

Ext2 File Undeletion

USER FRIENDLY by Illiad



Preventing catastrophe

- Do regular backups.
- Do regular backups!
- Have regular *tested, known-good* backups!

What's the best data recovery strategy? (Listed in order of increasing effectiveness)

- Doing nothing.
- Praying.
- "Being careful".
- Attempting undeletion.
- Having any kind of backup plan.
- Having a regular backup plan, in which you periodically verify the integrity of the backup media and files.

Preparing for the worst

- Type carefully, especially as root.
- Even when you're not root, still be careful. Sure, the system will be safe, but what about your personal files?
- Count to 10 before hitting enter after you've typed a command involving 'rm' and wildcards.
- Better yet, do an 'ls -d' on the wildcard pattern you're going to be deleting. Then, if you're using the bash shell, type your 'rm' command and hit <ESC>. The idea is to verify what you're doing and prevent a subsequent typo.
- Separate partitions are very important; the idea is to unmount the partition in question as soon after deletion as possible.

This becomes very difficult if the partition in question is the root partition.

The mechanics of actual undeletion

- In general:

- Unmount (or remount as read-only) the partition (we'll call it \$oops) where the deleted files are located:

```
# umount $oops
or
# mount -o remount,ro $oops
```

- Get a listing of all inodes which have been deleted (make sure the output goes someplace safe):

```
# echo lsdel | debugfs $oops > $lsdel.out
```

- Edit the file so that it has only the inodes that you want it to recover (you should be able to tell which ones these are from the time stamp, as well as the fact that they'll probably be toward the end and there'll be a bunch of them with the same timestamp).
- Get a couple more useful files:

```
# awk '{print $1}' $lsdel.out > $inodes
# sed 's/./*/stat <&>/' inodes |debugfs $oops > $stats
```

- Perform the actual undeletion:

```
# for i in $(cat $inodes); do echo "dump <$i> -p $safeflace/
recovered.$i" |debugfs $oops; done
```

- At this point, it's "just" a matter of finding out what all the files are and renaming them. Assuming that you actually recovered them.

- Note:

- \$oops is the partition that once housed the now-deleted files
- \$lsdel.out is a filename that you should specify
- \$inodes is a filename that you should specify
- \$stats is a filename that you should specify
- \$safeflace is a path to some directory that is not on the same partition as the deleted files.
- If you have a lot of data to recover, it might be best to do it in batches. For example, I was doing this once on a list of over 1500 inodes, and the data was going to be too big to fit in a free partition, so I made several files of the form inodes.01, inodes.02, and so forth, each containing a list of 100 unique inodes.

- The [Linux Ext2fs Undeletion mini-HOWTO](http://www.billjonas.com/papers/undeletion.html) has more in-depth information, but it written more towards Linux 2.0.
 - Note: 'awk' works better than the 'cut' commands which are suggested in the HOWTO; the 'cut' commands given in the HOWTO will cause mysterious errors in your undeletion if you have inodes with more than 6 digits.

In conclusion:

- Make regular backups, and test them.

- Separate out your partitions; have at least two.

- /
- /home

It's also a good idea to have separate partitions for /var, /usr, and others.

- Have backups.
 - If you must undelete, unmount (or remount as read-only) the partition on which the file resided as soon as possible. This will prevent the recently-freed inodes from being overwritten.
 - Did I mention backups?
-

Above is how this appeared on Wednesday, September 6, 2000. Since then, I have become aware of a new [HOWTO](#) available at the [LDP](#). I haven't used it yet myself (Read: I haven't done a repeat performance of the incident that caused me to need to learn enough on this subject in order to write the above), but it looks to be even more useful.

Also note that I'm not aware of any tools that might exist to attempt undeletion with other filesystems, such as [ReiserFS](#). Theoretically, the above steps might work with [Ext3](#), since it's basically just *<oversimplification type="gross">* Ext2 with journaling *</oversimplification>*. If anyone tries this and succeeds, please [let me know](#) so I can update this. It would be appreciated.

HTML hand-coded by bill@billjonas.com

(Valid HTML 3.2!)

Last modified Sat Jun 8 2002.