Lab Assignment 1

# Task – Working with evidence

In this assignment you will be introduced to the basics of forensic evidence acquisition and verification. This lab will require access to the Cone Forensics Lab. Items in **RED/BOLD** are deliverable.

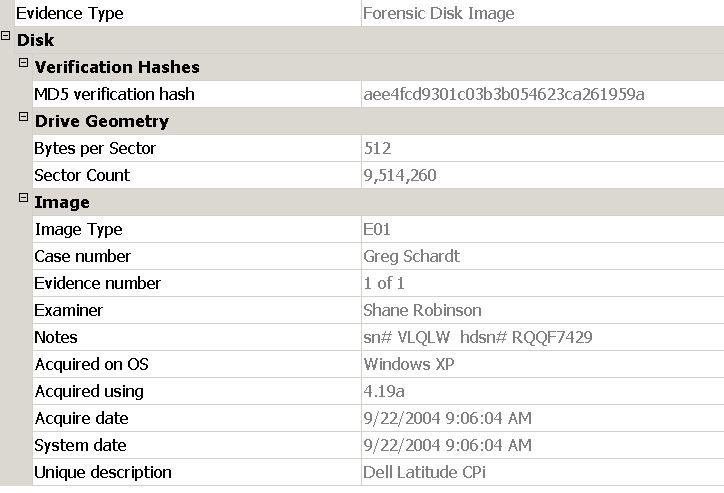
If we have not already covered the definitions for certain terms, or you are unfamiliar with them, I have included some below.

**Forensic Image**: A bit for bit copy of a physical piece of of media, which can be verified to be identical to the original through a mathematical formula (known as hash comparison). Examples include DD (RAW), E01 (EnCase Expert Witness Format), AFF, SMART.

**HASH value**: A number, often represented as a string of hexadecimal characters, used to verify a piece of data as identical to another.

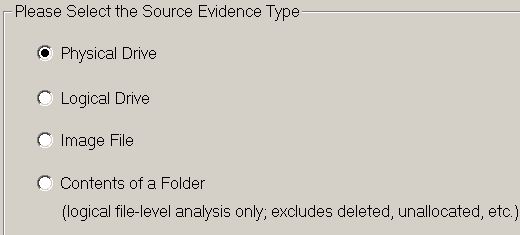
**Geometry**: Disk or Drive Geometry are represented as Cylinders, Heads and Sectors after the tradition of spindle based mechanical hard drives. The numbers for CHS can be used to calculate drive size by finding the total number of sectors across all platters in the disk drive. In modern drives, this number is translated to Logical Block Addressing (LBA) and each sector can be addressed in linear order. In FTK Imager Geometry is represented by a total count of sectors and the specified size for a sector on the original disk.

In FTK Imager, these items can be seen outlined in red in the graphic below:



1. From a workstation: access the server’s shared directory and copy the file ‘nps-2008-jean.e01’ and ‘nps-2008-jean.e02’ to a folder on your desktop. If the file is already there, remove it and make a fresh copy. Create a folder on your desktop.
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.



*Optional: Try to add a physical drive (your workstation hard drive should be* [*\\PHYSICALDRIVE0*](file:///\\PHYSICALDRIVE0)*), an image file (use nps-2008-jean.e01) and a folder containing files (the folder you created). What are noticeable differences in the representation of an image file and the physical drive? *

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

1. Right click on the nps-2008-jean.e01 image you loaded into Imager. Select “Verfiy”. Use the snipping tool (Start Menu, search snipping tool) to create a screen capture of the result. Save the capture to your folder as Verify\_[name], where [name] is your first and last name.
2. Open your text file and enter answers to the following questions:
   1. **What was the MD5 hash value for nps-2008-jean.e01?**
   2. **What file systems are present within nps-2008-jean.e01? (FAT32, NTFS, EXT3, Reiser, ZFS, UDF, etc)**
   3. **What is the total file size for nps-2008-jean.e01 + nps-2008-jean.e02, and what was the size of the original device (hard drive) that nps-2008-jean.e01 is imaged from?**
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 Renee` via canvas for grading, please remove the E01 you created and the copy of nps-2008-jean from the local machine. You may delete your lab files folder as well if you have a copy to provide to Renee`.