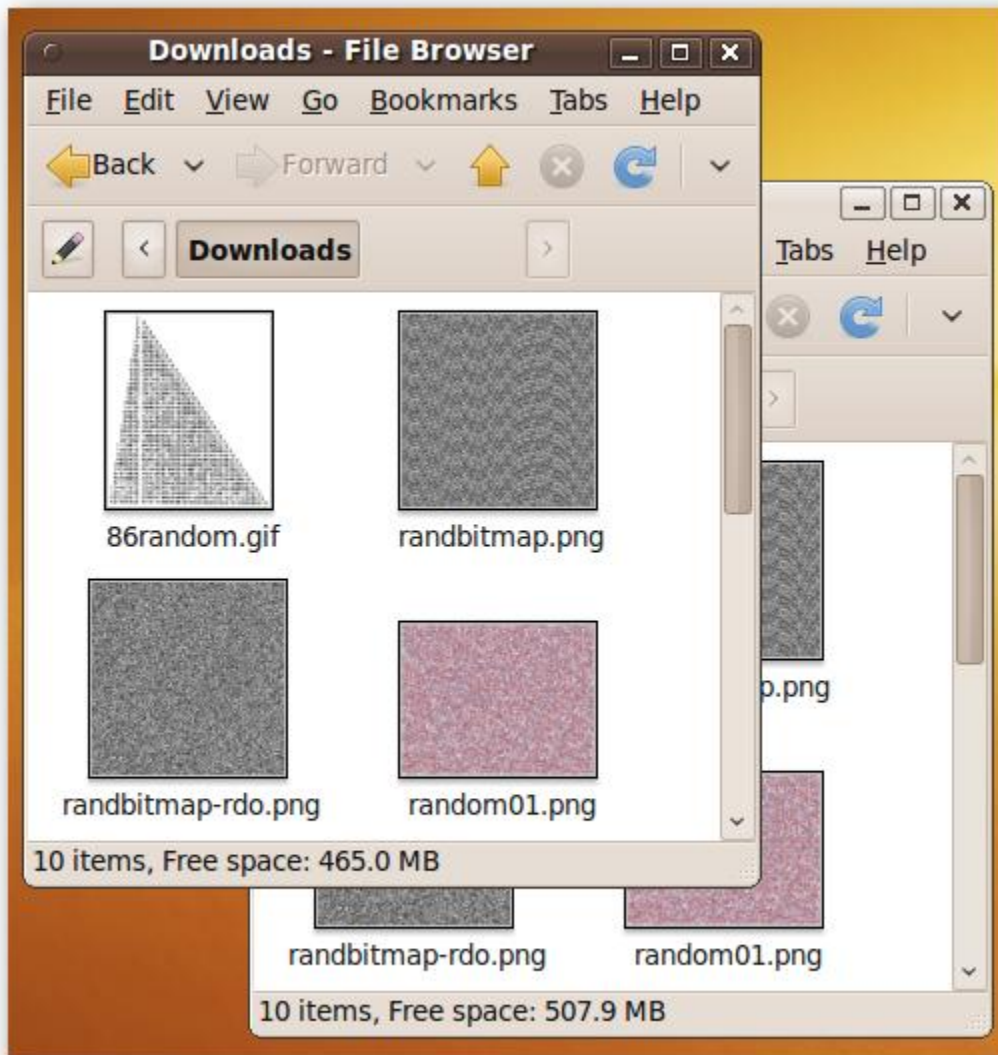


Recover Data Like a Forensics Expert Using an Ubuntu Live CD

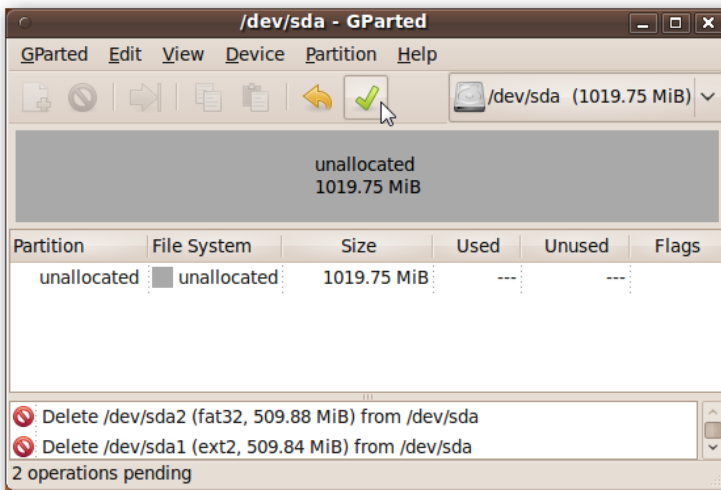
There are lots of utilities to recover deleted files, but what if you can't boot up your computer, or the whole drive has been formatted? We'll show you some tools that will dig deep and recover the most elusive deleted files, or even whole hard drive partitions.

Our setup

To show these tools, we've set up a small 1 GB hard drive, with half of the space partitioned as ext2, a file system used in Linux, and half the space partitioned as FAT32, a file system used in older Windows systems. We stored ten random pictures on each hard drive.



We then wiped the partition table from the hard drive by deleting the partitions in GParted.



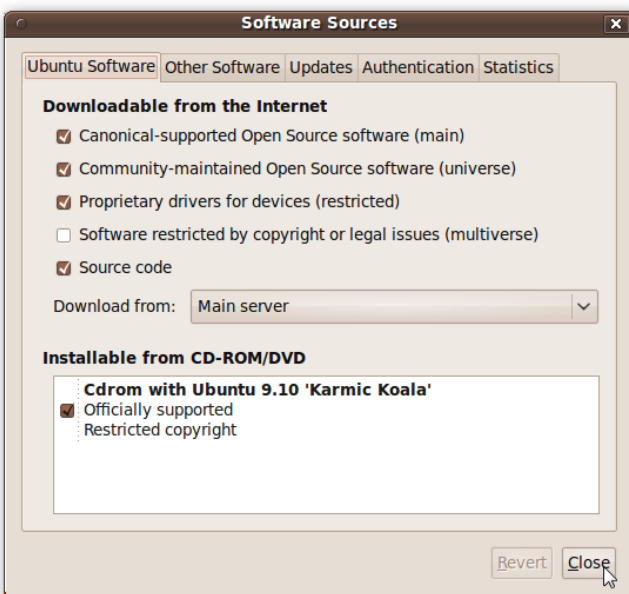
Is our data lost forever?

Installing the tools

All of the tools we're going to use are in Ubuntu's *universe* repository.

To enable the repository, open Synaptic Package Manager by clicking on System in the top-left, then Administration > Synaptic Package Manager.

Click on Settings > Repositories and add a check in the box labelled "Community-maintained Open Source software (universe)".



Click Close, and then in the main Synaptic Package Manager window, click the Reload button. Once the package list has reloaded, and the search index rebuilt, search for and mark for installation one or all of the following packages: **testdisk**, **foremost**, and **scalpel**.

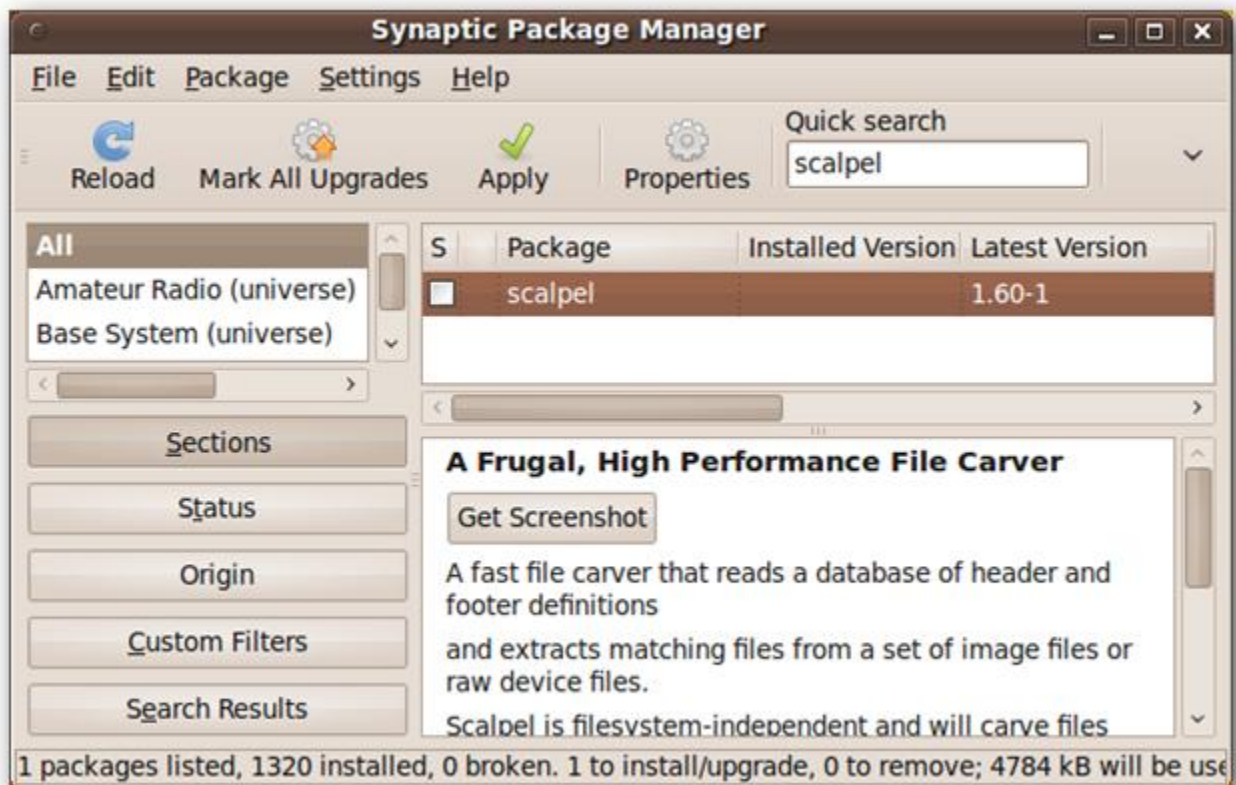
Testdisk includes TestDisk, which can recover lost partitions and repair boot sectors, and PhotoRec, which can recover many different types of files from tons of different file systems.



