

Recovering a Lost Partition With TestDisk

I use GParted LiveCD for just about everything. There is no icon on your rescue disk desktop for TestDisk, you just have to know TestDisk is one of the programs.

The hard disk you want to work on should be unmounted, so unless you have more than one disk in your computer, it is probably easier to run TestDisk from a Live CD.

```
gparted ~ # testdisk
```

To start TestDisk, the testdisk command is entered into a terminal.

If you are using Ubuntu you need to type 'sudo testdisk' instead, and then you will be prompted for your password.

```
TestDisk 6.6, Data Recovery Utility, February 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 errors.

Information gathered during TestDisk use can be recorded for later review. If you choose to create a text file, testdisk.log , it will contain TestDisk options, technical information and various outputs, including any folders/file names TestDisk was used to find and list on screen.

Use Arrow keys to select, then press Enter key:

```
[ Create ] Create a new log file
[ Append ] Append information to the log file
[ No Log ] Don't record anything
```

This is the first TestDisk menu I saw. I chose to let it create a log file. TestDisk will work anyway even if you don't want a log file. I don't think it really matters, but a log file might be nice.

```
TestDisk 6.6, Data Recovery Utility, February 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
```

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

Select a media (use Arrow keys, then press Enter):

```
Disk /dev/hda - 60 GB / 55 GiB
Disk /dev/hdc - 139 MB / 132 MiB (RO)
```

```
[Proceed] [ Quit ]
```

Recovering a Lost Partition With TestDisk

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.

This is the disk selection menu. When you have more than one hard disk you can choose which disk you want to work on. It is a good idea to try TestDisk out on a hard drive with nothing important on it for practice before running TestDisk on a real disk with possibly valuable information.

The disk capacity looks correct to me, that looks like the hard disk I want to work on. I decided to proceed.

```
TestDisk 6.6, Data Recovery Utility, February 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
```

```
Disk /dev/hda - 60 GB / 55 GiB
```

Please select the partition table type, press Enter when done.

```
[ Intel ] Intel/PC partition
[ 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'.

I have an Intel/PC type of Master Boot Record.

Main Menu

```
TestDisk 6.6, Data Recovery Utility, February 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
```

```
Disk /dev/hda - 60 GB / 55 GiB - CHS 7295 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 the 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.

Recovering a Lost Partition With TestDisk

I selected the first option 'Analyse', because I want to analyse my current partition structure and search for lost partitions.

Here is a list of these options and the subsequent options each one offers, we won't be covering all these in this how-to, only the 'Analyse' option.

But here's a quick look all the stuff TestDisk can do if we wanted:

Analyse = Analyse current partition structure and search for lost partitions

--> Proceed

--> Backup = Save current partition list to backup.log file and proceed

--> Proceed --> Quit = Return to Main Menu

--> Search = Search Deeper, try to find more partitions

--> Write = Write partition table to disk

Advanced Filesystem Utils = FAT: Boot and FAT repair

NTFS: Boot and MFT repair

EXT2/EXT3: Find Backup SuperBlock

Geometry = Change disk geometry

--> Cylinders = Change cylinder geometry

--> Heads = Change head geometry

--> Sectors = Change sector geometry

--> Sector Size = Change sector size (WARNING: VERY DANGEROUS!)

--> Ok = Done with changing geometry

Options = Modify options

--> Expert mode: Yes/No -Expert mode adds some functionalities

--> cylinder boundary: Yes/No/Head boundary only Partitions are aligned on cylinder head boundaries

--> Allow partial last cylinder Yes/No

--> Dump = Yes/No Dump essential sectors

--> Ok = Done with changing options

MBR Code = Write TestDisk MBR code to the first sector (similar to fdisk, includes aa55 sig too)

--> Write a new copy of MBR code to first sector? (Y/N)

Delete = Delete all data in the partition table

Quit = Return to disk selection

```
TestDisk 6.6, Data Recovery Utility, February 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
```

```
Disk /dev/hda - 60 GB / 55 GiB - CHS 7295 255 63
```

```
Current partition structure:
```

Partition	Start	End	Size in sectors
-----------	-------	-----	-----------------

```
check_FAT: Unusual number or reserved sectors 9 (FAT), should be 1.
```

1 P FAT16	0 1 1 22 254 63	369432 [NO NAME]
-----------	-----------------	------------------

2 * Linux	23 0 1 1552 254 63	24579450 [ACER]
-----------	--------------------	-----------------

Recovering a Lost Partition With TestDisk

```
*=Primary bootable P=Primary L=Logical E=Extended D=Deleted  
[Proceed ] [ Save ]  
          Try to locate partition
```

This panel is showing me my current partition information.

My first partition begins in cylinder 0, head 1, sector 1 and ends at cylinder 22, head 254, sector 63

My second partition begins in cylinder 23, head 0, sector 1 and ends at cylinder 1552, head 254, sector 63

...and now we are going to have TestDisk examine my hard disk for lost partitions. With 'Proceed' selected by default, I press 'Enter'.

