you will be asked to perform Quick search select it and press Enter

```
Select C:\Users\Karthik\Downloads\testdisk-7.3-WIP.win (1)\testdisk-7.3-WIP\testdisk_win.exe

TestDisk 7.3-WIP, Data Recovery Utility, April 2025
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    996118527 995551232 [Basic data partition]
3 P MS Data             567296    996118527 995551232 [Basic data partition]
4 P Windows Recovery Env 996118528 1000214527 4096000 [Basic data partition]
```

Step-6: TestDisk scans the disk and lists lost partitions.

```
C:\Users\dhyam\Downloads\testdisk-7.3-WIP.win\testdisk-7.3-WIP\testdisk_win.exe
TestDisk 7.3-WIP, Data Recovery Utility, April 2025
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk \\.\PhysicalDrive0 - 1000 GB / 931 GiB - CHS 121601 255 63
Partition      Start      End      Size in sectors
* HPFS - NTFS   0 32 33 121601 57 56 1953521664 [DATA]

Structure: Ok. Use Up/Down Arrow keys to select partition.
Use Left/Right Arrow keys to CHANGE partition characteristics:
*Primary bootable P=Primary L=Logical E=Extended D=Deleted
Keys A: add partition, L: load backup, T: change type, P: list files,
Enter: to continue
NTFS, blocksize=4096, 1000 GB / 931 GiB
```

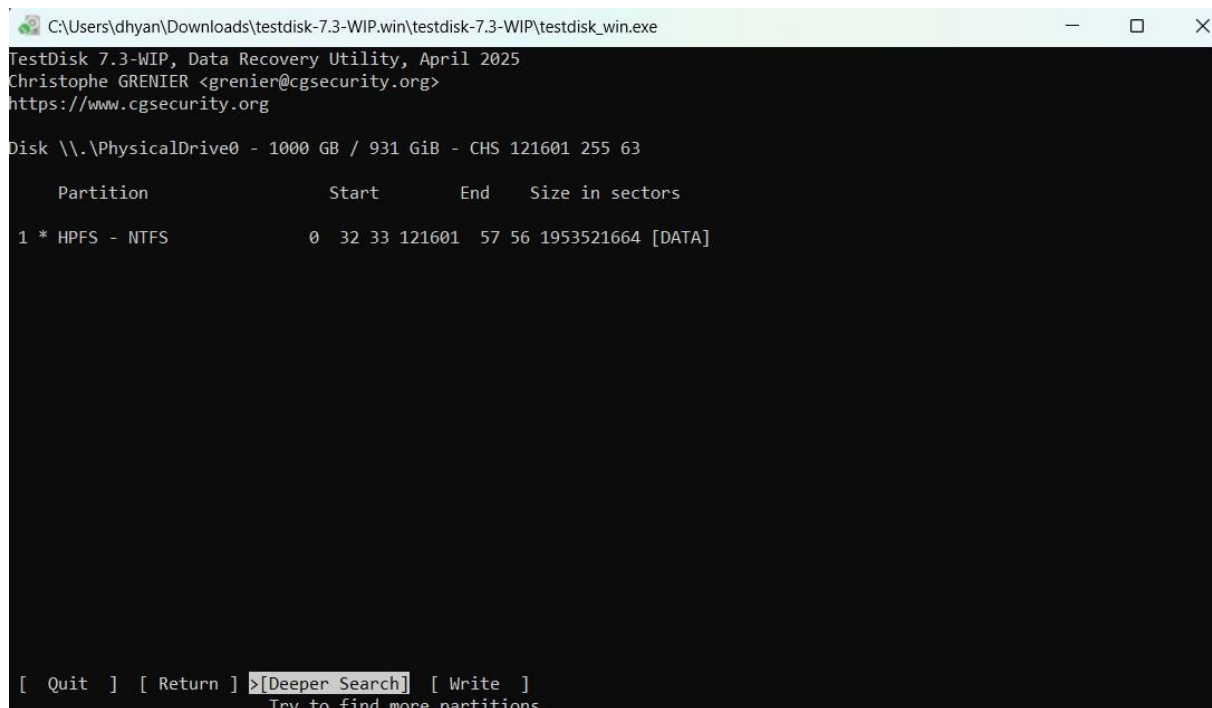
Step-7: Press “P” to view the list of files and “C” to copy the files

```
C:\Users\dhyam\Downloads\testdisk-7.3-WIP.win\testdisk-7.3-WIP\testdisk_win.exe
TestDisk 7.3-WIP, Data Recovery Utility, April 2025
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
* HPFS - NTFS   0 32 33 121601 57 56 1953521664 [DATA]
Directory /

dr-xr-xr-x  0 0 0 28-Aug-2025 21:01 .
dr-xr-xr-x  0 0 0 28-Aug-2025 21:01 ..
dr-xr-xr-x  0 0 0 18-Jan-2025 12:24 $RECYCLE.BIN
dr-xr-xr-x  0 0 0 19-Aug-2022 22:04 2148104239
dr-xr-xr-x  0 0 0 4-Oct-2022 17:13 Program Files
dr-xr-xr-x  0 0 0 12-Dec-2023 19:51 System Volume Information
dr-xr-xr-x  0 0 0 2-Jan-2025 22:16 MDownloadCache
dr-xr-xr-x  0 0 0 4-Oct-2022 17:13 WindowsApps
dr-xr-xr-x  0 0 0 4-Oct-2022 17:13 WpSystem
-r--r--r--  0 0 0 63 24-Aug-2022 22:06 1a.py

Next
Use Right to change directory, 'h' to hide Alternate Data Stream
'q' to quit, ':' to select the current file, 'a' to select all files
'C' to copy the selected files, 'c' to copy the current file.
```

