CCF Lab 1 - Data Acquisition

This lab will introduce you to forensic imaging and data handling using a live environment. You also will work in groups (2 persons per group) in Task 3.

Task 1 - Setting up your environment

You need to prepare 2 USB drives.

- The first one should have a CAINE live environment that will be used to collect evidence.
- On the second one (this drive will be called drive A) you should deploy that disk image. The disk image is compressed with special utility that preserves original bits intact. You should uncompress it (using FTK imager) and burn it on the flash drive (do not forget about unallocated space).

Task 2 - Imaging

1. Discuss how you can retrieve an image from an, currently off-line, USB stick 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 / dc3dd, kpartx.
3. Follow your method to retrieve the image from drive A. Please use timestamps, explain every tool and note down the version. For the purpose of speed. Make sure both team members have access to the retrieved image. You can use your PCs as an evidence sharing platform.
4. Read about CAINE Linux and its features while waiting on the dump to finish.
    1. Why would you use a Forensic distribution and what are the main differences between a regular distribution?
    2. When would you use a live environment and when would you use an installed environment?
    3. What are the policies of CAINE?
5. As soon as your dump finishes, start a tool to create a timeline on the image. You will need this timeline later in the assignment. *Hints: log2timeline.py.*

Task 3 - Verification

Verification of the retrieved evidence is also required. You are going to exchange your evidence between your group of students. This can be done by sharing your USB device (drive A) with your teammate.

1. Create and describe a method that enables the verification of your method. Write this down in steps that your teammate can follow.
2. Exchange USB images with your partner. Verify the procedure that he 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.

Task 4 - Technical analysis

1. Mount your image (image of drive A) and make sure that it is mounted as read-only.

2. 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:
    1. What is the size of the image?
    2. What partition type(s) does this image have?
    3. Does it have an MBR/GPT?
    4. etc.
3. Using the information from the timeline you create above, write a small paragraph on what you think happened on this specific USB device. The device owner is suspected in a crime. Try to find the evidence that can support this accusation. Please remain objective, as you would be preparing evidence for a court case. Make it a maximum of 300 words, and use timestamps.
4. What would help to investigate this evidence further?