RECOVER DELETED FILES IN LINUX

Have you accidentally deleted an important file because you have the habit of using Shift+Del instead of only Del? Well, don't panic. I had this very problem some time ago, and found some utilities that helped me recover the so-called "permanently deleted" files; so thought of sharing this useful discovery

You must be wondering how we could recover a deleted file, because the very word "delete" implies "permanently gone". However, when you delete a file (accidentally or intentionally), its contents are not removed from your hard disk; the blocks that the file occupied on the storage device (like a hard disk) still contain the data, until the blocks are overwritten with new data. Deleting a file by its name only removes the reference to the inode of the file, and not the inode itself. (For more information, refer to the Wikipedia article on inode.) It is always recommended that you unmount a device immediately after you realise you've deleted important files, to prevent the data blocks of those files from being overwritten with other data. Thus, you should ideally shut down the system, and do the recovery process by booting from a Live CD/USB, and then searching the partition that contained the files (e.g., `/dev/sda1`). I am

using the Ubuntu 10.04 32-bit desktop edition, and the information here is specific to that distro.
Note: Be sure that you have enough space to accommodate the deleted files; otherwise, you will face some crazy errors during the post-recovery boot-up process and login.

Scalpel

This is a filesystem-independent recovery tool for Linux and Mac OS, which you can also run on Windows by compiling it with MinGW. The latest version is 2.0. Install it in Ubuntu with `sudo apt-get install scalpel`.
Next is some text editing — the configuration file is `/etc/scalpel/scalpel.conf`. You will find that everything has been commented out — uncomment the specific file format that you want to recover. For example, if I want to recover a deleted zip file, I will uncomment the `.zip` file section in `scalpel.conf`, as shown in Figure 1.

```
# MISCELLANEOUS
#-------------------------------------------------------------------
#
        zip     y       10000000        PK\x03\x04      \x3c\xac
#
#       java    y       1000000 \xca\xfe\xba\xbe
#
```

Figure 1: Scalpel.config file

Next, in a terminal, run:

```
sudo scalpel  [device/directory/file name] -o [output directory]
```

The output directory, in which you want to store recovered files, should be empty before running Scalpel; otherwise, you will get an error.

Foremost

Foremost is a console program to recover files based on their headers, footers, and internal data structures. This process is commonly referred to as data carving. Foremost can work on disk or partition image files, such as those generated by `dd`, Safeback, Encase, etc, or directly on a drive.
The headers and footers can be specified by a configuration file, or you can use command-line switches to specify built-in file types. Install in Ubuntu and its derivatives with the following command:

```
sudo apt-get install foremost
```

There are a lot of options available. For example, to search for a deleted JPEG file, use:

```
sudo foremost -t jpg -i /dev/sda1
```

The `-t` (“type”) option can be given as `-t all` to search for all file types. Multiple file types are comma-separated, like `-t jpg, pdf`. The (required) option `-i` is the base device/directory for the search. You can also specify an output directory with `-o`.

Photorec

This is the fastest utility of the three. It’s installed by the `testdisk` utility package. If you don’t want to mess with the command-line, this is the best utility for you. Just run `photorec`as the root user in a terminal, and you will see a nice ncurses-based UI as shown in Figure 2.