Step-8: If Quick Search does not find your partition/files, select “Deeper Search” and Enter. This takes longer but finds more recoverable partitions.

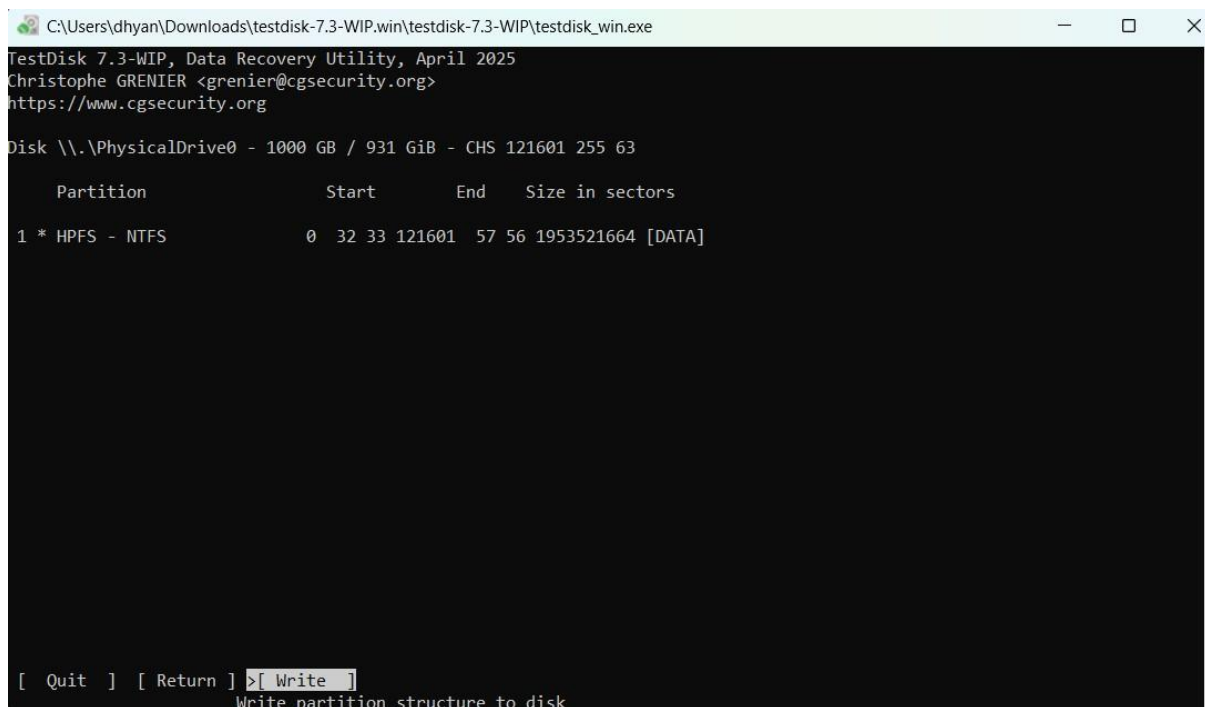


The screenshot shows the TestDisk 7.3-WIP interface. At the top, it displays the title bar 'C:\Users\dhyan\Downloads\testdisk-7.3-WIP.win\testdisk-7.3-WIP\testdisk_win.exe'. Below the title bar, the text reads: 'TestDisk 7.3-WIP, Data Recovery Utility, April 2025', 'Christophe GRENIER <grenier@cgsecurity.org>', and 'https://www.cgsecurity.org'. The main display area shows 'Disk \\.\PhysicalDrive0 - 1000 GB / 931 GiB - CHS 121601 255 63'. Below this, a table lists the partitions:

Partition	Start	End	Size in sectors
1 * HPFS - NTFS	0 32 33 121601	57 56 1953521664	[DATA]

At the bottom, the menu options are: '[Quit] [Return] >[Deeper Search] [Write]'. The 'Deeper Search' option is highlighted, and a prompt below it says 'Try to find more partitions.'

