Lab 4 - Forensic Analysis

Part I - Image Acquisition and Analysis

A tool called `foremost` can be used to view existing as well as deleted files. Remember that when we are carving, we only want to take a snapshot of the existing filesystem and not modify the current filesystem.

I have provided an image that I want you to look at.

Image

You should analyze the image and see what you find. A 'key' that you might find useful is 'forensics'. You will also want to mount the iso. You can do this with the mount command and `-o loop`. As in `mount -o loop file.img temp\` where `temp` is a directory that you have created and `file.img` is the file that you have downloaded.

You will want to look in a directory in the image for a file called index.dat. Look at what my browsing habits were to perhaps figure out what I might have downloaded or created. Take a screenshot of my browsing history.

You will obviously want to use a tool like `foremost` to analyze the image (can't do it while it is mounted).

Make a list of everything that you have found, screenshot as applicable. Put it in a single PDF document.

Part II - Other forensics tools

Experiment with another computer forensics tool of your choice. You might experiment with a different tool within the kali distro, or download another of your choice. Become familiar with the tool.

In a half page summary write up your synopsis of the tool. You might want to answer the following: 1. What does the tool do? How does it work? 2. What is it good for? How would a forensic investigator use the tool? 3. Was it cool?

Include a screenshot of the tool.

To Pass Off

Upload the PDF document of the above stuff by the required due date.