**ST. FRANCIS INSTITUTE OF TECHNOLOGY**

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**SECURITY LAB**

**Experiment – 10: Study of Intrusion detection system using SNORT**

**Aim:** To study the Intrusion detection system using SNORT.

**Objective:** After performing the experiment, the students will be able to explore and use the Snort-IDS tool.

**Lab objective mapped:** L502.6: Students should be able to apply network security basics, analyze different attacks on networks and evaluate the performance of firewalls and security protocols, such as SSL, IPSEC, and PGP, and authentication mechanisms to design secure applications.

**Prerequisite:** Basic knowledge of network security.

**Requirements:** Windows OS, SNORT

**Pre-Experiment Theory:**

Snort is an open-source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Combining the benefits of signature, protocol, and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide. With millions of downloads and nearly 400,000 registered users, Snort has become the de facto standard for IPS.

Snort can be configured to run in three modes:

1. **Sniffer mode**: It simply reads the packets of the network and displays them for you in a continuous stream on the console (screen)
2. **Packet Logger mode**: logs the packets to disk.
3. **Network Intrusion Detection System (NIDS) mode**: It performs detection and analysis on network traffic. This is the most complex and configurable mode.

**Implementation:**

1. Install snort on your system. Refer/download the snort user manual from its official website [1].
2. Test snort IDS using following commands, observe the output of each command. Take screenshots (SS). Write your observations under each SS.
   1. Snort –V
   2. Snort -h
   3. Snort –W
   4. Snort –i *interface number* -v
   5. Snort –i *interface number* -vd
3. Run following command to use snort in Packet logger mode. View the log file created. Observe the content of log file using any packet logger software (e.g. Wireshark). Take SS of command output, the log file creation and the content of the log file. Write your observations under each SS.

Snort –i *interface number* -dev -1 C:\Snort\log

1. Learn commands to use snort as IDS. Observe the snort rule file *(i.e., snort.conf file)*. Analyze the rule file to configure it for your network environment.

Snort –i *interface number* -dev -l C:\Snort\log -h 192.168.1.0/24 -c snort.conf

**Post Experimental Exercise-** *(to be handwritten on journal sheets. Refer snort user manual for answers)*

1. \_\_\_\_\_\_\_ snort command displays packet header, packet data as well as the data link layer headers.
2. Explain the snort command that will be used for logging the packets on a high-speed network.
3. Explain the use of ‘-h’ option/switch while writing the snort rule.
4. Explain in detail Snort’s NIDS mode output options.
5. Explain the following snort command ‘snort -c snort.conf -A fast -h 192.168.1.0/24’

**Conclusion:**

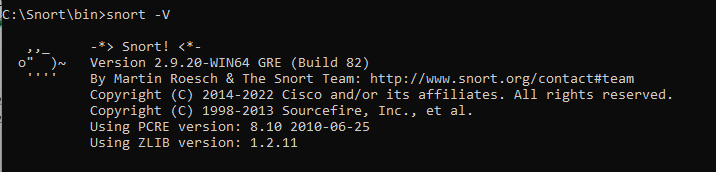
In this experiment we were introduced to most used IPS/IDS software ‘Snort’. Snort acts as a security guard for any network, providing a proactive detection and prevention of any type of intrusion. Snort can perform packet sniffing, logging, and intrusion detection. We studied various options/switches that can be used for writing intrusion detection rules, for sniffing the network and for logging the network traffic.

**References:**

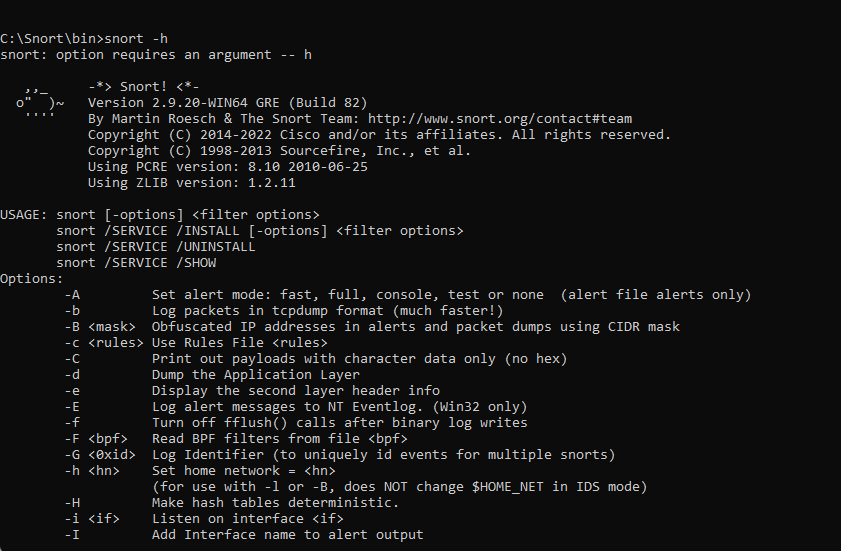
1. “Snort User’s Manual 2.9.16”, <https://snort.org/>
2. Bart Lenaerts-Bergmans , “SNORT AND SNORT RULES EXPLAINED”, <https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/snort-rules/>
3. “Basic snort rules syntax and usage”, <https://resources.infosecinstitute.com/topics/penetration-testing/snort-rules-workshop-part-one/>
4. “Writing Snort Rules with Examples and Cheat Sheet”, <https://cyvatar.ai/write-configure-snort-rules/>
5. “INSTALLING & CONFIGURING SNORT| INSTALASI SNORT WINDOWS 11”, https://youtu.be/V6B8B7\_6gfE

