**IT IS 5250**

**Sahil Bhirud – 801138029**

**Lab - 1**

**Overview:**

Dr. Robert Quincy, the chief of Forensics Examiner at UNCC Forensics Laboratory, directed me to perform technical work on a forensics image. Specifically, he asked me to verify an image provided by the Cybersecurity Center at UNCC and create a new single image from the given split images.

**Forensic Acquisition and Exam Preparation:**

I began working on verifying the image provided to me. Firstly, I mounted the first image of the two split images in FTK Imager software. Then, I verified the MD5 hash value using FTK and observed that the computed MD5 hash value is the same as that of the original hash value.

A screenshot of a cell phone

Description automatically generated

**Findings and Report (Forensic Analysis)**

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

78a52b5bac78f4e711607707ac0e3f93

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

NTFS

A screenshot of a social media post

Description automatically generated

1. **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?**

Total file size for nps-2008-jean.e01 + nps-2008-jean.e02 = 2.83 GB

A screenshot of a cell phone

Description automatically generated

The size of original device (hard drive) = 10,737,418,240 Bytes

I calculated this by multiplying the number of sectors with the number of bytes per sector (20,971,520 \* 512 Bytes = 10,737,418,240 Bytes).

A screenshot of a cell phone

Description automatically generated

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

The image is divided into Partition 1 and Unpartitioned space while the physical drive is divided into EFI system partition, Microsoft reserved partition, Basic Data Partition, three other partitions and unpartitioned space.

The parameters of the properties also change when it comes to the type of evidence attached. They are Drive Geometry and Physical Drive Information when physical drive is attached and Verification Hashes, Drive Geometry and Image when an image of the disk is attached.

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

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

The FTK Imager does generate a log for the newly created image and the computed hash value also matches with that of the original.

A screenshot of a social media post

Description automatically generated