Foremost, originally developed by the US Air Force Office of Special Investigations, recovers files based on their headers and other internal structures. Foremost operates on hard drives or drive image files generated by various tools.



Finally, **scalpel** performs the same functions as foremost, but is focused on enhanced performance and lower memory usage. Scalpel may run better if you have an older machine with less RAM.



Recover hard drive partitions

If you can't mount your hard drive, then its partition table might be corrupted. Before you start trying to recover your important files, it may be possible to recover one or more partitions on your drive, recovering all of your files with one step.

Testdisk is the tool for the job. Start it by opening a terminal (Applications > Accessories > Terminal) and typing in:

```
sudo testdisk
```

```
ubuntu@ubuntu: ~
File Edit View Terminal Help
TestDisk 6.11, Data Recovery Utility, April 2009
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 sym
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
```

If you'd like, you can create a log file, though it won't affect how much data you recover. Once you make your choice, you're greeted with a list of the storage media on your machine. You should be able to identify the hard drive you want to recover partitions from by its size and label.

```
ubuntu@ubuntu: ~
File Edit View Terminal Help
TestDisk 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

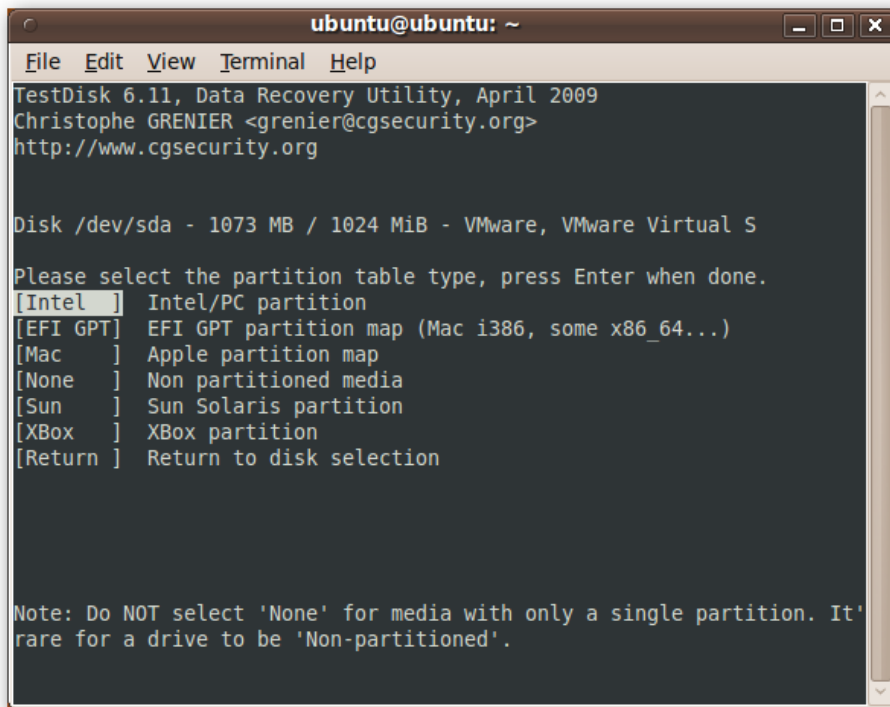
TestDisk is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
Disk /dev/sda - 1073 MB / 1024 MiB - VMware, VMware Virtual S
Disk /dev/sdb - 136 GB / 127 GiB - VMware, VMware Virtual S
Disk /dev/sdc - 4025 MB / 3839 MiB - SanDisk Cruzer Micro
Disk /dev/sr0 - 1703 KB / 1664 KiB (R0) - NECVMwar VMware IDE CDR10

[ Proceed ] [ Quit ]

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

TestDisk asks you select the type of partition table to search for. In most cases (ext2/3, NTFS, FAT32, etc.) you should select Intel and press Enter.



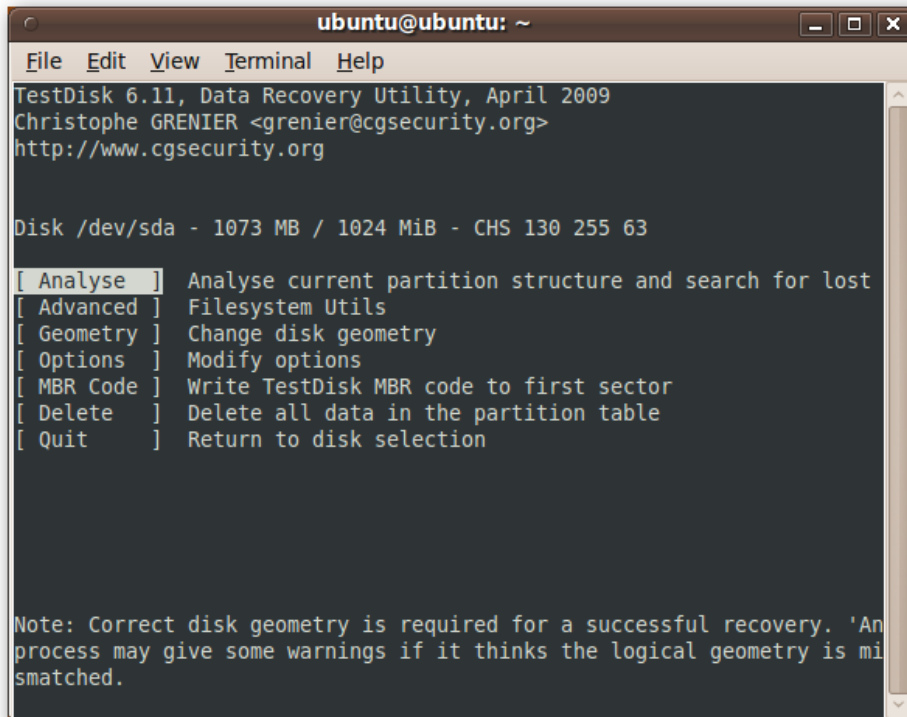
```
ubuntu@ubuntu: ~
File Edit View Terminal Help
TestDisk 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 1073 MB / 1024 MiB - VMware, VMware Virtual S

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

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

Highlight Analyse and press enter.



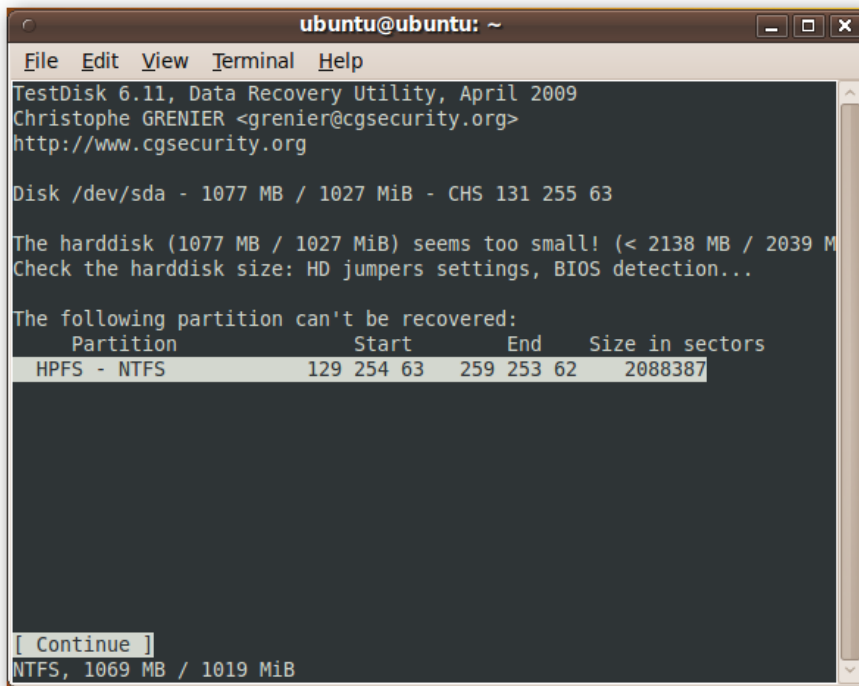
```
ubuntu@ubuntu: ~
File Edit View Terminal Help
TestDisk 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 1073 MB / 1024 MiB - CHS 130 255 63

[Analyse ] Analyse current partition structure and search for lost
[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. 'An
process may give some warnings if it thinks the logical geometry is mi
smatched.
```