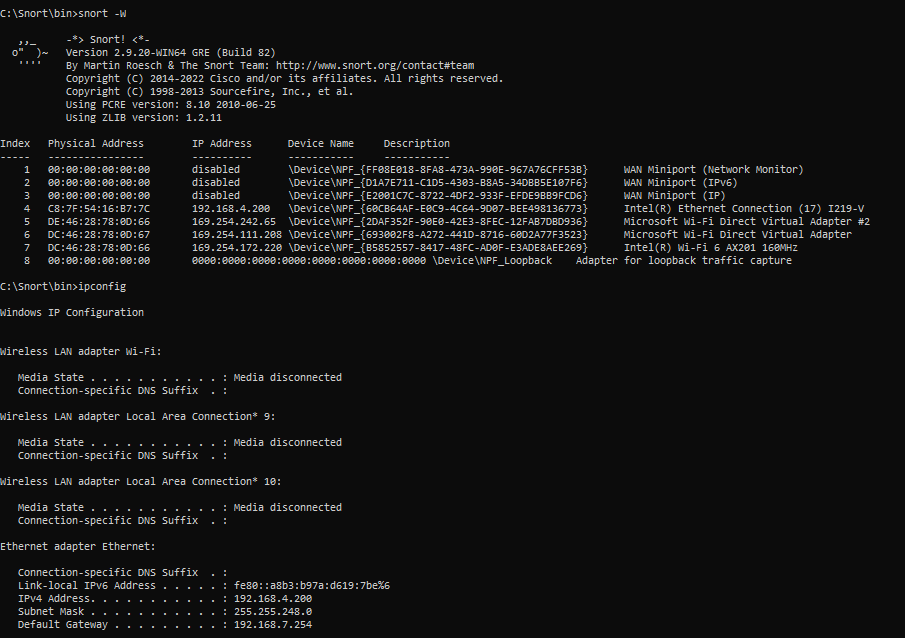
Laboratory Exercise:

Snort -v :Gives the current version of the snort installed

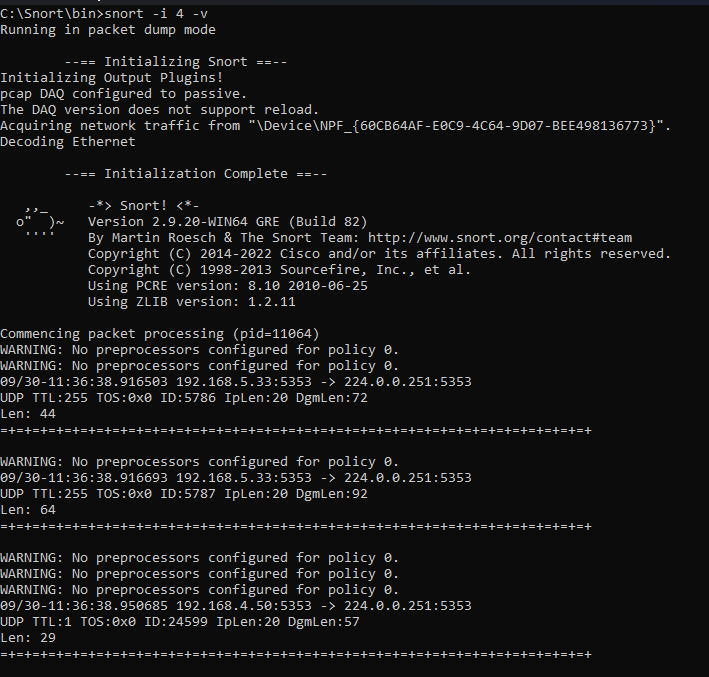


* Snort -h:is the helping tool which gives the meaning of every command along with the ways to use that command.



