Lab Assignment 2

# Task – Working with evidence

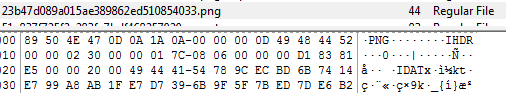
In this assignment you will be introduced to the basics of forensic evidence validation and preview. This lab may require access to the Cone Forensics Lab. Items in **RED/BOLD** are deliverable. If we have not already covered the definitions for certain terms, or you are unfamiliar with them, I have included some below.

The following items are represented in FTK Imager:

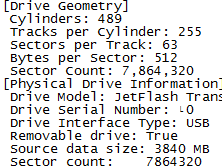
**SQL Lite**: A self contained database popular in Apps and web browsing.



**PNG**: Portable Network Graphics, a graphic file used in conjunction with JPG and others on the Internet and by many types of applications. Identifiable by the “.png” extension and the File Signature “89504E47” or “ PNG” in ASCII.



**Sector**: The smallest unit of measure for disk storage. Sectors are normally 512 bytes (4096 bits) or greater.

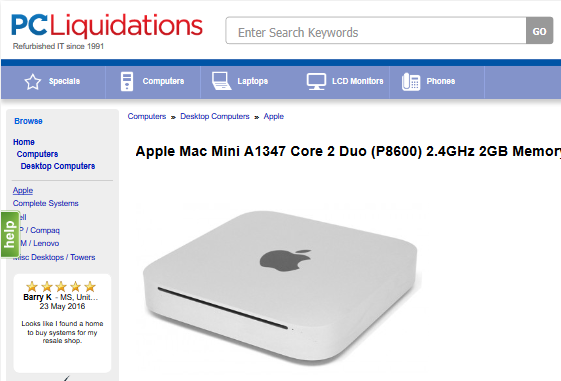


1. From a workstation: access the server’s shared directory and copy the file ‘CoffeeShopThumb.e01’ and ‘PortableThumb.e01’ to your Desktop in a folder you create for this exercise. Don’t forget to copy the log files also!! These files can be found at [\\cci-forensic\forensic\Labs\CoffeeShopper](file:///\\cci-forensic\forensic\Labs\CoffeeShopper)\ and [\\cci-forensic\forensic\Labs\CoffeeShopper\Portable\](file:///\\cci-forensic\forensic\Labs\CoffeeShopper\Portable\) If the files are already there, remove them and make a fresh copy.
2. Create a TXT file in the same folder. This file should be named Lab1\_[name], where [name] is your first and last name.
3. Open FTK Imager and use the green ‘+’ icon to add items to FTK Imager.



* 1. Look at the properties window for both images and note geometry, serial number and md5 hash information if they exist.

1. Right click on the images you loaded into Imager. Select “Verfiy”. Be certain the images are unaltered.
2. Open your text file and enter answers to the following questions:
   1. **Judging by geometry, hash value, folder structure and the log files do these images appear to be of the same thumb drive? How are they similar and how are they dissimilar?**
   2. **How many sectors do each of the images represent in total? Are there any errors showing one image did not record some of the sectors?**
   3. **Can you locate the following picture and where did you find it? (Hint: a file listing spreadsheet is provided with the .e01 files, look for png files there and browse to that location with Imager)**

****

1. Ensure you have SQL Lite Browser installed ([www.sqlitebrowser.org](http://www.sqlitebrowser.org)) and find the places.sqlite file from the Firefox portable \Interwebz\FF\Data\Profile\. Open the file with SQLite and select the Browse tab. Find the moz\_places table and then locate the visited page with this title “Apple Mac Mini A1347 Core 2 Duo (P8600) 2.4GHz 2GB Memory 320GB HDD”.
   1. When was this page accessed? The date is in epoch format and will need to be converted (try www.epochconverter.com).
2. Verify the images once more to ensure you have not altered them.
   1. Was a record added to your log file to show you verified the image?
3. Use the answers in you TXT and your screen captures to write a SANS style forensics report.
4. Once you have completed your report and provided to Elizabeth for grading, please remove the E01s you created from the local machine. You may delete your lab files folder as well if you have a copy to provide to Elizabeth.