In our case, our small hard drive has previously been formatted as NTFS. Amazingly, TestDisk finds this partition, though it is unable to recover it.



```
ubuntu@ubuntu: ~
File Edit View Terminal Help
TestDisk 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

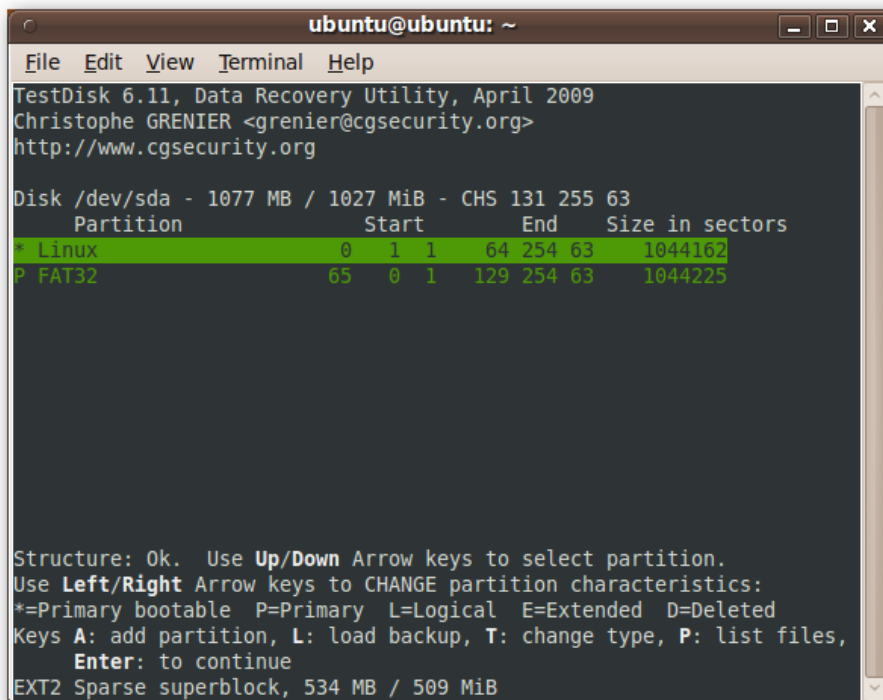
Disk /dev/sda - 1077 MB / 1027 MiB - CHS 131 255 63

The harddisk (1077 MB / 1027 MiB) seems too small! (< 2138 MB / 2039 M
Check the harddisk size: HD jumpers settings, BIOS detection...

The following partition can't be recovered:
Partition          Start      End      Size in sectors
-----
HPFS - NTFS        129 254 63 259 253 62 2088387

[ Continue ]
NTFS, 1069 MB / 1019 MiB
```

It also finds the two partitions we just deleted. We are able to change their attributes, or add more partitions, but we'll just recover them by pressing Enter.

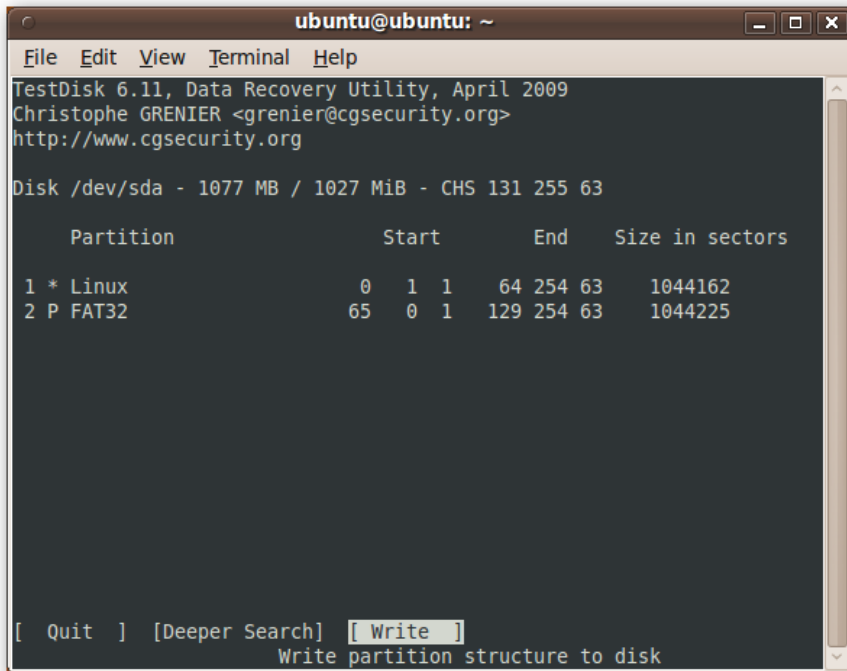


```
ubuntu@ubuntu: ~
File Edit View Terminal Help
TestDisk 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 1077 MB / 1027 MiB - CHS 131 255 63
Partition          Start      End      Size in sectors
-----
* Linux             0  1  1  64 254 63 1044162
P FAT32             65  0  1 129 254 63 1044225

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
EXT2 Sparse superblock, 534 MB / 509 MiB
```

If TestDisk hasn't found all of your partitions, you can try doing a deeper search by selecting that option with the left and right arrow keys. We only had these two partitions, so we'll recover them by selecting Write and pressing Enter.



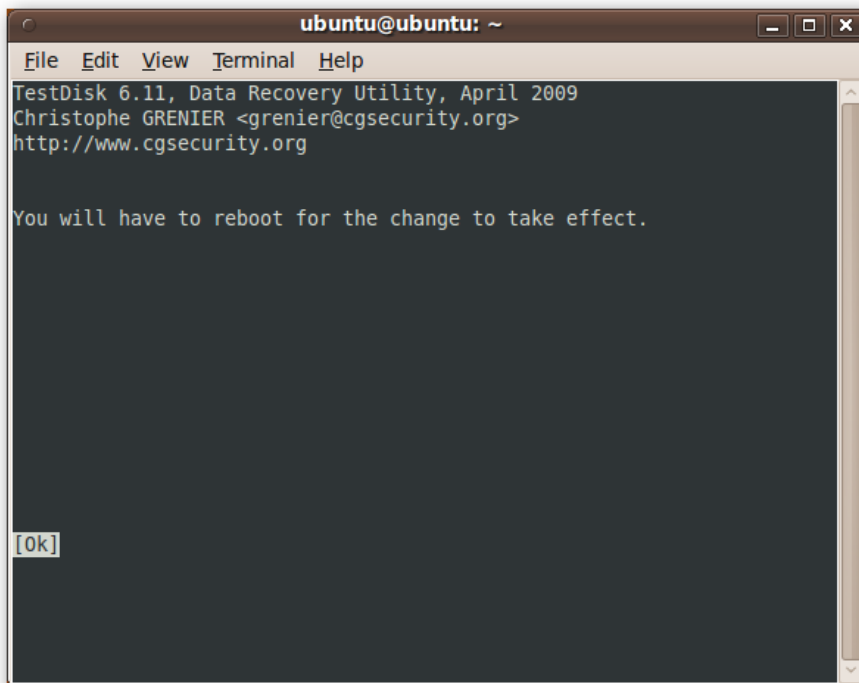
```
ubuntu@ubuntu: ~
File Edit View Terminal Help
TestDisk 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 1077 MB / 1027 MiB - CHS 131 255 63

Partition          Start          End      Size in sectors
1 * Linux           0  1  1      64 254 63    1044162
2 P FAT32           65  0  1     129 254 63    1044225

[ Quit ] [Deeper Search] [ Write ]
                        Write partition structure to disk
```

Testdisk informs us that we will have to reboot.



