ITIS 4250 / 5250

Lab # 1

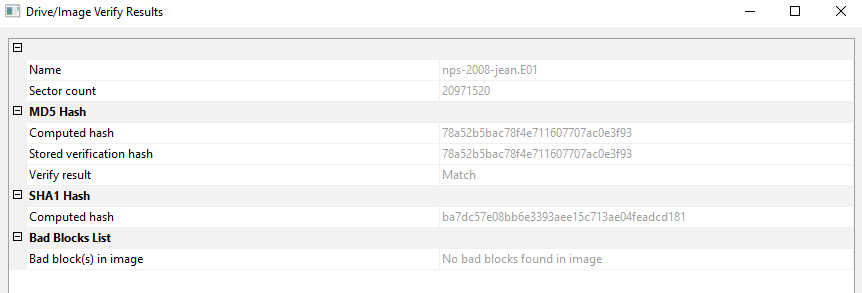
9/12/2019

**Overview:**

Dr. Robert Quincy, the chief Forensic Examiner here at the University of North Carolina Charlotte forensic lab has directed me to verify the ‘nps-2008-jean’ forensic images as well as create a new image by combining these files. There has been proper legal authority consent for this task.

**Forensic Acquisition & Exam Preparation**

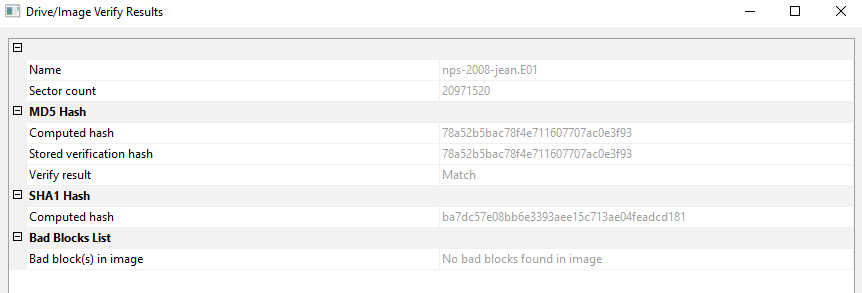
The first step was transferring the files from the Canvas into a fresh folder on my work machine. My machine is a Lenovo Yoga 13 with 8gb of ddr4 ram along with an i5-8500. After transferring the files, the next part of the process was to verify the hash using *Access Data FTK Imager 4.1.1*. When verifying the image, I received the following hash: 78a52b5bac78f4e711607707ac0e3f93



After verifying the image, I conducted export to disk image to create a single file.

**Findings and Report (Forensic Analysis)**

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

**The MD5 hash of ‘nps-2008-jean.e01’ is 78a52b5bac78f4e711607707ac0e3f93. This was found by verifying the image in Access Data FTK Imager** 

