TestDisk Step By Step - CGSecurity

CGSecurity ⋮ 9-11 minutes ⋮ 1/20/2016

This ***recovery example*** guides you through TestDisk step by step to recover a missing partition and repair a corrupted one. After reading this tutorial, you should be ready to recover your own data. Translations of this TestDisk manual to other languages are welcome.

Example problem

We have a 36GB hard disk containing 3 partitions. Unfortunately;

- the boot sector of the primary NTFS partition has been damaged, and
- a logical NTFS partition has been accidentally deleted.

This ***recovery example*** guides you through TestDisk, step by step, to recover these 'lost' partitions by:

- rewriting the corrupted NTFS boot sector, and
- recovering the accidentally deleted logical NTFS partition.

Recovery of a FAT32 partition (instead of an NTFS partition) can be accomplished by following exactly the same steps. Other recovery examples are also available. For Information about FAT12, FAT16, ext2/ext3, HFS+, ReiserFS and other partition types, read Running the TestDisk Program.

> One condition:
>
> - TestDisk must be executed with Administrator privileges.
>
> Important points for using TestDisk:
>
> - To navigate in TestDisk, use the `Arrow` and `PageUp/PageDown` keys.
> - To proceed, confirm your choice(s) with the `Enter` key.
> - To return to a previous display or quit TestDisk, use the ***q*** (Quit) key.
> - To save modifications under TestDisk, you must confirm them with the **y** (Yes) and/or `Enter` keys, and
> - To actually write partition data to the MBR, you must choose the "Write" selection and press the `Enter` key.

Symptoms

If this hard disk's primary partition contained an operating system, it would most likely no longer boot up - due to its corrupted boot sector. If the hard disk was a secondary (data) drive or you can connect the drive to another computer in its secondary channel (usually where a CD/DVD drive is connected), the following symptoms would be observed:

1. Windows Explorer or Disk Manager displays the first primary partition as *raw* (unformatted) and Windows prompts:
   `The drive is not formatted, do you want to format it now?`
   [You should *never* do so without knowing why!]
2. A logical partition is missing. In Windows Explorer, that logical drive is no longer available. The Windows Disk Management Console now displays only "unallocated space" where this logical partition had been located.

Running TestDisk executable

If TestDisk is not yet installed, it can be downloaded from TestDisk Download. Extract the files from the archive including the sub-directories.

To recover a lost partition or repair the filesystem from a hard disk, USB key, Smart Card, etc., you need enough rights to access a physical device.

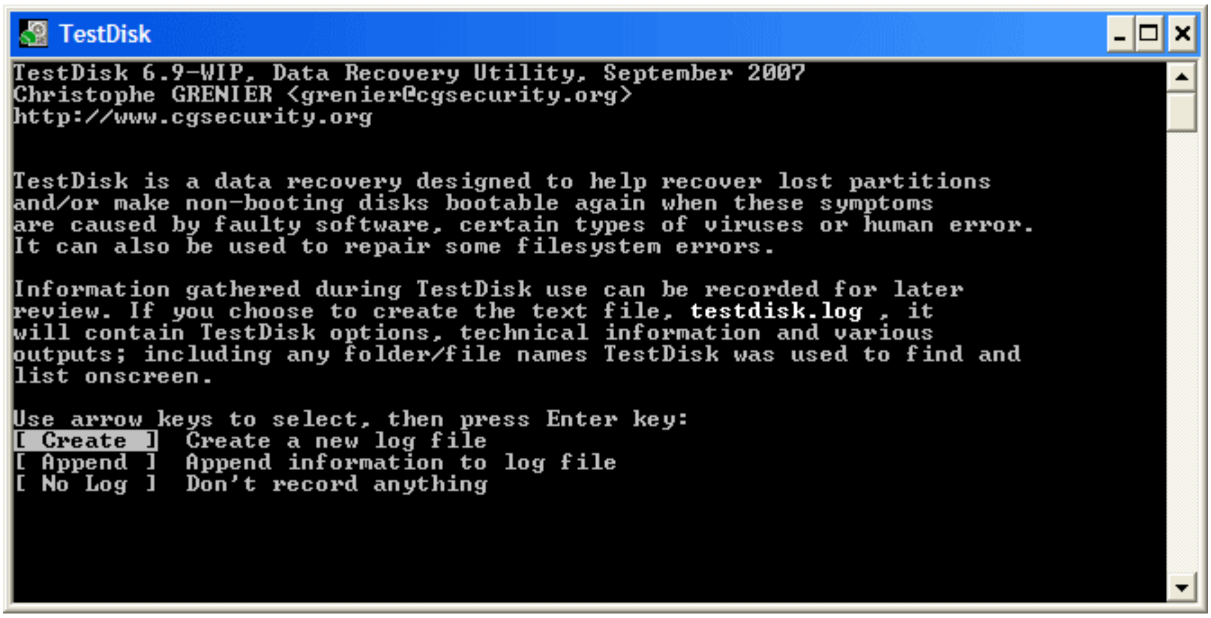
To recover partition from a media image or repair a filesystem image, run

- `testdisk image.dd` to work from a raw disk image
- `testdisk image.E01` to recover files from an Encase EWF image
- `testdisk 'image.???'` if the Encase image is split into several files.

🐧 X To repair a filesystem not listed by TestDisk, run `testdisk device`, i.e.

- `testdisk /dev/mapper/truecrypt0` or `testdisk /dev/loop0` to repair the NTFS or FAT32 boot sector files from a TrueCrypt partition. The same method works with filesystem encrypted with cryptsetup/dm-crypt/LUKS.
- `testdisk /dev/md0` to repair a filesystem on top of a Linux RAID device.