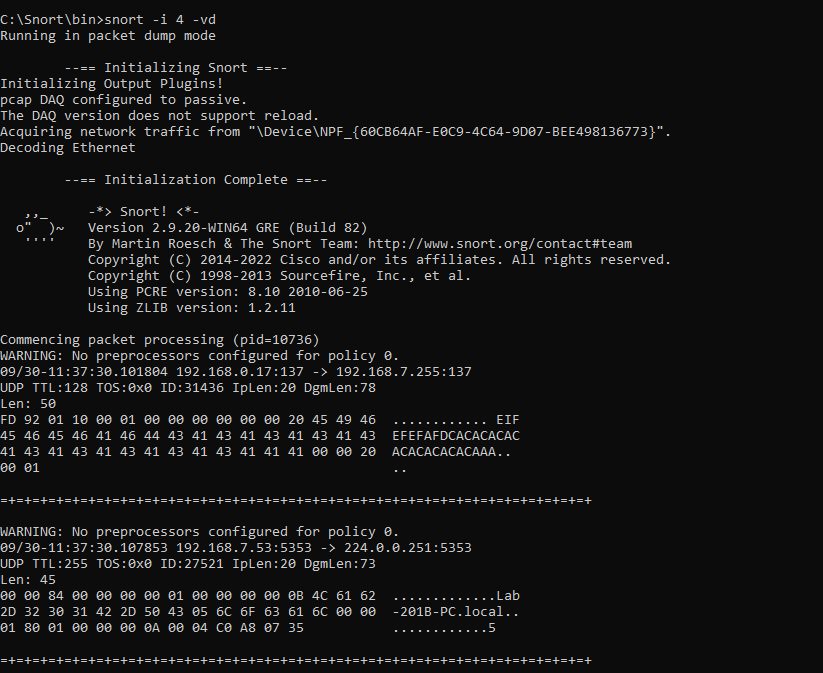


Snort -w: The -w option allows you to specify a file where Snort will write its packet captures in binary format. The packet capture below includes the ip address of the internet connected to the system checked using ‘ipconfig’ command whose index was found to be’4’ along with other connections.



* Snort –i interface number -v

As the index of my system’s IP address was found to be 4,it is used in this command to listen on the interface 4 which is under network intrusion detection.Snort is monitoring the traffic coming in and out of that Ethernet interface 4 which is visible in the attached screenshot.

