Computer Forensics and Cybercrime - 7CCSMCFC – Dr Richard E Overill
Forensics Lab "FTK Imager" – By Noora Al Khater
Lab TA - Matus Vadura

Lab1: Add Evidence

This is an introductory lab on how to use FTK Imager

- Login to CentOS
- Start virtualized Windows and login there
  (Applications -> System Tools -> Microsoft Windows)
- Copy folder 7CCSMCFC from This PC -> Network Drive mnt/nms-tier2/kcl-project/ForensicCourse/7CCSMCFC to C drive and name it ftklab

Open AccessData FTK Imager

- Login using following User name and Password
- User name: .\ftk
- Password: Labwork17

Add evidence

- From the File menu, select Add Evidence Item
- Select the Source Evidence Type, Image File.
- Click Next
- Select the image "Lab1.e01"
- Click Finish

Search in the evidence files
What type of system do you find?
By looking at the folders in the evidence tree you can know the system type.

From the view menu you can change the sitting of the view.

Verify Image:

- From the File menu, select Verify Drive/Image
- Or right click on the image in the evidence tree, and select Verify Drive/Image

Check the result of verification (MD5 Hash, SHA1 Hash) is it matching?
Is there any bad sector?

When you finish!

- From the file menu, select Remove all evidence Items.
- Close FTK Imager