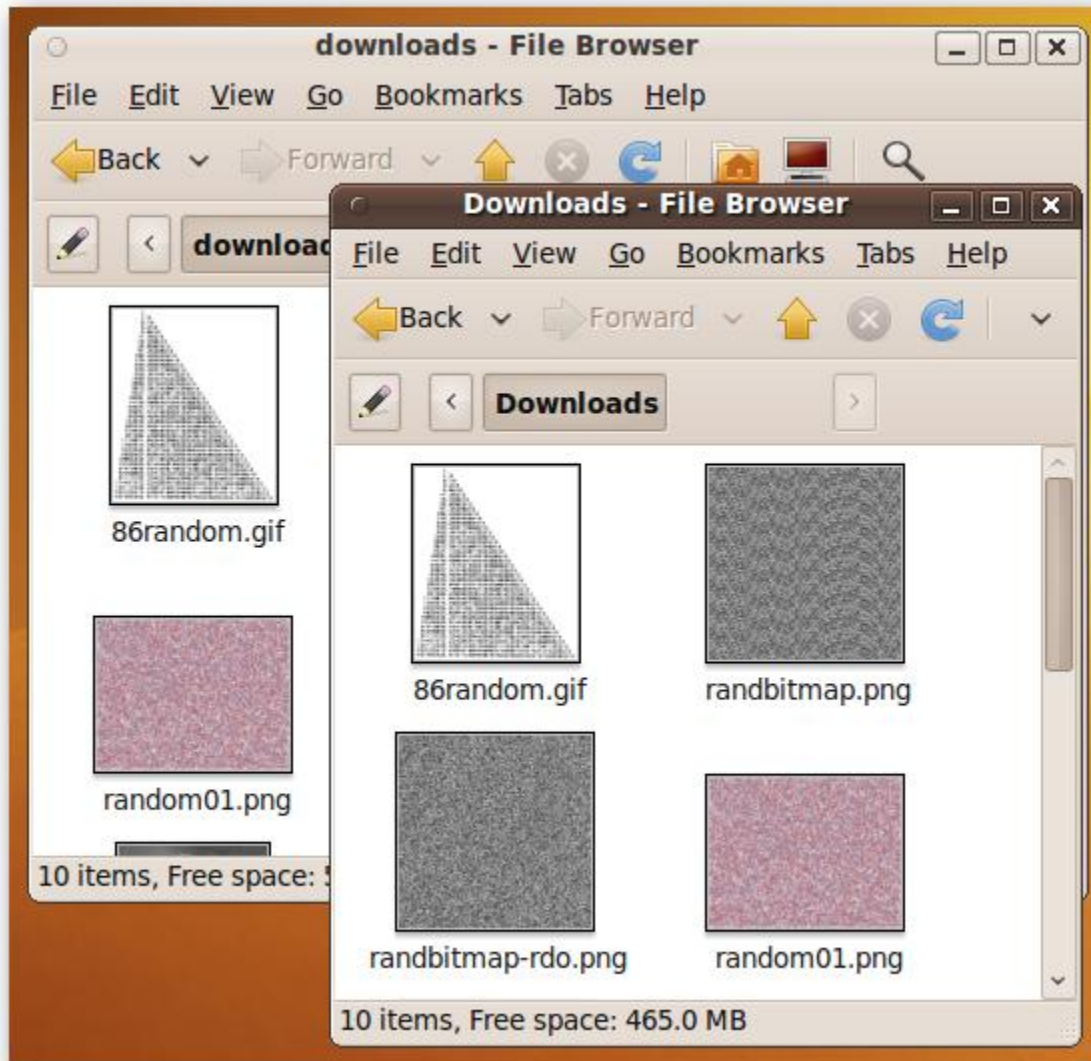
```
ubuntu@ubuntu: ~
File Edit View Terminal Help
TestDisk 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

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

[Ok]
```

Note: If your Ubuntu Live CD is not [persistent](#), then when you reboot you will have to reinstall any tools that you installed earlier.

After restarting, both of our partitions are back to their original states, pictures and all.



Recover files of certain types

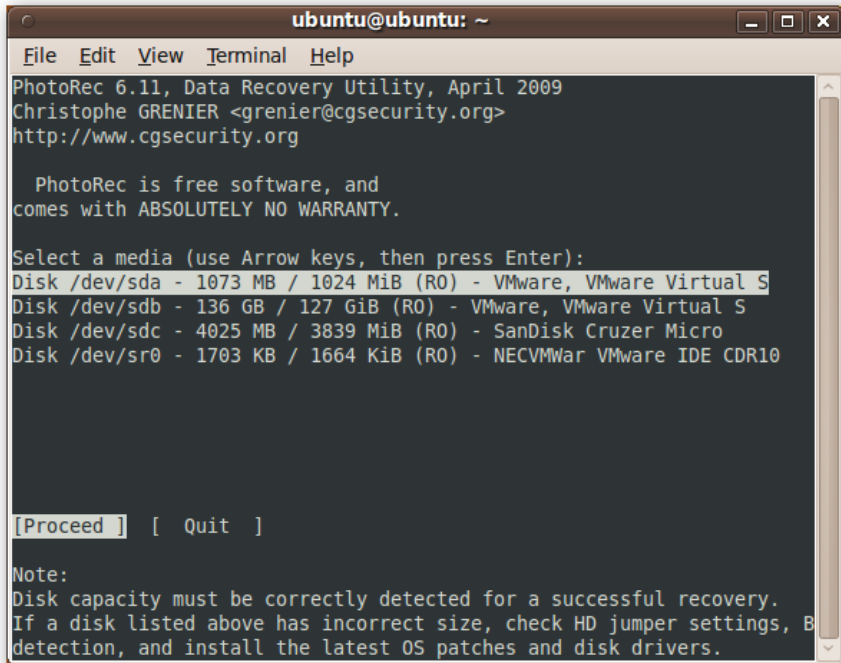
For the following examples, we deleted the 10 pictures from both partitions and then reformatted them.

PhotoRec

Of the three tools we'll show, **PhotoRec** is the most user-friendly, despite being a console-based utility. To start recovering files, open a terminal (Applications > Accessories > Terminal) and type in:

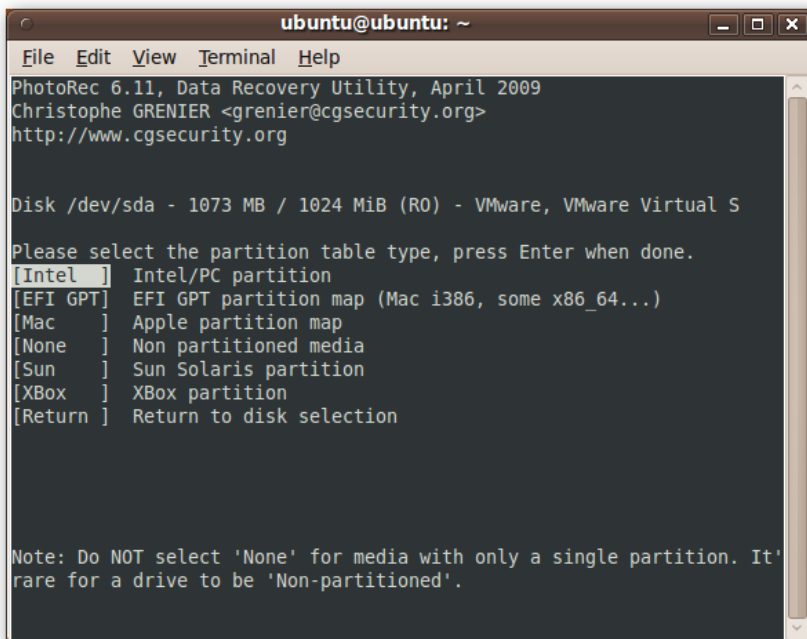
sudo photorec

To begin, you are asked to select a storage device to search. You should be able to identify the right device by its size and label. Select the right device, and then hit Enter.



```
ubuntu@ubuntu: ~  
File Edit View Terminal Help  
PhotoRec 6.11, Data Recovery Utility, April 2009  
Christophe GRENIER <grenier@cgsecurity.org>  
http://www.cgsecurity.org  
  
PhotoRec is free software, and  
comes with ABSOLUTELY NO WARRANTY.  
  
Select a media (use Arrow keys, then press Enter):  
Disk /dev/sda - 1073 MB / 1024 MiB (R0) - VMware, VMware Virtual S  
Disk /dev/sdb - 136 GB / 127 GiB (R0) - VMware, VMware Virtual S  
Disk /dev/sdc - 4025 MB / 3839 MiB (R0) - SanDisk Cruzer Micro  
Disk /dev/sr0 - 1703 KB / 1664 KiB (R0) - NECVMWar VMware IDE CDR10  
  
[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.
```

