

Lab 5-Module 5.3: Scalpel

Objectives

- File carving using Scalpel

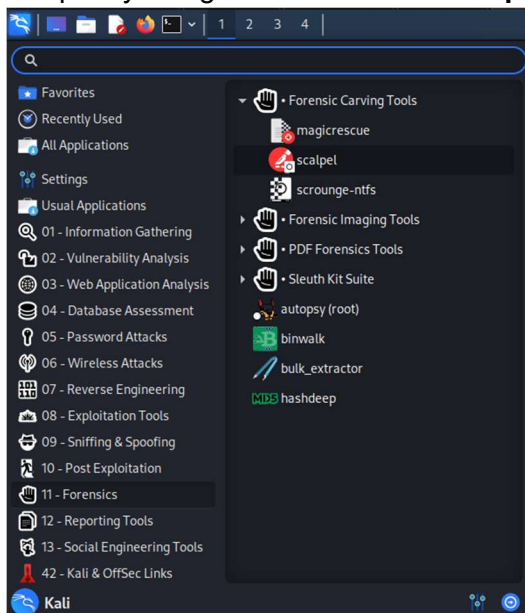
Scalpel is a complete rewrite of the Foremost 0.69 file carver and is useful for both digital forensics investigations and file recovery.

Task

If you are using the prepared Kali Linux image, you don't need to do Task 1 and Task 2. All the materials needed for this lab will be located on Desktop/INFER/File carving/Scalpel

Task 1. Software Preparation

1. Download the prepared image - m5demo.img to the desktop.
2. Kali linux has pre-installed Scalpel, for other linux distributions, you may need to install scalpel by using the command **sudo apt install scalpel**



Task 2. Prepare configuration file

1. Open the terminal and enter **cd /etc/scalpel**
2. Type **ls** to see if the configuration file exists.

```
(kali@kali)-[/etc/scalpel]
$ ls
scalpel.conf
```

3. Copy the file to the desktop by using **cp scalpel.conf /home/{hostname}/Desktop/**

```
(kali@kali)-[/etc/scalpel]
$ cp scalpel.conf /home/kali/Desktop/
```

(you should see the configuration file appear on desktop)

4. Enter `cd /home/{hostname}/Desktop/`

Task 3. Carving file using scalpel

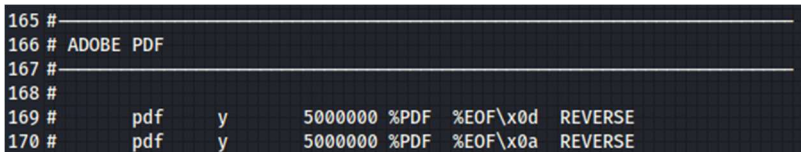
1. Click on the configuration file on the desktop or edit the file using any text editor from the terminal (gedit is preferred).



```
scalpel.conf
~/Desktop

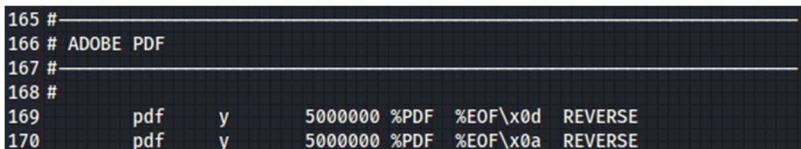
1 # Scalpel configuration file
2
3 # This configuration file controls the
4 # types and sizes of files that are carved by Scalpel. Currently,
5 # Scalpel can read Foremost 0.69 configuration files, but Scalpel
6 # configuration files may not be backwards-compatible with Foremost.
7 # In particular, maximum file carve size under Foremost 0.69 is 4GB,
8 # while in the current version of Scalpel, it's 16EB (16 exabytes).
9
10 # For each file type, the configuration file
```

2. Scroll down and you can find all the extension types that scalpel support. In this lab, we will carve a pdf file, so find **ADOBE PDF**.



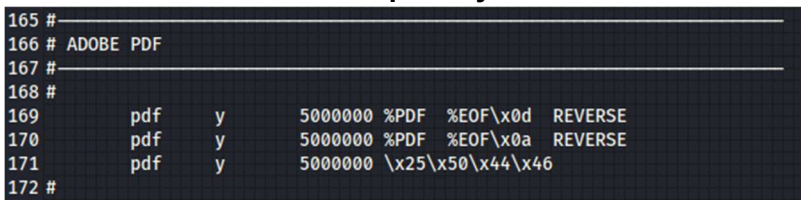
```
165 #
166 # ADOBE PDF
167 #
168 #
169 # pdf y 5000000 %PDF %EOF\x0d REVERSE
170 # pdf y 5000000 %PDF %EOF\x0a REVERSE
```

3. Take out the # signs in front of the lines indicate the file types that you want scalpel to look for.



```
165 #
166 # ADOBE PDF
167 #
168 #
169 pdf y 5000000 %PDF %EOF\x0d REVERSE
170 pdf y 5000000 %PDF %EOF\x0a REVERSE
```

