CIT 425/L Fall 2018 **Homework 2**

*Due to Canvas on **Monday October 8th 2018** at 11:55pm as a single .pdf including all typed answers and screen-shots.*

This work can be done in ***groups of up to 2 students.*** Each such team must include both team members' names on the submission to Canvas. Only one team member needs to submit to Canvas (only one total submission) as long as **all team names are on it**.

---

1. Download an .iso of SecurityOnion (from the official source, to be safe)
    a. Set up the VM with at least 4 GB of DRAM and at least 20 GB of hard drive.
    b. Boot the live OS from the .iso file
        i. When the Desktop loads, click the appropriate icon to install the OS on your computer (really a VM).
        ii. Reboot as necessary to complete the installation.
        iii. Open a terminal, and run …

            sudo soup

            (which will update your SecurityOnion installation)
        iv. At the top of your virtual machine window, select Devices->Install Guest Additions…
            1. Then inside a terminal, change-directory to /media/
            2. Find the subdirectory that has VBoxLinuxAdditions.run using the find command
            3. Change to this subdirectory and run…

            sudo ./VBoxLinuxAdditions.run

        v. Click the Setup icon on the Desktop
            1. Your VM is probably on the NAT network, so you can use DHCP to set up the network.
            2. **After the reboot, *launch the Setup icon again!***
            3. Set up usernames and passwords for the various SecurityOnion agents.
            4. Finally, click "yes, proceed with the changes" until you receive a series of message boxes telling you about logs, PulledPork, Snort tools, etc.

2. Take an Oracle VirtualBox *snapshot* of your VM. (You can find this option in the upper right of the VirtualBox manager: Details and Snapshots. You can select Snapshots, and you can then click the appropriate icon to take a Snapshot.)
3. ***Now take a screen-capture of the installation and paste it into your team's submission***

For the rest of this homework, do some research on the web and answer the questions below…

4. What is a .pcap file? Does it have a standard format? What are its contents?

5. What is the tool *tcpreplay*. How does it work?

6. Before using a tool like tcpreplay on a dangerous .pcap file, why is it **mandatory** to disable your network connection from your host operating system, and/or disable the wireless adapter? (In other words, *what is the danger of replaying a .pcap on a VM with a host machine connected to the internet?*)