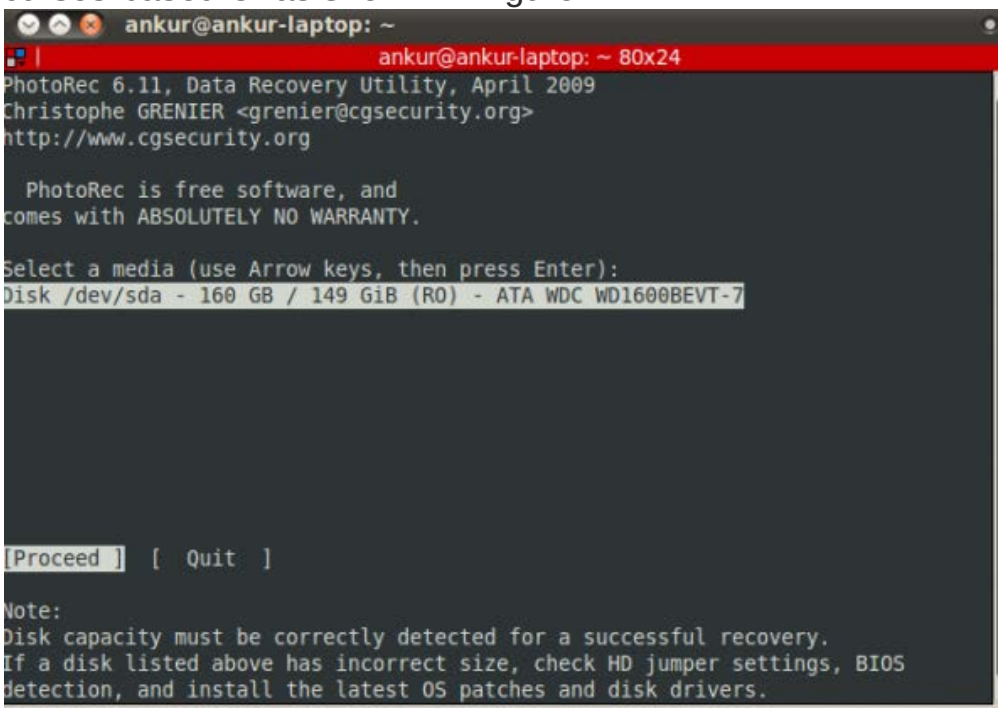

Figure 2: Photorec welcome screen

Select the device to *search*, and it will ask you for the partition table type. Select yours; in my case, it’s Intel. Next, you have to select the filesystem or partition of the device disk. Next, it prompts you to choose the file system, as shown in Figure 3. `*` indicates a mounted partition. Last, it will ask for an output folder in which to store recovered files. After making a selection, press *y* to proceed.

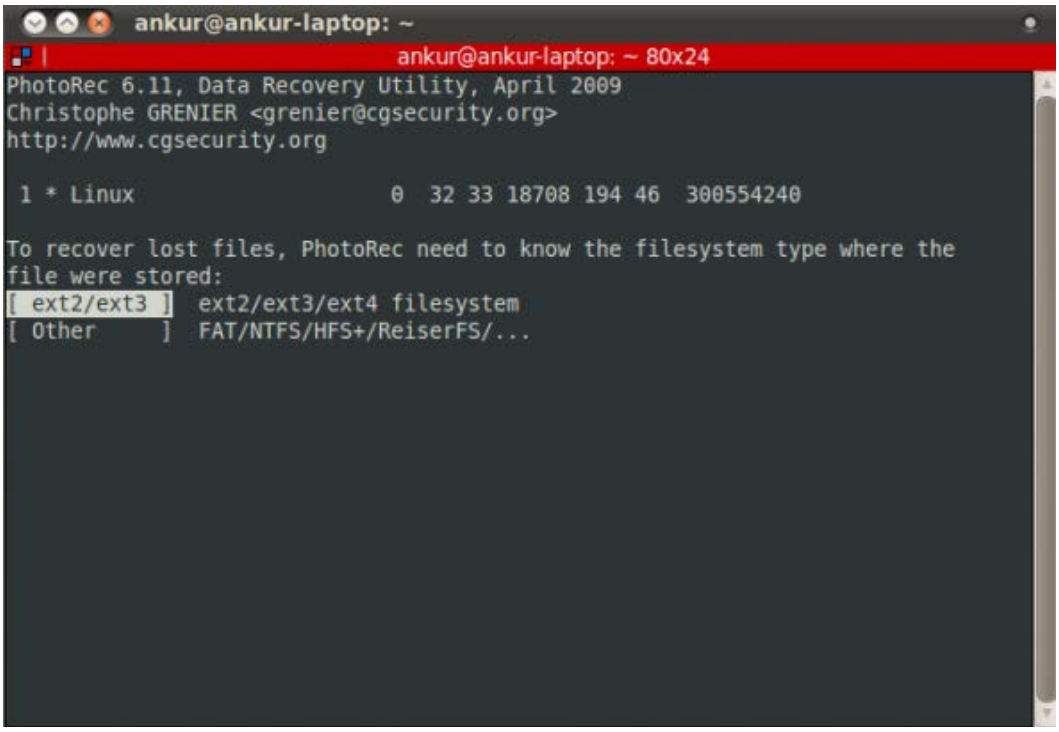

Figure 3: Filesystem selection in Photorec

Note: The above utilities will not recover replaced files, because in the case of replacement you are replacing the inode itself, so it's not possible to recover it.

Although there are utilities to recover deleted files, I recommend that prevention is always better than cure so don't use *Shift+Del* or `rm` indiscriminately.

Source : http://www.opensourceforu.com/2011/09/recover-deleted-files-in-linux/