Step-9: Once you are confident the partition is correct, select “write” and press Enter.

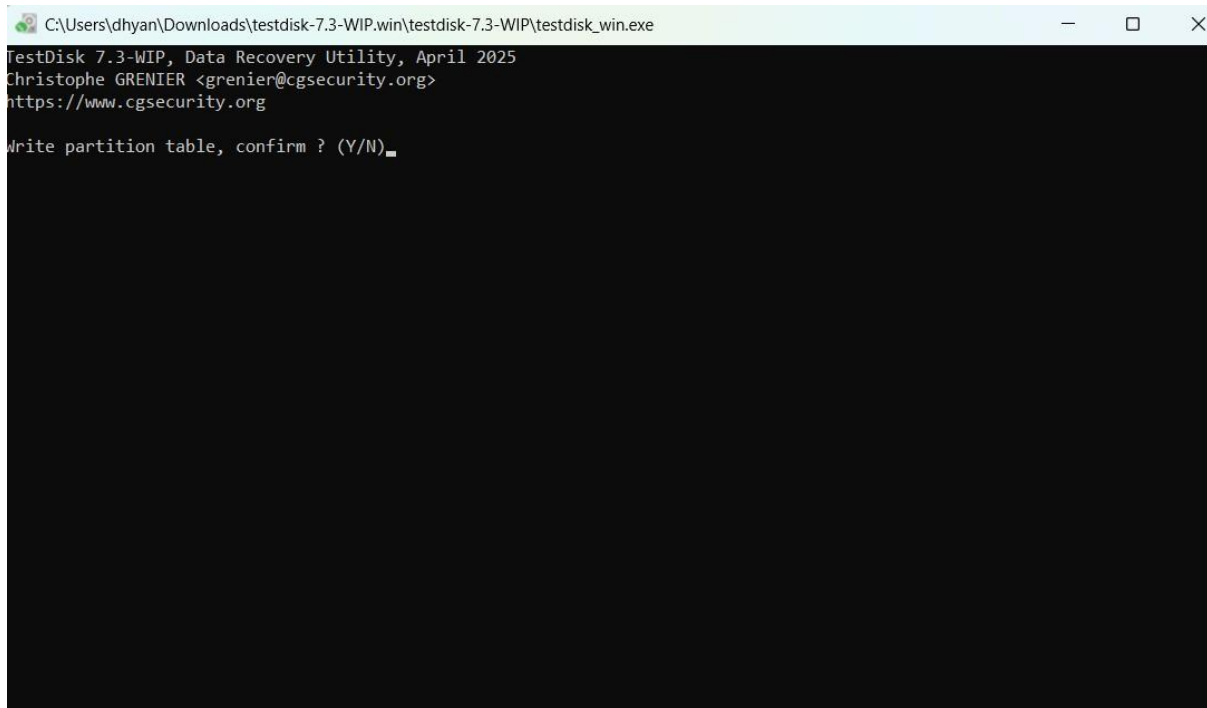


The screenshot shows the TestDisk 7.3-WIP interface. At the top, it displays the title bar 'C:\Users\dhyan\Downloads\testdisk-7.3-WIP.win\testdisk-7.3-WIP\testdisk_win.exe'. Below the title bar, the text reads: 'TestDisk 7.3-WIP, Data Recovery Utility, April 2025', 'Christophe GRENIER <grenier@cgsecurity.org>', and 'https://www.cgsecurity.org'. The main display area shows 'Disk \\.\PhysicalDrive0 - 1000 GB / 931 GiB - CHS 121601 255 63'. Below this, a table lists the partitions:

Partition	Start	End	Size in sectors
1 * HPFS - NTFS	0 32 33 121601	57 56 1953521664	[DATA]

At the bottom, the menu options are: '[Quit] [Return] >[Write]'. The 'Write' option is highlighted, and a prompt below it says 'Write partition structure to disk'.

Step-10: Confirm the operation by pressing “Y”. This will write partition table to your disk.



```
C:\Users\dhyan\Downloads\testdisk-7.3-WIP.win\testdisk-7.3-WIP\testdisk_win.exe
TestDisk 7.3-WIP, Data Recovery Utility, April 2025
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
Write partition table, confirm ? (Y/N)_
```

- Once recovery is complete, exit TestDisk by selecting “Quit”.
- Verify recovered files in the destination folder.
- TestDisk detected lost/deleted partitions.
- Files marked as deleted were listed and successfully copied to a safe location.
- Recovery was possible without altering original disk contents.