Lab2: Acquiring an image

- Make sure lab1.e01 is in folder C:\ftklab

- Open FTK Imager.

How to create RAW image!

- From the File menu, select Create Disk Image.
- Select the Source Evidence type "Image file".
- Select Evidence Source Selection Lab1.e01.
- Click on Add Image destination, and select the destination image type Raw (dd).

- Add evidence item information:

Case number:1
Evidence Number: 2
Unique Description: My first case
Examiner: Your name

- Image destination folder select "ftklab", and name the file "evidence1".
- Click finish.

To calculate MD5 and SHA1 hashes of the acquired image!

- Make sure the option verify images after they are created is selected.
- Click start, to start the acquisition.

Check the results of verification are they matching?
Click image summary to see the information of the created image.

- Open the folder "ftklab", how many files has been created?
- Open the notepad file to see all the information of the created image.

What is the different between the tow images (lab1 and evidence1)?

- Add evidence item to see the contents of this image.
- Search for jpg files
- Check date modified

What is the signature of a jpg file?
Check the headers on hex view; what is the hex value of jpg file?
What is the hex value that this file ends with?

- Close FTK Imager.