

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.

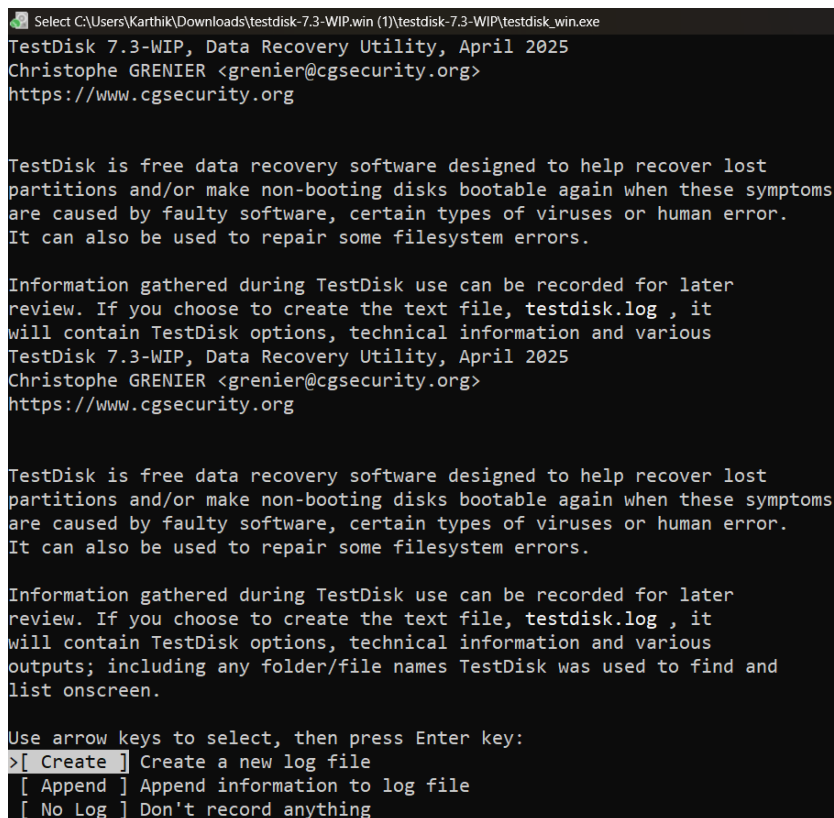
Requirements:

- 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\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
Analyse cylinder 79/62259: 00%

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

00

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

```
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
https://www.cgsecurity.org

TestDisk 7.3-WIP, Data Recovery Utility, April 2025

Please select a destination where /EFI and any files below will be copied.
Keys: Arrow keys to select another directory
      C when the destination is correct
      Q to quit
Directory C:\Users\Karthik\Downloads\testdisk-7.3-WIP.win (1)\testdisk-7.3-WIP_
drwx----- 197609 197121      0 3-Sep-2025 23:41 .
drwx----- 197609 197121      0 3-Sep-2025 23:38 ..
drwx----- 197609 197121      0 3-Sep-2025 23:38 63
drwx----- 197609 197121      0 3-Sep-2025 23:38 platforms
-rwx----- 197609 197121     220 3-Sep-2025 23:38 AUTHORS.txt
-rwx----- 197609 197121    18326 3-Sep-2025 23:38 COPYING.txt
-rwx----- 197609 197121     120 3-Sep-2025 23:38 INFO
-rwx----- 197609 197121    20989 3-Sep-2025 23:38 NEWS.txt
-rwx----- 197609 197121   6762631 3-Sep-2025 23:38 Qt5Core.dll
-rwx----- 197609 197121   7646324 3-Sep-2025 23:38 Qt5Gui.dll
-rwx----- 197609 197121   7935180 3-Sep-2025 23:38 Qt5Widgets.dll
-rwx----- 197609 197121     350 3-Sep-2025 23:38 THANKS.txt
-rwx----- 197609 197121     41 3-Sep-2025 23:38 VERSION.txt
-rwx----- 197609 197121   4210072 3-Sep-2025 23:38 cygwinf-2.dll
-rwx----- 197609 197121   731857 3-Sep-2025 23:38 cygwinf_s-1.dll
-rwx----- 197609 197121  1315500 3-Sep-2025 23:38 cygiconv-2.dll
-rwx----- 197609 197121  1964540 3-Sep-2025 23:38 cygjpeg-8.dll
-rwx----- 197609 197121  3462774 3-Sep-2025 23:38 cygncursesw-10.dll
-rwx----- 197609 197121  3274927 3-Sep-2025 23:38 cygwin1.dll
-rwx----- 197609 197121   289410 3-Sep-2025 23:38 cygz.dll
-rwx----- 197609 197121     504 3-Sep-2025 23:38 documentation.html
-rwx----- 197609 197121   369200 3-Sep-2025 23:38 fididentify_win.exe
-rwx----- 197609 197121    37788 3-Sep-2025 23:38 iconv.dll
-rwx----- 197609 197121   116814 3-Sep-2025 23:38 libbz2-1.dll
-rwx----- 197609 197121   6788902 3-Sep-2025 23:38 libbz2-2.dll
-rwx----- 197609 197121   869036 3-Sep-2025 23:38 libfreetype-6.dll
-rwx----- 197609 197121   1072581 3-Sep-2025 23:38 libgcc_s_dw2-1.dll
-rwx----- 197609 197121   1673663 3-Sep-2025 23:38 libglib-2.0-0.dll
-rwx----- 197609 197121   7083896 3-Sep-2025 23:38 libharfbuzz-0.dll
-rwx----- 197609 197121    239106 3-Sep-2025 23:38 libintl-8.dll
-rwx----- 197609 197121   776886 3-Sep-2025 23:38 libjpeg-62.dll
-rwx----- 197609 197121   620258 3-Sep-2025 23:38 libpcre2-16-0.dll
-rwx----- 197609 197121   675308 3-Sep-2025 23:38 libpcre2-8-0.dll
```