4. In addition, add another line `pdf y 5000000 \x25\x50\x44\x46`



```
165 #
166 # ADOBE PDF
167 #
168 #
169 pdf y 5000000 %PDF %EOF\x0d REVERSE
170 pdf y 5000000 %PDF %EOF\x0a REVERSE
171 pdf y 5000000 \x25\x50\x44\x46
172 #
```

5. Click Save and quit the editor.



(There should be two files on your desktop, m5demo.img and scalpel.conf)

6. Open the terminal, and enter `cd /home/{hostname}/Desktop/`
7. Enter `scalpel -h` to see the help menu, we will be using `-c` and `-o` for this lab.

```

(kali@kali)-[~/Desktop]
$ scalpel -h
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.
Carves files from a disk image based on file headers and footers.

Usage: scalpel [-b] [-c <config file>] [-d] [-h|V] [-i <file>]
              [-m blocksize] [-n] [-o <outputdir>] [-O num] [-q clustersize]
              [-r] [-s num] [-t <blockmap file>] [-u] [-v]
              <imgfile> [<imgfile>] ...

-b Carve files even if defined footers aren't discovered within
  maximum carve size for file type [foremost 0.69 compat mode].
-c Choose configuration file.
-d Generate header/footer database; will bypass certain optimizations
  and discover all footers, so performance suffers. Doesn't affect
  the set of files carved. **EXPERIMENTAL**
-h Print this help message and exit.
-i Read names of disk images from specified file.
-m Generate/update carve coverage blockmap file. The first 32bit
  unsigned int in the file identifies the block size. Thereafter
  each 32bit unsigned int entry in the blockmap file corresponds
  to one block in the image file. Each entry counts how many
  carved files contain this block. Requires more memory and
  disk. **EXPERIMENTAL**
-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.
-p Perform image file preview; audit log indicates which files
  would have been carved, but no files are actually carved.
-q Carve only when header is cluster-aligned.
-r Find only first of overlapping headers/footers [foremost 0.69 compat mode].
-s Skip n bytes in each disk image before carving.
-t Set directory for coverage blockmap. **EXPERIMENTAL**
-u Use carve coverage blockmap when carving. Carve only sections
  of the image whose entries in the blockmap are 0. These areas
  are treated as contiguous regions. **EXPERIMENTAL**
-v Print copyright information and exit.
-V Verbose mode.

```

8. Enter **scalpel -c scalpel.conf -o scalpelOutput m5demo.img**
 (-c specify the configuration file, -o specify the output directory, in this case, scalpelOutput is the name of the output folder, m5demo.img is the image file.)
9. It may take some time for the carving process.

```

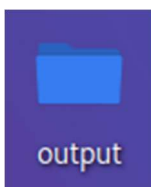
(kali@kali)-[~/Desktop]
$ scalpel -c scalpel.conf -o output m5demo.img
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/home/kali/Desktop/m5demo.img"

Image file pass 1/2.
m5demo.img: 100.0% |*****| 949.4 MB 00:00 ETA
Allocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built. Workload:
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0d" → 0 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0a" → 0 files
pdf with header "\x25\x50\x44\x46" and footer "" → 1 files
Carving files from image.
Image file pass 2/2.
m5demo.img: 100.0% |*****| 949.4 MB 00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 1, elapsed = 3 seconds.

```

10. After it is finished, you can view the carved file under the output folder.



Common question:

If the folder is shown as locked, this is because you are at root or using sudo, to fix this, you can enter **sudo chmod -R 777 output** to change the folder permission

```
(root@kali)-[/home/kali/Desktop]
# sudo chmod -R 777 output
```

(Additional, not required)

Scalpel also support disk partitions as input. To do this, first we check the disk by using **sudo fdisk -l**

```
(kali@kali)-[~]
$ sudo fdisk -l
Disk /dev/sda: 80 GiB, 85899345920 bytes, 167772160 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x72bd05d3

Device Boot      Start         End      Sectors  Size Id Type
/dev/sda1 *        2048     165771263   165769216    79G 83 Linux
/dev/sda2          165773310   167770111    1996802    975M  5 Extended
/dev/sda5          165773312   167770111    1996800    975M 82 Linux swap / Solaris

Disk /dev/sdb: 949.36 MiB, 995474944 bytes, 1944287 sectors
Disk model: TransMemory
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xabae6bcf

Device Boot      Start         End      Sectors  Size Id Type
/dev/sdb1 *         8    1944286    1944279    949.4M  7 HPFS/NTFS/exFAT
```

(You can see there is a partition called **/dev/sdb1** in this example)

To carve file on the partition, enter

sudo scalpel -c scalpel.conf -o fdiskoutput /dev/sdb1

Questions:

1. How many files are in the output folder? What are they?
2. What is the message in the pdf file?