Log creation

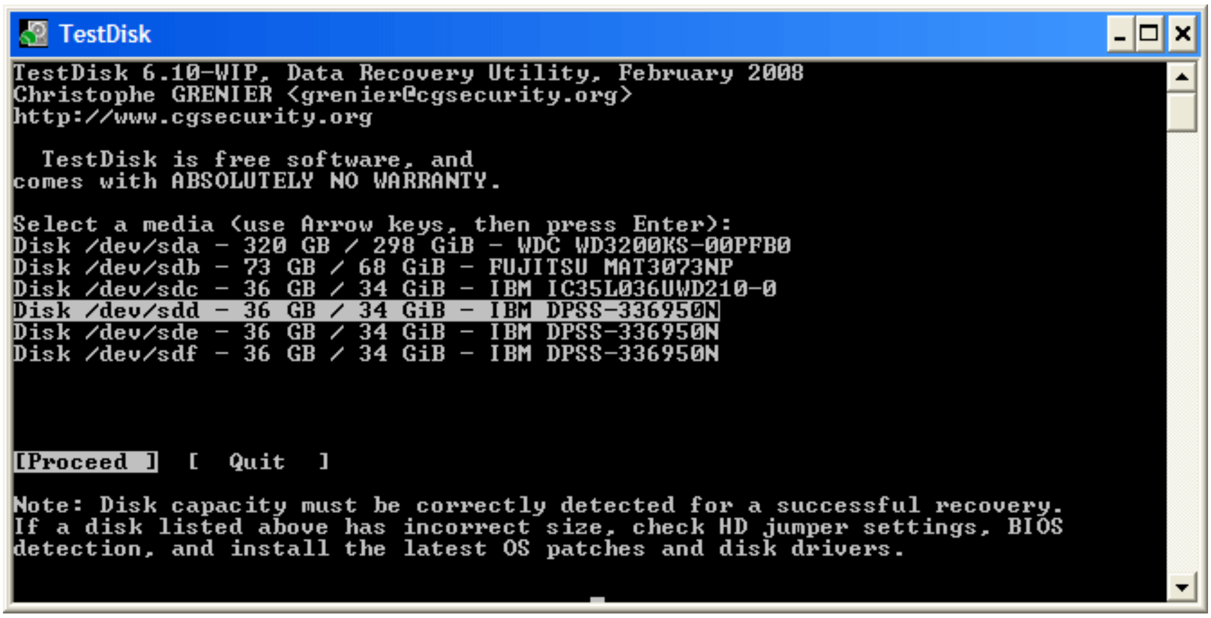


```
TestDisk 6.9-WIP, Data Recovery Utility, September 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org


TestDisk is a data recovery 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
```

- Choose Create to instruct Testdisk to create a log file containing technical information and messages, unless you have a reason to append data to the log or you execute TestDisk from read only media and must create the log elsewhere.
- Choose None if you do not want messages and details of the process to be written into a log file (useful if for example Testdisk was started from a read-only location).
- Press Enter to proceed.

Disk selection

All hard drives should be detected and listed with the correct size by TestDisk:



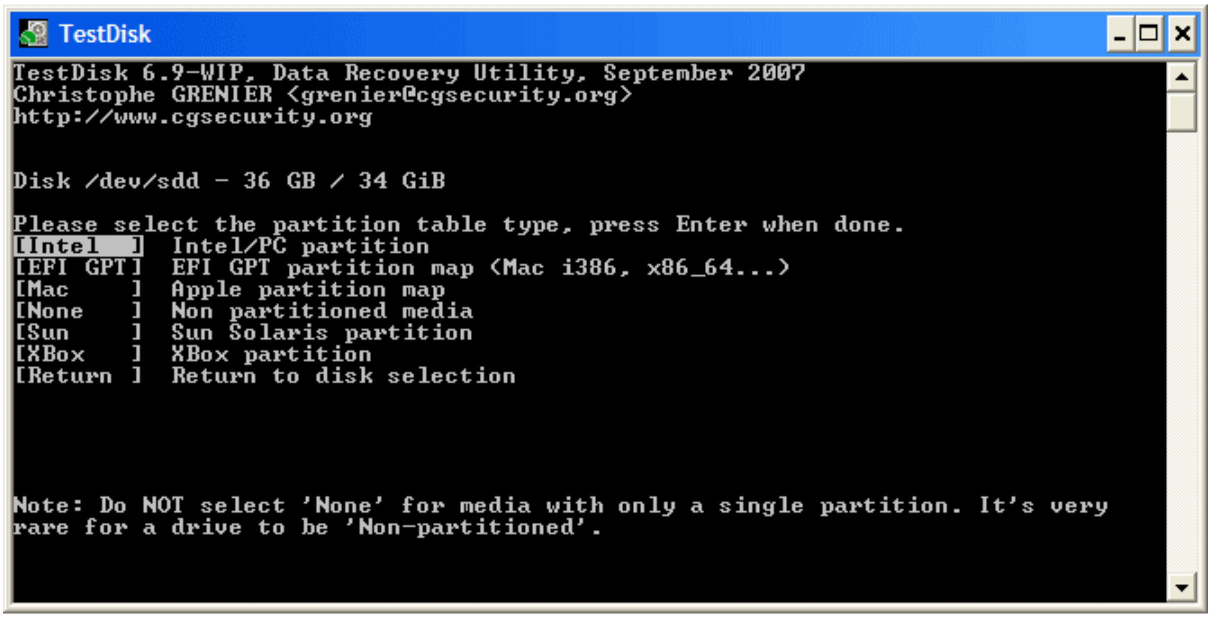
```
TestDisk 6.10-WIP, Data Recovery Utility, February 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

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

Select a media (use Arrow keys, then press Enter):
Disk /dev/sda - 320 GB / 298 GiB - WDC WD3200KS-00PFB0
Disk /dev/sdb - 73 GB / 68 GiB - FUJITSU MAT3073NP
Disk /dev/sdc - 36 GB / 34 GiB - IBM IC35L036UWD210-0
Disk /dev/sdd - 36 GB / 34 GiB - IBM DPSS-336950N
Disk /dev/sde - 36 GB / 34 GiB - IBM DPSS-336950N
Disk /dev/sdf - 36 GB / 34 GiB - IBM DPSS-336950N




[Proceed ]  [  Quit  ]

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

- Use up/down arrow keys to select your hard drive with the lost partition/s.
- Press Enter to Proceed.

X If available, use raw device `/dev/rdisk*` instead of `/dev/disk*` for faster data transfer.

Partition table type selection

TestDisk displays the partition table types.

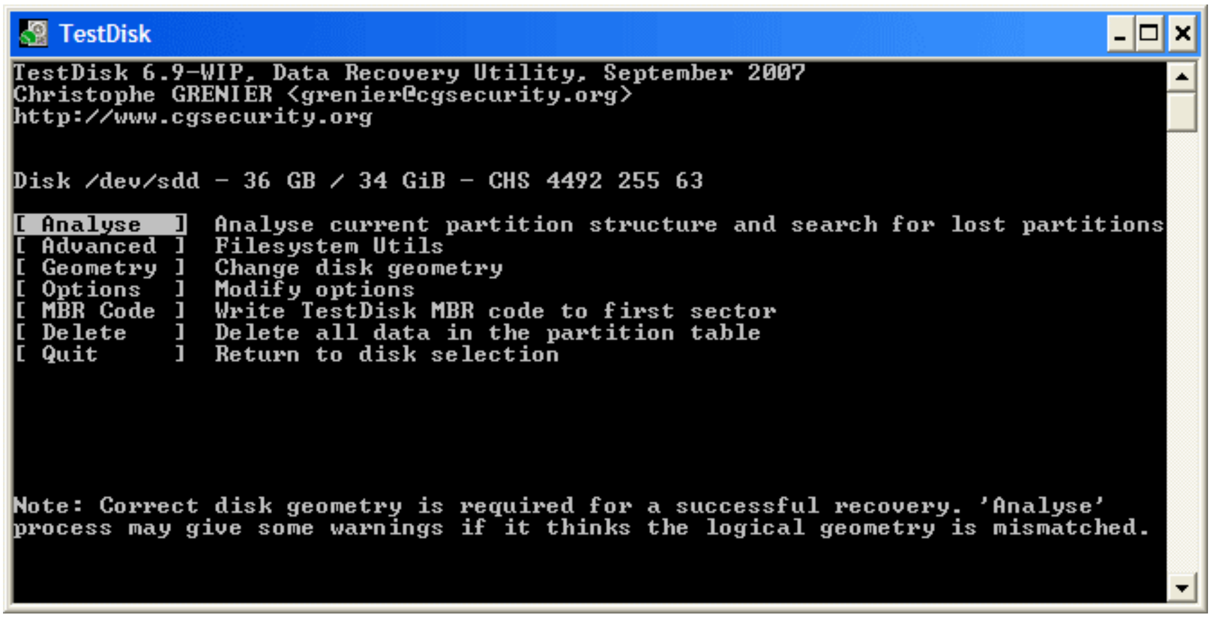


