

TestDisk Step By Step

CGSecurity

This Recovery example guides you through TestDisk step by step to recover a missing partition and repair a corrupted one. Translation 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.

TestDisk Step By Step

CGSecurity

To recover lost partition or repair file system from hard disk, USB key, Smart Card..., you need enough rights to access physical device.

- Under Dos, run **TestDisk.exe**
- Under Windows, start TestDisk (ie testdisk-6.9/win/testdisk_win.exe) from an account in the Administrator Group. Under Vista, use right-click "run as administrator" to launch TestDisk.
- Under Unix/Linux/BSD, you need to be root to run TestDisk (ie. sudo testdisk-6.9/linux/testdisk_static)
- Under MacOSX, if you are not root, TestDisk (ie testdisk-6.9/darwin/TestDisk) will restart itself using sudo after confirmation of your part.
- Under OS/2, TestDisk doesn't handle physical device, only disk image, sorry.

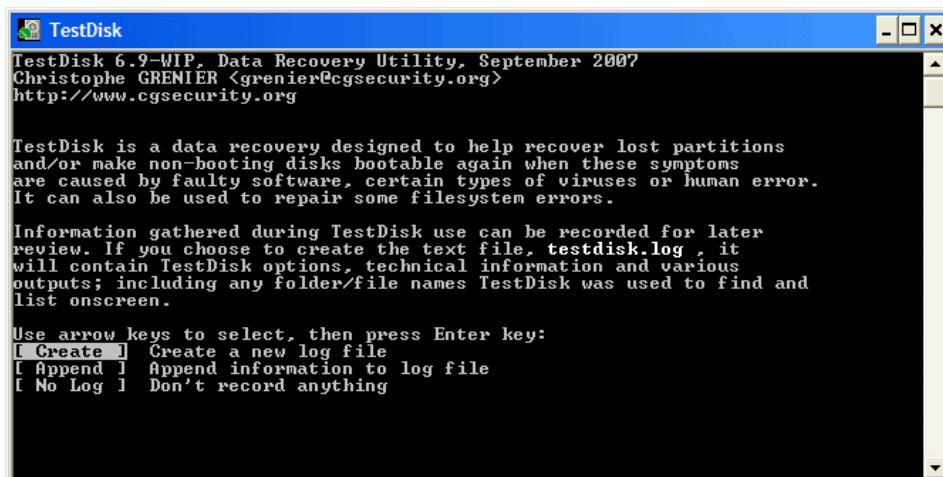
To recover partition from a media image or repair a file system image, run

- **testdisk image.dd** to carve a raw disk image
- **testdisk image.E01** to recover files from an Encase EWF image
- **testdisk 'image.*'** if the Encase image is splitted in several files.

To repair a file system 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 file system encrypted with cryptsetup/dm-crypt/LUKS.
- **testdisk /dev/md0** to repair a file system on top of a Linux Raid device.

Log Creation



```
TestDisk
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
```

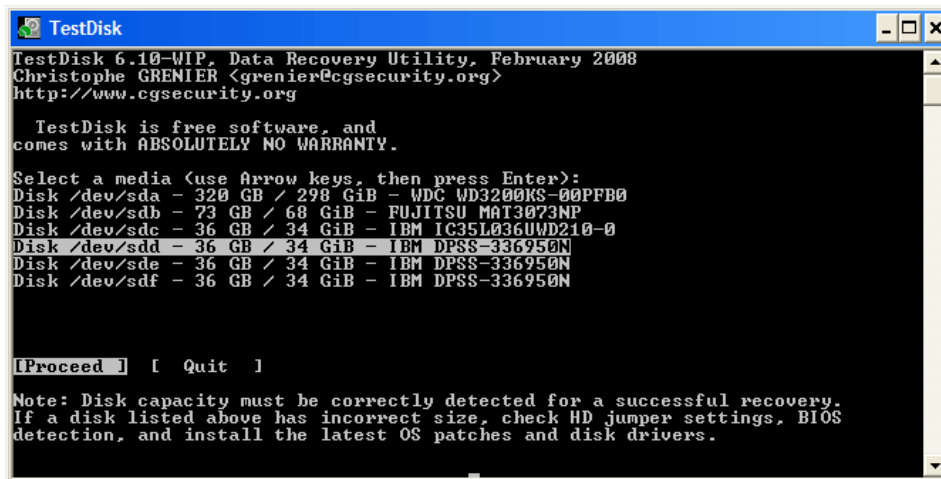
- Choose Create unless you have a reason to append data to the log or if you execute TestDisk from a read only media and nowhere else to create it.
- Press Enter to proceed.

TestDisk Step By Step

CGSecurity

Disk Selection

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



```
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 WD3200RS-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 ]

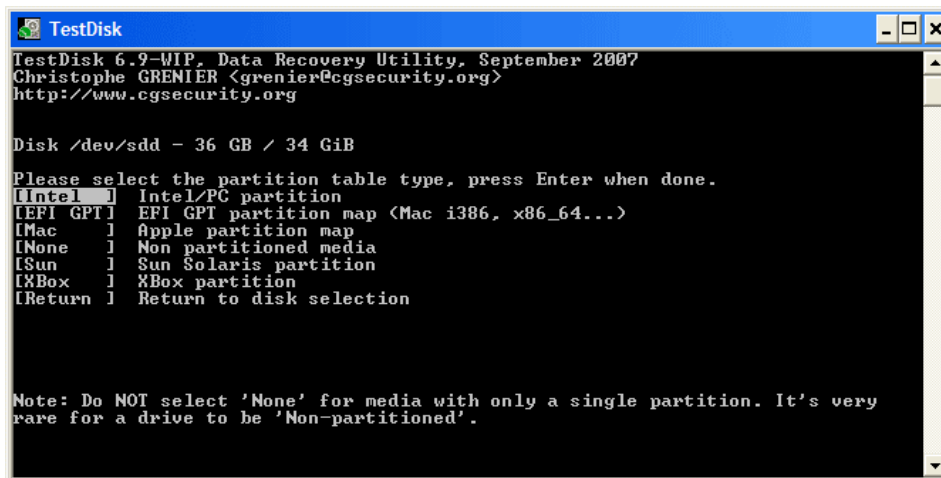
Note: Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has incorrect size, check HD jumper settings, BIOS
detection, and install the latest OS patches and disk drivers.
```

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

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

Partition Table Selection

TestDisk displays the partition table types.



```
TestDisk
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...)
[IMac ] Apple partition map
[None ] Non partitioned media
[ISun ] 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'.
```

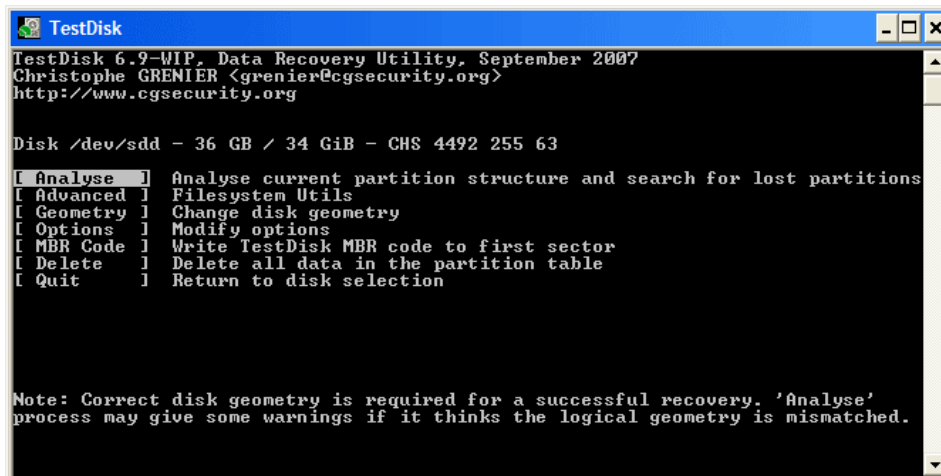
- Select the partition table type, usually the default value is the correct one as TestDisk auto-detects the partition table type.
- Press Enter to Proceed.

Current Partition Table Status

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

TestDisk Step By Step

CGSecurity



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

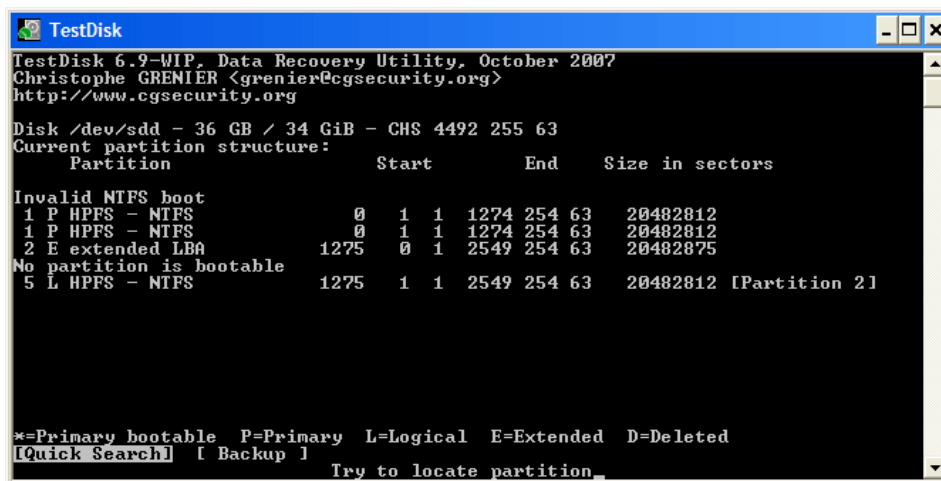
Disk /dev/sdd - 36 GB / 34 GiB - CHS 4492 255 63

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

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

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



```
TestDisk
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_
```

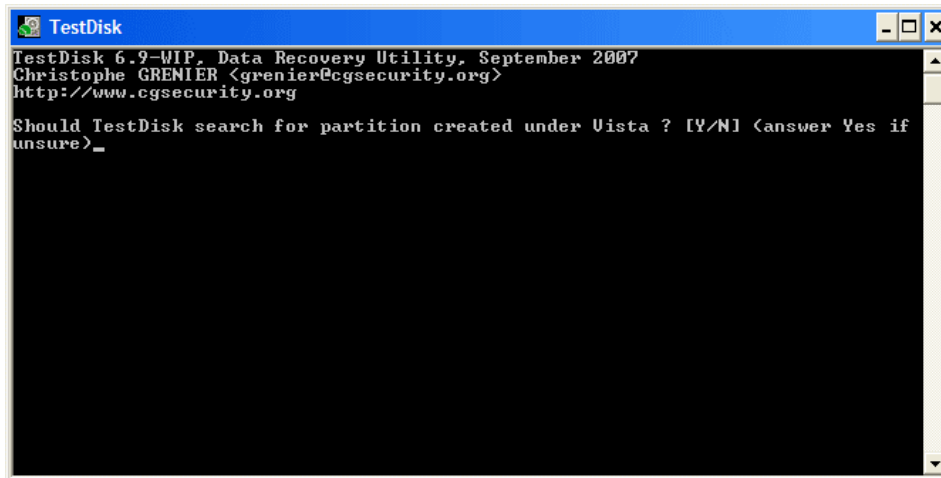
The first partition is listed twice which points to a corrupted partition or an invalid partition table entry, Invalid NTFS boot points to a faulty NTFS boot sector, so it's a corrupted filesystem. Only one logical partition (label Partition 2) is available in the extended partition. One logical partition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

- Confirm at Quick Search to proceed.

