There wasn't anything unusual about getting a call at 7pm on a Friday; when one works at home, one is always accessible. What *was* unusual was the tone of voice on the other end; the stress level was unmistakeable. One of my coworkers was on the other end of the line explaining how an errant space in a script had, ahem, removed the entire home directory tree of one of our development machines.

Once I had explained that Linux doesn't have a true undelete utility, we started to recover files from our backup tapes. By Monday morning, most everything was back as it should have been.

In the stress of the moment, I had forgotten something. It *is* possible to recover deleted files from Linux systems, but it needs to be done soon after the files were nuked. Just like in Windows, if you wait too long, there's a chance the contents of the files will be overwritten.

I had learned about this feature while working with the Midnight Commander file manager in 1998. The delete keystroke will either delete the file under the cursor, or all of the selected files if any are selected. I wanted to delete the file under the cursor but had forgotten that all of the files in my documents directory were selected − you can guess what happened. It certainly wasn't the file manager's fault; I acknowledged the request before thinking about the fact that multiple files were selected.

I certainly thought about it afterwards! *smile*

Steven Hirsch, a good friend and Linux mentor, was kind enough to explain how to use a (then specially−compiled version of) Midnight Commander to recover the files. It was more than a bit ironic that the tool that had erased my files with the blinding speed one finds in Linux was my best hope for getting them back.

While I'm *sincerely* hoping that you never see hundreds of needed files evaporating at high speed, I'd like you to be ready when that day comes. You'll probably want to do this as root; we'll be mounting and unmounting partitions and working with raw drive partitions. This may be especially necessary if, like in the following example, you'll be unmounting a partition like /home.

- Get a copy of Midnight Commander on your system.

  While it's certainly not the only program that could have the undelete ability, it's the program with which I'm most familiar. These days, MC contains the undelete code by default. If your distribution doesn't have it, get a copy from http://www.gnome.org/mc/ and install it.

  The best time to do this is *before* you delete the files − you want to make as few changes as possible to a filesystem from which you hope to recover files.
- Create a test file and delete it.

  You'll need to do this on a system where you can mount and unmount partitions as needed − no fair doing this on your primary web server!

  Pick a partition other than your root partition (use the

  ```
  mount
  ```

  command to see what partitions are mounted). For this example, let's assume that /dev/sdd1 is mounted on /home. Create a test file with:

  ```
  echo "Just a test file" >/home/testfile
  ```

```
rm −f /home/testfile
```

- Unmount the partition with the erased file(s).

  In this example, that can be accomplished with

  ```
  umount /dev/sdd1
  ```

  You should *not* attempt to undelete files from a mounted partition − you risk corrupting the drive.
- Start up Midnight Commander and select the files to recover.

  ```
  mc
  ```

  Inside mc, type:

  ```
  cd undel:/dev/sdd1
  ```

  . You can't do this anywhere else but mc. Using the "cd" command in mc normally does what it would at a shell prompt; it changes directories. This special syntax instructs mc to display all the undeleted files on that partition instead of the files in a directory.

  Wait a moment while it searches through that ext2 filesystem for deleted inodes (an inode holds the _contents_ of a file, but not the directory name, etc.). In a minute or so, you'll see a list of files with names like "23434632:2" in that window. The dates and times for the entries are the dates and times when that inode was deleted. I find it most useful to sort this window according to time:

  ```
  <F9>, r, s, m, <Enter>
  ```

  or

  ```
  <F9>, l, s, m, <Enter>
  ```

  You can use the <F3> "View" feature to look at the contents of the inode. Press <ins> on top of the files that have times around the time you think you deleted the file(s). This tags them to be undeleted in a moment.
- Undelete the files.

  In the other window (use <tab> to switch windows in mc), make an empty directory under /tmp, such as /tmp/deletedfiles.

  ```
  mkdir /tmp/deletedfiles
  ```

  Now switch back to your undel window and press <F5> to copy those files to your real filesystem. If you're done, you can leave mc with the <F10> key − see the legend at the bottom of the screen.

  This would also be a good time to remount the /home partition with

  ```
  mount /home
  ```

  At this point you'll probably want to look at each one and decide what the real name should be. Now that the files are in /tmp/deletedfiles, they can be manipulated just like any other file, such as:

  ```
  cd /tmp/deletedfiles
  mv 23434632:2 /home/testfile
  ```

There's a chance you might get multiple copies of some of your files if you deleted that file more than once; you'll need to decide which is the one you want to keep.

That's it! You've recovered a file from a Linux partition.

There are a few more important notes about this process. First, this particular undelete trick only works for ext2 partitions. Second, if the files were deleted on a system running a 2.0.x kernel, the undelete process is limited to recovering the first 12288 bytes of the file. There was a bug in the deletion process that didn't keep the entire file as a single unit when it was deleted. While it has not been fixed in the 2.0.x kernels, I do know it has been fixed in 2.2.x kernels.

The credit for this feature go to Ted T'so and the other authors of the ext2 filesystem, and to Miguel de Icaza and the other MC authors.

William is an Open−Source developer, enthusiast, writer, and advocate from New Hampshire, USA. His day job at SANS pays him to work on network security and Linux projects.

Last updated 12/18/2003.