```
TestDisk 6.9-WIP, Data Recovery Utility, September 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org


Disk /dev/sdd - 36 GB / 34 GiB

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





Note: Do NOT select 'None' for media with only a single partition. It's very
rare for a drive to be 'Non-partitioned'.
```

- Select the partition table type - usually the default value is the correct one as TestDisk auto-detects the partition table type.
- Press Enter to Proceed.

Current partition table status

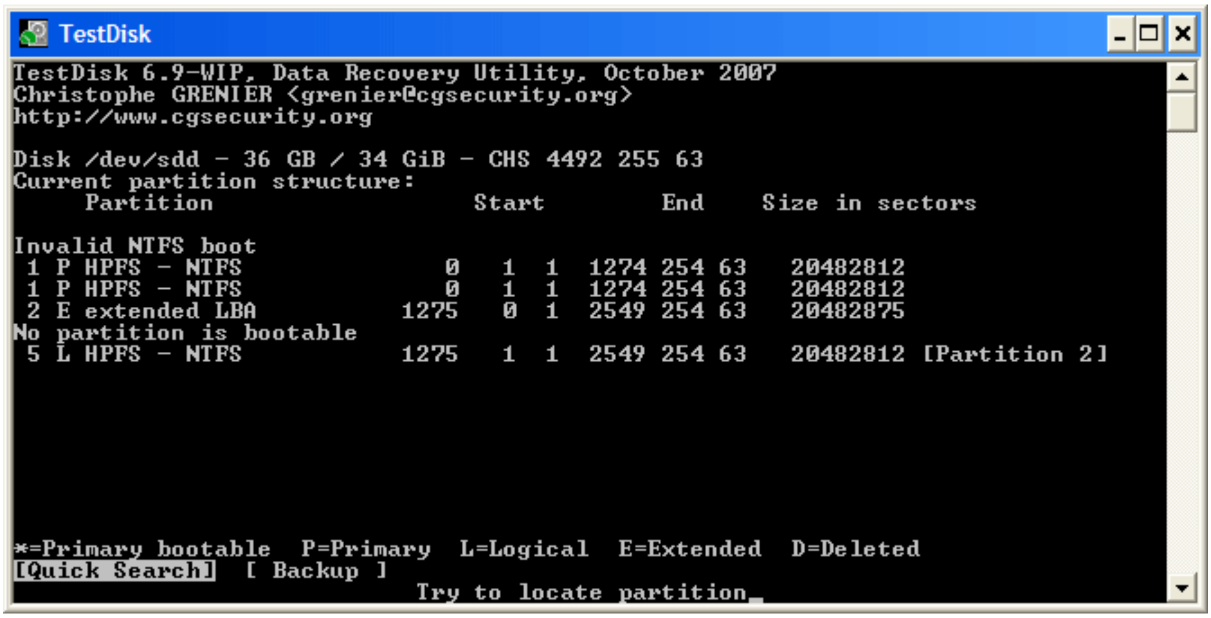
TestDisk displays the menus (also see TestDisk Menu Items).