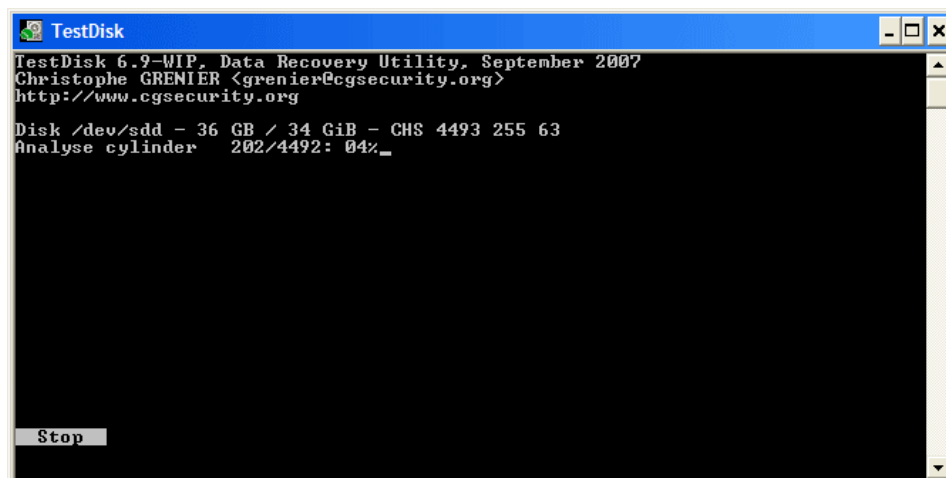
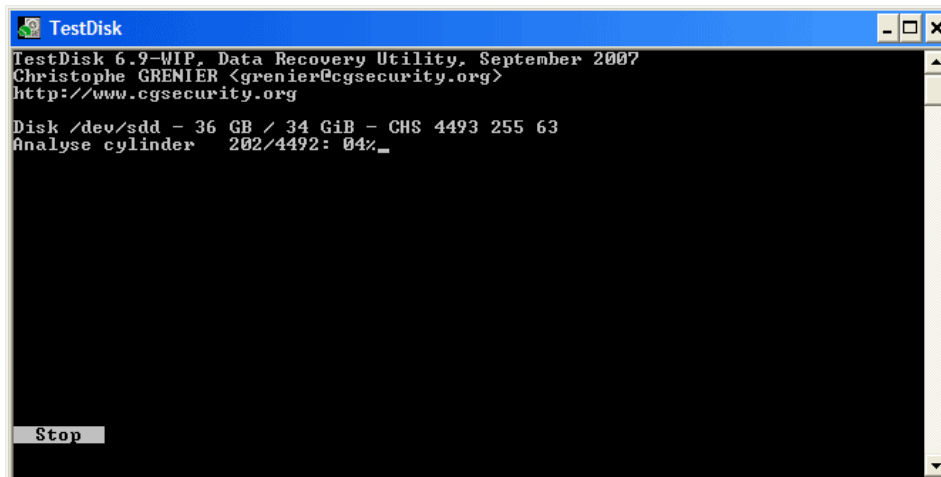
TestDisk Step By Step

CGSecurity

Quick Search for Partitions



- Confirm according to your OS and created partitions to proceed.

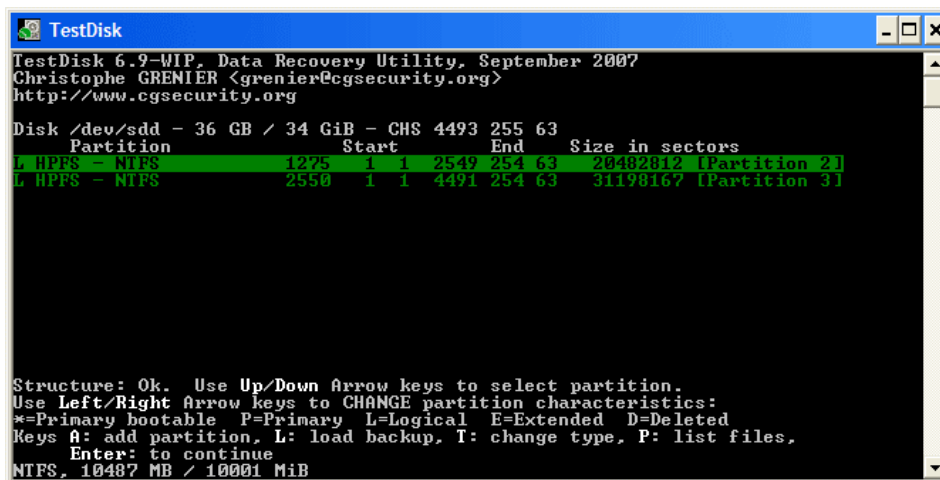


- TestDisk displays the first results in real time.

TestDisk Step By Step

CGSecurity

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



```
TestDisk
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      2549    20482812 [Partition 2]
L HPFS - NTFS  2550      4491    31198167 [Partition 3]

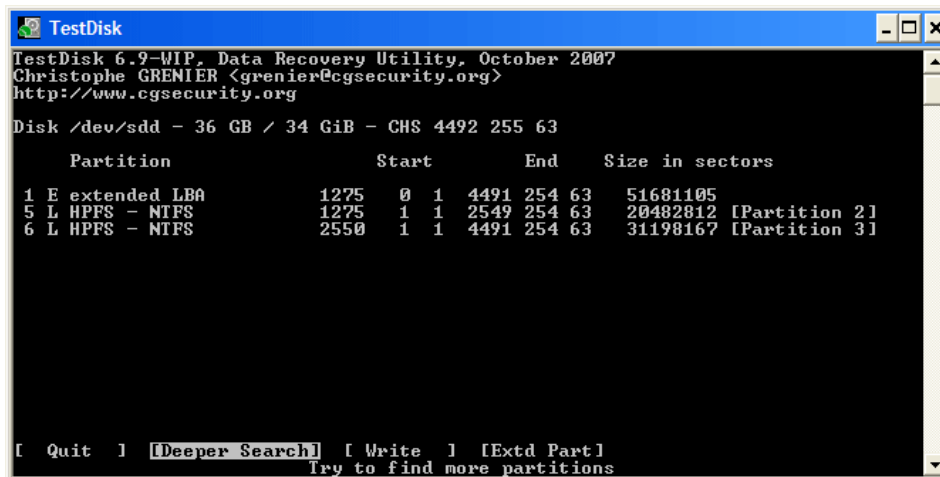
Structure: Ok. Use Up/Down Arrow keys to select partition.
Use Left/Right Arrow keys to CHANGE partition characteristics:
*=Primary bootable P=Primary L=Logical E=Extended D=Deleted
Keys A: add partition, L: load backup, T: change type, P: list files,
Enter: to continue
NTFS, 10487 MB / 10001 MiB
```

- Highlight this partition and press p to list your files (to go back to the previous display, press q to Quit).

All directories and data are correctly listed.

- Press Enter to proceed.

Save the partition table or search for more partitions?



```
TestDisk
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      4491    51681105
5 L HPFS - NTFS  1275      2549    20482812 [Partition 2]
6 L HPFS - NTFS  2550      4491    31198167 [Partition 3]

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

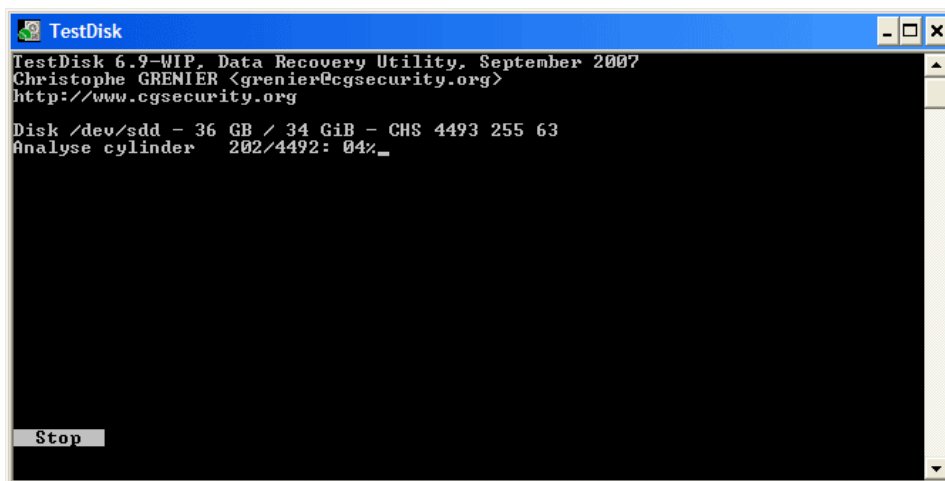
- When all partitions are available and data correctly listed, you should go to the menu Write to save the partition structure. The menu Extd Part gives you the opportunity to decide if the extended partition will use all available disk space or only the required (minimal) space.
- Since a partition,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

TestDisk Step By Step

CGSecurity



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

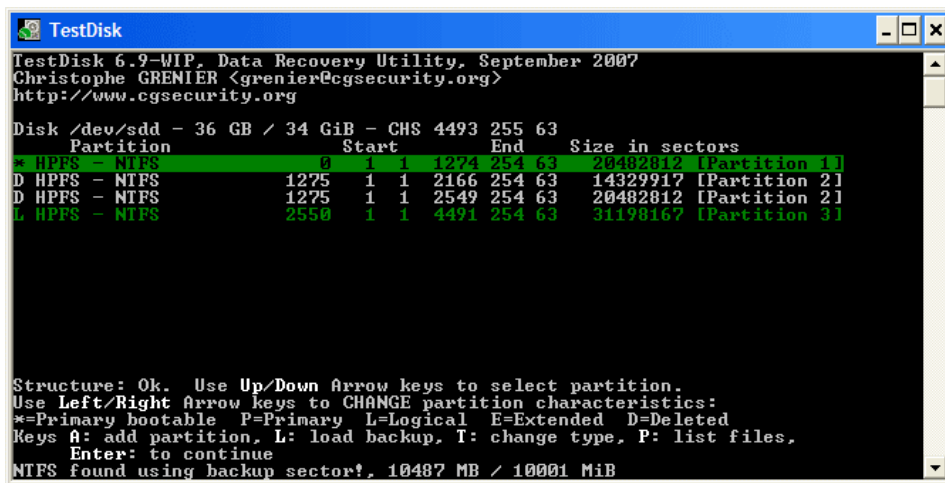
Disk /dev/sdd - 36 GB / 34 GiB - CHS 4493 255 63
Analyse cylinder 202/4492: 04%_

Stop
```

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.

Both partitions are listed with status D for deleted, because they overlap each other.



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

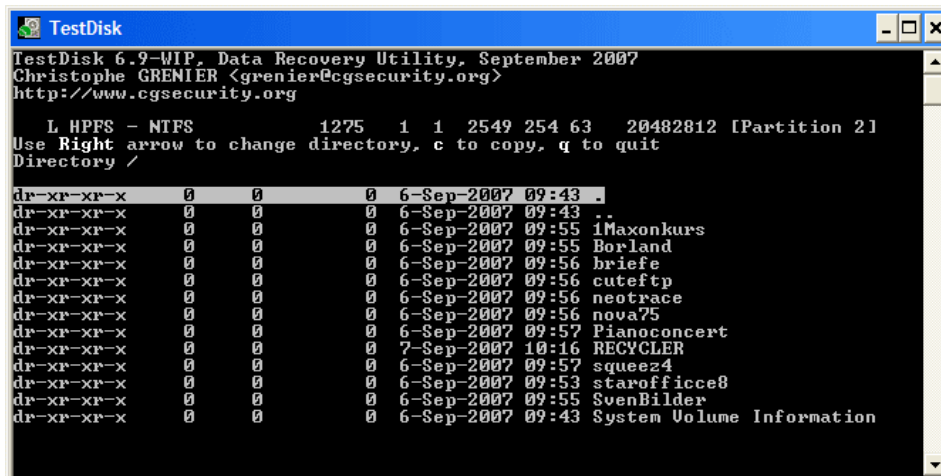
Disk /dev/sdd - 36 GB / 34 GiB - CHS 4493 255 63
Partition
Partition Start End Size in sectors
* HPFS - NTFS 0 1 1274 254 63 20482812 [Partition 1]
D HPFS - NTFS 1275 1 1 2166 254 63 14329917 [Partition 2]
D HPFS - NTFS 1275 1 1 2549 254 63 20482812 [Partition 2]
L HPFS - NTFS 2550 1 1 4491 254 63 31198167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

CGSecurity



```
TestDisk
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 squeeze4
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
```

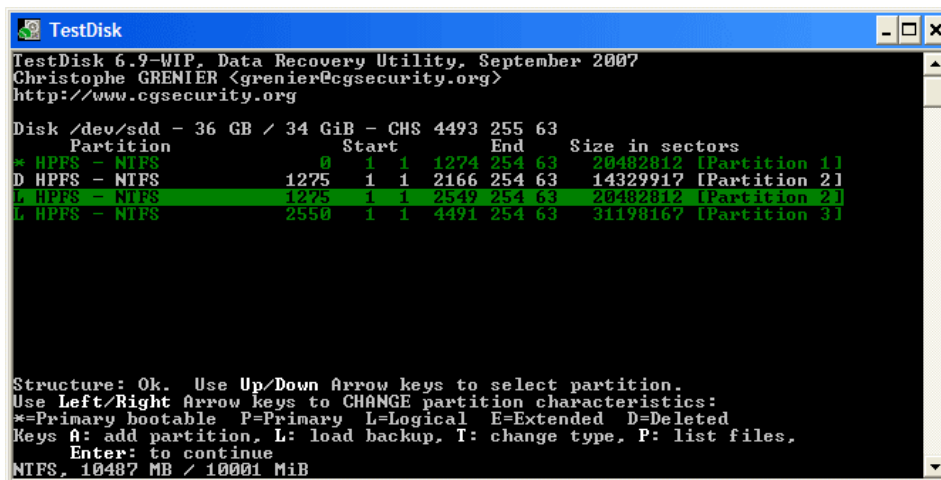
It works, you have found the correct partition!

- 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 to *L(ogical)*



```
TestDisk
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          0          0 [Partition 1]
D HPFS - NTFS   1275      1  1  2166 254 63  14329917 [Partition 2]
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
```

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 Primary partition.

