Recover your files!

Author: **Alexandre Borges**
Revision: **rev. A**
Date: **May/23/2014**

A few days ago a student deleted pdf files from his pen drive by mistake and he was desperate. Honestly, there wasn't any reason for that because an old software and effective tool can be very useful for this kind of disasters: Foremost.

Foremost is a command line and reliable program able to recovery (carving) files from image files (Encase, dd, etc.) or devices such as disk drives, pen-drives, external hd, etc, and it's available from many distributions and repositories.

The Foremost program can be downloaded from http://foremost.sourceforge.net/pkg/foremost-1.5.7.tar.gz. However, if you are using Kali Linux (http://www.kali.org/downloads/), installing the Foremost tool is extremely easy:

```
root@hacker:/# apt-get install foremost
```

Proceeding with our example, we can recover pdf files from a pen drive by running the following commands:

```
root@hacker:~# mkdir /tmp/recovered

root@hacker:~# df -h

Filesystem                                              Size  Used Avail Use% Mounted on
rootfs                                                  673G  537G  102G  85% /
udev                                                     10M     0   10M   0% /dev
tmpfs                                                   1.6G  812K  1.6G   1% /run
/dev/disk/by-uuid/88cd030b-409f-4848-a1b6-b5d1342be5f1  673G  537G  102G  85% /
tmpfs                                                   5.0M     0  5.0M   0% /run/lock
tmpfs                                                   6.3G   36M  6.3G   1% /run/shm
/dev/mapper/truecrypt1                                  138G  117G   15G  90%
/media/truecrypt1
/dev/sdb1                                               3.8G   20K  3.8G   1%
/media/BC53-4A3F

root@hacker:~# foremost -t pdf -o /tmp/recovered -i /dev/sdb1

Processing: /dev/sdb1
|*************************************|
```

Where the options chose are:

- -t → used to specify the file type (pdf,jpeg,etc)
- -o → used to specify where the audit file and recovered files will be saved.
- -i → used to specify from either an image file or a device that files will be recovered (carved).

As the result from our carving operation, we've got the following content:

Recover your files!

```
root@hacker:/# cd /tmp/recovered

root@hacker:/tmp/recovered# ls

audit.txt  pdf


root@hacker:/tmp/recovered# more audit.txt

Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Fri May 23 01:36:47 2014
Invocation: foremost -t pdf -o /tmp/recovered -i /dev/sdb1
Output directory: /tmp/recovered
Configuration file: /etc/foremost.conf
------------------------------------------------------------------
File: /dev/sdb1
Start: Fri May 23 01:36:47 2014
Length: 3 GB (3983740928 bytes)

Num     Name (bs=512)             Size    File Offset  Comment

0:     00015208.pdf        5 MB       7786496
1:     00089856.pdf        3 MB      46006272
2:     00099408.pdf        2 MB      50896896
3:     00106992.pdf       19 MB      54779904
4:     00147752.pdf        4 MB      75649024
5:     00218696.pdf        5 MB     111972352
6:     00231040.pdf        5 MB     118292480
7:     00243104.pdf       19 MB     124469248
Finish: Fri May 23 01:42:49 2014

8 FILES EXTRACTED

pdf:= 8
------------------------------------------------------------------

root@hacker:/tmp/recovered# cd pdf

root@hacker:/tmp/recovered/pdf# ls -al

total 67340
drwxr-xr-- 2 root root     4096 May 23 01:37 .
drwxr-xr-x 3 root root     4096 May 23 01:36 ..
-rw-r--r-- 1 root root  6222844 May 23 01:37 00015208.pdf
-rw-r--r-- 1 root root  4126823 May 23 01:37 00089856.pdf
-rw-r--r-- 1 root root  3124597 May 23 01:37 00099408.pdf
-rw-r--r-- 1 root root 20129605 May 23 01:37 00106992.pdf
-rw-r--r-- 1 root root  4515460 May 23 01:37 00147752.pdf
-rw-r--r-- 1 root root  5465565 May 23 01:37 00218696.pdf
-rw-r--r-- 1 root root  5287669 May 23 01:37 00231040.pdf
-rw-r--r-- 1 root root 20059974 May 23 01:37 00243104.pdf

root@hacker:/tmp/recovered/pdf#
```

Perfect! No more tears!

Alexandre Borges.