

Recover Deleted Files With foremost

By Falko Timme

foremost is a forensics application to recover files based on their headers, footers, and internal data structures. Foremost can work on image files, such as those generated by dd, Safeback, Encase, etc, or directly on a drive. This short article shows how you can use foremost to recover deleted files.

I do not issue any guarantee that this will work for you!

Preliminary Note

Currently foremost can recover the following file types:

- jpg - Support for the JFIF and Exif formats including implementations used in modern digital cameras.
- gif
- png
- bmp - Support for windows bmp format.
- avi
- exe - Support for Windows PE binaries, will extract DLL and EXE files along with their compile times.
- mpg - Support for most MPEG files (must begin with 0x000001BA)
- wav
- riff - This will extract AVI and RIFF since they use the same file format (RIFF). note faster than running each separately.
- wmv - Note may also extract -wma files as they have similar format.
- mov
- pdf
- ole - This will grab any file using the OLE file structure. This includes PowerPoint, Word, Excel, Access, and StarWriter
- doc - Note it is more efficient to run OLE as you get more bang for your buck. If you wish to ignore all other ole files then use this.
- zip - Note it will extract .jar files as well because they use a similar format. Open Office docs are just zipâd XML files so they are extracted as well. These include SXW, SXC, SXI, and SX? for undetermined OpenOffice files.
- rar
- htm
- cpp - C source code detection, note this is primitive and may generate documents other than C code.

You can tweak /etc/foremost.conf to add support for more file types.

Please note that there's no guarantee that foremost will succeed in recovering your files, but at least there's a chance.

Installing foremost

On Debian and Ubuntu, foremost can be installed as follows:

```
apt-get install foremost
```

Recover Deleted Files With foremost

By Falko Timme

Using foremost

Take a look at

```
man foremost
```

to learn how to use foremost.

In this example I delete a jpg file:

```
server1:/home/administrator# ls -l
total 324
-rw-r--r-- 1 root root 324383 2008-02-19 01:25 k-
p1170003_13_20080217_1058163689.jpg
```

```
server1:/home/administrator#
```

```
rm -f k-p1170003_13_20080217_1058163689.jpg
```

foremost can be used as follows to try to recover the file:

```
foremost -t jpeg -i /dev/sda1
```

(If you don't know what partition to search, take a look at

```
mount
```

```
server1:~# mount
/dev/sda1 on / type ext3 (rw,errors=remount-ro)
tmpfs on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)
proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
udev on /dev type tmpfs (rw,mode=0755)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=620)
nfsd on /proc/fs/nfsd type nfsd (rw)
server1:~#
)
```

After foremost has finished, you will find a folder called output in the directory from where you called foremost:

```
ls -la
```

```
server1:~# ls -la
total 36
drwxr-xr-x 5 root root 4096 2009-03-12 17:53 .
drwxr-xr-x 21 root root 4096 2009-02-16 13:10 ..
```

Recover Deleted Files With foremost

By Falko Timme

```
drwx----- 2 root root 4096 2009-02-16 13:15 .aptitude
-rw----- 1 root root 377 2009-02-16 13:32 .bash_history
-rw-r--r-- 1 root root 412 2004-12-15 23:53 .bashrc
drwxr-xr-x 2 root root 4096 2009-02-16 13:17 .debtags
drwxr-xr-- 3 root root 4096 2009-03-12 17:53 output
-rw-r--r-- 1 root root 140 2007-11-19 18:57 .profile
-rw----- 1 root root 3480 2009-03-12 17:06 .viminfo
```

```
server1:~#
ls -l output
```

```
server1:~# ls -l output/
total 8
-rw-r--r-- 1 root root 714 2009-03-12 18:02 audit.txt
drwxr-xr-- 2 root root 4096 2009-03-12 17:57 jpg
```

```
server1:~#
```

The audit.txt contains a summary of what foremost has done:

```
cat output/audit.txt
server1:~# cat output/audit.txt
Foremost version 1.5.4 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File
```

```
Foremost started at Thu Mar 12 17:53:48 2009
Invocation: foremost -t jpeg -i /dev/sda1
Output directory: /root/output
Configuration file: /etc/foremost.conf
```

```
-----
File: /dev/sda1
Start: Thu Mar 12 17:53:48 2009
Length: 28 GB (30836542464 bytes)
```

```
Num Name (bs=512) Size File Offset Comment
```

```
0: 11157504.jpg 320 KB 5712642048
1: 29556752.jpg 324 KB 15133057024
Finish: Thu Mar 12 18:02:10 2009
```

```
2 FILES EXTRACTED
```

```
jpg:= 2
-----
```

```
Foremost finished at Thu Mar 12 18:02:10 2009
server1:~#
```

Recover Deleted Files With foremost

By Falko Timme

And the jpg/ subdirectory contains the jpg files that foremost has recovered:

```
ls -l output/jpg/
```

```
server1:~# ls -l output/jpg/  
total 660  
-rw-r--r-- 1 root root 328479 2009-03-12 17:55 11157504.jpg  
-rw-r--r-- 1 root root 332575 2009-03-12 17:57 29556752.jpg
```

```
server1:~#
```

Before you run foremost the next time from the same directory, you must either delete/rename the current output/ directory (because foremost will not start if there's already an output/ directory) or use the -T switch (time stamp the output directory so you don't have to delete the output/ dir when running multiple times):

```
foremost -t pdf -T -i /dev/sda1
```