- Press Enter to proceed.

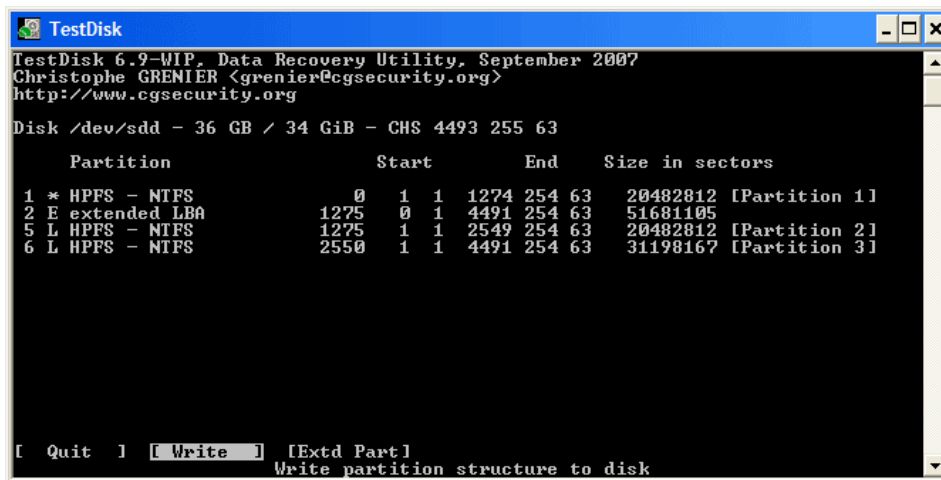
TestDisk Step By Step

CGSecurity

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
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 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]

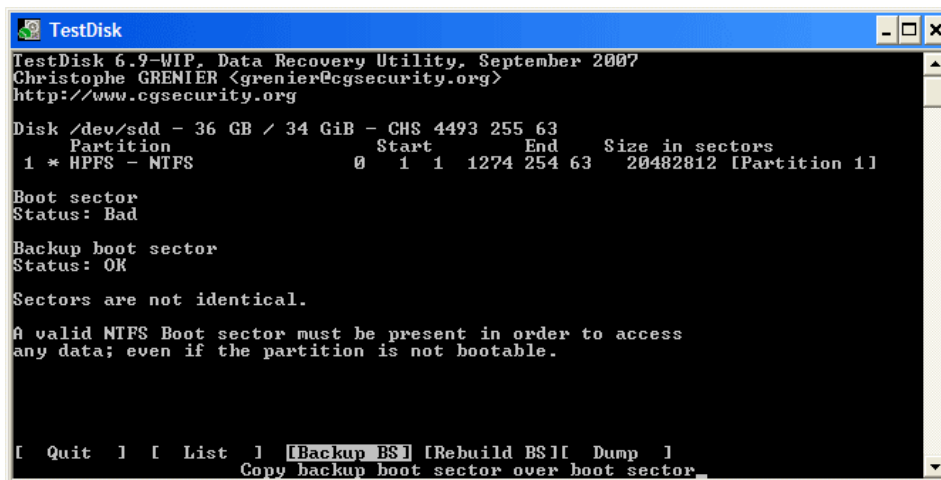
[ Quit ] [ Write ] [Extd Part]
Write partition structure to disk
```

- Confirm at Write with Enter, y and and Ok.

Now, all 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
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 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.

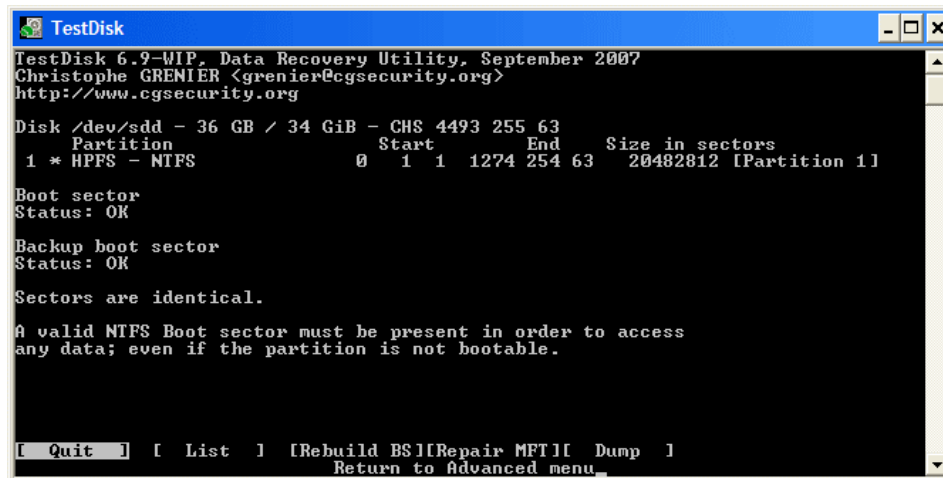
[ Quit ] [ List ] [Backup BS] [Rebuild BS][ Dump ]
Copy backup boot sector over boot sector.
```

- 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 Step By Step

CGSecurity



```
TestDisk
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

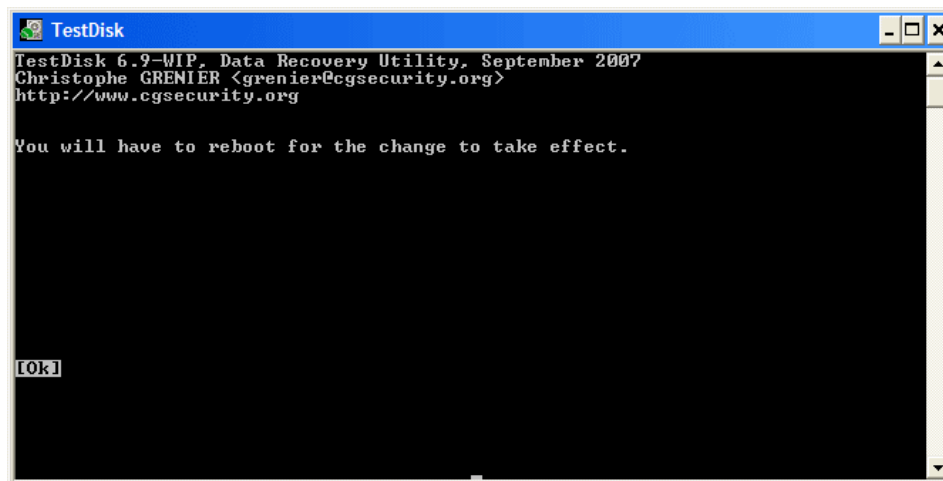
Sectors are identical.

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
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.

TestDisk: Undelete File for FAT

This Recovery example guides you through TestDisk step by step to undelete files from FAT filesystem. It's possible to recover your deleted files: when a file is deleted, the filename is marked as deleted and the data as unallocated/free, but TestDisk can read the deleted directory entry and find

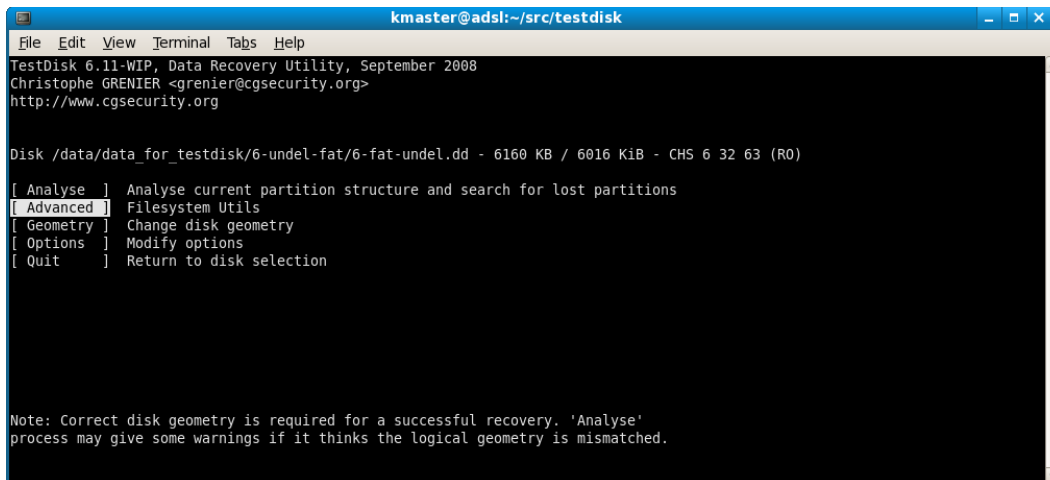
TestDisk Step By Step

CGSecurity

where the file was beginning. If the data space hasn't been overwritten by a new file, the file is recoverable.

Start the Undelete Process

- Select Advanced



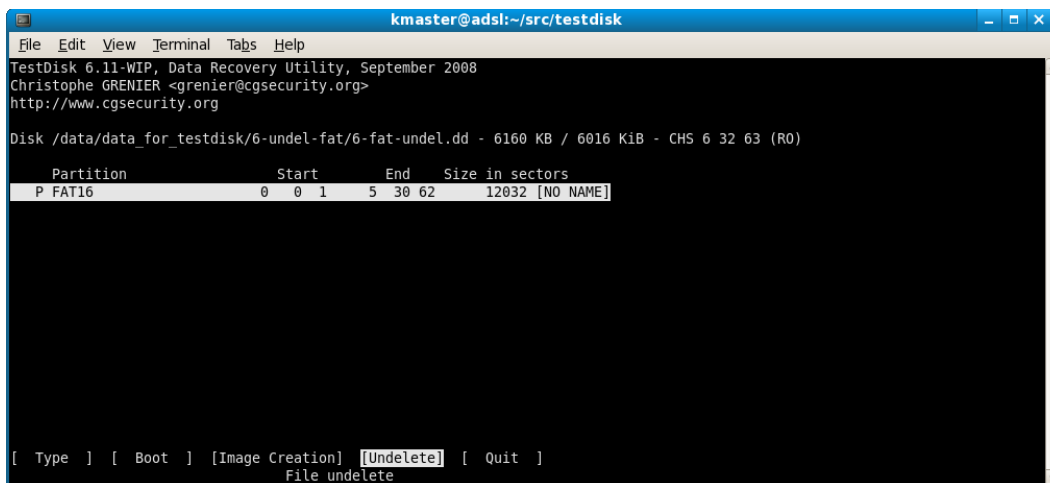
```
kmaster@adsl:~/src/testdisk
File Edit View Terminal Tabs Help
TestDisk 6.11-WIP, Data Recovery Utility, September 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /data/data_for_testdisk/6-undel-fat/6-fat-undel.dd - 6160 KB / 6016 KiB - CHS 6 32 63 (R0)

[ 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.
```

- Select the partition that was holding the lost files and choose Undelete



```
kmaster@adsl:~/src/testdisk
File Edit View Terminal Tabs Help
TestDisk 6.11-WIP, Data Recovery Utility, September 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /data/data_for_testdisk/6-undel-fat/6-fat-undel.dd - 6160 KB / 6016 KiB - CHS 6 32 63 (R0)

Partition      Start      End      Size in sectors
P FAT16        0 0 1      5 30 62      12032 [NO NAME]

