ENPM687 – Digital Forensics and Incidence Responses

Assignment – 1.2

Author – Syed Mohammad Ibrahim

UMD ID: iamibi

UID: 118428369

Email: iamibi@umd.edu

1.What's your sift computer machine name?

A. The SIFT machine is an Ubuntu 20.04.2 virtual machine, codename Focal. The virtual machine itself is called ENPM687 – SIFT.

2. What's your windows computer machine name?

A. Windows 10 (Host) name is DESKTOP-3BNDREF.

3. Which method did you use to install sift(direct image or command line build)

A. I used the direct virtual machine image from the SIFT official website.

4. What's the IP address of your sift vm compared to your host machine? Why are they different?

A. The IP address of my SIFT VM is 192.168.81.132 whereas the Host windows machine has an IP address 10.0.0.174. The IP addresses are different because of the VMware using a different IP range that are reserved for the virtual machines in a different subnet.

5. Did you face any difficulties or learn anything new during this exercise? If yes, elaborate on one item.

A. I was pretty much aware of how-to setup a virtual machine from an image. However, as a side challenge, I did try installing SIFT from command line on another Ubuntu 20.04 VM which was unsuccessful as the Salt Stack certificates were invalid which are required for installing SIFT on the machine. Specifically, certificate 3001 was unavailable for Ubuntu 20.04 (Py/AMD64).