```
TestDisk 6.9-WIP, Data Recovery Utility, September 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org


Disk /dev/sdd - 36 GB / 34 GiB - CHS 4492 255 63

[ Analyse  ]  Analyse current partition structure and search for lost partitions
[ Advanced ]  Filesystem Utils
[ Geometry ]  Change disk geometry
[ Options  ]  Modify options
[ MBR Code ]  Write TestDisk MBR code to first sector
[ Delete   ]  Delete all data in the partition table
[ 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.
```

- Use the default menu "Analyse" to check your current partition structure and search for lost partitions.
- Confirm at Analyse with Enter to proceed.

Now, your current partition structure is listed. Examine your current partition structure for missing partitions and errors.

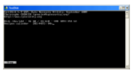


```
TestDisk 6.9-WIP, Data Recovery Utility, October 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdd - 36 GB / 34 GiB - CHS 4492 255 63
Current partition structure:
     Partition                  Start        End    Size in sectors

Invalid NTFS boot
 1 P HPFS - NTFS              0   1  1  1274 254 63   20482812
 1 P HPFS - NTFS              0   1  1  1274 254 63   20482812
 2 E extended LBA          1275   0  1  2549 254 63   20482875
No partition is bootable
 5 L HPFS - NTFS           1275   1  1  2549 254 63   20482812 [Partition 2]




*=Primary bootable  P=Primary  L=Logical  E=Extended  D=Deleted
[Quick Search]  [ Backup ]
                            Try to locate partition
```

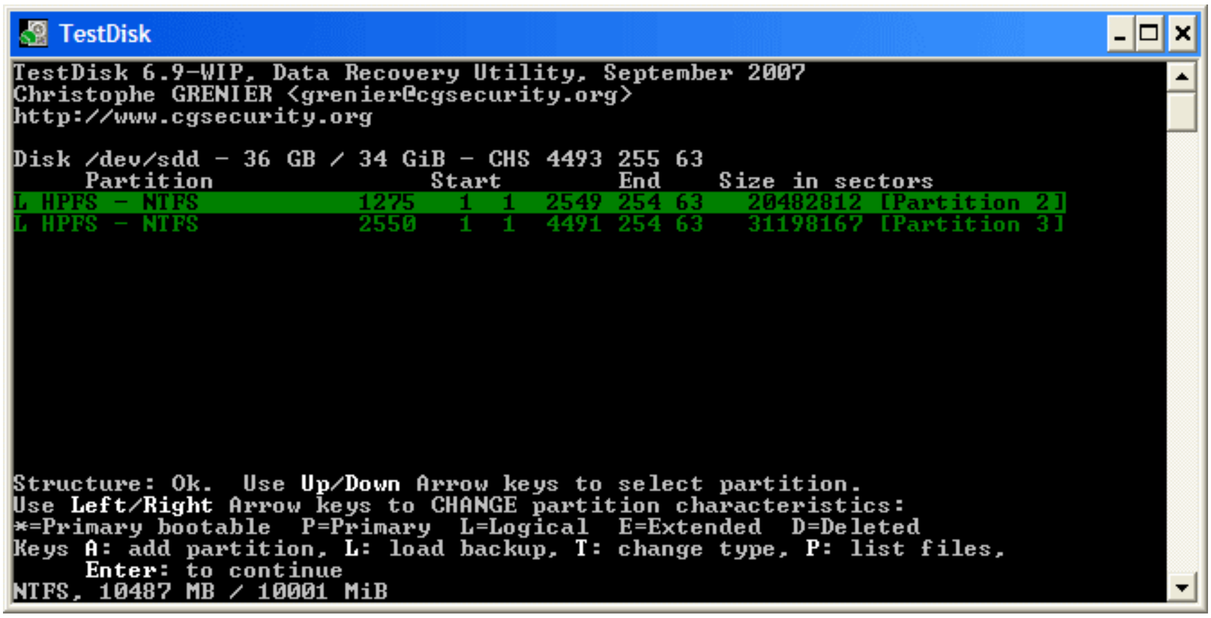
The first partition is listed twice which points to a corrupted partition or an invalid partition table entry.
Invalid NTFS boot points to a faulty NTFS boot sector, so it's a corrupted filesystem.
Only one logical partition (label Partition 2) is available in the extended partition. One logical partition is missing.

- Confirm at ***Quick Search*** to proceed.

Quick Search for partitions

TestDisk displays the first results in real time.		(click on thumb to display the image).

During the ***Quick Search***, TestDisk has found two partitions including the missing logical partition labeled ***Partition 3***.



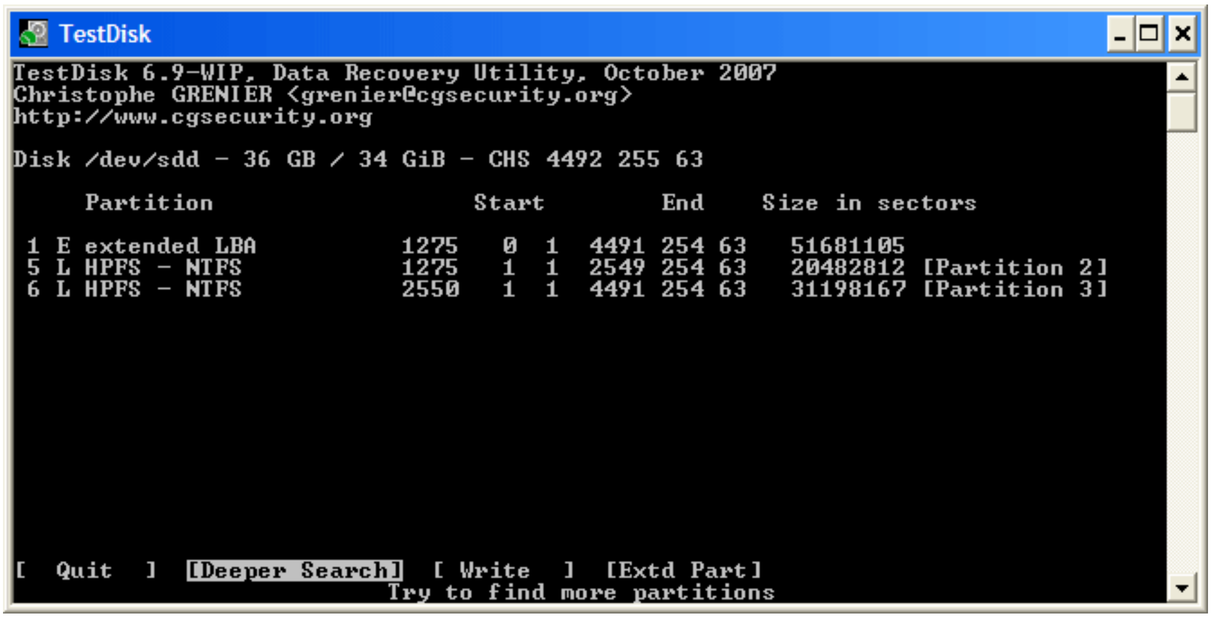
```
TestDisk 6.9-WIP, Data Recovery Utility, September 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdd - 36 GB / 34 GiB - CHS 4493 255 63
     Partition               Start        End    Size in sectors
L HPFS - NTFS            1275   1  1  2549 254 63   20482812 [Partition 2]
L HPFS - NTFS            2550   1  1  4491 254 63   31198167 [Partition 3]









