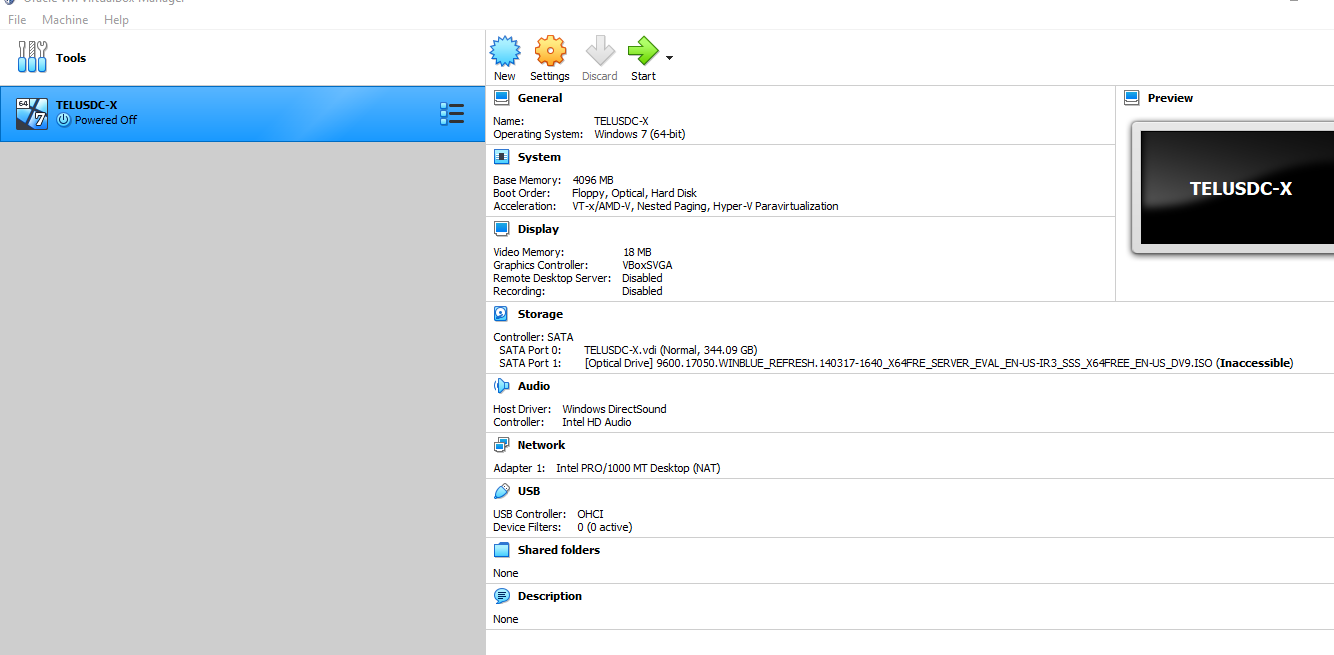
**STUDENT NAME**

**COLLEGE NUMBER**

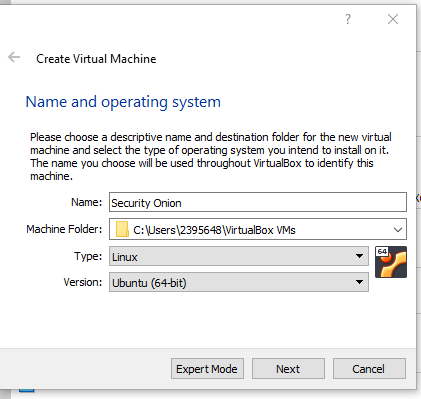
**Introduction**

The labs works through the process of establishing Security Onion on a virtual machine. For this particular activity, the virtual machine chosen was the Virtual Box development environment as shown below.