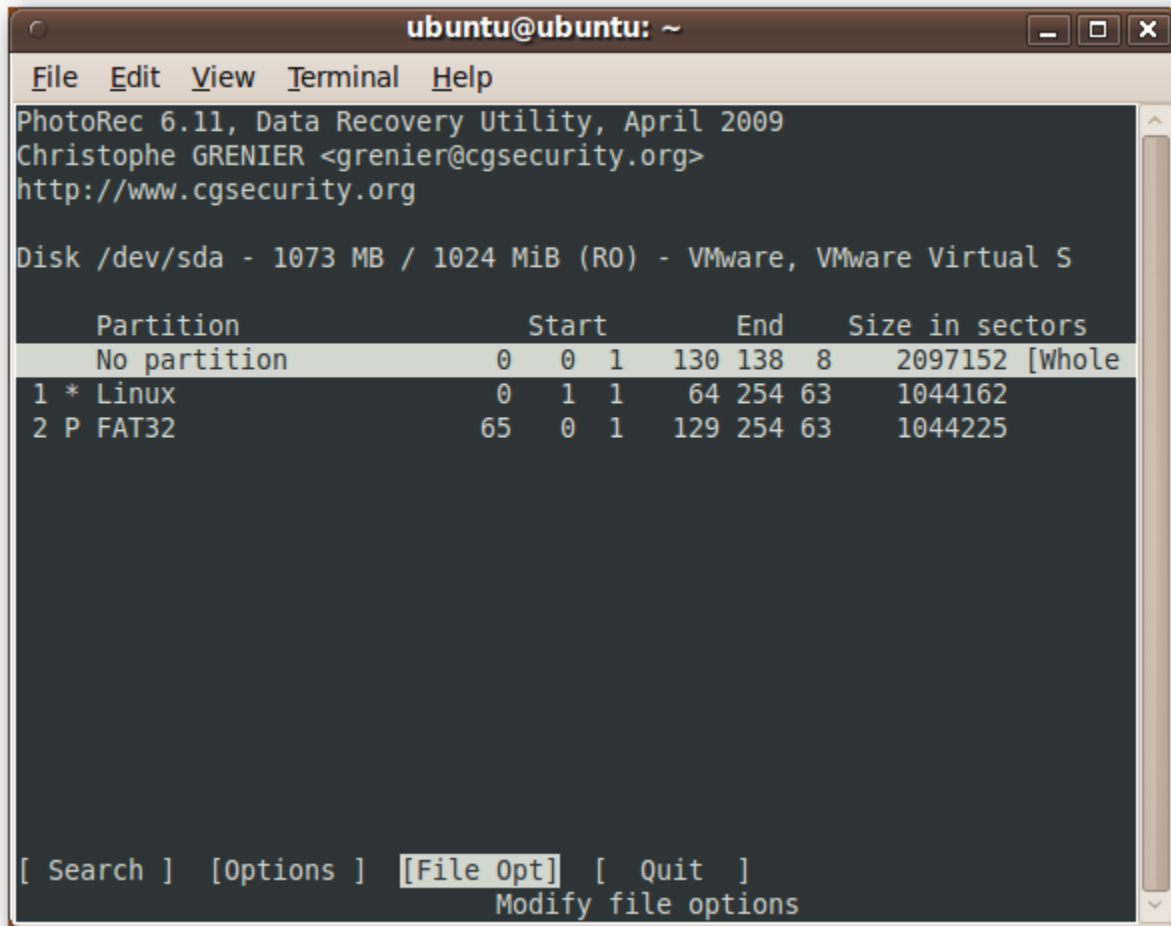
PhotoRec asks you select the type of partition to search. In most cases (ext2/3, NTFS, FAT, etc.) you should select Intel and press Enter.



```
ubuntu@ubuntu: ~  
File Edit View Terminal Help  
PhotoRec 6.11, Data Recovery Utility, April 2009  
Christophe GRENIER <grenier@cgsecurity.org>  
http://www.cgsecurity.org  
  
Disk /dev/sda - 1073 MB / 1024 MiB (R0) - VMware, VMware Virtual S  
  
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  
  
Note: Do NOT select 'None' for media with only a single partition. It'  
rare for a drive to be 'Non-partitioned'.
```

You are given a list of the partitions on your selected hard drive. If you want to recover all of the files on a partition, then select Search and hit enter.

However, this process can be very slow, and in our case we only want to search for pictures files, so instead we use the right arrow key to select File Opt and press Enter.



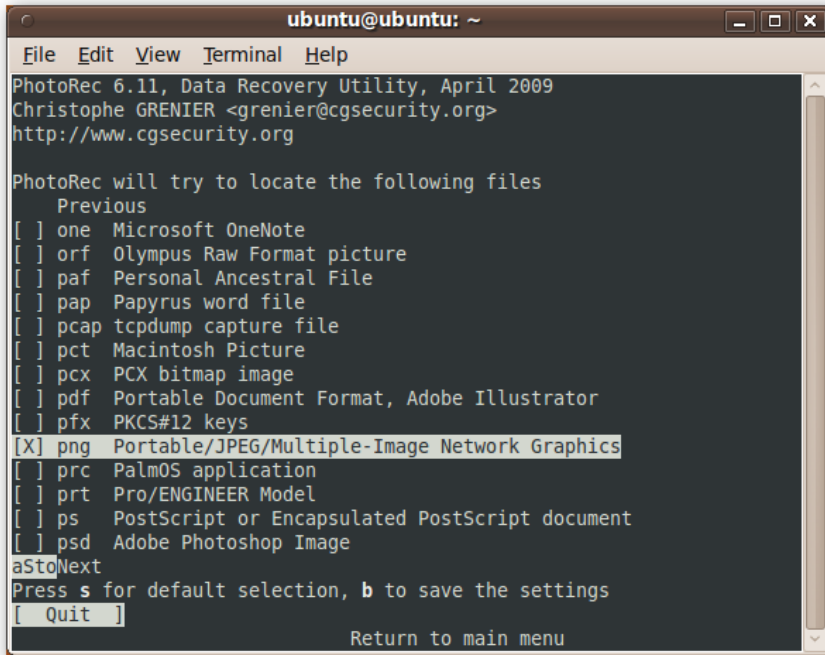
```
ubuntu@ubuntu: ~
File Edit View Terminal Help
PhotoRec 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 1073 MB / 1024 MiB (R0) - VMware, VMware Virtual S

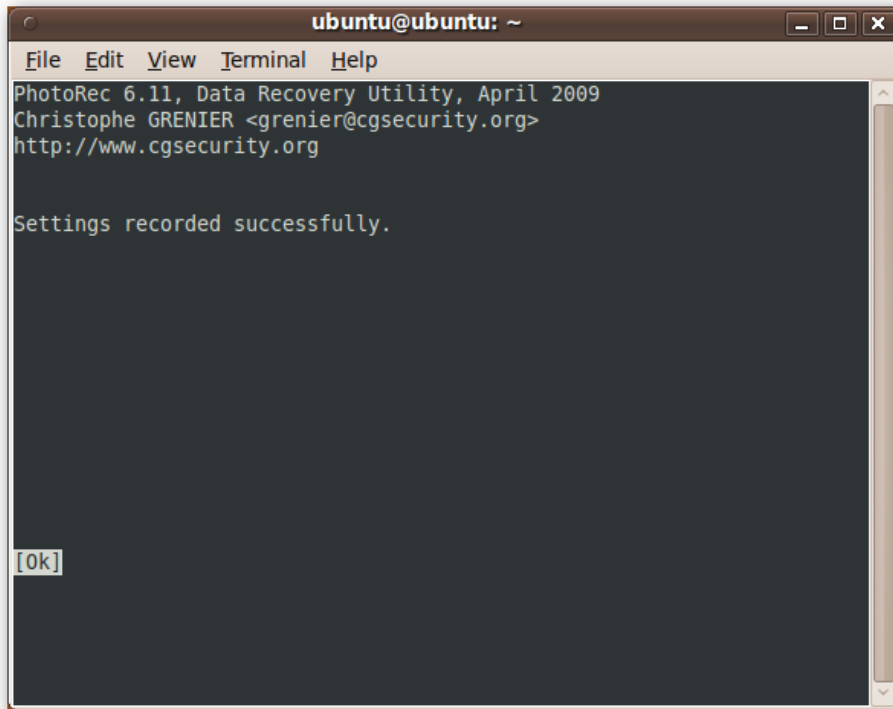
Partition          Start      End      Size in sectors
No partition       0 0 1 130 138 8 2097152 [Whole
1 * Linux          0 1 1 64 254 63 1044162
2 P FAT32          65 0 1 129 254 63 1044225

[ Search ] [Options ] [File Opt] [ Quit ]
                        Modify file options
```

PhotoRec can recover many different types of files, and deselecting each one would take a long time. Instead, we press “s” to clear all of the selections, and then find the appropriate file types – jpg, gif, and png – and select them by pressing the right arrow key.



Once we've selected these three, we press "b" to save these selections.



Press enter to return to the list of hard drive partitions. We want to search both of our partitions, so we highlight "No partition" and "Search" and then press Enter.

```
ubuntu@ubuntu: ~
File Edit View Terminal Help
PhotoRec 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 1073 MB / 1024 MiB (R0) - VMware, VMware Virtual S

Partition      Start      End      Size in sectors
No partition    0  0  1  130 138  8  2097152 [Whole]
1 * Linux      0  1  1  64 254 63 1044162
2 P FAT32      65 0  1  129 254 63 1044225

[ Search ] [Options] [File Opt] [ Quit ]
Start file recovery
```

PhotoRec prompts for a location to store the recovered files. If you have a different healthy hard drive, then we recommend storing the recovered files there. Since we're not recovering very much, we'll store it on the Ubuntu Live CD's desktop.

Note: Do not recover files to the hard drive you're recovering from.