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, 10487 MB / 10001 MiB
```

- Highlight this partition and press ***p*** to list your files (to go back to the previous display, press q to Quit, Files listed in red are deleted entries).

All directories and data are correctly listed.

- Press Enter to proceed.

Save the partition table or search for more partitions?

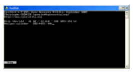


```
TestDisk 6.9-WIP, Data Recovery Utility, October 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdd - 36 GB / 34 GiB - CHS 4492 255 63

     Partition                  Start         End    Size in sectors

 1 E extended LBA            1275   0  1  4491 254 63   51681105
 5 L HPFS - NTFS             1275   1  1  2549 254 63   20482812 [Partition 2]
 6 L HPFS - NTFS             2550   1  1  4491 254 63   31198167 [Partition 3]











[  Quit  ] [Deeper Search] [ Write  ] [Extd Part]
                                 Try to find more partitions
```

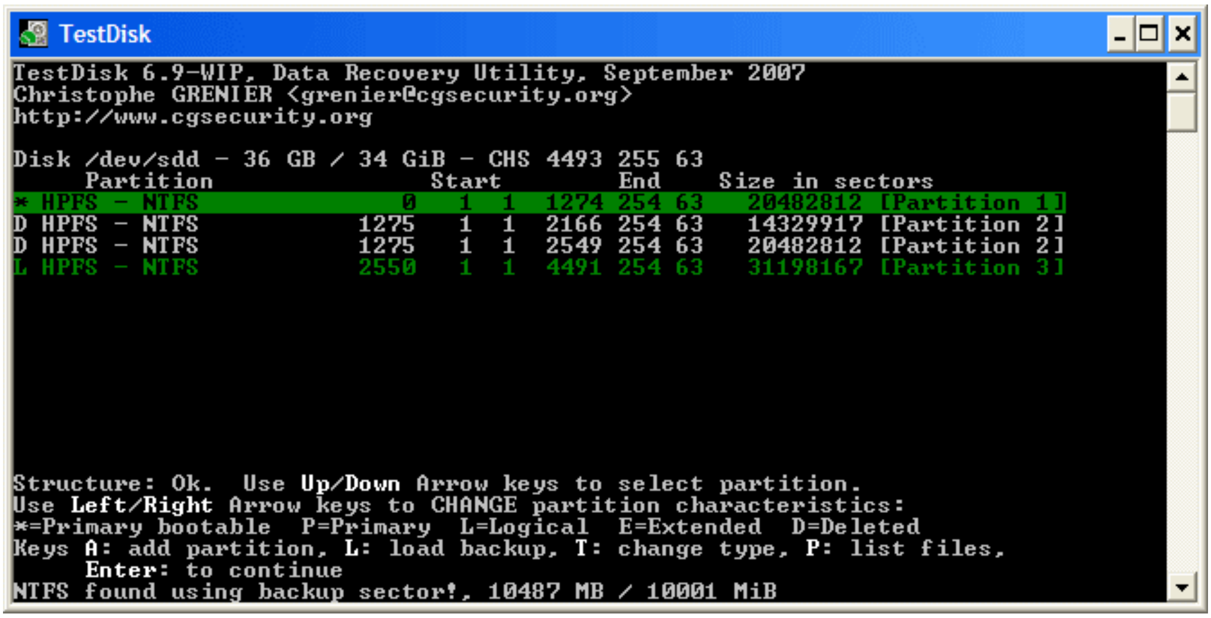
- ***When all partitions are available*** and data correctly listed, you should go to the menu **Write** to save the partition structure. The menu `Extd Part` gives you the opportunity to decide if the extended partition will use all available disk space or only the required (minimal) space.
- ***Since a partition, the first one, is still missing***, highlight the menu ***Deeper Search*** (if not done automatically already) and press Enter to proceed.

A partition is still missing: Deeper Search

Deeper Search will also search for FAT32 backup boot sector, NTFS backup boot superblock, ext2/ext3 backup superblock to detect more partitions,

it will scan each cylinder		(click on thumb).

After the Deeper Search, the results are displayed as follows:
The first partition ***"Partition 1"*** was found by using backup boot sector. In the last line of your display, you can read the message ***"NTFS found using backup sector!"*** and the size of your partition. The "partition 2" is displayed twice with different size.
Partitions listed as D(eleted) will not be recovered if you let them listed as deleted. Both partitions are listed with status ***D*** for deleted, because they overlap each other. You need to identify which partition to recover.

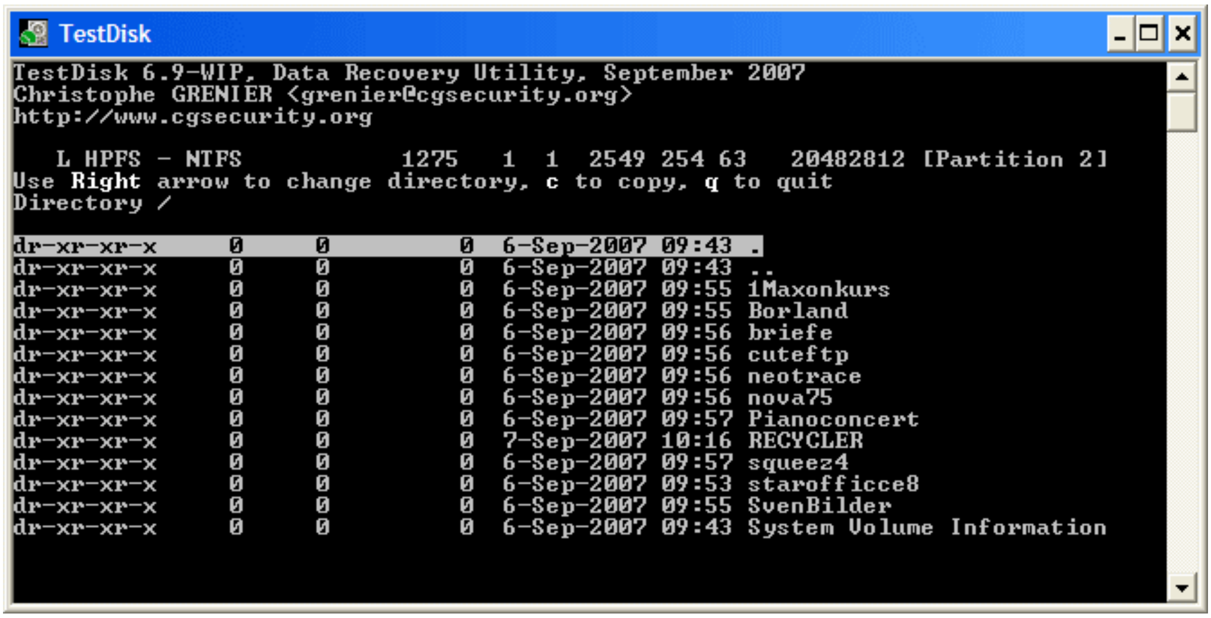