[ Type ] [ Boot ] [Image Creation] [Undelete] [ Quit ]
File undelete
```

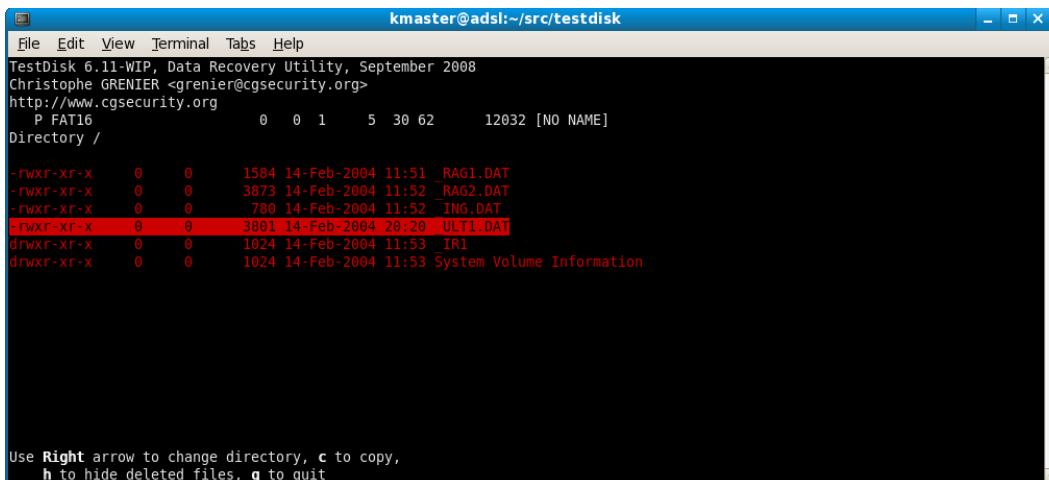
FAT File Undelete

Deleted files and directories are displayed in red.

- To undelete a file, select the file to recover and press 'c' to copy the file.
- To recover a deleted directory, select the directory and press 'c' to undelete the directory and its content.

TestDisk Step By Step

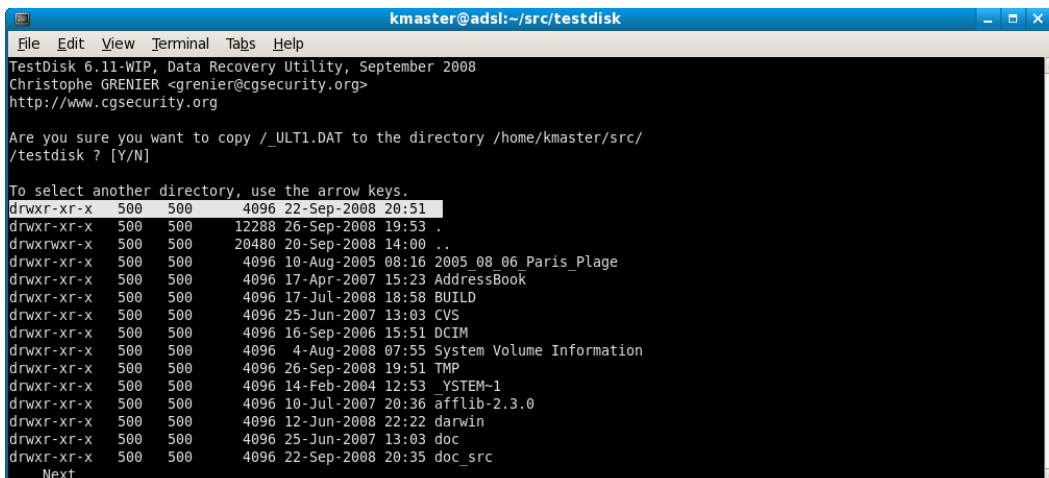
CGSecurity



```
kmaster@adsl:~/src/testdisk
File Edit View Terminal Tabs Help
TestDisk 6.11-WIP, Data Recovery Utility, September 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
P FAT16          0  0  1   5 30 62   12032 [NO NAME]
Directory /
-rwxr-xr-x  0  0   1584 14-Feb-2004 11:51 _RAG1.DAT
-rwxr-xr-x  0  0   3873 14-Feb-2004 11:52 _RAG2.DAT
-rwxr-xr-x  0  0    780 14-Feb-2004 11:52 _ING.DAT
-rwxr-xr-x  0  0   3881 14-Feb-2004 20:20 _ULT1.DAT
drwxr-xr-x  0  0   1024 14-Feb-2004 11:53 IR1
drwxr-xr-x  0  0   1024 14-Feb-2004 11:53 System Volume Information

Use Right arrow to change directory, c to copy,
h to hide deleted files, q to quit
```

- Select where recovered files should be written
- Select the destination

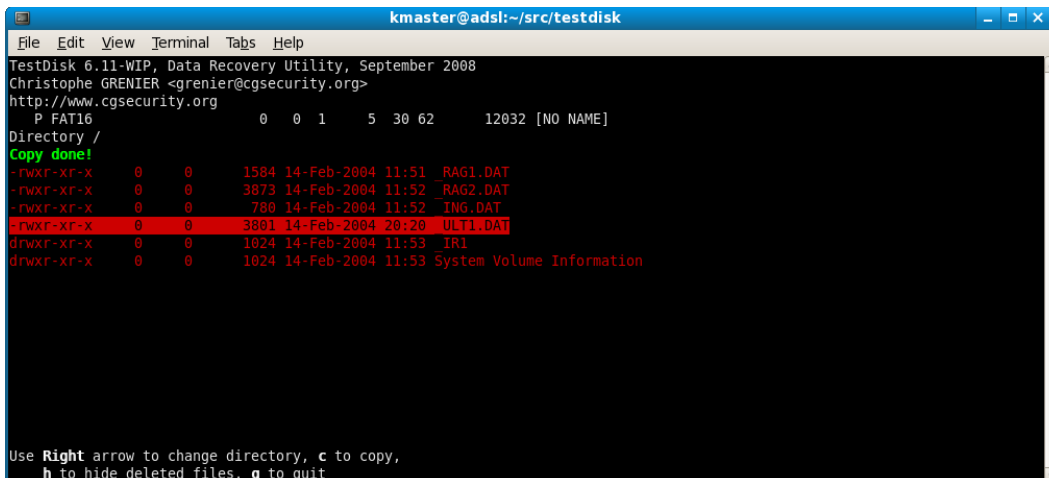


```
kmaster@adsl:~/src/testdisk
File Edit View Terminal Tabs Help
TestDisk 6.11-WIP, Data Recovery Utility, September 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Are you sure you want to copy /_ULT1.DAT to the directory /home/kmaster/src/
/testdisk ? [Y/N]

To select another directory, use the arrow keys.
drwxr-xr-x  500 500   4096 22-Sep-2008 20:51
drwxr-xr-x  500 500  12288 26-Sep-2008 19:53 .
drwxrwxr-x  500 500  20480 20-Sep-2008 14:00 ..
drwxr-xr-x  500 500   4096 10-Aug-2005 08:16 2005_08_06_Paris_Plage
drwxr-xr-x  500 500   4096 17-Apr-2007 15:23 AddressBook
drwxr-xr-x  500 500   4096 17-Jul-2008 18:58 BUILD
drwxr-xr-x  500 500   4096 25-Jun-2007 13:03 CVS
drwxr-xr-x  500 500   4096 16-Sep-2006 15:51 DCIM
drwxr-xr-x  500 500   4096  4-Aug-2008 07:55 System Volume Information
drwxr-xr-x  500 500   4096 26-Sep-2008 19:51 TMP
drwxr-xr-x  500 500   4096 14-Feb-2004 12:53 _YSTEM-1
drwxr-xr-x  500 500   4096 10-Jul-2007 20:36 afflib-2.3.0
drwxr-xr-x  500 500   4096 12-Jun-2008 22:22 darwin
drwxr-xr-x  500 500   4096 25-Jun-2007 13:03 doc
drwxr-xr-x  500 500   4096 22-Sep-2008 20:35 doc_src
Next
```

- FAT file recovery is completed
- When you get your files back, use Quit to exit.



```
kmaster@adsl:~/src/testdisk
File Edit View Terminal Tabs Help
TestDisk 6.11-WIP, Data Recovery Utility, September 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
P FAT16          0  0  1   5 30 62   12032 [NO NAME]
Directory /
Copy done!
-rwxr-xr-x  0  0   1584 14-Feb-2004 11:51 _RAG1.DAT
-rwxr-xr-x  0  0   3873 14-Feb-2004 11:52 _RAG2.DAT
-rwxr-xr-x  0  0    780 14-Feb-2004 11:52 _ING.DAT
-rwxr-xr-x  0  0   3881 14-Feb-2004 20:20 _ULT1.DAT
drwxr-xr-x  0  0   1024 14-Feb-2004 11:53 IR1
drwxr-xr-x  0  0   1024 14-Feb-2004 11:53 System Volume Information

Use Right arrow to change directory, c to copy,
h to hide deleted files, q to quit
```

TestDisk Step By Step

CGSecurity

For a maximum of security, TestDisk doesn't try to unerase files but let you copy the deleted files on another partition or disk. Remember you must avoid to write anything on the filesystem that was holding the data, otherwise deleted files may be overwritten by new ones.

TestDisk can undelete:

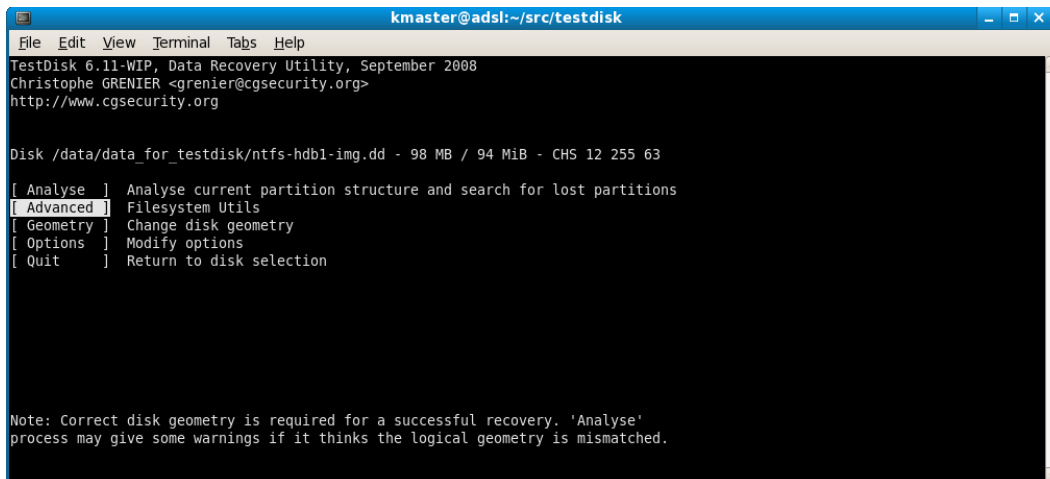
- files and directory from FAT12, FAT16 and FAT32 filesystem,
- files from NTFS partition since version 6.11,
- files from ext2 filesystem.

If a lost file is still missing, give PhotoRec a try. PhotoRec is a signature based file recovery utility and may be able to recover your data where other methods failed.

TestDisk: Undelete File for NTFS

This Recovery example guides you through TestDisk step by step to undelete files from NTFS filesystem. When a file is deleted, the data remains on the disk, unless new data have overwritten your lost file, TestDisk can recover it.

- Start the undelete process
- Select Advanced



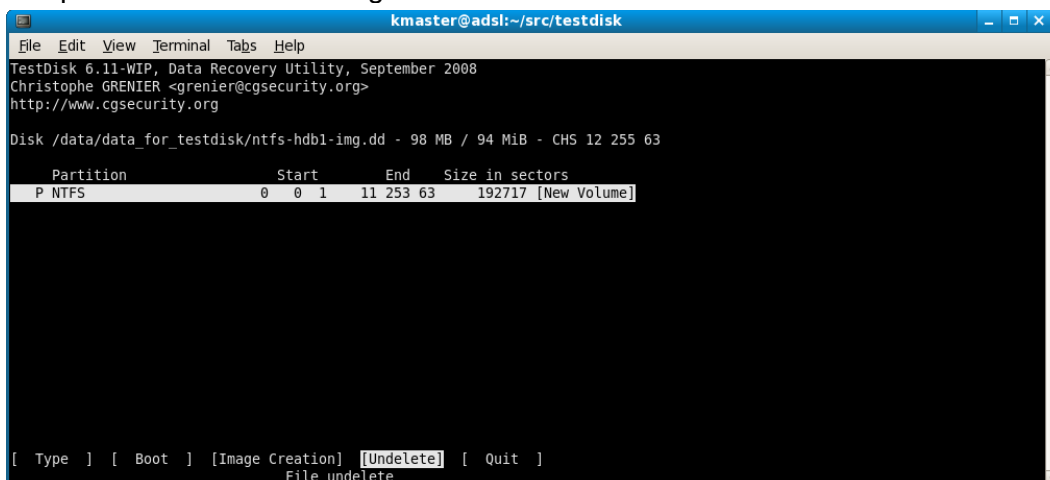
```
kmaster@adsl:~/src/testdisk
File Edit View Terminal Tabs Help
TestDisk 6.11-WIP, Data Recovery Utility, September 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /data/data_for_testdisk/ntfs-hdb1-img.dd - 98 MB / 94 MiB - CHS 12 255 63

[ 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.
```

- Select the partition that was holding the lost files and choose Undelete



```
kmaster@adsl:~/src/testdisk
File Edit View Terminal Tabs Help
TestDisk 6.11-WIP, Data Recovery Utility, September 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /data/data_for_testdisk/ntfs-hdb1-img.dd - 98 MB / 94 MiB - CHS 12 255 63

Partition      Start      End      Size in sectors
P NTFS         0 0 1     11 253 63 192717 [New Volume]

