DFSC1316: Digital Forensic and Information Assurance I

Lab 5 disk imaging and file recovering

This lab is to introduce you with the basic concept and skills of making images of a disk, and using automated tools to conduct basic forensics investigation based on the image.

Note that the whole procedure is extremely simplified and you should not assume a real investigation is actually conducted this way.

Install FTK Imager

1. go to http://accessdata.com/product-download/ftk-imager-version-4.1.1 and download FTK Imager version 4.1.1. You will need to provide your personal information in order to obtain the download link. At least you will leave your real email since you will receive the download link from there.
2. FTK (Forensics Tool Kit) by AccessData is a leading software in digital forensics field. The FTK Imager is a free and small application provided by AccessData that can be used to create and analysis disk images.
3. Install FTK Imager on your computer.

Operate the floppy

1. A floppy disk and a floppy drive is provided. Floppy was the mostly used storage media in the 90's and early 2000's. You ever wonder why your hard drive starts with the letter C? This is because A and B is assigned to floppy, and this convention does not change even though we never use floppy that much nowadays.
2. Plug the floppy drive into your computer. Your computer should automatically recognize it, and give it the letter A.
3. Create a text file named DFSC1316.txt on the floppy disk. Open the file, and type "hello from DFSC 1316 Fundamental of Digital Forensics and Information Assurance", save and close the file.

4. Do something else on the floppy, such as create another text file, copy a photo. Then, delete some files you just created, make sure the DFSC1316.txt is deleted (using "shift + delete" to "permanently" delete them). Bear with the slow speed of the drive.

Question 1 (15 pts): what did you do on the floppy? Briefly describe your operation with screenshots.

Create image

1. Open FTK Imager. Read the help docs if necessary. Create an image of the floppy, and store it somewhere on your computer. The image will be of the **.dd** format.
2. The imaging process will take some time. When it finishes, answer the following questions.

Question 2 (15 pts):

Make a screen copy of the completion prompt.

Question 3 (15 pts):

What is the Hash value of this image?

Analyze image

1. Go to https://www.sleuthkit.org/, download and install Autopsy. Autopsy and The Sleuth Kit is developed by Brian Carrier, which is one of the most popular open-source (i.e., free) software for disk forensics investigation.
2. After the installation, start Autopsy, click on Help tab, and read the help document either online or offline.
3. Based on the help doc, load the floppy image you just created, and do analysis. All the functions of Autopsy are clearly explained in its help doc, and you can ask me for any questions.
4. After the automated analysis, look at the result. And answer the following questions.

Question 4 (15 pts):

Are you able to recover the DFSC1316.txt file you just deleted? Attach a screenshot of your result.

Question 5 (40 pts):

Based on what we have discussed in class, and your online search, try some ways to "actually" erase the DFSC1316.txt, that is, make the file really gone from the floppy and can't be recovered even with forensics tools. You probably need to redo the previous steps multiple times, i.e., you'll first try some operation on the floppy, and create the image, and then load the image into Autopsy to see if the file can still be recovered.

Write down and briefly describe what you have tried, and you should at least find one way that can effectively erase the file from the floppy.