```
TestDisk 6.9-WIP, Data Recovery Utility, September 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdd - 36 GB / 34 GiB - CHS 4493 255 63
     Partition               Start        End    Size in sectors
* HPFS - NTFS                0   1  1  1274 254 63   20482812 [Partition 1]
D HPFS - NTFS             1275   1  1  2166 254 63   14329917 [Partition 2]
D HPFS - NTFS             1275   1  1  2549 254 63   20482812 [Partition 2]
L HPFS - NTFS             2550   1  1  4491 254 63   31198167 [Partition 3]









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 found using backup sector!, 10487 MB / 10001 MiB
```

- Highlight the first partition `Partition 2` and press ***p*** to list its data.

The file system of the upper logical partition (label Partition 2) is damaged		(click on thumb).

- Press q for Quit to go back to the previous display.
- Let this partition `Partition 2` with a damaged file system marked as `D(deleted)`.
- Highlight the second partition `Partition 2` below
- Press p to list its files.



```
TestDisk 6.9-WIP, Data Recovery Utility, September 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

  L HPFS - NTFS           1275   1  1  2549 254 63   20482812 [Partition 2]
Use Right arrow to change directory, c to copy, q to quit
Directory /

dr-xr-xr-x     0     0         0  6-Sep-2007 09:43 .
dr-xr-xr-x     0     0         0  6-Sep-2007 09:43 ..
dr-xr-xr-x     0     0         0  6-Sep-2007 09:55 1Maxonkurs
dr-xr-xr-x     0     0         0  6-Sep-2007 09:55 Borland
dr-xr-xr-x     0     0         0  6-Sep-2007 09:56 briefe
dr-xr-xr-x     0     0         0  6-Sep-2007 09:56 cuteftp
dr-xr-xr-x     0     0         0  6-Sep-2007 09:56 neotrace
dr-xr-xr-x     0     0         0  6-Sep-2007 09:56 nova75
dr-xr-xr-x     0     0         0  6-Sep-2007 09:57 Pianoconcert
dr-xr-xr-x     0     0         0  7-Sep-2007 10:16 RECYCLER
dr-xr-xr-x     0     0         0  6-Sep-2007 09:57 squeez4
dr-xr-xr-x     0     0         0  6-Sep-2007 09:53 staroffice8
dr-xr-xr-x     0     0         0  6-Sep-2007 09:55 SvenBilder
dr-xr-xr-x     0     0         0  6-Sep-2007 09:43 System Volume Information
```