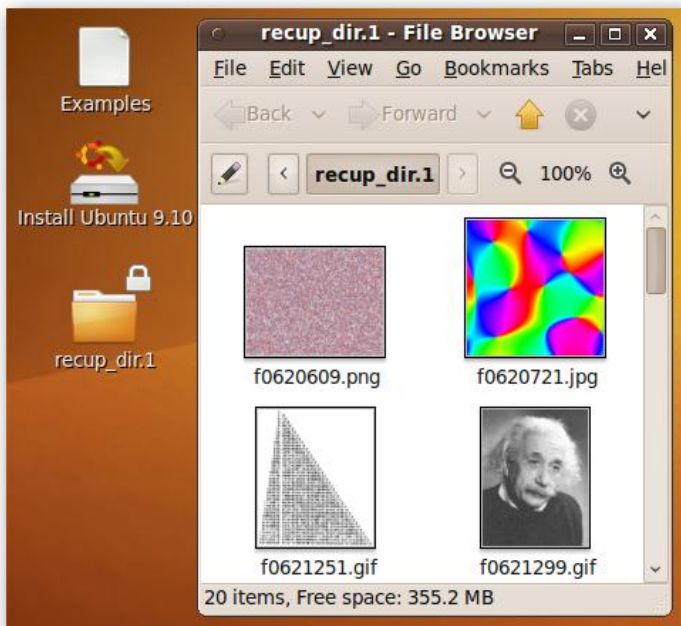
```
ubuntu@ubuntu: ~
File Edit View Terminal Help
PhotoRec 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Do you want to save recovered files in /home/ubuntu ? [Y/N]
Do not choose to write the files to the same partition they were stored on.
To select another directory, use the arrow keys.
drwxr-xr-x  999  999    740 26-Apr-2010 02:36 .
drwxr-xr-x   0   0     60 26-Apr-2010 02:24 ..
drwxr-xr-x  999  999    80 26-Apr-2010 02:24 Desktop
drwxr-xr-x  999  999    40 26-Apr-2010 02:24 Documents
drwxr-xr-x  999  999    40 26-Apr-2010 02:24 Downloads
drwxr-xr-x  999  999    40 26-Apr-2010 02:24 Music
drwxr-xr-x  999  999    40 26-Apr-2010 02:24 Pictures
drwxr-xr-x  999  999    40 26-Apr-2010 02:24 Public
drwxr-xr-x  999  999    40 26-Apr-2010 02:24 Templates
drwxr-xr-x  999  999    40 26-Apr-2010 02:24 Videos
-rw-r--r--   0   0   40960 26-Apr-2010 02:34 photorec.ses
```

PhotoRec is able to recover the 20 pictures from the partitions on our hard drive!

```
ubuntu@ubuntu: ~  
File Edit View Terminal Help  
PhotoRec 6.11, Data Recovery Utility, April 2009  
Christophe GRENIER <grenier@cgsecurity.org>  
http://www.cgsecurity.org  
  
Disk /dev/sda - 1073 MB / 1024 MiB (R0) - VMware, VMware Virtual S  
Partition      Start      End      Size in sectors  
No partition   0 0 1 130 138 8 2097152 [Whole  
disk]  
  
20 files saved in /home/ubuntu/Desktop/recup_dir directory.  
Recovery completed.  
jpg: 8 recovered  
png: 8 recovered  
gif: 4 recovered  
  
[ Quit ]
```

A quick look in the recup_dir.1 directory that it creates confirms that PhotoRec has recovered all of our pictures, save for the file names.



Foremost

Foremost is a command-line program with no interactive interface like PhotoRec, but offers a number of command-line options to get as much data out of your hard drive as possible.

For a full list of options that can be tweaked via the command line, open up a terminal (Applications > Accessories > Terminal) and type in:

```
foremost -h
```

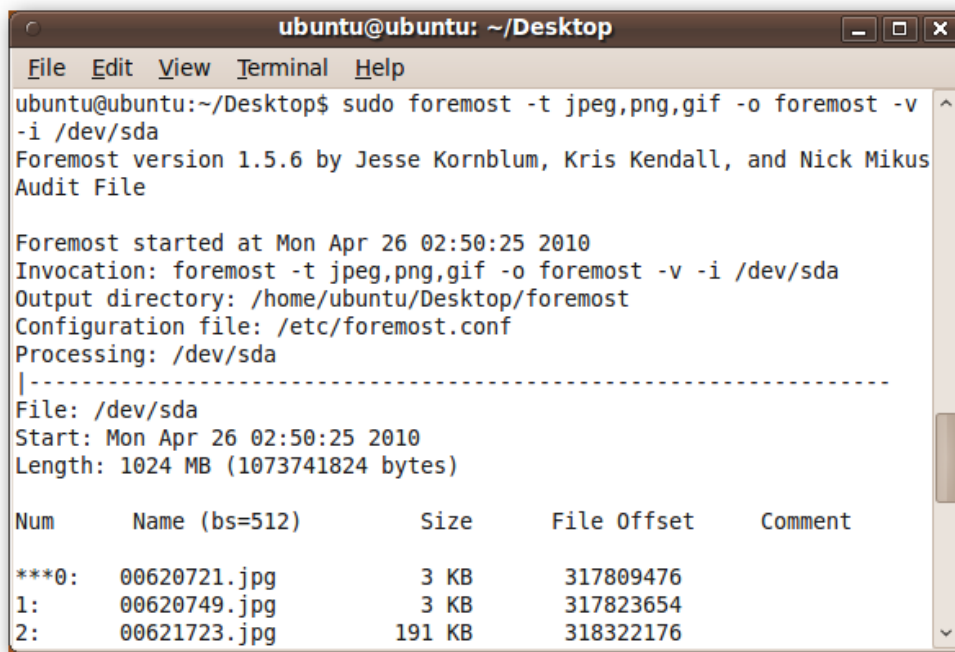
In our case, the command line options that we are going to use are:

- `-t`, a comma-separated list of types of files to search for. In our case, this is "jpeg,png,gif".
- `-v`, enabling verbose-mode, giving us more information about what foremost is doing.
- `-o`, the output folder to store recovered files in. In our case, we created a directory called "foremost" on the desktop.
- `-i`, the input that will be searched for files. This can be a disk image in several different formats; however, we will use a hard disk, `/dev/sda`.

Our foremost invocation is:

```
sudo foremost -t jpeg,png,gif -o foremost -v -i /dev/sda
```

Your invocation will differ depending on what you're searching for and where you're searching for it.



```
ubuntu@ubuntu: ~/Desktop
File Edit View Terminal Help
ubuntu@ubuntu:~/Desktop$ sudo foremost -t jpeg,png,gif -o foremost -v
-i /dev/sda
Foremost version 1.5.6 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Mon Apr 26 02:50:25 2010
Invocation: foremost -t jpeg,png,gif -o foremost -v -i /dev/sda
Output directory: /home/ubuntu/Desktop/foremost
Configuration file: /etc/foremost.conf
Processing: /dev/sda
|-----
File: /dev/sda
Start: Mon Apr 26 02:50:25 2010
Length: 1024 MB (1073741824 bytes)

Num      Name (bs=512)      Size      File Offset      Comment
***0:    00620721.jpg       3 KB      317809476
1:       00620749.jpg       3 KB      317823654
2:       00621723.jpg      191 KB    318322176
```

Foremost is able to recover 17 of the 20 files stored on the hard drive.

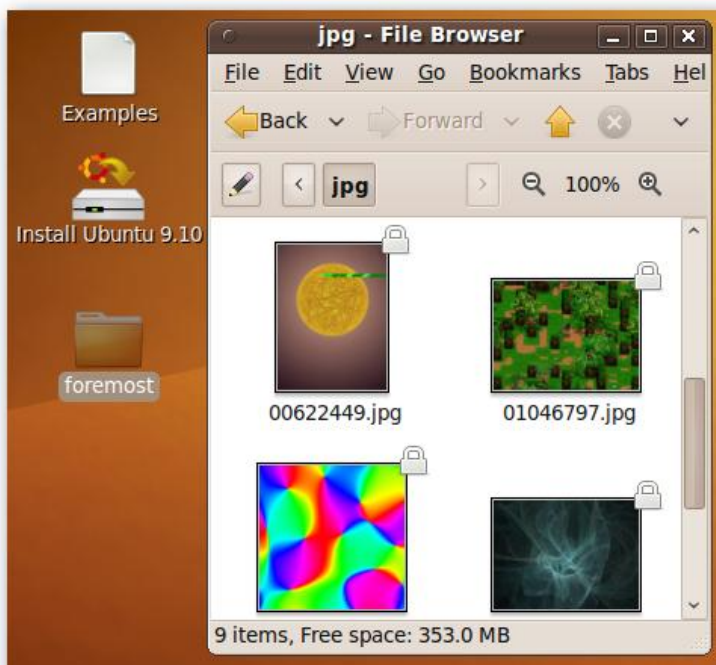
```
ubuntu@ubuntu: ~/Desktop
File Edit View Terminal Help
9: 01047765.jpg 190 KB 536455680
10: 01048149.jpg 76 KB 536652288
11: 01046357.png 67 KB 535734784 (512 x 512)
12: 01046493.png 67 KB 535804416 (512 x 512)
13: 01046629.png 54 KB 535874048 (381 x 298)
14: 01046741.png 26 KB 535931392 (400 x 400)
15: 01046309.gif 22 KB 535710208 (472 x 562)
16: 01047085.gif 25 KB 536107520 (896 x 1160)
*****|
Finish: Mon Apr 26 02:50:40 2010

17 FILES EXTRACTED

jpg:= 9
png:= 4
gif:= 4

-----
Foremost finished at Mon Apr 26 02:50:40 2010
ubuntu@ubuntu:~/Desktop$
```

