Lab Work 2
Network Security

1. Make sure you have the Security Onion Setup done.

2. Inside Security Onion go to this website link https://www.malware-traffic-analysis.net/2019/12/25/index.html

3. Download the pcap(Don't download and run it in your main OS)

4. Extract and execute using command (tcpreplay -i (int name) -M 10 “pcap name”)

5. For OVA use the command(sudo so-import “Pcap-Name”)

6. Analyze the PCAP and note down the following findings:
   a. **What was the time when this event occurred**
   b. **What are the internal & external IP's**
   c. **What was NIC vendor info for the client**
   d. **What was NIC vendor info for the host/attacker**
   e. **Name of the Malware that infected**
   f. **What was the MD5 hash generated for the malware**
   g. **How did the malware get into the Victim's PC?**
   h. **What are the characteristics of the malware**
   i. **Was there more than one malware at play in this scenario?**
   j. **What is the malware group or family?**
   k. **Summarize the whole event from how the victim got attacked and what data was stolen as per your research**