Lab4: Memory Analysis

- Make sure the folder "lab4" is in folder C:\ftklab

- Open FTK Imager.
- To capture data stored in the memory within a running system.
- From the File menu, select Capture Memory.
- You need to select the destination folder for the memory to be located in. But for this lab, you will be using created memory images, so click Cancel.

- Add the evidence file "lab4-1".
- Right click on the evidence to verify the image.
- What is the computed MD5 hash and SHA1 Hash?

- Switch to hex format.
- To find if the Notepad, WordPad and command prompt were running on this machine
- Right click and select Find
- Choose the type of search text
- Search for these words individually (Notepad, WordPad, command prompt, password).
- Click on Find next or F3, to find the next word.
- Change the setting of the search from down to up, to see the difference.
- From the file menu, select remove all the evidence items

- Then, add the evidence file "lab4-2"
- Search for the words "password, www, org, .com, edu, http "
- Use find to check if the Internet Explorer/Firefox was running on this machine?
- Add the evidence file "lab4-3" and do the same search.