ITIS 5250

Ruchira Pokhriyal

Lab 1

09/21/2018

**Overview:**

In this forensics lab, I am introduced to FTK Imager and the basic concepts of forensic investigation such as verification of hash values of the forensic image, disc geometry and type of file system in the given forensic image. I will perform hash verification, find the type of file system and the original disk size.

**Forensic Acquisition & Exam Preparation**

I first downloaded the image files **nps-2008-jean-e01** and **nps-2008-jean-e02** from canvas, then downloaded FTK Imager version 4.2.0 and loaded the image file in FTK imager.

Image Type : E01

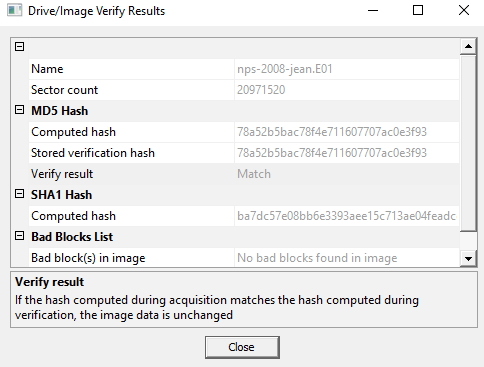
Acquired on OS : Darwin

Acquired Using : 20101104

Acquired Date : 1/31/2011 4:38:29pm

System Date : 1/31/2011 4:38:29pm

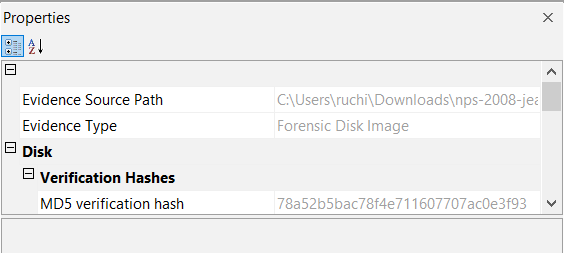
The verified hash of the image is as follows:



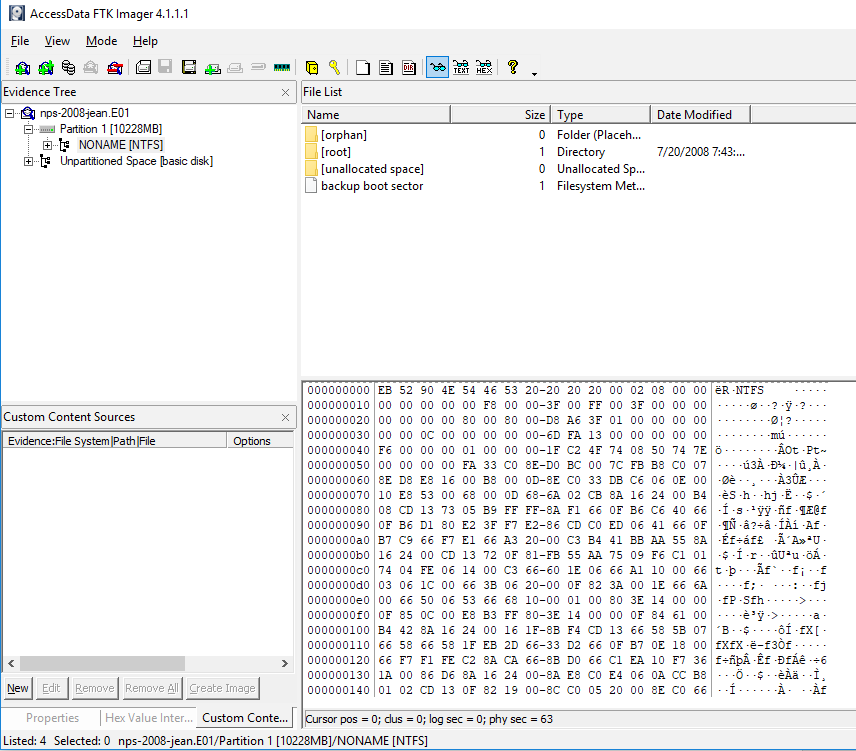
**Findings and Report (Forensic Analysis)**