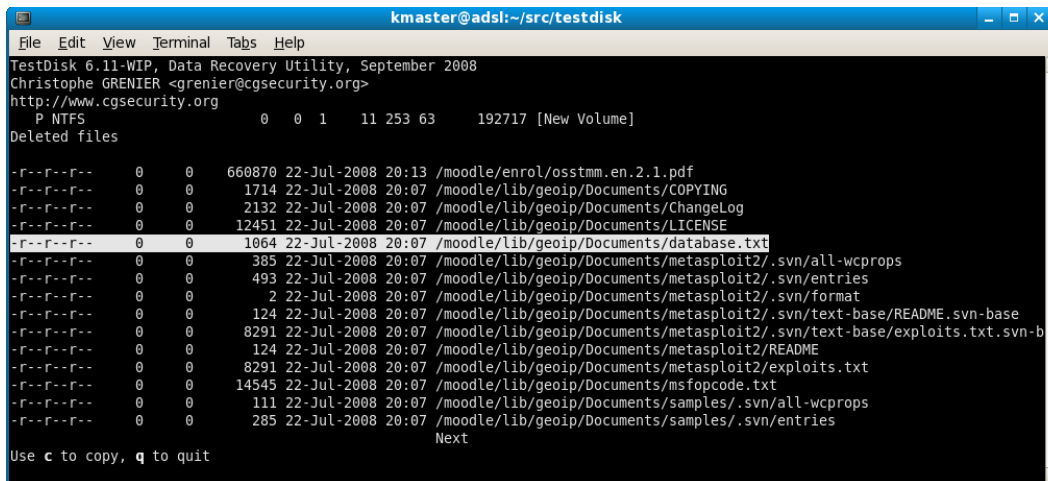
[ Type ] [ Boot ] [Image Creation] [Undelete] [ Quit ]
File undelete
```

TestDisk Step By Step

CGSecurity

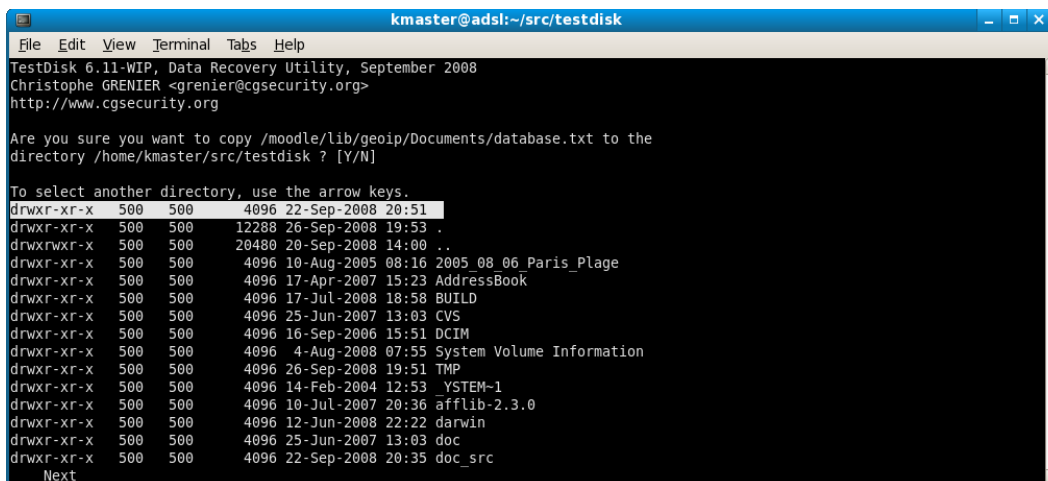
NTFS File Undelete

TestDisk scans MFT entries for deleted files. NTFS deleted files found by TestDisk are listed.



```
kmaster@adsl:~/src/testdisk
TestDisk 6.11-WIP, Data Recovery Utility, September 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
P NTFS 0 0 1 11 253 63 192717 [New Volume]
Deleted files
-r--r--r-- 0 0 660870 22-Jul-2008 20:13 /moodle/enrol/osstmm.en.2.1.pdf
-r--r--r-- 0 0 1714 22-Jul-2008 20:07 /moodle/lib/geoip/Documents/COPYING
-r--r--r-- 0 0 2132 22-Jul-2008 20:07 /moodle/lib/geoip/Documents/ChangeLog
-r--r--r-- 0 0 12451 22-Jul-2008 20:07 /moodle/lib/geoip/Documents/LICENSE
-r--r--r-- 0 0 1064 22-Jul-2008 20:07 /moodle/lib/geoip/Documents/database.txt
-r--r--r-- 0 0 385 22-Jul-2008 20:07 /moodle/lib/geoip/Documents/metasploit2/.svn/all-wcprops
-r--r--r-- 0 0 493 22-Jul-2008 20:07 /moodle/lib/geoip/Documents/metasploit2/.svn/entries
-r--r--r-- 0 0 2 22-Jul-2008 20:07 /moodle/lib/geoip/Documents/metasploit2/.svn/format
-r--r--r-- 0 0 124 22-Jul-2008 20:07 /moodle/lib/geoip/Documents/metasploit2/.svn/text-base/README.svn-base
-r--r--r-- 0 0 8291 22-Jul-2008 20:07 /moodle/lib/geoip/Documents/metasploit2/.svn/text-base/exploits.txt.svn-b
-r--r--r-- 0 0 124 22-Jul-2008 20:07 /moodle/lib/geoip/Documents/metasploit2/README
-r--r--r-- 0 0 8291 22-Jul-2008 20:07 /moodle/lib/geoip/Documents/metasploit2/exploits.txt
-r--r--r-- 0 0 14545 22-Jul-2008 20:07 /moodle/lib/geoip/Documents/msfopcode.txt
-r--r--r-- 0 0 111 22-Jul-2008 20:07 /moodle/lib/geoip/Documents/samples/.svn/all-wcprops
-r--r--r-- 0 0 285 22-Jul-2008 20:07 /moodle/lib/geoip/Documents/samples/.svn/entries
Next
Use c to copy, q to quit
```

- Pickup the file to recover and press 'c' to copy the file.
- Select where recovered files should be written
- Select the destination

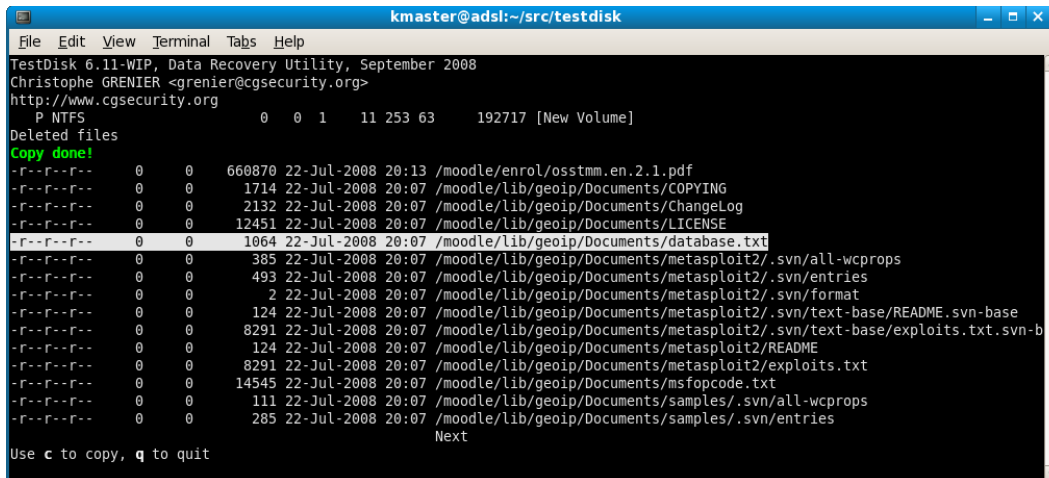


```
kmaster@adsl:~/src/testdisk
TestDisk 6.11-WIP, Data Recovery Utility, September 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
Are you sure you want to copy /moodle/lib/geoip/Documents/database.txt to the
directory /home/kmaster/src/testdisk ? [Y/N]
To select another directory, use the arrow keys.
drwxr-xr-x 500 500 4096 22-Sep-2008 20:51
drwxr-xr-x 500 500 12288 26-Sep-2008 19:53 .
drwxr-xr-x 500 500 20480 20-Sep-2008 14:00 ..
drwxr-xr-x 500 500 4096 10-Aug-2005 08:16 2005_08_06_Paris_Plage
drwxr-xr-x 500 500 4096 17-Apr-2007 15:23 AddressBook
drwxr-xr-x 500 500 4096 17-Jul-2008 18:58 BUILD
drwxr-xr-x 500 500 4096 25-Jun-2007 13:03 CVS
drwxr-xr-x 500 500 4096 16-Sep-2006 15:51 DCIM
drwxr-xr-x 500 500 4096 4-Aug-2008 07:55 System Volume Information
drwxr-xr-x 500 500 4096 26-Sep-2008 19:51 TMP
drwxr-xr-x 500 500 4096 14-Feb-2004 12:53 YSTEM-1
drwxr-xr-x 500 500 4096 10-Jul-2007 20:36 afflib-2.3.0
drwxr-xr-x 500 500 4096 12-Jun-2008 22:22 darwin
drwxr-xr-x 500 500 4096 25-Jun-2007 13:03 doc
drwxr-xr-x 500 500 4096 22-Sep-2008 20:35 doc_src
Next
```

- Recovery is completed
- When the NTFS file recovery is finished, choose Quit.

TestDisk Step By Step

CGSecurity



```
kmaster@adsl:~/src/testdisk
File Edit View Terminal Tabs Help
TestDisk 6.11-WIP, Data Recovery Utility, September 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
P NTFS 0 0 1 11 253 63 192717 [New Volume]
Deleted files
Copy done!
-r--r--r-- 0 0 660870 22-Jul-2008 20:13 /moodle/enrol/osstmm.en.2.1.pdf
-r--r--r-- 0 0 1714 22-Jul-2008 20:07 /moodle/lib/geiop/Documents/COPYING
-r--r--r-- 0 0 2132 22-Jul-2008 20:07 /moodle/lib/geiop/Documents/ChangeLog
-r--r--r-- 0 0 12451 22-Jul-2008 20:07 /moodle/lib/geiop/Documents/LICENSE
-r--r--r-- 0 0 1064 22-Jul-2008 20:07 /moodle/lib/geiop/Documents/database.txt
-r--r--r-- 0 0 385 22-Jul-2008 20:07 /moodle/lib/geiop/Documents/metasploit2/.svn/all-wcprops
-r--r--r-- 0 0 493 22-Jul-2008 20:07 /moodle/lib/geiop/Documents/metasploit2/.svn/entries
-r--r--r-- 0 0 2 22-Jul-2008 20:07 /moodle/lib/geiop/Documents/metasploit2/.svn/format
-r--r--r-- 0 0 124 22-Jul-2008 20:07 /moodle/lib/geiop/Documents/metasploit2/.svn/text-base/README.svn-base
-r--r--r-- 0 0 8291 22-Jul-2008 20:07 /moodle/lib/geiop/Documents/metasploit2/.svn/text-base/exploits.txt.svn-b
-r--r--r-- 0 0 124 22-Jul-2008 20:07 /moodle/lib/geiop/Documents/metasploit2/README
-r--r--r-- 0 0 8291 22-Jul-2008 20:07 /moodle/lib/geiop/Documents/metasploit2/exploits.txt
-r--r--r-- 0 0 14545 22-Jul-2008 20:07 /moodle/lib/geiop/Documents/msfopcode.txt
-r--r--r-- 0 0 111 22-Jul-2008 20:07 /moodle/lib/geiop/Documents/samples/.svn/all-wcprops
-r--r--r-- 0 0 285 22-Jul-2008 20:07 /moodle/lib/geiop/Documents/samples/.svn/entries
Next
Use c to copy, q to quit
```

For a maximum of security, TestDisk doesn't try to unerase files but lets you copy the deleted files you want to recover on another partition or disk. Be careful, do not write anything on the file system that was holding the data, writing new files may overwrite the files you want to recover.

TestDisk can undelete:

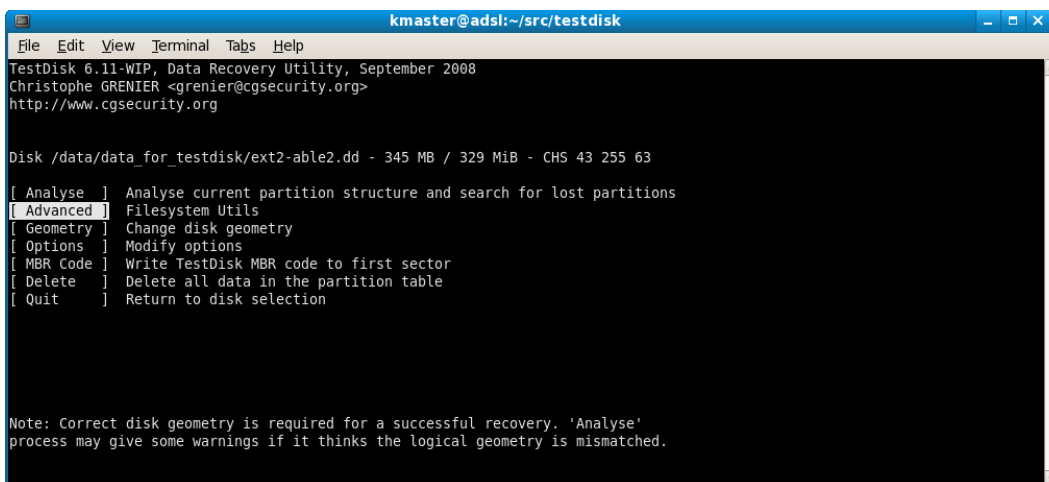
- files from NTFS partition since version 6.11,
- files and directory from FAT12, FAT16 and FAT32 filesystem,
- files from ext2 filesystem.

If a lost file is still missing, give PhotoRec a try. PhotoRec is a signature based file recovery utility and may be able to recover your data where other methods failed.

TestDisk: Undelete File for ext2

This Recovery example guides you through TestDisk step by step to undelete files from ext2 filesystem. The ext2 or second extended filesystem is a file system for the Linux kernel.

- Start the undelete process
- Select Advanced



