CCF Lab Assignment:
Memory and Filesystems[*]

Arno Bakker
Arno.Bakker@os3.nl

Mick Pouw

Feedback deadline:
February 19, 2018 10:00 CET

Abstract

This lab will introduce you to memory and filesystem forensics. You should work alone on this assignment, again from the CAINE forensics environment.

1 Memory

Recall: to use the local disk for storage:

1. Using the BlockOn/Off tool on the CAINE desktop, set device `sda` to writable.
2. Open Terminal (Ctrl-Alt-T)
3. Type `sudo -i`
4. Type `mkdir /local`
5. Type `mount /dev/sda2 /local`
6. Type `cd /local`
7. You can now work from this `/local` directory.

Questions

1. First download and extract the file `evidence.tar.gz` from `https://software.os3.nl/CCF/`. Make sure you check the tar-ball and included files. Keep in mind that the extracted files will be around 5GB.
2. Read about Volatility and its features.
   (a) What does Volatility do?
   (b) Would Volatility be useful in the acquiring stage?
   (c) What parts of Volatility would you use in your investigation on the acquired memory?

[*] Version February 12, 2018.

3. Identify the operating system that is running. Note down the steps you take to detect this.
4. Find out if there is any malware running on the computer.
5. What kind of connections are currently open?
6. Find out what programs and services are running.
7. How can you retrieve files out of the memory? What files can contain artifacts?
8. Write a small paragraph of maximum 200 words about your findings. Please remain objective.

2 Disk

9. Read up on Scalpel and its features. Explain what it does and how it works.
10. Inspect the image manually and look for any artifacts. Describe this process completely.
11. Let Scalpel inspect the disk image. What files are useful for your investigation?
12. Investigate the techniques that have been used to hide files.
13. How would you securely hide or delete your information?
14. Write a small paragraph of maximum 200 words about your findings. Please remain objective.
15. Did you find any traps that were interfering with your work?

3 Combining

16. Create a timeline of the evidence and explain what happened. Include both the memory and the disk forensics. Use a maximum of 400 words.