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

* I loaded the image file by clicking the ‘Add Evidence Item’ icon (the green ‘+’ icon) on the top left in FTK imager. Under the evidence tree, I right clicked on **nps-2008-jean.E01** and selected the ‘ Verify Drive/Image ‘ option. I found the MD5 hash value of the image to be: **78a52b5bac78f4e711607707ac0e3f93**

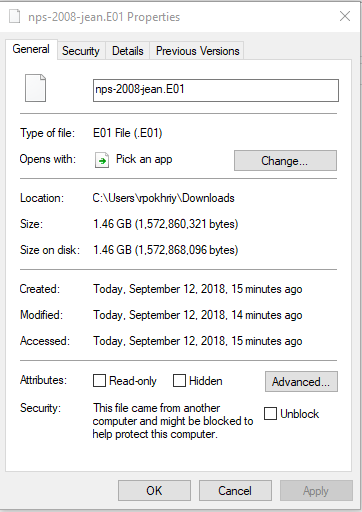
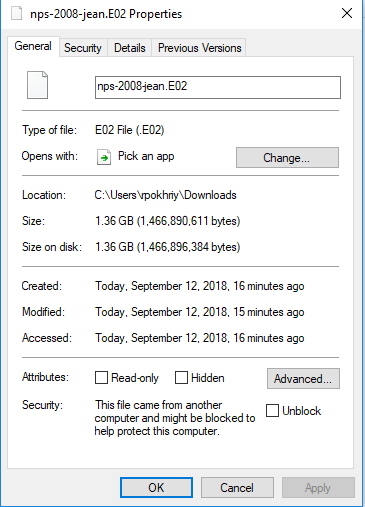


1. **What file systems are present within nps-2008-jean.e01? (FAT32, NTFS, EXT3, Reiser, ZFS, UDF, etc)**

* The file system which is present within nps-2008-jean.e01 is **NTFS**.

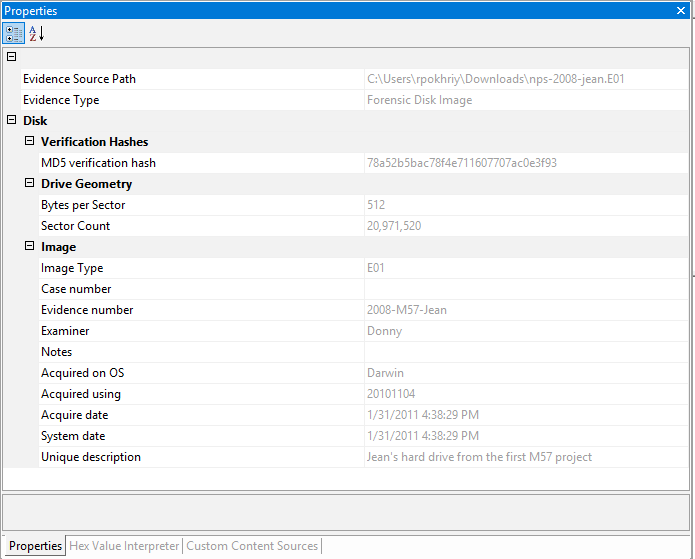
1. **What is the total file size for nps-2008-jean.e01 + nps-2008-jean.e02, an what was the size of the original device (hard drive) that nps-2008-jean.e01 is imaged from?**

* The file size of nps-2008-jean.e01 is: 1,572,860,321 bytes
* The file size of nps-2008-jean.e02 is: 1,466,890,611 bytes
* Hence, the total file size for nps-2008-jean.e01 + nps-2008-jean.e02 is :   
  1,572,860,321 bytes+ 1,466,890,611 bytes = **3,039,750,932 bytes**

These values were found by right clicking on the properties of both the images.

The size of the original device that nps-2008-jean.e01 is imaged from is: **10,737,418,240 bytes**.

This value is calculated by multiplying **Bytes per Sector** and **Sector Count.** To view these values, I selected nps-2008-jean.e01 under ‘Evidence Tree’, clicked on the ‘View’ tab and selected ‘properties’.



**Conclusion**

After loading the image in FTK imager, I verified the integrity of the given image by comparing the two hash values. Furthermore, I found that the file system used is NTFS. Additionally, I calculated the total size of the original hard disk using the properties tab.