It works, your files are listed, you have found the correct partition!

- Use the left/right arrow to navigate into your folders and watch your files for more verification

Note: FAT directory listing is limited to 10 clusters - some files may not appear but it doesn't affect recovery.

- Press q for Quit to go back to the previous display.

- The available status are Primary, * bootable, Logical and Deleted.

Using the left/right arrow keys, change the status of the selected partition from `D(eleted)` to ***`L(ogical)`***. This way you will be able to recover this partition.

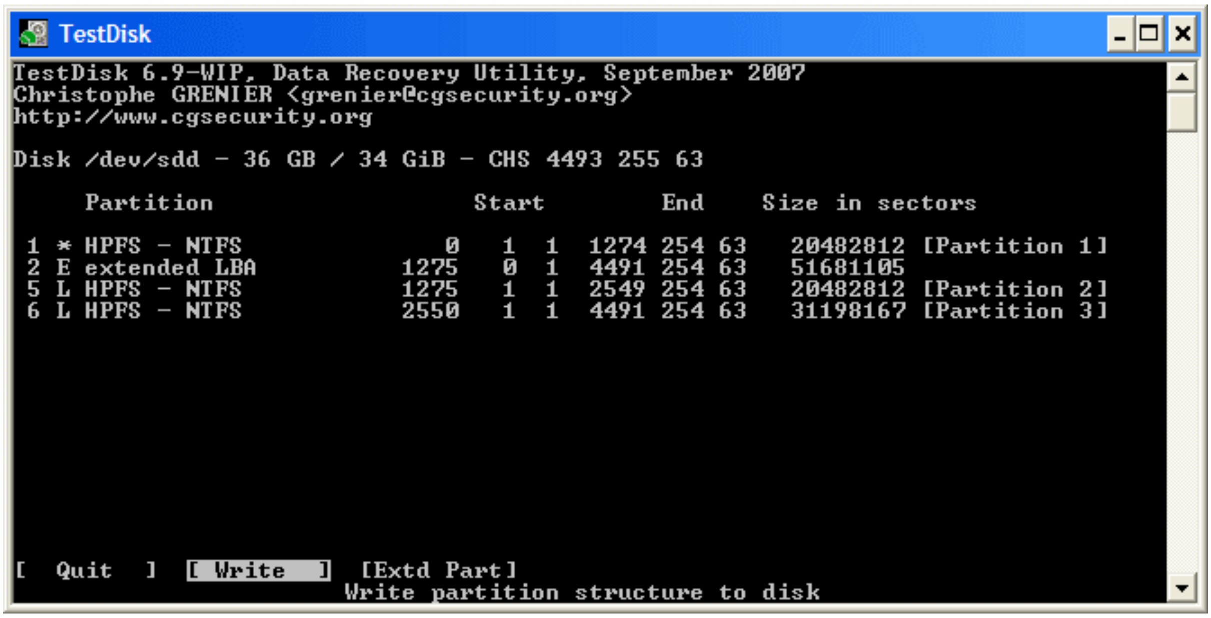
set partition to recover

Hint: read ***How to recognize primary and logical partitions?***
Note: If a partition is listed *(bootable) but if you don't boot from this partition, you can change it to ***P***rimary partition.

- Press Enter to proceed.

Partition table recovery

It's now possible to write the new partition structure.
Note: The extended partition is automatically set. TestDisk recognizes this using the different partition structure.



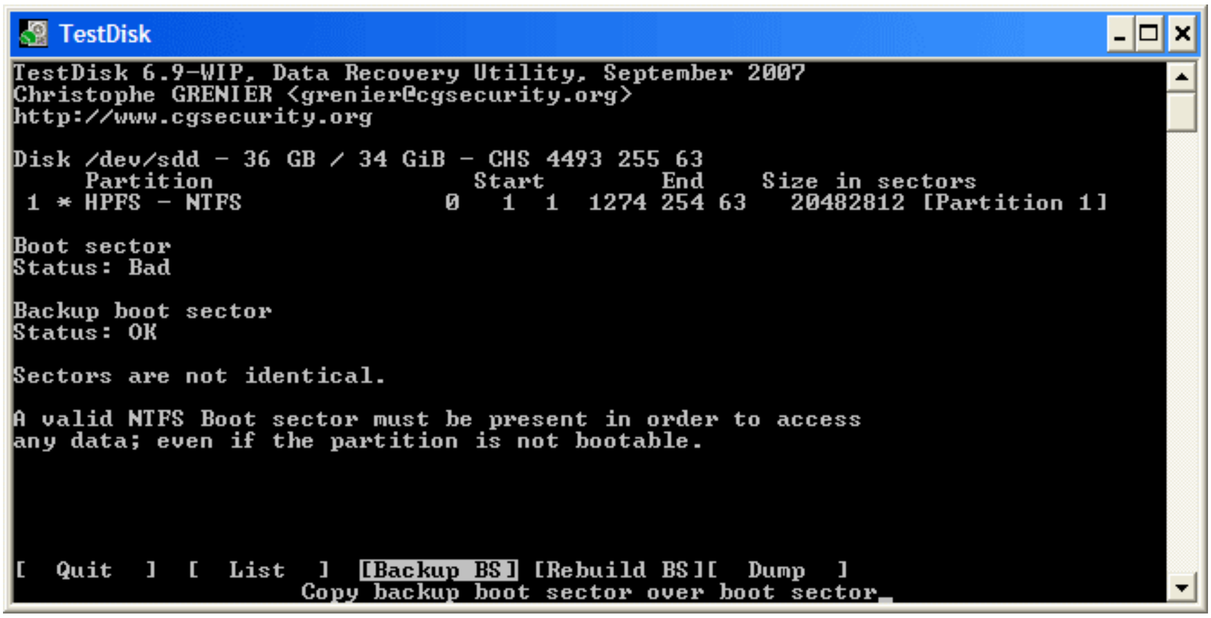
```
TestDisk 6.9-WIP, Data Recovery Utility, September 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdd - 36 GB / 34 GiB - CHS 4493 255 63

     Partition                  Start        End    Size in sectors

 1 * HPFS - NTFS              0   1  1  1274 254 63   20482812 [Partition 1]
 2 E extended LBA          1275   0  1  4491 254 63   51681105
 5 L HPFS - NTFS           1275   1  1  2549 254 63   20482812 [Partition 2]
 6 L HPFS - NTFS           2550   1  1  4491 254 63   31198167 [Partition 3]









[  Quit  ]  [ Write  ]  [Extd Part]
                               Write partition structure to disk
```

- If **all partitions are listed** and only in this case, confirm at ***Write*** with Enter, y and OK.

Now, the partitions are registered in the partition table.

NTFS Boot sector recovery

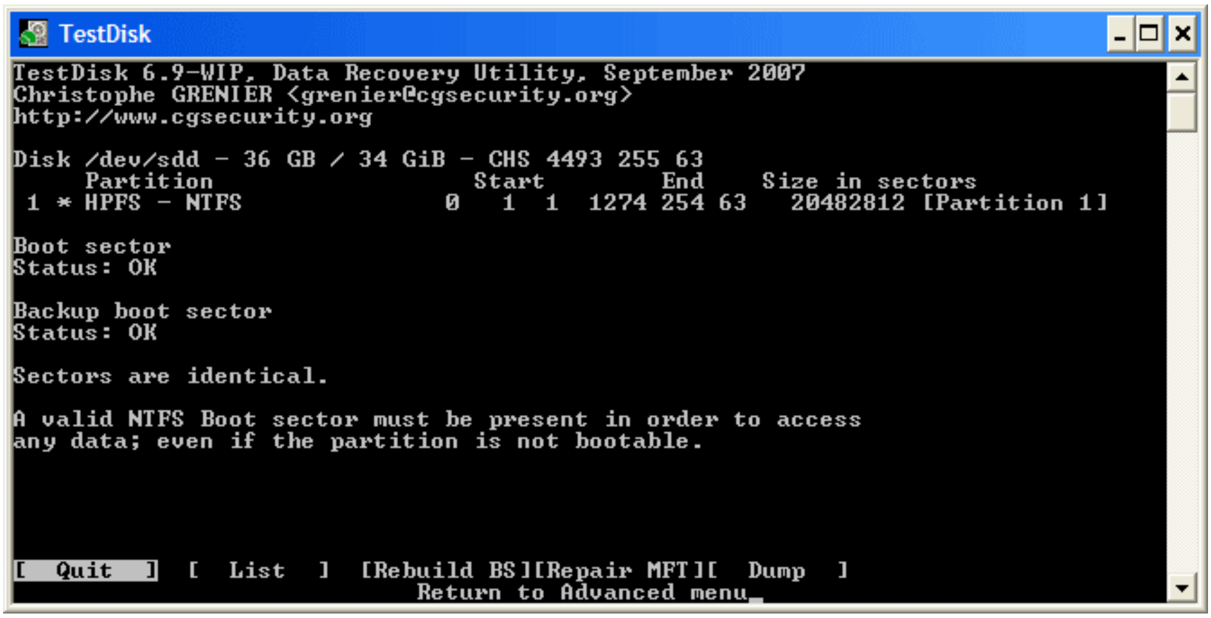
The boot sector of the first partition named `Partition 1` is still damaged. It's time to fix it. The status of the NTFS boot sector is bad and the backup boot sector is valid. Boot sectors are not identical.