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

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

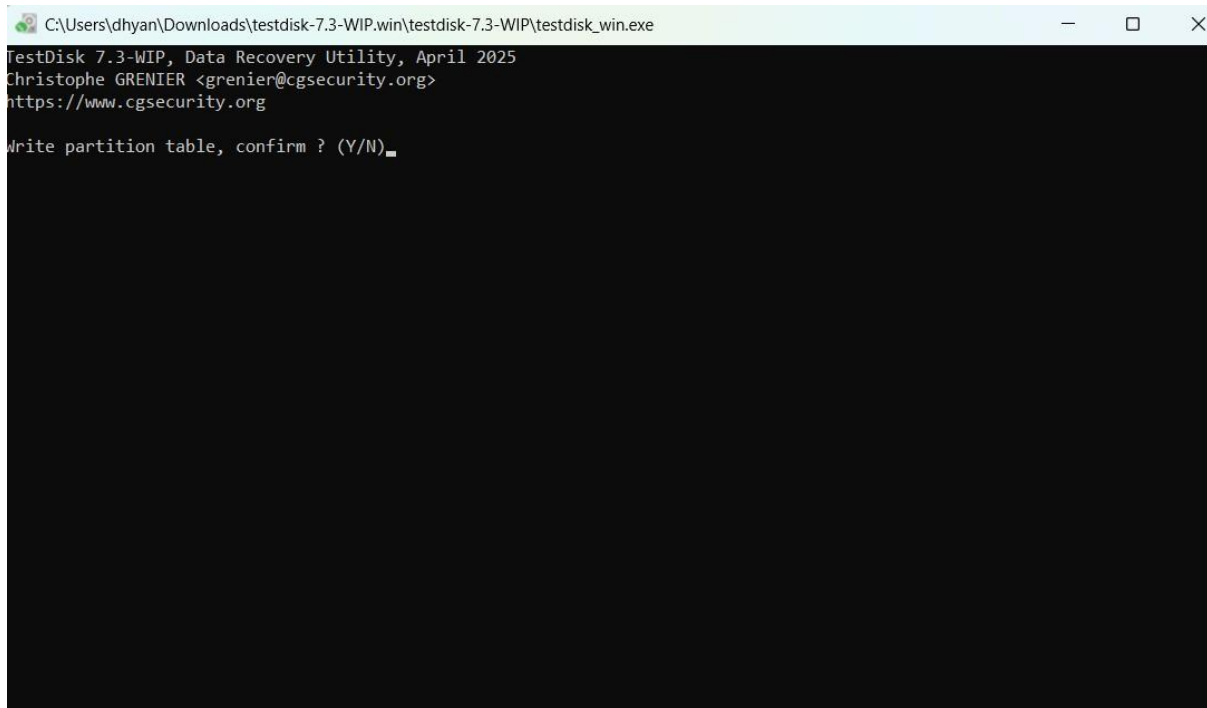
TestDisk 7.3-WIP, Data Recovery Utility, April 2025
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
P EFI System 2048 534527 532480 [EFI System Partition] [SYSTEM_DRV]
Directory /EFI
Copy done! 1193 ok, 0 failed
>drwxr-xr-x 0 0 0 30-May-2025 13:19 EFI
drwxr-xr-x 0 0 0 17-Jun-2024 15:36 BOOT
-rwxr-xr-x 0 0 8388608 17-Jun-2024 15:37 BackupSbb.bin
drwxr-xr-x 0 0 0 17-Jun-2024 15:44 System Volume Information
drwxr-xr-x 0 0 4096 17-Jun-2024 15:49 MSI1a47a.tmp
drwxr-xr-x 0 0 4096 17-Jun-2024 15:49 MSI1a480.tmp
drwxr-xr-x 0 0 4096 17-Jun-2024 15:50 MSI1a485.tmp
drwxr-xr-x 0 0 0 17-Jun-2024 15:50 $RECYCLE.BIN
```

Step-9: Once you are confident the partition is correct, select “write” 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
P EFI System 2048 534527 532480 [EFI System Partition] [SYSTEM_DRV]
Directory /EFI/
>drwxr-xr-x 0 0 0 17-Jun-2024 15:36 .
drwxr-xr-x 0 0 0 17-Jun-2024 15:36 ..
drwxr-xr-x 0 0 0 30-May-2025 13:19 Microsoft
drwxr-xr-x 0 0 0 17-Jun-2024 15:36 Boot
```

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.