CCF Lab Assignment: Data Acquisition*

Arno Bakker Mick Pouw
Arno.Bakker@os3.nl

Feedback deadline:
February 15, 2018 10:00 CET

Abstract

This lab will introduce you to forensic imaging and data handling using a live environment. You will work in pairs to achieve this. Document your work on one of your personal logs, and link to that log from the other person's log.

1 Imaging

First boot into the CAINE 9.0 live environment. This can be done using PXE boot. There is no persistent storage in this environment. To get some storage space to work on, set the desktop's internal disk to writable using the BlockOn/Off utility on the CAINE desktop, and mount it read/write in the live environment. *Tips: Work as root (*`sudo -i`*) and in the Terminal preferences set the number of Scrollback lines that it will remember to "Unlimited".*

1. Form a group of two and discuss how you can retrieve an image from an, currently off-line, hard disk in a forensically sound manner. Create and describe this method.

2. Write a one-line description, or note a useful feature for the following tools included in CAINE: `Guymager`, `Disk Image Mounter`, `dcfldd`, `kpartx`

3. Retrieve one of the evidence harddisks and SATA-to-USB interfaces from the lab teachers. Take extra care to check and maintain the chain of custody!

4. Follow your method to retrieve the image. Please use timestamps, explain every tool and note down the version. For the purpose of speed, you can assume that the disk is empty after the first 19 GiB[1]. If you don't trust this, go ahead, but take into account that a full dump can take hours. Make sure both team members have access to the retrieved image. You can use your servers as an evidence sharing platform[2].

5. Read about CAINE Linux and its features while waiting on the dump to finish.
   (a) Why would you use a Forensic distribution and what are the main differences between a regular distribution?

*Version February 8, 2018.
[1]Note some tools cannot do a partial acquire.
[2]Make sure that the image is only reachable within the OS3 network.

(b) When would you use a live environment and when would you use an installed environment?

(c) What are the policies of CAINE?

6. As soon as your dump finishes, start a tool to create a timeline on the image. This can take a long time, so either (1) tune the tool to do less work, or (2) go for the full scan and use the time to discuss project ideas with your planned project partner. You will need this timeline later in the assignment. `Hints: log2timeline.py, pinfo.py, psort.py, XLSX`

2 Verification

Verification of the retrieved evidence is also required. You are going to exchange your evidence with another group of students. This can be done by sharing your HDD with a different group.

7. Create and describe a method that enables the verification of your method. Write this down in steps that the other team can follow.

8. Exchange HDDs and images with another team. Verify the procedure that they used and the resulting image. Write a small paragraph of max 200 words. Write as if you were verifying the evidence gathering procedure for a court case.

3 Live Forensics

Procedures and preferences change during live forensics acquisition. Take, for example, memory into account.

9. What kind of things would be less important during live acquisition?

10. What would be different in your method?

11. Describe the new method that you would use to gather data during live forensics. Make sure to categorize by priority.

4 Technical analysis

12. Mount your image and make sure that it is mounted as read-only.

13. Identify and write a small paragraph of max 200 words about what kind of image it is. Don't go into file specific details just yet. This includes but is not limited to:

(a) What is the size of the image?

(b) What partition type(s) does this image have?

(c) Does it have an MBR/GPT?

(d) etc.

14. Using the information from the timeline you create above, write a small paragraph on what you think happened on this specific HDD device. Make it a maximum of 300 words. Please remain objective, as you would preparing evidence for a court case

15. What would help to investigate this evidence further?

16. OPTIONAL: There is much more to find on this HDD than you will have time for during the official lab hours. You can turn finding all evidence into a competition with your fellow students, or a joint effort where you collectively try to analyse the disk more thoroughly.