Lab3: File signature analysis

- Make sure lab33.E01 is in folder C:\ftklab
- Create a folder on the C drive and name it “evidence”.

- Open FTK Imager.
- Add the evidence (the image file lab33.E01).
- Verify the Image.
- Does the acquisition and verification hash match?

- In the evidence file, search for the folder “FileSignatureAnalysis”.
- How many files located under this folder?
- How many files are visible (as picture)?
- Check the signature of these files; is it JPG signature?
- What is their extension?

- What is the hex value of the file “jpeg image renamed extension.dll”?
- Are you able to see this picture?
- Right click on this file and select Export Files, to the folder “evidence”. Try to view this file with another program (e.g. Windows Photo Viewer).
- What was the problem with this file “jpeg image renamed extension.dll”?

- How many pictures did you find with incorrect extensions?

- What is the hex value of this file “jpeg image with bad or unk header”?
- What is the extension of this file?
- Why you can not see this picture “jpeg image with bad or unk header”?

- Remove all the evidence
- Close FTK Imager