```
kmaster@adsl:~/src/testdisk
File Edit View Terminal Tabs Help
TestDisk 6.11-WIP, Data Recovery Utility, September 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /data/data_for_testdisk/ext2-able2.dd - 345 MB / 329 MiB - CHS 43 255 63

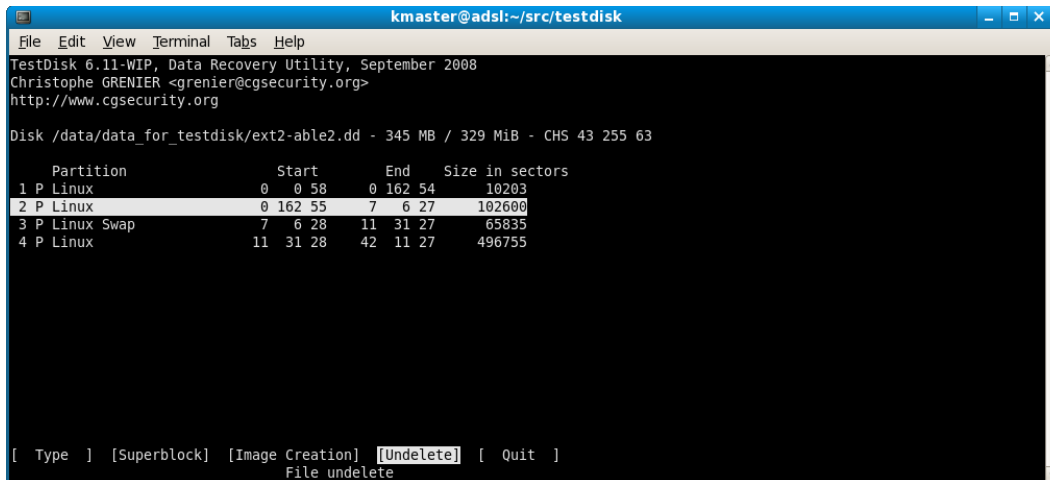
[ Analyse ] Analyse current partition structure and search for lost partitions
[ Advanced ] Filesystem Utils
[ Geometry ] Change disk geometry
[ Options ] Modify options
[ MBR Code ] Write TestDisk MBR code to first sector
[ Delete ] Delete all data in the partition table
[ Quit ] Return to disk selection

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

- Select the partition that was holding the lost files and choose Undelete

TestDisk Step By Step

CGSecurity



```
kmaster@adsl:~/src/testdisk
TestDisk 6.11-WIP, Data Recovery Utility, September 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

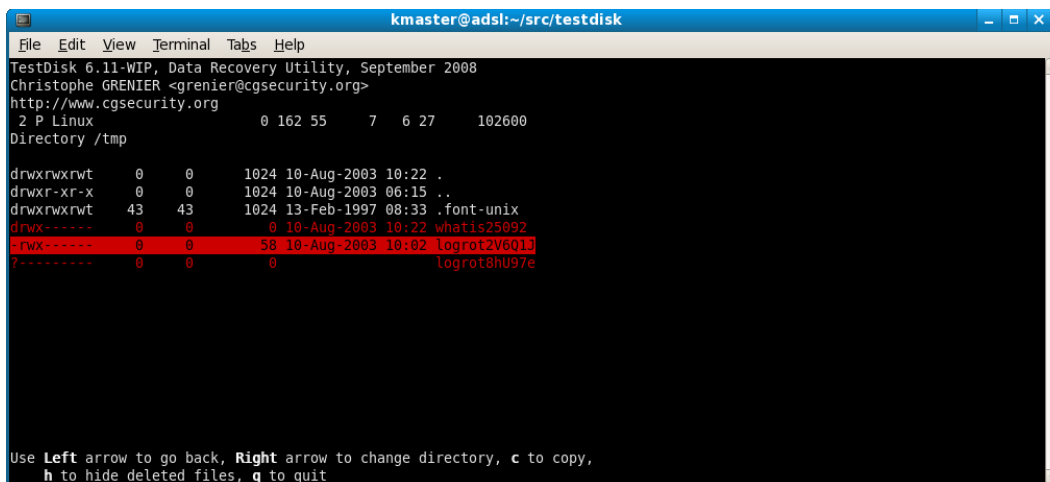
Disk /data/data_for_testdisk/ext2-able2.dd - 345 MB / 329 MiB - CHS 43 255 63

Partition              Start          End          Size in sectors
1 P Linux              0 0 58       0 162 54     10203
2 P Linux              0 162 55     7 6 27     102600
3 P Linux Swap         7 6 28     11 31 27     65835
4 P Linux             11 31 28     42 11 27    496755

[ Type ] [Superblock] [Image Creation] [Undelete] [ Quit ]
File undelete
```

ext2 File Undelete

Navigate in the directory structure until you have found the directory that was holding the file you are trying to recover. Deleted files are displayed in red. To undelete a file, select the file to recover and press 'c' to copy the file



```
kmaster@adsl:~/src/testdisk
TestDisk 6.11-WIP, Data Recovery Utility, September 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

2 P Linux              0 162 55     7 6 27     102600
Directory /tmp

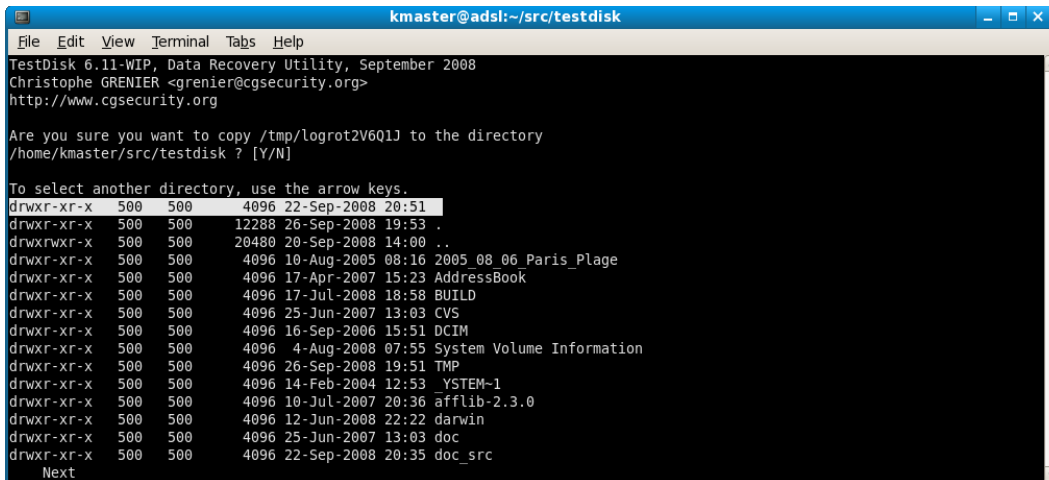
drwxrwxrwt  0  0      1024 10-Aug-2003 10:22 .
drwxr-xr-x  0  0      1024 10-Aug-2003 06:15 ..
drwxrwxrwt 43 43      1024 13-Feb-1997 08:33 .font-unix
drwx----- 0  0      0 10-Aug-2003 10:22 whatis25092
-rwx----- 0  0      58 10-Aug-2003 10:02 logrot2V601L
?----- 0  0      0 logrot8hU97e

Use Left arrow to go back, Right arrow to change directory, c to copy,
h to hide deleted files, q to quit
```

- Select where recovered files should be written
- Select the destination

TestDisk Step By Step

CGSecurity

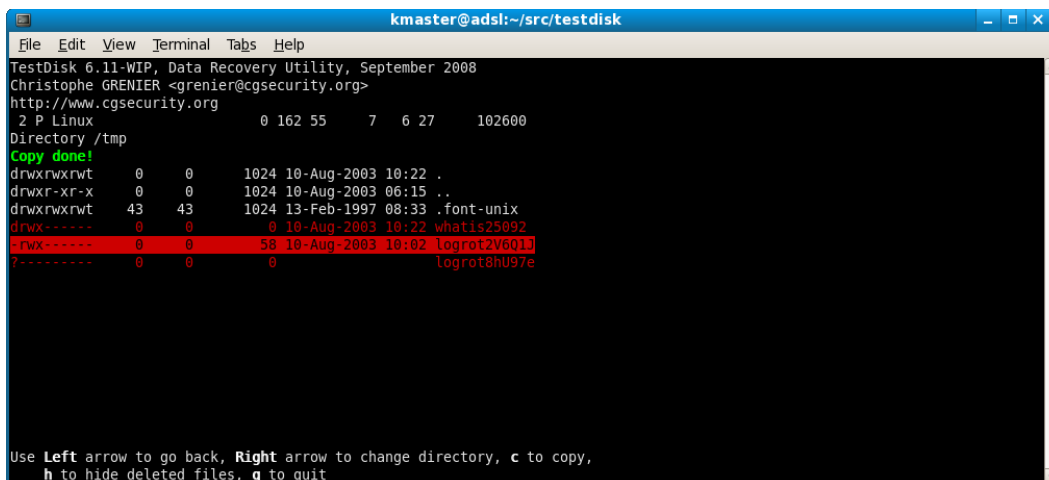


```
kmaster@adsl:~/src/testdisk
TestDisk 6.11-WIP, Data Recovery Utility, September 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Are you sure you want to copy /tmp/logrot2V6Q1J to the directory
/home/kmaster/src/testdisk ? [Y/N]

To select another directory, use the arrow keys.
drwxr-xr-x  500  500  4096 22-Sep-2008 20:51
drwxr-xr-x  500  500 12288 26-Sep-2008 19:53 .
drwxrwxr-x  500  500 20480 20-Sep-2008 14:00 ..
drwxr-xr-x  500  500  4096 10-Aug-2005 08:16 2005_08_06_Paris_Plage
drwxr-xr-x  500  500  4096 17-Apr-2007 15:23 AddressBook
drwxr-xr-x  500  500  4096 17-Jul-2008 18:58 BUILD
drwxr-xr-x  500  500  4096 25-Jun-2007 13:03 CVS
drwxr-xr-x  500  500  4096 16-Sep-2006 15:51 DCIM
drwxr-xr-x  500  500  4096  4-Aug-2008 07:55 System Volume Information
drwxr-xr-x  500  500  4096 26-Sep-2008 19:51 TMP
drwxr-xr-x  500  500  4096 14-Feb-2004 12:53 _YSTEM-1
drwxr-xr-x  500  500  4096 10-Jul-2007 20:36 afflib-2.3.0
drwxr-xr-x  500  500  4096 12-Jun-2008 22:22 darwin
drwxr-xr-x  500  500  4096 25-Jun-2007 13:03 doc
drwxr-xr-x  500  500  4096 22-Sep-2008 20:35 doc_src
Next
```

- Recovery is completed
- Once the ext2 file recovery completed, choose Quit.



```
kmaster@adsl:~/src/testdisk
TestDisk 6.11-WIP, Data Recovery Utility, September 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
2 P Linux 0 162 55 7 6 27 102600
Directory /tmp
Copy done!
drwxrwxrwt  0  0  1024 10-Aug-2003 10:22 .
drwxr-xr-x  0  0  1024 10-Aug-2003 06:15 ..
drwxrwxrwt 43 43  1024 13-Feb-1997 08:33 .font-unix
drwx----- 0  0  0 10-Aug-2003 10:22 whatis25092
drwx----- 0  0  58 10-Aug-2003 10:02 logrot2V6Q1J
?----- 0  0  0 logrot8HU97e

Use Left arrow to go back, Right arrow to change directory, c to copy,
h to hide deleted files, q to quit
```

For a maximum of security, TestDisk doesn't try to unerase files but let you copy the deleted files on another partition or disk. Remember you must avoid to write anything on the file system that was holding the data, otherwise deleted files may be overwritten by new ones.

TestDisk can undelete:

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

If a lost file is still missing, give PhotoRec a try. PhotoRec is a signature based file recovery utility and may be able to recover your data where other methods failed. Note that it can recover deleted files from ext3 and ext4 filesystem.

Running the TestDisk Program

TestDisk Startup

When TestDisk is executed, you may see the phrase Please wait... on your screen until it has gathered enough data from the BIOS or OS to get the hard disk list.

TestDisk Step By Step

CGSecurity

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

TestDisk is a 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 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
```

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 - 120 GB / 111 GiB - ATA ST3120026AS
Disk /dev/sdb - 120 GB / 111 GiB - ATA ST3120026AS

```
[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.