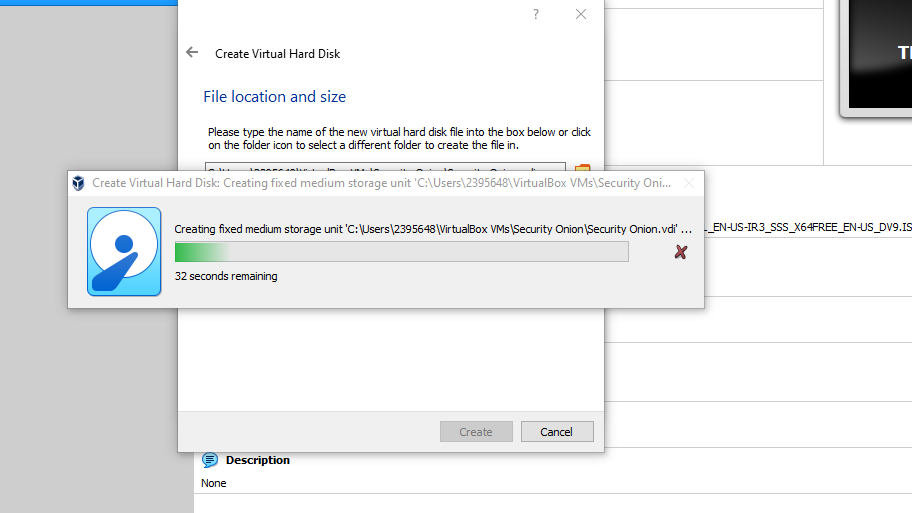


The initial process was to load virtual box and create a new machine. This was done after downloading the security onion image from the official website locate at

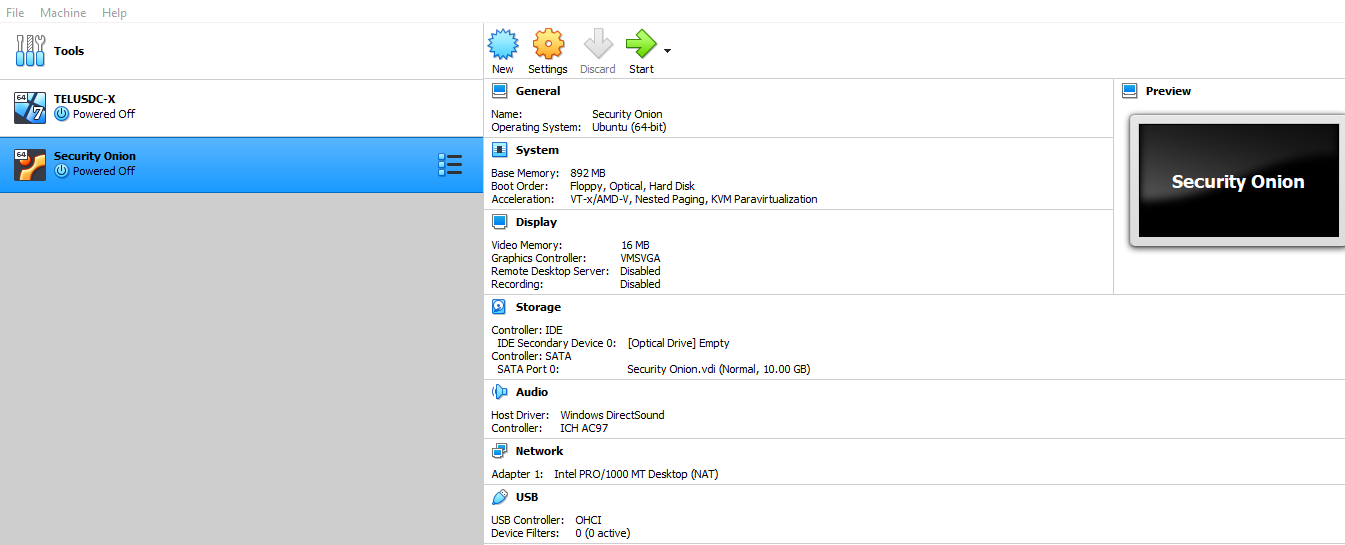
<https://github.com/Security-Onion-Solutions/securityonion/blob/master/VERIFY_ISO.md>



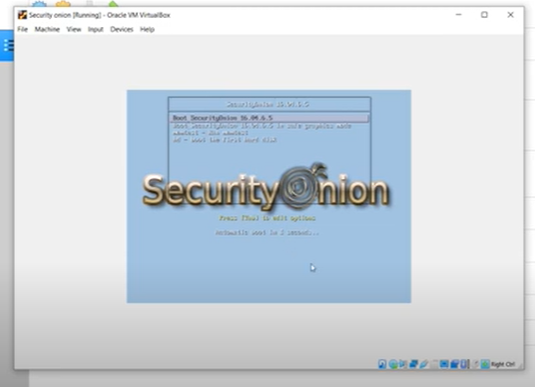
The next step was to give the new Security Onion a name and this context was the ‘security onion’. This was done by selecting the Linux operating system type and then selecting the Ubuntu 64 bit version of the document. The machine getting the folder activities would be automatically stored by virtual box in a location specifically designated by Virtual box itself.



The next step in the installation process was to configure the network requirements of the specific machine. So in virtual box, the settings icon gives certain properties administered by the machine, so the NAT onion was selected for the first option and then selecting bridge network with the local access to the realtek option under it. This is necessary since we would like to monitor the traffic and flow of data flowing within our network. Once all these is done, the new machine is created with details of the machine and the next process is now to start the machine with the given details. However, the machine still relies on and needs the ISO image that was earlier downloaded for boot up. Once the ISO is uploaded, the system goes to directly start undergoing its installation.