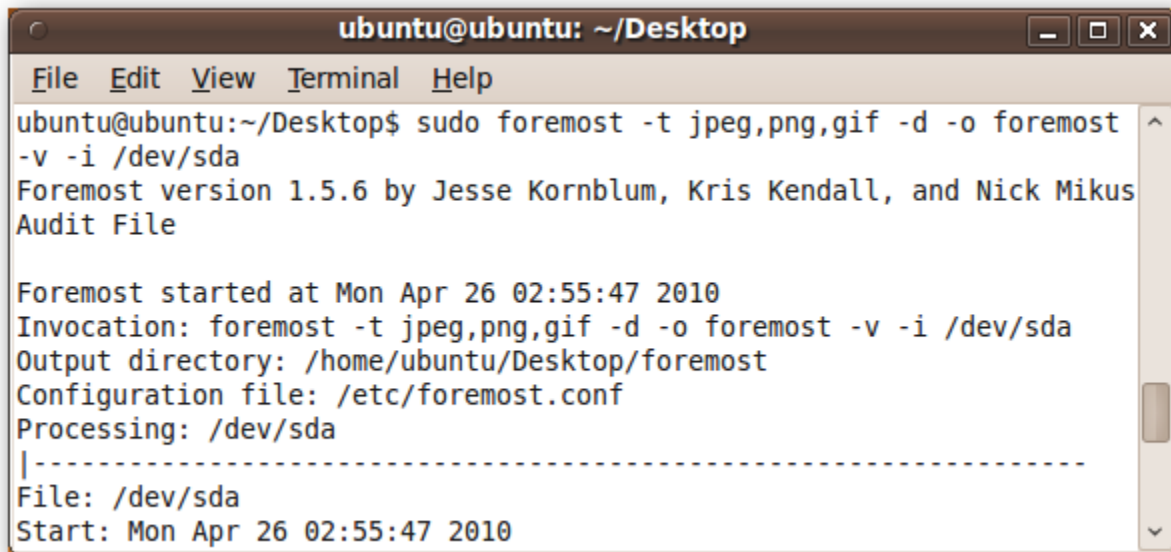
Looking at the files, we can confirm that these files were recovered relatively well, though we can see some errors in the thumbnail for 00622449.jpg.



Part of this may be due to the ext2 filesystem. Foremost recommends using the `-d` command-line option for Linux file systems like ext2.

We'll run foremost again, adding the `-d` command-line option to our foremost invocation:

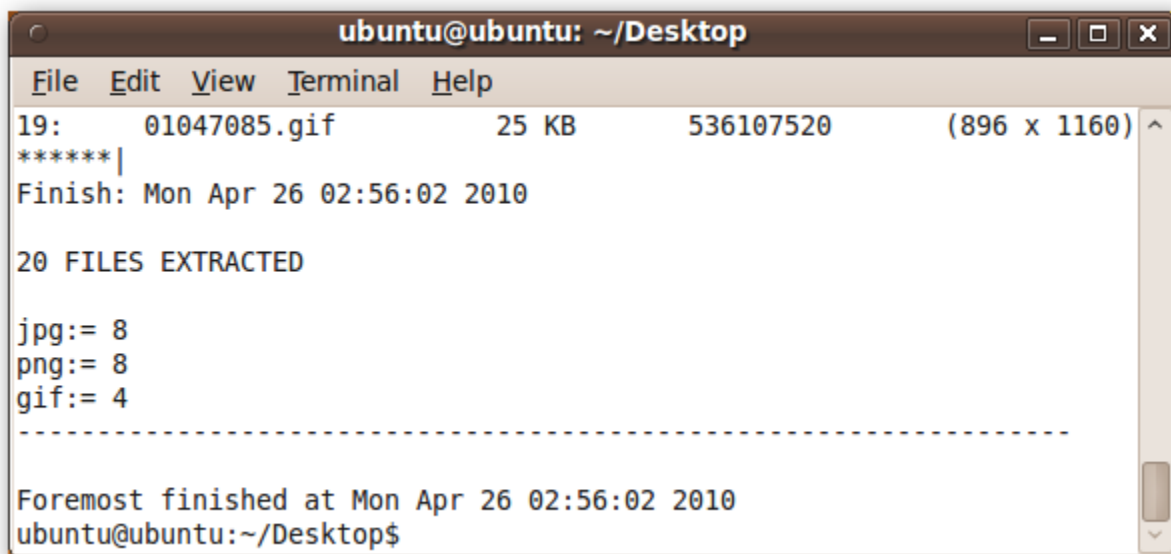
```
sudo foremost -t jpeg,png,gif -d -o foremost -v -i /dev/sda
```



```
ubuntu@ubuntu: ~/Desktop
File Edit View Terminal Help
ubuntu@ubuntu:~/Desktop$ sudo foremost -t jpeg,png,gif -d -o foremost
-v -i /dev/sda
Foremost version 1.5.6 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Mon Apr 26 02:55:47 2010
Invocation: foremost -t jpeg,png,gif -d -o foremost -v -i /dev/sda
Output directory: /home/ubuntu/Desktop/foremost
Configuration file: /etc/foremost.conf
Processing: /dev/sda
|-----
File: /dev/sda
Start: Mon Apr 26 02:55:47 2010
```

This time, foremost is able to recover all 20 images!

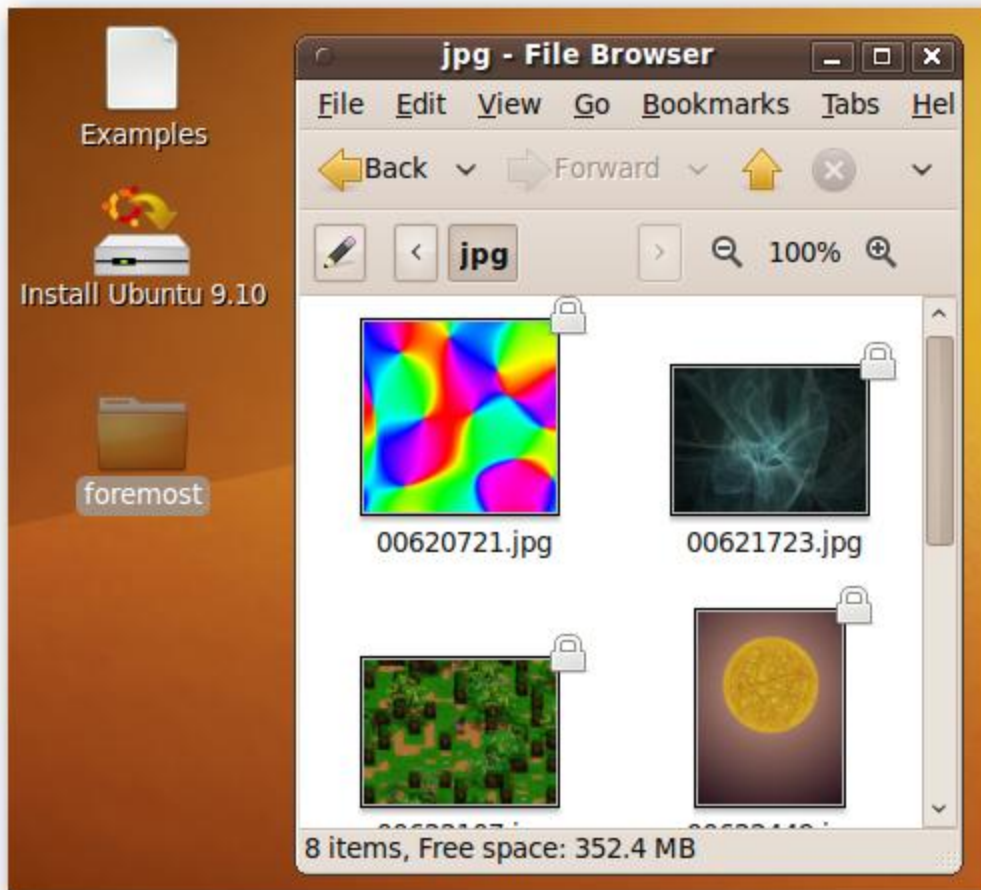


```
ubuntu@ubuntu: ~/Desktop
File Edit View Terminal Help
19: 01047085.gif      25 KB      536107520   (896 x 1160)
*****|
Finish: Mon Apr 26 02:56:02 2010

20 FILES EXTRACTED

jpg:= 8
png:= 8
gif:= 4
|-----
Foremost finished at Mon Apr 26 02:56:02 2010
ubuntu@ubuntu:~/Desktop$
```

A final look at the pictures reveals that the pictures were recovered with no problems.