```
TestDisk 6.9-WIP, Data Recovery Utility, September 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdd - 36 GB / 34 GiB - CHS 4493 255 63
     Partition                  Start        End    Size in sectors
 1 * HPFS - NTFS              0   1  1  1274 254 63   20482812 [Partition 1]

Boot sector
Status: Bad

Backup boot sector
Status: OK

Sectors are not identical.

A valid NTFS Boot sector must be present in order to access
any data; even if the partition is not bootable.




[  Quit  ]  [  List  ]  [Backup BS] [Rebuild BS][  Dump  ]
                              Copy backup boot sector over boot sector
```

- To copy the backup of the boot sector over the boot sector, select ***Backup BS***, validate with Enter, use y to confirm and next OK.

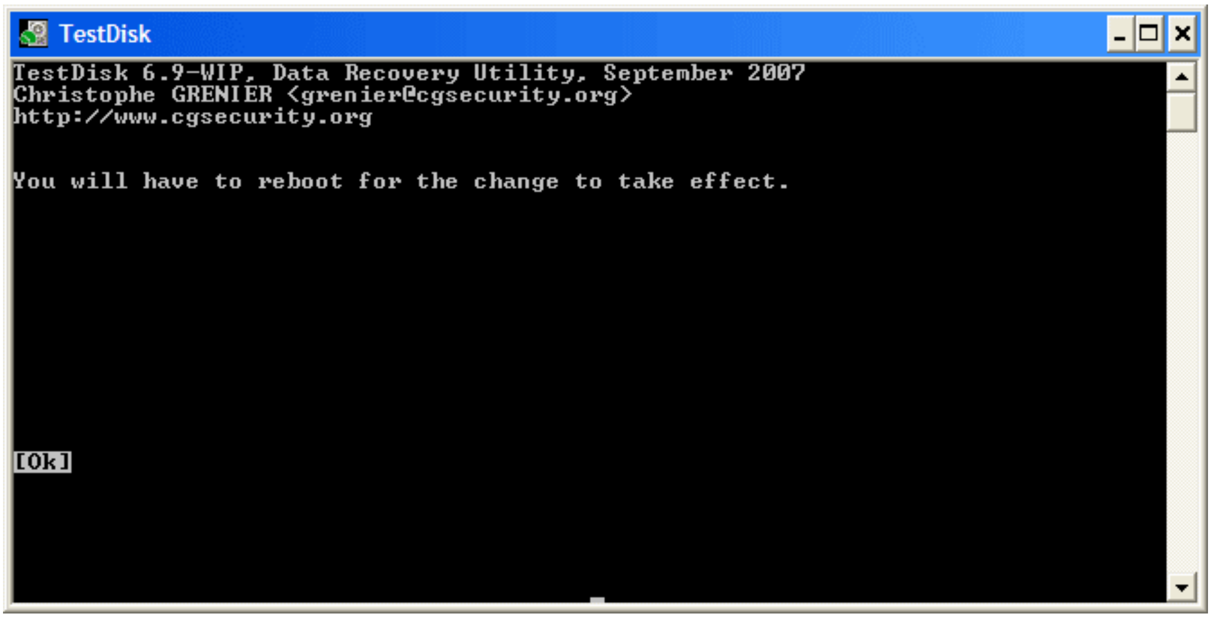
More information about repairing your boot sector under TestDisk Menu Items. The following message is displayed:



```
TestDisk 6.9-WIP, Data Recovery Utility, September 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdd - 36 GB / 34 GiB - CHS 4493 255 63
     Partition                  Start        End    Size in sectors
 1 * HPFS - NTFS              0   1  1  1274 254 63   20482812 [Partition 1]

Boot sector
Status: OK

Backup boot sector
Status: OK

Sectors are identical.

A valid NTFS Boot sector must be present in order to access
any data; even if the partition is not bootable.




[  Quit  ]  [  List  ]  [Rebuild BS][Repair MFT][  Dump  ]
                               Return to Advanced menu
```

The boot sector and its backup are now both OK and identical: the NTFS boot sector has been successfully recovered.

- Press Enter to quit.



```
TestDisk 6.9-WIP, Data Recovery Utility, September 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org


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












[Ok]
```

- TestDisk displays ***You have to restart your Computer to access your data*** so press `Enter` a last time and reboot your computer.

Recover deleted files

TestDisk can undelete

- files and directory from FAT12, FAT16 and FAT32 filesystem,
- files from ext2 filesystem,
- files from NTFS partition since version 6.11.

If it doesn't work or for other filesystem, try PhotoRec, a signature based file recovery utility.

Return to TestDisk main page

Please support the project
with your donations.