

theevilbit.blogspot.com

The Evil Bit Blog: Backtrack Forensics: scalpel

<http://theevilbit.blogspot.com/2013/01/backtrack-forensics-scalpel.html>

Forensics -> Forensic Carving Tools

`/usr/local/bin/scalpel`

Scalpel is a very similar tool to foremost, it will data carve files, based on their header and footer information, it's also file system independent. It can work on drives directly or on image files.

Usage:

The biggest difference to foremost is that we need to edit the scalpel.conf file (`/etc/scalpel/scalpel.conf`), and uncomment lines (remove #) that specifies the file type we would like to recover.

Few of the many options:

- c Choose configuration file.
- n Don't add extensions to extracted files.
- o Set output directory for carved files.
- O Don't organize carved files by type. Default is to organize carved files into subdirectories.
- v Verbose mode.

`scalpel -c /etc/scalpel/scalpel.conf -o output2/ Desktop/forensics/11-carve-fat/11-carve-fat.dd`

I used the same test forensic image as with foremost.

Editing the conf file:

```
scalpel.conf (/etc/scalpel) - gedit
File Edit View Search Tools Documents Help

scalpel.conf
#
#
# AOL ART files
#   art   y   150000  \x4a\x47\x04\x0e      \xcf\xcb\xcb
#   art   y   150000  \x4a\x47\x03\x0e      \xd0\xcb\x00\x00
#
# GIF and JPG files (very common)
#   gif   y   5000000  \x47\x49\x46\x38\x37\x61      \x00\x3b
#   gif   y   5000000  \x47\x49\x46\x38\x39\x61      \x00\x00\x3b
#   jpg   y   200000000  \xff\xd8\xff\xe0\x00\x10      \xff\xd9
#   jpg   y   200000000  \xff\xd8\xff\xe1      \xff\xd9
#
#
# PNG
#   png   y   20000000  \x50\x4e\x47?  \xff\xfc\xfd\xfe
#
#
# BMP (used by MSWindows, use only if you have reason to think there are
# BMP files worth digging for. This often kicks back a lot of false
# positives
```

Running the command:

```
root@bt: ~
File Edit View Terminal Help

root@bt:~# scalpel -c /etc/scalpel/scalpel.conf -o output2/ Desktop/forensics/11-
-carve-fat/11-carve-fat.dd
Scalpel version 2.0
Written by Golden G. Richard III and Lodovico Marziale.
Multi-core CPU threading model enabled.
Initializing thread group data structures.
Creating threads...
Thread creation completed.

Opening target "/root/Desktop/forensics/11-carve-fat/11-carve-fat.dd"

Image file pass 1/2.
Desktop/forensics/11-carve-fat/11-carve-fat.dd: 100.0% 62.0 MB 00:00 ETAAl
locating work queues...
Work queues allocation complete. Building work queues...
Work queues built. Workload:
jpg with header "\xff\xd8\xff\xe0\x00\x10" and footer "\xff\xd9" --> 5 files
jpg with header "\xff\xd8\xff\xe1" and footer "\xff\xd9" --> 1 files
wmv with header "\x30\x26\xb2\x75\x8e\x66\xcf\x11\xa6\xd9\x00\xaa\x00\x62\xce\x6
C" and footer "" --> 2 files
Carving files from image.
Image file pass 2/2.
Desktop/forensics/11-carve-fat/11-carve-fat.dd: 100.0% 62.0 MB 00:00 ETAPT
rocessing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 8, elapsed = 2 secs.
root@bt:~#
```

MD5 check, based on this it successfully extracted only 2 files, which means that foremost performed better in this case.

```
root@bt: ~  
File Edit View Terminal Help  
root@bt:~# md5deep -r output2/  
635ed8b379942f6cda5e6c809c52f8a1 /root/output2/jpg-0-0/00000004.jpg  
635ed8b379942f6cda5e6c809c52f8a1 /root/output2/jpg-0-0/00000003.jpg  
37a49f97ed279832cd4f7bd002c826a2 /root/output2/jpg-0-0/00000001.jpg  
7e0b420a2ea2258b8743b9abef7c6946 /root/output2/jpg-0-0/00000002.jpg  
84e1dceac2eb127fef5bfcdb0eae324b /root/output2/jpg-0-0/00000000.jpg  
d965a3e7b4c889a9ecc1b28b75bc9876 /root/output2/jpg-1-0/00000005.jpg  
916d0c85d7ead5186a91b6c26e199f79 /root/output2/wmv-2-0/00000007.wmv  
e81b6ca6cf83f2ec269b5909a1c3e3c6 /root/output2/wmv-2-0/00000006.wmv  
6a0cb78b403f6d59e03afa594a3072d9 /root/output2/audit.txt  
root@bt:~#
```

audit file:

```
audit.txt (~/.output2) - gedit  
File Edit View Search Tools Documents Help  
Open Save Undo  
audit.txt  
#  
#-----  
#-----  
#-----  
----- END COPY OF CONFIG FILE USED -----  
  
Opening target "/root/Desktop/forensics/11-carve-fat/11-carve-fat.dd"  
  
The following files were carved:  
File Start Chop Length Extracted From  
00000005.jpg 10125824 NO 5126 11-carve-fat.dd  
00000001.jpg 10095104 NO 29885 11-carve-fat.dd  
00000000.jpg 8522240 NO 24367 11-carve-fat.dd  
00000006.wmv 164352 YES 20000000 11-carve-fat.dd  
00000004.jpg 10574693 NO 2655 11-carve-fat.dd  
00000003.jpg 10570636 NO 2655 11-carve-fat.dd  
00000002.jpg 10570240 NO 3051 11-carve-fat.dd  
00000007.wmv 11227648 YES 20000000 11-carve-fat.dd  
  
Completed at Sun Jan 6 03:43:50 2013  
Plain Text Tab Width: 8 Ln 1, Col 1 INS
```