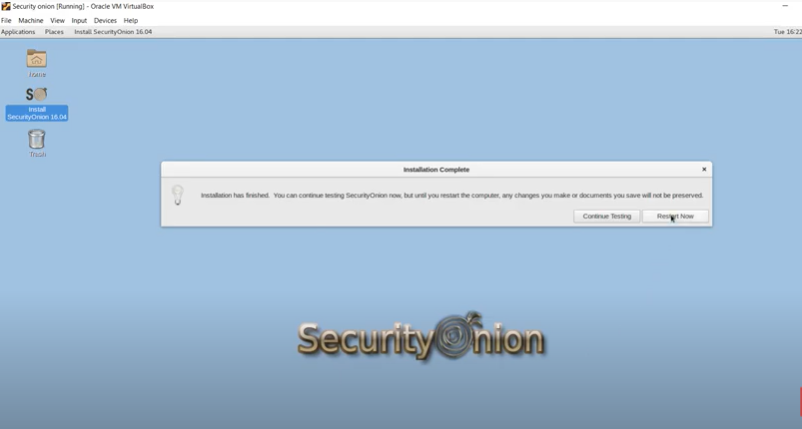
The final loaded OS image installation looks like the one below



However, the installation is not complete until all the Onion files are extracted and downloaded into the system.



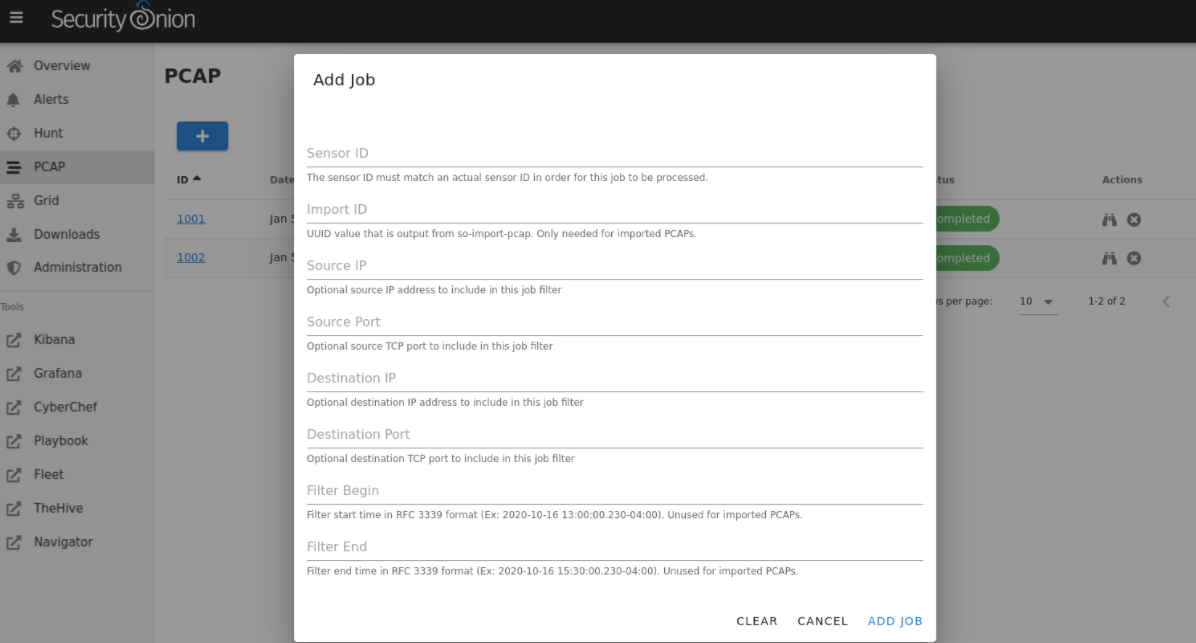
After the installation is complete, we get the window below showing the successful installation and execution of the program. The next step is to try to use this tool and software to capture some network packets.