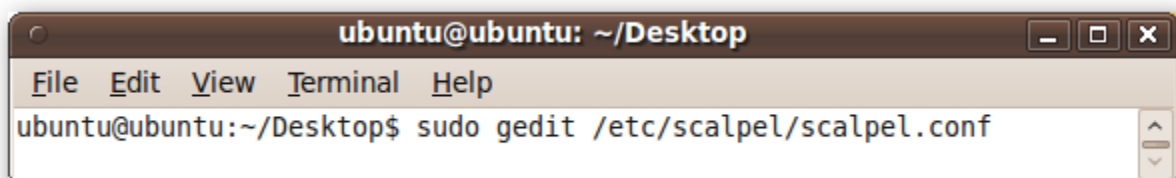


Scalpel

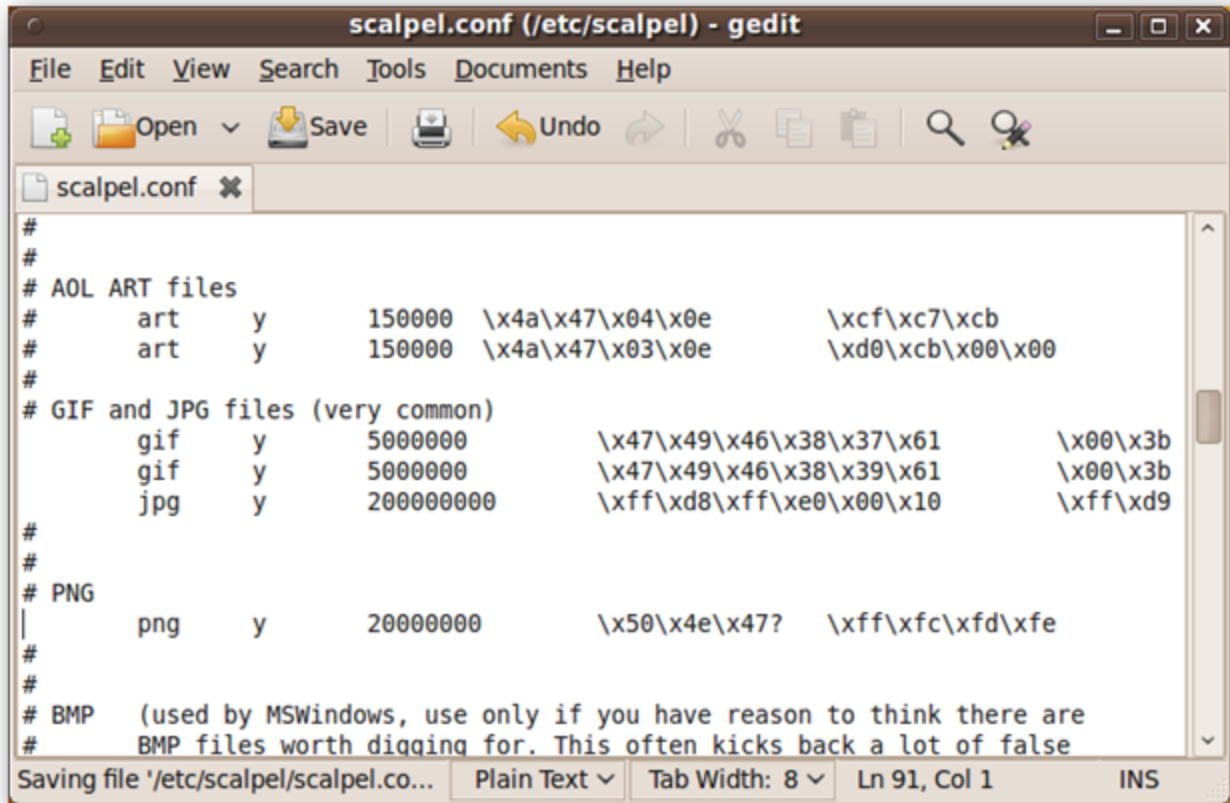
Scalpel is another powerful program that, like Foremost, is heavily configurable. Unlike Foremost, Scalpel requires you to edit a configuration file before attempting any data recovery.

Any text editor will do, but we'll use gedit to change the configuration file. In a terminal window (Applications > Accessories > Terminal), type in:

```
sudo gedit /etc/scalpel/scalpel.conf
```



scalpel.conf contains information about a number of different file types. Scroll through this file and uncomment lines that start with a file type that you want to recover (i.e. remove the “#” character at the start of those lines).

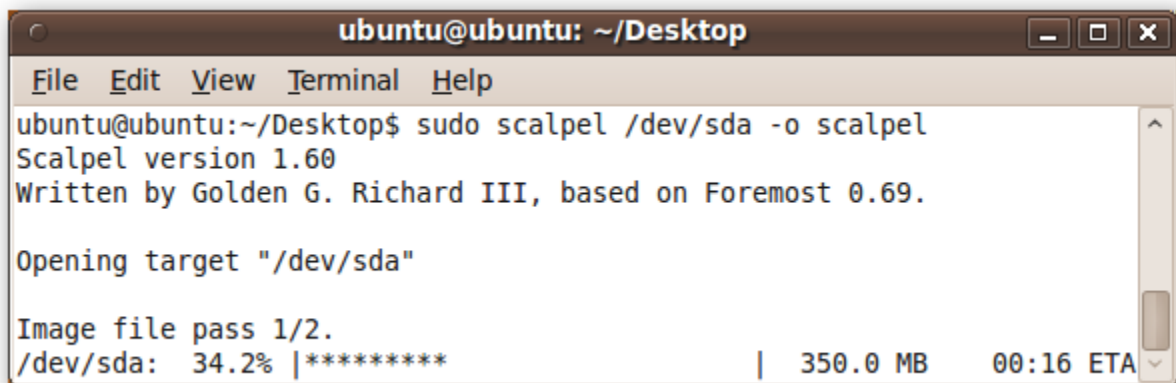


Save the file and close it. Return to the terminal window.

Scalpel also has a ton of command-line options that can help you search quickly and effectively; however, we'll just define the input device (/dev/sda) and the output folder (a folder called "scalpel" that we created on the desktop).

Our invocation is:

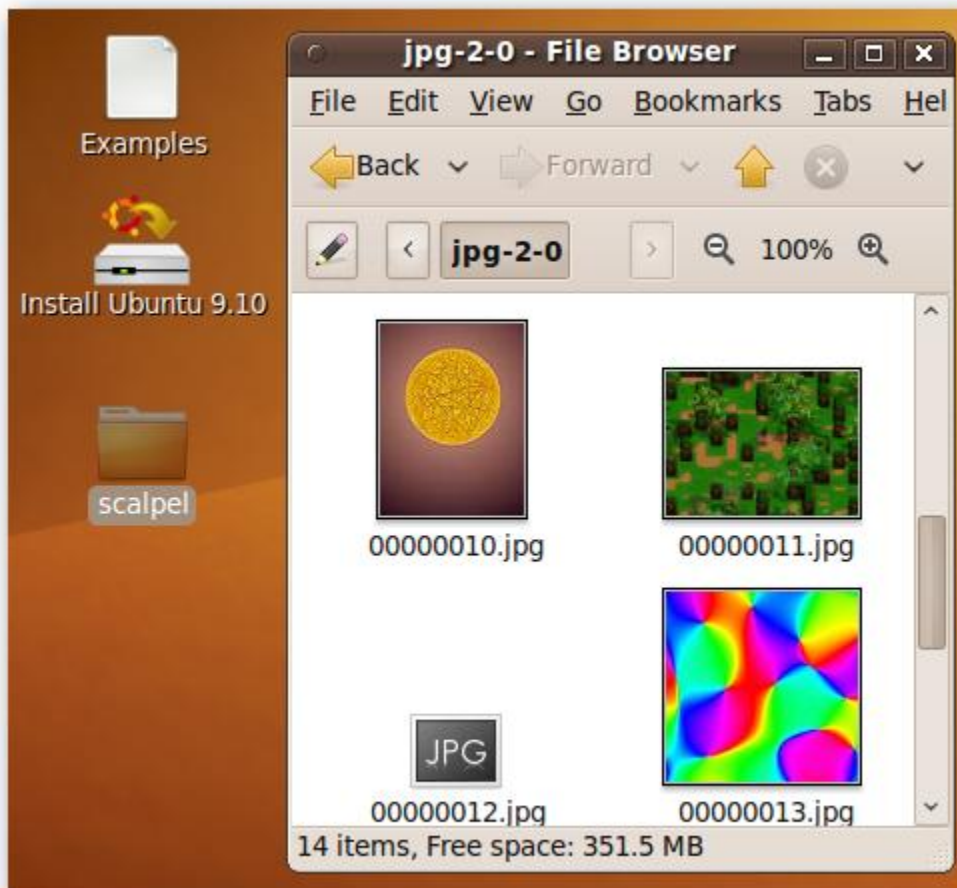
```
sudo scalpel /dev/sda -o scalpel
```



Scalpel is able to recover 18 of our 20 files.

```
ubuntu@ubuntu: ~/Desktop
File Edit View Terminal Help
png with header "\x50\x4e\x47\x3f" and footer "\xff\xfc\xfd\xfe" --> 0
files
Carving files from image.
Image file pass 2/2.
/dev/sda: 100.0% |*****| 1.0 GB 00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 18, elapsed = 28 seconds.
ubuntu@ubuntu:~/Desktop$
```

A quick look at the files scalpel recovered reveals that most of our files were recovered successfully, though there were some problems (e.g. 00000012.jpg).



Conclusion

In our quick toy example, TestDisk was able to recover two deleted partitions, and PhotoRec and Foremost were able to recover all 20 deleted images. Scalpel recovered most of the files, but it's very likely that playing with the command-line options for scalpel would have enabled us to recover all 20 images.

These tools are lifesavers when something goes wrong with your hard drive. If your data is on the hard drive somewhere, then one of these tools will track it down!