If the reported size doesn't match the hard disk size - i.e. a 120 GB hard disk is recognized as only a 32 GB hard disk - check your BIOS hard disk settings and the jumpers on the disk. On most large hard disks, there are jumpers to limit the size to only 32 or 8 GB. If your HD is detected as only 130 GB, LBA48 support may not be available in your OS - read OS notes for more information. Next step is to select the partition table type.

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

Disk /dev/sda - 120 GB / 111 GiB - ATA ST3120026AS

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...)
[Mac ] Apple partition map
[None ] Non partitioned media
[Sun ] Sun Solaris partition
[XBox ] Xbox partition
[Return ] Return to disk selection
```

TestDisk Step By Step

CGSecurity

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

TestDisk Menu Items

Menu Analyse

TestDisk queries the BIOS or the OS in order to find the hard disks and their characteristics (LBA size and CHS geometry). TestDisk does a quick check of your disk's structure and compares it with your partition table for entry errors. If the partition table has entry errors, TestDisk can repair them. If you have missing partitions or a completely empty partition table, TestDisk can search for partitions and create a new table or even a new MBR if necessary.

However, it's up to the user to look over the list of possible partitions found by TestDisk and to select the one(s) which were being used just before the drive failed to boot or the partition(s) were lost. In some cases, especially after initiating a detailed search for lost partitions, TestDisk may show partition data which is from the remnants of a partition that had been deleted and overwritten long ago.

Analyse

TestDisk 6.5-WIP, Data Recovery Utility, October 2006

Christophe GRENIER <grenier@cgsecurity.org>

<http://www.cgsecurity.org>

Disk /dev/sda - 120 GB / 111 GiB - CHS 14593 255 63

Current partition structure:

Partition	Start	End	Size in sectors
1 * FAT32	0 1 1 1010 254 63		16241652 [NO NAME]
2 P Linux	1011 0 1 1023 254 63		208845 [/boot]
3 E extended LBA	1024 0 1 14592 254 63		217985985
5 L Linux RAID	1024 1 1 3573 254 63		40965687 [md0]
X extended	3574 0 1 4210 254 63		10233405
6 L Linux RAID	3574 1 1 4210 254 63		10233342 [md1]
X extended	4211 0 1 14592 254 63		166786830
7 L Linux	4211 1 1 14592 254 63		166786767

*=Primary bootable P=Primary L=Logical E=Extended D=Deleted

[Proceed] [Backup]

Try to locate partition

Analyzes a drive's current partition structure and finds partitions, making it possible to recover lost partitions.

Partition Checks

TestDisk's Analyse does a quick check of the partition structure. TestDisk can handle several type of partitions: - Intel - Mac - None (i.e.: small media without partition) - Sun - XBox

The Intel partition structure is composed of the MBR table and extended partitions. The MBR is limited to four entries. One of the entries can be an extended partition allowing several logical partitions. Each logical partition is contained by an extended partition/container. The MBR and each extended partition must end with the two bytes 0x55 and 0xAA, in that order; which make up the hex word 0xAA55 (since x86 CPU systems are little-endian). A partition entry is composed of: - the start of the partition in CHS - the end of the partition in CHS - the filesystem type - the logical start - the size in sectors - the boot flag Only one primary partition can have the boot flag set. CHS information storage is limited to a maximum of 1024 cylinders (0-1023), that's why we have the famous 8 GB limitation ($1024*255*63 = 16450560$ sectors = 8422686720 bytes).

TestDisk Step By Step

CGSecurity

Modern operating systems and BIOS chips use LBA mode to access the data, but FAT12/16/32 boot sectors still make reference to CHS geometry. TestDisk checks that each value is in the authorized range: i.e., no sector value less than 1 nor higher than the number of sectors per head. The partition entries are read using the logical start and size in sectors, then TestDisk checks to see if the logical values match the CHS values. TestDisk also checks that no partition data shows a partition as ending after the end of the disk, and that none of them are overlapping each other.

Sun label can have up to 8 partition entries. Entry number 2 is reserved for the whole disk.

Filesystem Checks

Following the filesystem type, TestDisk runs some basic checks on the boot sector/superblock of each filesystem. As ext2/ext3/reiserfs/jfs share the same filesystem type: 0x83, TestDisk has to check for each filesystem. The checks are the same as those used when TestDisk is searching for partitions: - presence of magic value or signature (i.e., 0xAA55 at offset 0x1FE of either FAT or NTFS boot sectors). - coherent values (i.e., free_blocks_count lower than blocks_count for ext2) This phase is very quick as the checks are minimal.

Partition Recovery

In a second step, TestDisk searches for 'lost partitions' without making use of any results from the previous step. This is the heart of TestDisk's powerful capabilities! TestDisk assumes the existence of partitions and scans all relevant locations for them. With a PC/Intel partition table, a primary partition usually starts at the beginning of a cylinder (head=0, sector=1), while a logical partition starts a little further along (head=1, sector=1). For each possible partition starting location, TestDisk can search for the presence of a file system header (FAT or NTFS boot sector, ext2/ext3 superblock, BSD disklabel...), which confirms the presence of a known partition type. Thus, the size of a partition is determined directly from its structure on the disk. Each partition that TestDisk discovers is added to a list of found partitions.

To detect a FAT32 partition, TestDisk searches for a 0xAA55 end mark and the signature FAT32 - it also runs the corresponding FAT file system checks: - jump signature must be of the form 0xeb 0xXX 0x90 or 0xe9 0xXX 0xXX where 0xXX could be any byte, and...

0xeb: A Short Jump, displacement relative to next instruction (only 8 bit).
0x90: NOP (do nothing).
0xe9: A Near Jump, displacement relative to next instruction (32 or 16 bit).

- sector size is 512 - cluster size must be 1, 2, 4, 8, 16, 32, 64 or 128 - there must be 2 FAT copies - the media must be 0xF8 (no other value is seen - it's an obsolete feature) - If you follow MS guidelines, the signature FAT32 is meaningless but your file system should have it.

Following the number of clusters, TestDisk determine the kind of FAT (number of clusters is more or equal to 65525 for FAT32).

Some specific checks for FAT32 are done: - the root cluster number must be between 2 and the maximum cluster number, - some obsolete values (number of directory entries, 16-bit partition size) must be set to 0, - FAT32 version (unused) must be 0.0

To detect an NTFS partition, TestDisk searches for an 0xAA55 end mark and the signature NTFS - it also checks that some FAT specific values are all set to zero (0): the number of reserved sectors, number of FATs, number of directory entries, 16-bit size of file system, 32-bit size of file system, sectors per FAT. The number of Sectors per Cluster must be greater than zero.

For FAT and NTFS file system, the size of the partition will be read in the boot sector itself.

TestDisk Step By Step

CGSecurity

TestDisk 6.5-WIP, Data Recovery Utility, October 2006
Christophe GRENIER <grenier@cgsecurity.org>
<http://www.cgsecurity.org>

Disk /dev/sda - 120 GB / 111 GiB - CHS 14593 255 63
Analyse cylinder 1011/14592: 00%

```
FAT32          0  1  1  1010 254 63  16241652 [NO NAME]
```

Stop

Once the analysis is complete, TestDisk generates a report of found partitions.

TestDisk 6.5-WIP, Data Recovery Utility, November 2006
Christophe GRENIER <grenier@cgsecurity.org>
<http://www.cgsecurity.org>

```
Disk /dev/sda - 120 GB / 111 GiB - CHS 14593 255 63
  Partition          Start      End      Size in sectors
* FAT32              0  1  1  1010 254 63  16241652 [NO NAME]
P Linux             1011  0  1  1023 254 63   208845 [/boot]
D Linux             1024  1  1  3573 254 63  40965687
D Linux RAID        1024  1  1  3573 254 63  40965687 [md0]
D Linux             3574  1  1  4210 254 63  10233342
D Linux RAID        3574  1  1  4210 254 63  10233342 [md1]
L Linux             4211  1  1 14592 254 63 166786767
```

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
FAT32, 8315 MB / 7930 MiB

You can list files of NTFS, FAT, ext2/ext3 and ReiserFS partition by pressing P.

Notes:

- FAT directory listing is limited to 10 clusters, some files may not appear but it doesn't affect recovery.
- For NTFS, it's possible to copy files by pressing *c*.

TestDisk 6.5-WIP, Data Recovery Utility, October 2006
Christophe GRENIER <grenier@cgsecurity.org>
<http://www.cgsecurity.org>

```
* FAT32          0  1  1  1010 254 63  16241652 [NO NAME]
```

Use right arrow to change directory, q to quit

Directory /

```
-rwxr-xr-x  0  0  805306368 20-Jul-2005 10:35 PAGEFILE.SYS
drwxr-xr-x  0  0  0 14-Feb-2005 22:41 WINDOWS
-r-xr-xr-x  0  0  4952 28-Aug-2001 15:00 Bootfont.bin
-r-xr-xr-x  0  0  251712  3-Aug-2004 22:59 NTLDR
-r-xr-xr-x  0  0  47564  3-Aug-2004 22:38 NTDETECT.COM
-rwxr-xr-x  0  0  212 14-Feb-2005 22:51 BOOT.INI
```

TestDisk Step By Step

CGSecurity

```
drwxr-xr-x    0    0    0 14-Feb-2005 22:47 Documents and Settings
dr-xr-xr-x    0    0    0 14-Feb-2005 22:55 Program Files
-rwxr-xr-x    0    0    0 14-Feb-2005 22:56 CONFIG.SYS
-rwxr-xr-x    0    0    0 14-Feb-2005 22:56 AUTOEXEC.BAT
-r-xr-xr-x    0    0    0 14-Feb-2005 22:56 IO.SYS
-r-xr-xr-x    0    0    0 14-Feb-2005 22:56 MSDOS.SYS
drwxr-xr-x    0    0    0 14-Feb-2005 23:02 System Volume Information
-rwxr-xr-x    0    0 536399872 20-Jul-2005 10:36 HIBERFIL.SYS
```

Using the list of found partitions, you can edit the partition table.

There are three kinds of edits:

1. You can change the partition type with *T*
2. You can add a new partition with *A*.
3. You can change the status of the selected partition using the left/right arrow key. The available statuses are Primary, * bootable, Logical, Deleted.

As you make edits, watch the status of the partition table's structure. It will be either **Ok** or **Bad**.

Structure: Ok should appear if everything is ok, i.e., no primary partition between two extended partitions, one or no bootable partitions, no partitions using the same disk space.

When you are satisfied with the edited partition table, press Enter. If you've made any edits, TestDisk gives you a choice of writing that data to the drive's partition table, or of running a more detailed analysis.

Quit

Quits (exits) from the TestDisk program without making any changes (unless you pressed the ENTER key while **Write** was highlighted).

Search!

The quick first scan may have miss some partitions. 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.

Write

Writes the changes that have been made in TestDisk's memory buffer to the hard drive. If you are unsure of the changes (often to the MBR's partition table), then don't use this function!

Extd Part

If there is logical partition, this flag lets you decide if the extended partition will used all available disk space or only the required (minimal) space.

TestDisk 6.5-WIP, Data Recovery Utility, October 2006
Christophe GRENIER <grenier@cgsecurity.org>
<http://www.cgsecurity.org>

Disk /dev/sda - 120 GB / 111 GiB - CHS 14593 255 63

Partition	Start	End	Size in sectors
1 * FAT32	0 1 1 1010	254 63	16241652 [NO NAME]

TestDisk Step By Step

```
CGSecurity
 2 P Linux          1011  0  1  1023 254 63    208845 [/boot]
 3 E extended LBA  1024  0  1 14592 254 63  217985985
 5 L Linux RAID    1024  1  1  3573 254 63    40965687 [md0]
 6 L Linux RAID    3574  1  1  4210 254 63    10233342 [md1]
 7 L Linux         4211  1  1 14592 254 63  166786767
```

```
[ Quit ] [Search! ] [ Write ]
```

```
Return to main menu
```

Here TestDisk asks you to confirm the Write operation so that you have the last choice over what TestDisk will actually do.

