

ITIS 5250  
Parag Mhatre  
Lab #1  
September 15<sup>th</sup>, 2018

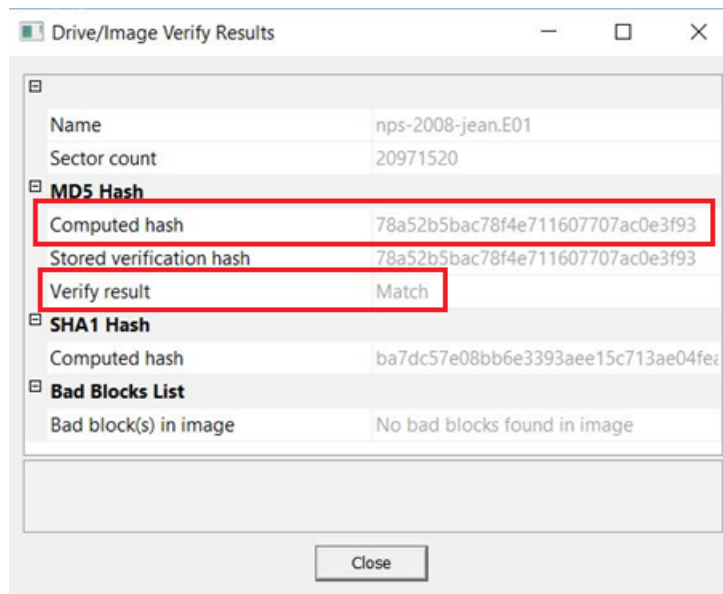
### **Overview:**

In this Lab, I have been given two files, viz. “nps-2008-jean.E01” and “nps-2008-jean.E02”. I have been asked to make use of the “FTK Imager” tool, and from the file, extract data like the MD5 Hash value, the file systems present in the image, the size of the original drive and compile a Forensic report.

### **Forensic Acquisition & Exam Preparation**

I accessed the Forensic image in the Shared Folder on the network through the Forensics Lab in Cone 169 and transferred it to my device.

The software used for accessing & extracting information from the image is FTK Imager 4.1.1.1. The first step undertaken after accessing the image file was the Hash verification. The MD5 Hash of the image is as given in the image below:

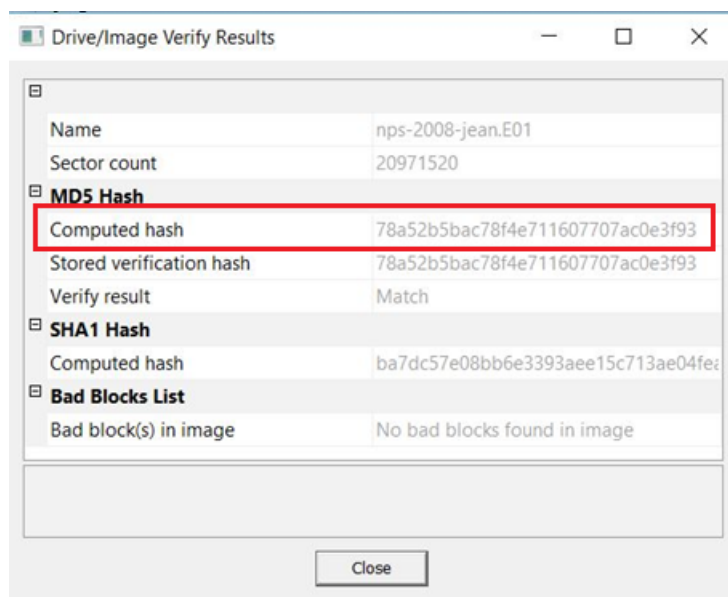


### **Findings and Report (Forensic Analysis)**

#### **a. What was the MD5 hash value for nps-2008-jean.e01?**

The E01 file was added to the FTK Imager using the “Add Evidence Item...” option from the File Menu. Once the Image was loaded, I selected “Verify Drive/Image” option by right clicking on the “nps-2008-jean.E01” under the Evidence Tree in the left pane of the software.

The MD5 Hash value that was calculated by the FTK Imager as shown in the image on the next page is: **78a52b5bac78f4e711607707ac0e3f93**



**b. What file systems are present within nps-2008-jean.e01? (FAT32, NTFS, EXT3, Reiser, ZFS, UDF, etc)**

The file systems present within nps-2008-jean.E01 is **NTFS**. I found this by reading the first few bits of “Partition 1” – the only partition in nps-2008-jean.E01

