By Falko Timme

Published: 2009-03-24 12:49

Recover Deleted Files With Scalpel

Version 1.0
Author: Falko Timme <ft [at] falkotimme [dot] com>
Last edited 12/03/2009

Scalpel is a fast file carver that reads a database of header and footer definitions and extracts matching files from a set of image files or raw device files. Scalpel is filesystem-independent and will carve files from FATx, NTFS, ext2/3, or raw partitions. It is useful for both digital forensics investigation and file recovery. This short article shows how you can use Scalpel to recover deleted files.

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

1 Preliminary Note

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

2 Installing Scalpel

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

```
apt-get install scalpel
```

3 Using Scalpel

Take a look at

```
man scalpel
```

to learn how to use Scalpel.

Before we can use Scalpel, we must define some file types that Scalpel should search for in `/etc/scalpel/scalpel.conf`. By default, all file types are commented out. In this example, I want to search for deleted PDF files, so I uncomment the following lines:

```
vi /etc/scalpel/scalpel.conf
```

```
[...]
      pdf    y      5000000 %PDF  %EOF\x0d  REVERSE
      pdf    y      5000000 %PDF  %EOF\x0a  REVERSE
[...]
```

Scalpel can be used as follows to try to recover the files:

```
scalpel /dev/sda1 -o output
```

`-o` defines the directory where Scalpel will place the recovered files - in this case the directory is named `output` and is a subdirectory of the directory where we are running the `scalpel` command from; the directory must not exist because otherwise scalpel will refuse to start.

(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 Scalpel has finished, you will find a folder called `output` in the directory from where you called Scalpel:

```
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 ..
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  386 2009-03-12 19:10 audit.txt
drwxr-xr-x 2 root root 4096 2009-03-12 19:10 pdf-0-0
server1:~#
```

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

```
cat output/audit.txt
```

```
server1:~# cat output/audit.txt

Scalpel version 1.60 audit file
Started at Thu Mar 12 19:01:50 2009
Command line:
scalpel /dev/sda1 -o output

Output directory: /root/output
Configuration file: /etc/scalpel/scalpel.conf

Opening target "/dev/sda1"

The following files were carved:
File              Start                 Chop            Length          Extracted From
00000000.pdf   5712642048               NO           437138             sda1


Completed at Thu Mar 12 19:10:33 2009
server1:~#
```

And the *pdf-0-0/* subdirectory contains the jpg files that Scalpel has recovered:

```
ls -l output/pdf-0-0/
```

```
server1:~# ls -l output/pdf-0-0/
total 432
-rw-r--r-- 1 root root 437138 2009-03-12 19:10 00000000.pdf
```

```
server1:~#
```

Before you run Scalpel the next time from the same directory, you must either delete/rename the current `output/` directory (because Scalpel will not start if the output directory is already existing) or use specify another output directory.

4 Links

- Scalpel: **http://www.digitalforensicssolutions.com/Scalpel/**