```
TestDisk 6.6, Data Recovery Utility, February 2007  
Christophe GRENIER <grenier@cgsecurity.org>  
http://www.cgsecurity.org  
  
Disk /dev/hda - 60 GB / 55 GiB - CHS 7295 255 63  
Current partition structure:  
  Partition      Start      End      Size in sectors  
* FAT16          0 1 1     22 254 63    369432 [PQSERVICE]  
P FAT32 LBA      23 0 1    1552 254 63   24579450 [ACER]  
L Linux Swap     1561 1 1    1691 254 63   2104452  
P Linux          1692 0 1    7294 254 63   90012195  
  
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  
FAT16, 189 MB /180 MiB
```

There are two possibly lost partitions here TestDisk has found already, just from a very quick scan. These two can be easily restored. Are any of these the ones I am looking for?

When I use my up or down arrow keys I can highlight a different line. That makes the output line at the very bottom show more information about whichever partition is selected.

If these partitions look like the ones I want to recover, I can skip to the last image in this how-to.....GO

But NOOO, ...in this example I have decided that neither of these partitions that TestDisk has automatically found for me that are easy to restore are the one I'm looking for.

I want to search deeper, for even less distinct lost partitions that may have been deleted ages ago, so I press 'Enter'.

Recovering a Lost Partition With TestDisk

```
TestDisk 6.6, Data Recovery Utility, February 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
```

```
Disk /dev/hda - 60 GB / 55 GiB - CHS 7295 255 63
```

```
Current partition structure:
```

Partition	Start	End	Size in sectors
1 * FAT16	0 1 1 22 254 63		369432 [NO NAME]
2 P FAT32 LBA	23 0 1 1552 254 63		24579450 [ACER]
3 E extended LBA	1553 0 1 1691 254 63		2233035
4 P Linux	1692 0 1 7294 254 63		90012195
5 L Linux Swap	1561 1 1 1691 254 63		2104452

```
[Quit ] [ Search! ] [ Write ]
        Search deeper, try to find more partitions
```

Quit = Return to main menu

Search = Search deeper, try to find more partitions

Write = Write partition table to disk

```
TestDisk 6.6, Data Recovery Utility, February 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
```

```
Disk /dev/hda - 60 GB / 55 GiB - CHS 7295 255 63
```

```
Analyse cylinder 852/7295: 12%
```

```
check_FAT: Unusual number or reserved sectors 9 (FAT), should be 1.
FAT16 >32M      0 1 1 22 254 63      369432 [NO NAME]
FAT32 LBA      23 0 1 1552 254 63      24579450 [ACER]
FAT32 LBA      23 0 1 1552 254 63      24579450 [ACER]
Linux Swap     1561 1 1 1691 254 63      2104452
Linux          1692 0 1 7294 254 63      90012195
FAT32 LBA      2279 0 1 3808 254 63      24579450 [ACER]
FAT32 LBA      2279 0 1 3808 254 63      24579450 [ACER]
FAT32 LBA      3809 0 1 5338 254 63      24579450 [ACER]
FAT32 LBA      3809 0 1 5338 254 63      24579450 [ACER]
```

```
[ Stop ]
```

This is what it looks like during the search, be patient and wait while it searches.....

The numbers on the line titled 'Analyse Cylinder' are changing to show the progress and the number of % increases as well in this display.

Recovering a Lost Partition With TestDisk

More lines are added to the list of partitions found, but when it's finished it doesn't stay on this display, it automatically changes to the completed list shown in the next window below.

```
TestDisk 6.6, Data Recovery Utility, February 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/hda - 60 GB / 55 GiB - CHS 7295 255 63
  Partition      Start      End      Size in sectors
* FAT16 >32M    0 1 1  22 254 63    369432 [NO NAME]
P FAT32 LBA     23 0 1 1552 254 63 24579450 [ACER]
L Linux Swap   1561 1 1 1691 254 63  2104452
P Linux        1692 0 1 7294 254 63 90012195
D Linux        1692 0 1 7294 254 63 90012195
D FAT32 LBA    2279 0 1 3808 254 63  24579450 [ACER]
D FAT32 LBA    3809 0 1 5338 254 63  24579450 [ACER]
D FAT16 LBA    7273 0 1 7294 254 63   369596 [ACER_SERVIC]
```

```
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
FAT16, 189 MB /180 MiB
```

The present healthy, easily restorable partitions are shown in green.

The ones shown in white are the ones I might look at for possible restoring. Now if I want to rescue one of these partitions I can have TestDisk write one or two of them to the partition table for me BUT first I must make sure I read the cylinder, heads and sector information. If I make a mistake and try to select a partition that is in an area of the hard disk that's now occupied, TestDisk will let me know about it with some comments in bright red print.

If you look at the number of cylinders for the whole disk, it is 7295, and that third green partition begins at 1692 and covers the whole remainder of the disk right up to cylinder 7294. Those white partitions are covered up by the fourth green partition. It will be only possible to recover any of the white partitions if I delete that green one first.

In some situations we also might need to remember the partitioning rules for Intel/PC hard disks. We can have up to four primary partitions or up to three primary partitions with one designated as 'extended'. The extended partition can contain many logical partitions, but they must be 'contiguous'. (no primary partition can be placed between two logical partitions).

Use your up and down arrow keys to scroll down the list.

Use the left and right arrow keys to change the 'D' to either an '*' or a 'P' or an 'E' or 'L' (for logical).

Use the letter keys A, L, T and P as the sign says.

Recovering a Lost Partition With TestDisk

P is a good idea, that gives you a new Window that shows you what files are in a partition. You can tell if it's an operating system if you're used to looking at operating systems that way. You can tell if it's your data partition too, because you'd recognize the names of your old directories. Type q to quit and return to this menu.

Back in this menu again, if this is a partition I want TestDisk to restore, I use my left-arrow or right-arrow key to change the first letter of the line from 'D' to either a * if I want it to be a primary partition with a boot flag or a P for an ordinary Primary, E for extended, and L for a logical partition.

You need to select all the partitions you'd like to have included in your new partition table if you are going to choose [write] in the next screen.

If you only pick out the lost one you will rescue that one okay, but you'll lose the other partitions. Don't worry, you can repeat this process and recover them again. But it's better to save time and get it right the first time.

When the partitions you want to keep as well as the ones to restore all have a *, P or an L in the beginning of their lines, you can press 'Enter' to continue. There will be a confirmation screen, just type Y, and your partition table will be re-written with the partitions you selected here.