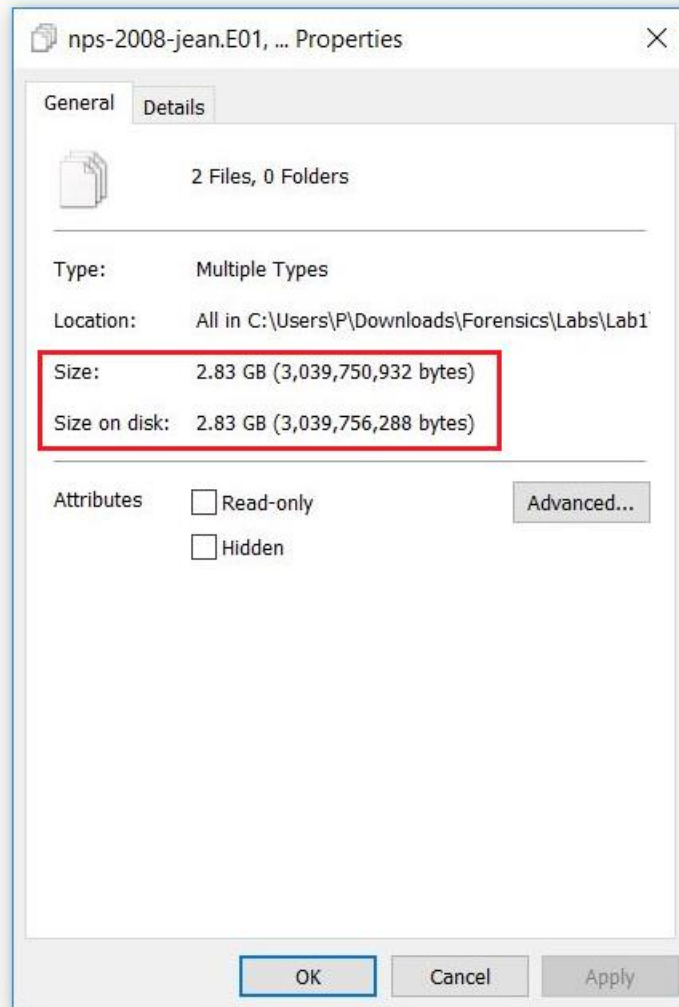
Cursor pos = 0; log sec = 0; phy sec = 63

Listed: 0 Selected: 0 nps-2008-jean.E01/Partition 1 [10228MB]

- c. 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?

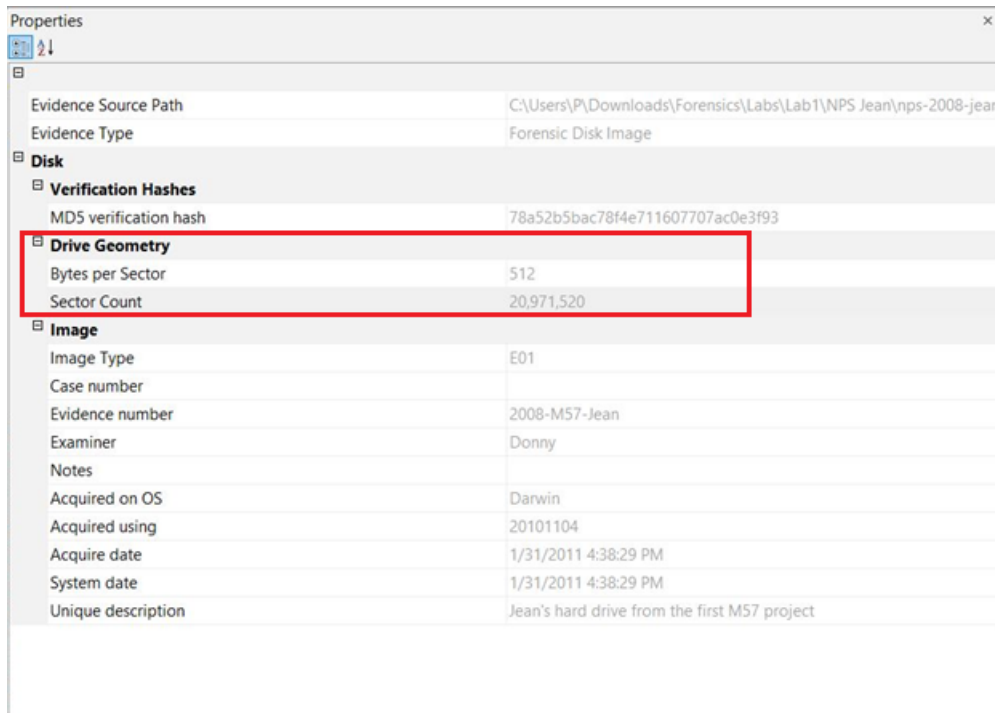
The combined file size of the files “nps-2008-jean.E01” and “nps-2008-jean.E02” is **3,039,750,932 Bytes**. I found this by selecting 2 files in a single selection and viewing the properties of the selection in Windows.

Lab1 ParaqMhatre.txt	9/15/2018 2:42 AM	Text Document	1 KB
nps-2008-jean.E01	3/27/2016 8:41 PM	E01 File	1,535,997 ...
nps-2008-jean.E02	3/27/2016 8:41 PM	E02 File	1,432,511 ...



The file size of the original drive that the nps-2008-jean.E01 was **10,737,418,240 Bytes**. I found this by checking the total number of sectors and multiplying that with the number of bytes per sector. I found this information in the “Drive Geometry” section shown after selecting “Properties” from the “View” Menu.

i.e.  $20,971,520 * 512 \text{ Bytes} = 10,737,418,240 \text{ Bytes}$



Properties	
Evidence Source Path	C:\Users\P\Downloads\Forensics\Labs\Lab1\NPS Jean\nps-2008-jean
Evidence Type	Forensic Disk Image
Disk	
Verification Hashes	
MD5 verification hash	78a52b5bac78f4e711607707ac0e3f93
Drive Geometry	
Bytes per Sector	512
Sector Count	20,971,520
Image	
Image Type	E01
Case number	
Evidence number	2008-M57-Jean
Examiner	Donny
Notes	
Acquired on OS	Darwin
Acquired using	20101104
Acquire date	1/31/2011 4:38:29 PM
System date	1/31/2011 4:38:29 PM
Unique description	Jean's hard drive from the first M57 project

### Conclusion:

After acquiring and verifying the forensic image, I performed various operations to find information like the Hash value, file systems present in the drive, the file size of the image and the size of the original drive from which the image was made.