```
TestDisk 6.5-WIP, Data Recovery Utility, October 2006
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
```

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

Advanced FAT Repair

If the FAT boot sector is damaged, data can not be accessed. Windows will prompt The drive is not formatted, do you want to format it now? A Linux mount will display wrong fs type, bad option, bad superblock.

TestDisk let you manipulate the boot sector of FAT partitions. In the Advanced menu, select the partition you want to modify and choose Boot.

Repair a FAT Boot Sector

```
TestDisk 6.2-WIP, Data Recovery Utility, November 2005
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
```

```
Disk /dev/sda - 120 GB / 111 GiB - CHS 14593 255 63
```

	Partition		Start		End		Size in sectors	
1	* FAT32		0	1	1010	254 63	16241652	[NO NAME]
2	P Linux		1011	0	1	1023 254 63	208845	[/boot]
3	E extended LBA		1024	0	1	14592 254 63	217985985	
5	L Linux RAID		1024	1	1	3573 254 63	40965687	[md0]
	X extended		3574	0	1	4210 254 63	10233405	
6	L Linux RAID		3574	1	1	4210 254 63	10233342	[md1]
	X extended		4211	0	1	14592 254 63	166786830	
7	L Linux		4211	1	1	14592 254 63	166786767	

```
[ Type ] [ Boot ] [ Quit ]
```

```
Boot sector recovery
```

Recover a FAT32 Boot Sector

TestDisk can fix corrupted FAT32 boot sectors. The quickest way is to restore the FAT32 boot sector from its backup. TestDisk checks the boot sector and the backup boot sector. If the boot sector and backup boot sector mismatch, you can:

- restore the boot sector from the FAT32 backup boot sector if it's valid (Backup BS);
- update the backup boot sector with the current FAT32 boot sector if it's valid (Org. BS).

TestDisk Step By Step

CGSecurity

Dump can be used to display the sector content in both hexadecimal and ASCII.

If the boot sector has been overwritten, it's often the case for its backup also as they are very close to each other:

- the primary boot sector is sector zero of the filesystem;
- the backup FAT32 boot sector is usually located at sector 6.

Fortunately TestDisk can deal with this problem by creating a new boot sector.

Rebuild a Valid FAT Boot Sector

There is no backup boot sector for FAT12 and FAT16, so if the boot sector is damaged, it has to be recreated. The same thing applies for FAT32 if both the boot sector and its backup are corrupted. TestDisk can rebuild a FAT boot sector. Choose RebuildBS in the menu - it's safe and doesn't modify the disk. Use List to check the result and Write if you have been able to list your files.

```
TestDisk 6.2-WIP, Data Recovery Utility, November 2005
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
```

```
Disk /dev/sda - 120 GB / 111 GiB - CHS 14593 255 63
  Partition      Start      End      Size in sectors
  1 * FAT32      0  1  1  1010 254 63  16241652 [NO NAME]
```

```
Boot sector
```

```
OK
```

```
Backup boot sector
```

```
OK
```

```
Sectors are identical.
```

```
[ Quit ] [Rebuild BS][ Dump ] [Repair FAT]
```

```
Return to Advanced menu
```

Technical Information About FAT Boot Sector Rebuild

To rebuild a FAT boot sector, TestDisk assumes that

- Filesystem size is equal to partition size;
- Fragmentation is low.

The steps are:

- Select which FAT type is compatible with the filesystem size;
- Identify the sectors where the two FAT (number of reserved sectors, FAT length) and the FAT type (FAT12/16/32) begin.

If only one FAT is found:

- If FAT12 or FAT16 is found, it assumes there is only one reserved sector. If it's the second FAT, it deduces the the FAT length.
- If the beginning of FAT32 and the first FAT is found at sector 32 or 33, it deduces the number of reserved sectors.

If two or more FAT sector beginnings have been found:

TestDisk Step By Step

CGSecurity

- It assumes the first two are the two copies of the FAT;
- Deduces the number of reserved sectors and FAT length.

If the number of reserved sectors or FAT length hasn't been found, TestDisk searches for directory structure. The first two entries of a directory are . (current directory) and .. (parent directory). Using the inode number of two or more . directory entries, TestDisk get the cluster size and deduces where the first cluster begins.

- From the number of clusters, it deduces if it's a FAT12, FAT16 or FAT32;
- If FAT12 or FAT16, it assumes there is only one reserved sector;
- Tries to find the number of directories entries (512 by default);
- Deduces the FAT length.

If FAT12 or FAT16:

- It finds the root directory size;
- Finds the cluster size.

If FAT32:

- It finds the root cluster;
- Creates a boot sector with this information;
- Asks the user if he wants to write this new boot sector or not.

The user can also list the files of the FAT partition.

Repair FAT Tables

File Allocation Tables are maps of the data region, indicating which clusters are used by files and directories. To repair the FAT, the menu Repair FAT will have TestDisk compare the two FAT copies. If the FATs mismatch (sector by sector check) or contains errors, TestDisk uses the FAT copy with less errors and removes the obvious errors. This function must only be used on FAT filesystems with correct values in the boot sector. It has been used with success when scandisk, chkdsk or fsck.vfat crashed or refused to repair the filesystem.

Advanced Find ext2 ext3 Backup SuperBlock

If the ext2/ext3 primary superblock is damaged, the filesystem cannot be mounted.

If the normal superblock is corrupted, fsck will search for an alternative superblock but may fail to find any of them. The location of the backup superblocks are dependent on the filesystem's block size. This size is stored in the superblock, so it isn't known while searching for the backup superblock. To search for them, run TestDisk and in the Advanced menu, select the partition and choose Superblock.

The superblock contains all the information about the configuration of the filesystem. The primary copy of the superblock is stored at an offset of 1024 bytes from the start of the partition, and it is essential to mounting the filesystem. Since it is so important, backup copies of the superblock are stored in block groups throughout the filesystem. The first version of ext2 (revision 0) stores a copy at the start of every block group, along with backups of the group descriptor block(s). Because this can consume a considerable amount of space for large filesystems, later revisions can optionally reduce the number of backup copies by only putting backups in specific groups (this is the sparse superblock feature). The groups chosen are 0, 1 and powers of 3, 5 and 7.

TestDisk Step By Step

CGSecurity

Now using the value given by TestDisk, you can use fsck to repair your ext2/ext3 filesystem. I.E. if TestDisk has found a superblock at block number 24577 and a blocksize of 1024 bytes, run

```
/sbin/fsck.ext3 -b 24577 -B 1024 /dev/hda1
```

Menu Geometry

TestDisk 6.2-WIP, Data Recovery Utility, November 2005

Christophe GRENIER <grenier@cgsecurity.org>

<http://www.cgsecurity.org>

```
Disk /dev/sda - 120 GB / 111 GiB - CHS 14593 255 63, sector size=512
```

Because these numbers change the way that TestDisk looks for partitions and calculates their sizes, it's important to have the correct disk geometry. PC partitioning programs often make partitions end on cylinder boundaries.

A partition's CHS values are based on disk translations which make them different than its physical geometry. The most common CHS head values are: 255, 240 and sometimes 16.

```
[ Cylinders ] [ Heads ] [ Sectors ] [ Sector Size ] [ Ok ]
```

Done with changing geometry

Change hard disk geometry parameters (Cylinders, Heads, Sectors).

PC partitioning programs often (always) make partitions end on cylinder boundaries. CHS numbers change the way that TestDisk looks for partitions and calculates their sizes, etc. It does not affect the hard drive itself, unless you actually write data about lost partitions to the drive. Choosing the wrong geometry settings and then saving any lost partitions based on those faulty settings might make it harder or impossible to recover your data.

Some Background Information

To access data, modern operating systems use logical block addressing. HD sectors are numbered 0,1, 2 up to N-1 where N is the total number of sectors.

But before IDE disks larger than 8 GB and SCSI disks existed, another method was used. To access data, the BIOS and the operating system (DOS/Win9x) used CHS addressing. CHS values are limited to 1023 cylinders, 255 heads and 63 sectors (8 GB). A common trick introduced with hard drives bigger than 504 MB (1023 cylinders, 16 heads, 63 sectors) was to use a geometry (Cylinder/Heads/Sector) different from the physical geometry (Extended CHS or large mode addressing).

A method used by BIOS is to read the partition table and to guess the number of heads. When the partition table is cleared or corrupted, the physical disk geometry may be used instead. It becomes harder for partition recovery utilities to find lost partitions on the hard disk.

This problem is not limited to DOS users. Linux users can also be affected. Under Linux, run dmesg and search for Partition check. In the following example, the geometry of hard disk hdc is determined by the partition table (PTBL).

Partition check:

```
hda: hda1 hda2 hda3 hda4 < hda5 hda6 hda7 hda8 hda9 hda10 hda11 hda12 hda13 >
hda3: <bsd: hda14 hda15 hda16 hda17 >
```

TestDisk Step By Step

CGSecurity

```
hdc: [PTBL] [7476/255/63] hdc1 < hdc5 hdc6 hdc7 hdc8 hdc9 hdc10 hdc11 hdc12 hdc13  
>
```

How Does TestDisk get the Disk Geometry?

- Under DOS, TestDisk gets the disk sizes using an extended BIOS function (ah=0x48, int 0x13), and geometry (number of heads and sectors) using a standard BIOS function (ah=0x08, int 0x13). TestDisk uses the default sector size of 512 bytes.
- Under Windows, TestDisk gets the numbers of cylinders, heads and sectors, and the sector size using the DeviceIoControl call, IOCTL_DISK_GET_DRIVE_GEOMETRY.
- Under Linux, TestDisk gets the sector size using BLKSSZGET ioctl, and the geometry using HDIO_GETGEO_BIG or HDIO_GETGEO ioctl; the disk sizes are from BLKGETSIZE64 or BLKGETSIZE.
- Under BSD, TestDisk gets all information using DIOCGDINFO. If that fails, TestDisk assumes the sector size is 512 bytes, and it uses DIOCGFWSECTORS, DIOCGFWHEADS and DIOCGMEDIASIZE to get all the other parameters.
- Under Sun Solaris, TestDisk uses the default sector size of 512 bytes, and gets the numbers of cylinders, heads and sectors using the DKIOCGGEO ioctl.

Some Hints About the Geometry

How to find the correct number of heads?

If the HD geometry mismatches the geometry used when creating the partition table, warning messages such as: Bad sector count, Bad relative sector or Bad ending head are displayed when Analyse is selected from the main menu. If you see such errors, you may need to use the Geometry menu to change the logical number of heads. Try 255, 16, 32, 64, 128 and 240 heads until TestDisk finds all your partitions. 255 and 240 are the most common head values. If you installed Linux as the only OS on your hard drive, it tends to default to only 16 heads.

How to find the correct number of sectors?

Usually the number of sectors per head is 63, but on some USB devices, the value 32 can be found.

Options

Can be changed by first 'highlighting' the Option and then **toggleing** the ENTER key.

Expert mode

If set, adds some functionality. (default: **No**)

Cylinder Boundary

Partitions are aligned on cylinder boundaries (default: **Yes**)

Allows partial last Cylinder

(default: **No**)

Dump

Dumps essential sectors (default: **No**)

Ok

Save Option changes and return to main Menu.

TestDisk Step By Step

CGSecurity

MBR Code

If you use this command, TestDisk will overwrite the code area of your disk necessary for booting the operating system(s). This might be useful if your system doesn't boot at all, and you've tried everything else! See below for details on how this new MBR will function on your system.

IBM PC/Intel Partition

If you use this command, TestDisk will overwrite the present code area of your Master Boot Record (MBR) and write the MBR signature (the Hex Word 0xAA55) to your drive's MBR sector. Beginning with version 5.7 of TestDisk, new MBR code was created specifically for TestDisk by Neil Turton (the author of mbr-install; version mbr-1.1.8 includes the source code for the TestDisk MBR). This change means that TestDisk is now 100% GPL (Open Source) code.

Versions prior to 5.7 overwrite the MBR code with a copy of the Standard Master Boot Record (similar to MS-DOS's fdisk with the 'undocumented' /MBR switch). For a fully-commented copy of this DOS standard (or 'Classic') MBR code, see [An Examination of the Standard MBR](#) (edited copy for CGSecurity.org; France) or [An Examination of the Standard MBR](#) (The Starman's web site).

The TestDisk MBR

If you use TestDisk to write its MBR code to the first sector of your hard disk, it will very briefly identify itself by displaying TestDisk on the screen at boot up. The code is programmed to try booting up from whatever Boot Sector resides in the first partition of the drive. If that's not possible, you will then see a mini-menu displayed on your screen like this:

```
TestDisk
```

```
1234F:
```

Pressing the 1, 2, 3 or 4 keys on your keyboard, will command the MBR to try booting up from any boot sector(s) it finds in the 1st, 2nd, 3rd or 4th partition table entries in the MBR sector. Failing to do so will simply repeat the TestDisk MBR menu on your screen each time it fails to boot. If you press the F/f keys on your keyboard, the MBR will try to boot up the system from a floppy disk in your first (A:\ or /dev/fd0) floppy drive.

In most cases, once you're able to boot up your drive's original OS again, you'll want to change the TestDisk MBR code back to whatever you were using before encountering a boot problem. Note: Be sure you know exactly how to do that before proceeding - you don't want to remove your Partition Table again!

Delete

Deletes all partition data from the Intel partition table only (by filling it with zero bytes). Both the MBR code and the signature bytes (if any) remain the same.

Some BIOS use the partition table content to set the harddisk geometry. Unexpected values can trigger some BIOS bugs. The DOS version of TestDisk is the most affected. If it detects a known bug, it displays Buggy BIOS after the disk geometry. Delete may solve the problem. Reboot your computer and autodetect your hard disk.