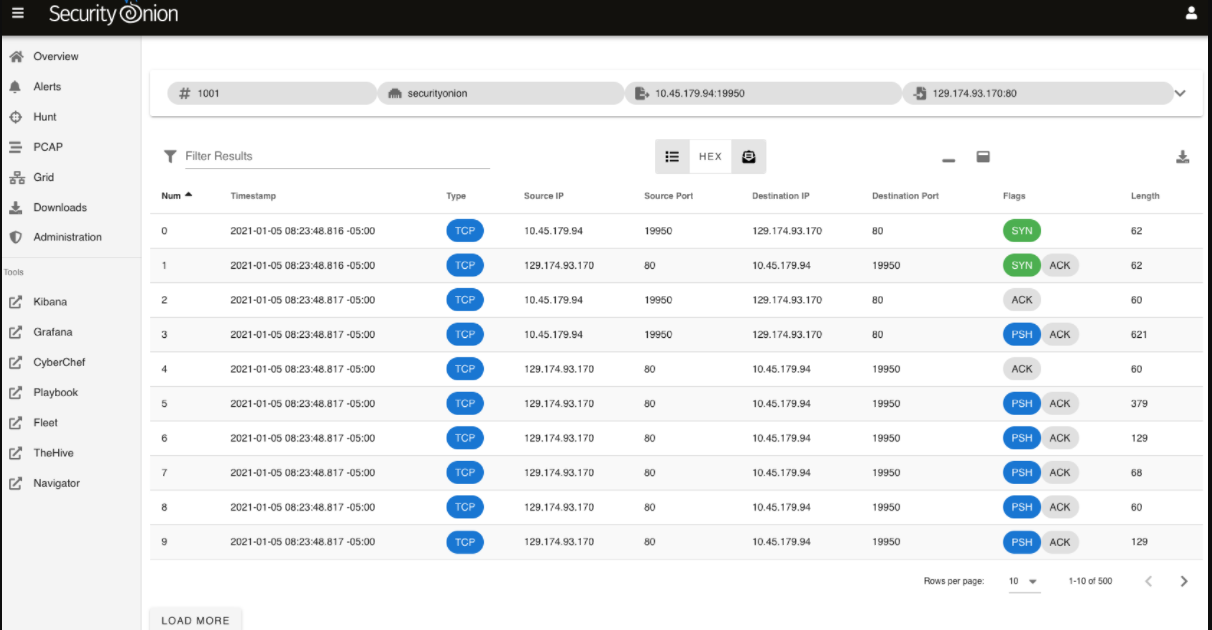


**PCAP**

This tool built inside the packet capture shall help the researcher to capture the network packets during this activity. The PCAP tool built inside the security onion tool helps to capture the data packets of stream of communication running on the TCP and UDP protocols. The captured packets of data are stored in a tcdp dump or tcp file that can be access further using the Pcap on the security onion tool. For this particular exercise, PCAP was used to monitor the transmission of data and packets on the local network address.

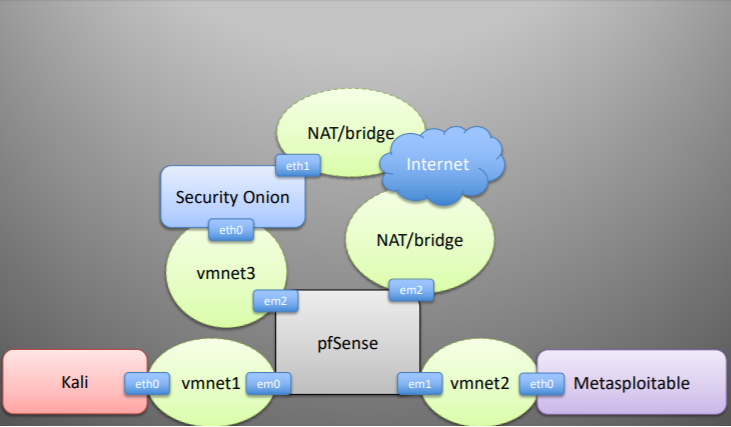
The significance of this is that the PCAP packet sniffer tool can always be applied and used on the network to detect abnormal activities on the network such as network intrusions. Where such a case has risen and the network administrator has discovered some case of anomaly traffic network coming or going out of the organisation, the admin can always take corrective action by identifying the source of the network, monitoring its behaviours and then defining its risk level as to whether it’s risky or just normal. Usually risky abnormal packets contain malicious code and should not be allowed into the organising. The network administrator on the hand can therefore take action and bring this IPS down by either blocking the ports that are bringing in the traffic or simple putting up firewalls.





The above diagram shows some of the packets that have been captured by the PCAP network sniffer and some of the statuses on the right.

**Network Architecture**



On the network design architecture above, the adoption is a distributed kind of network architecture where the security onion n application has the NAT sharing and communicating network resources across the environment. The virtual machine extends this and shares other virtual machine resources like the Kali Linux tools of which one of its resources is a database exploit tool called the metasploitable. The other architecture indicated below is linear distribution architecture and does the same activity as the latter mentioned.