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

**The file system that was found within of ‘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?

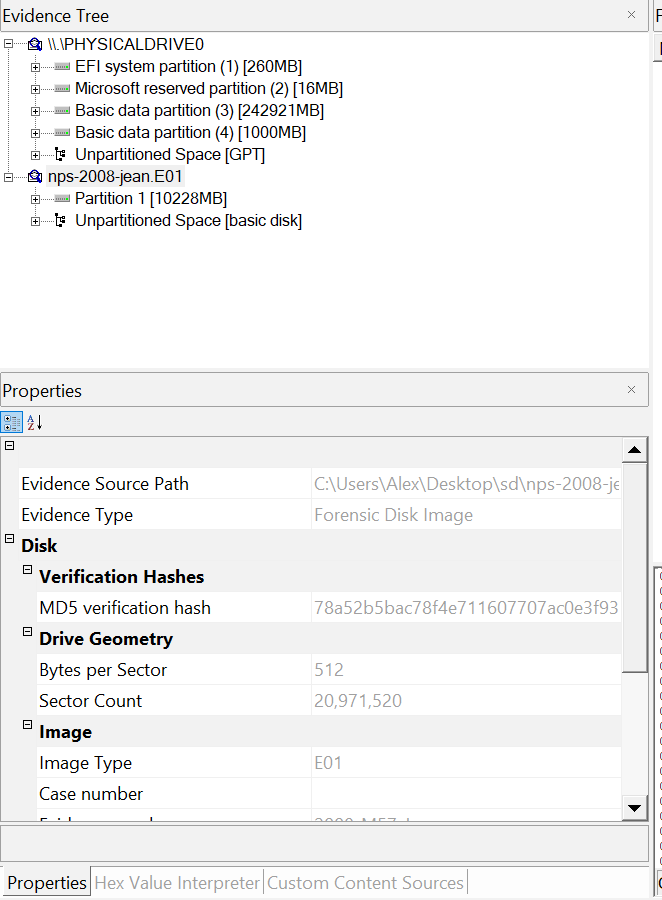
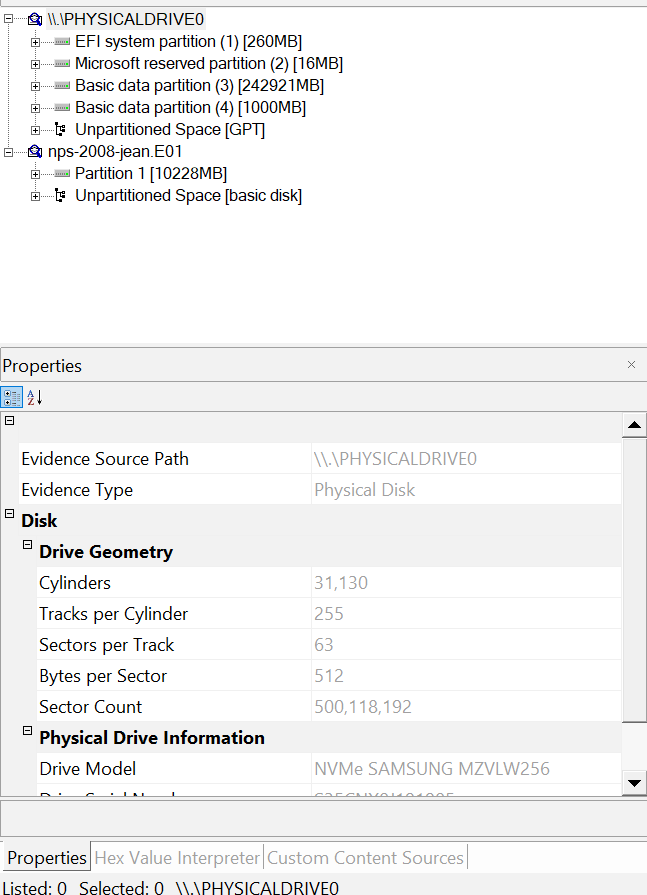
**The total file size of both files combined is 2.83 GB. The size of the original device that is it imaged is 10.7 gb.**

* 1. How are the image and the physical drive different (specifically about the details of their appearance in FTK Imager)?

**The Image differs from the physical drive by containing information regarding the actual image including the type, and other notes used by the examiner. The physical drive contains more information regarding the drive geometry, like Bytes per Sector. It also has a Physical Drive section with the drive model and serial number.**

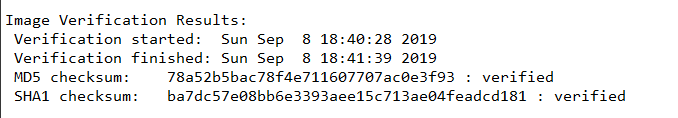
**Left: Image**

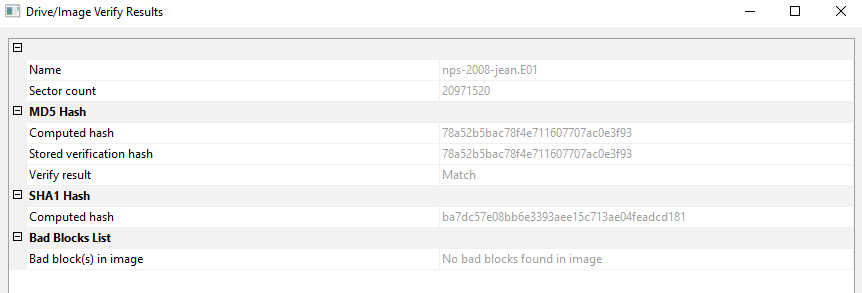
**Right: Physical drive**



* 1. Did FTK imager generate a log for your image? Does this hash value match the original?

**When combining both images together FRK imager generated a log of the image file. When comparing the hash to the original image they match and are the same.**





**Conclusion:**

The nps-2008-jean images have been verified (MD5 hash: 78a52b5bac78f4e711607707ac0e3f93**)** and I have created a new image combining both split images for this report. It was found that the original hard drive was 10.7gb and it contained a NTFS file system. After combining both images a log report was created with the verified MD5 that matched the original image for verification.