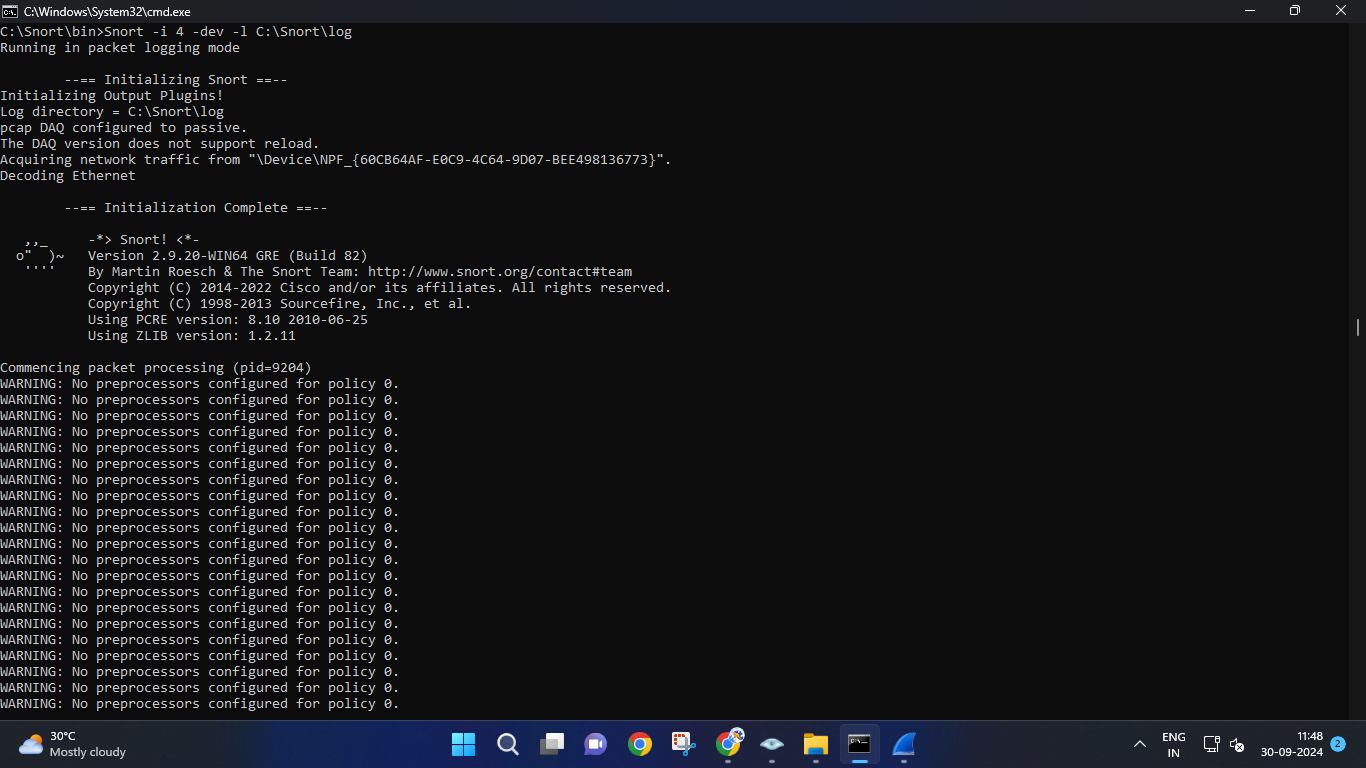


* snort -i interface -vd

-v enables verbose output, which means it will display packet information (such as IP headers) to the terminal in real-time.

-d dumps the application layer data for each packet (payload information), which allows inspection of the actual content being transmitted.

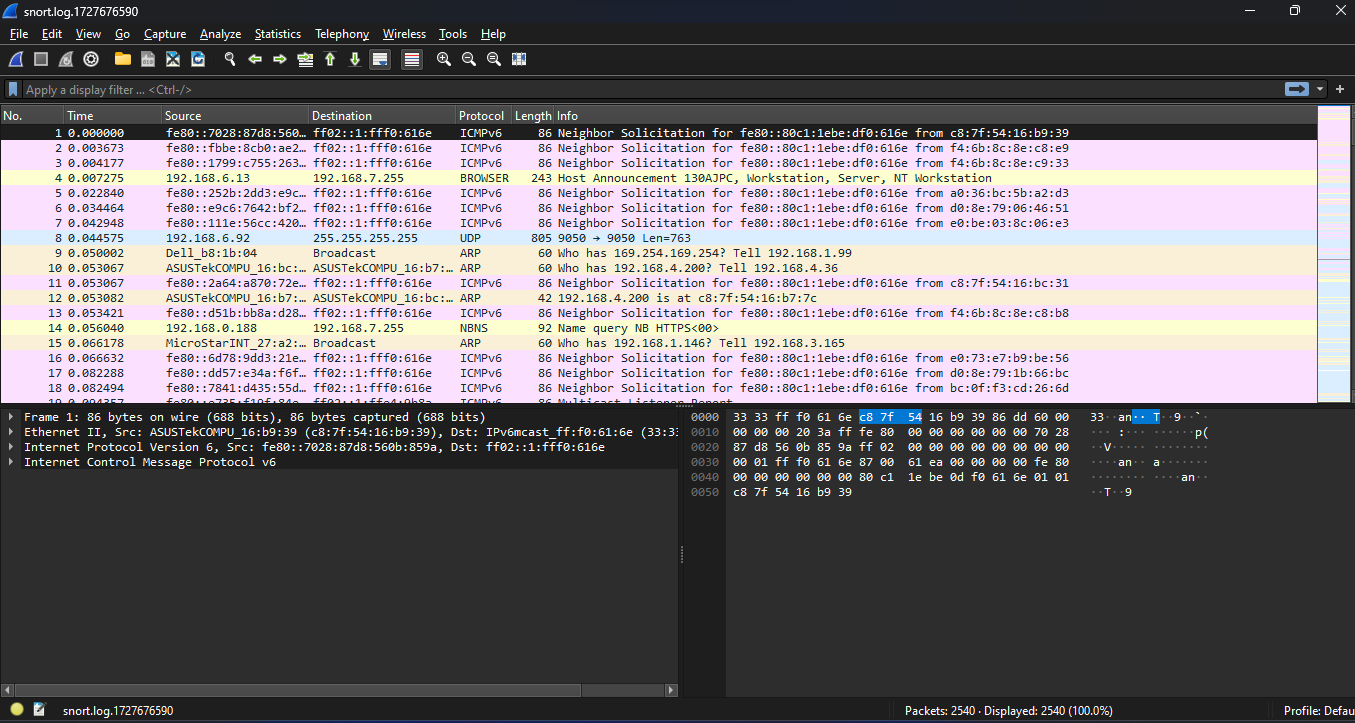
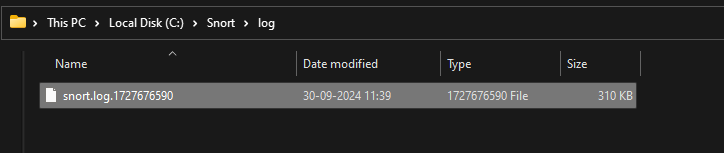
In the attached snippet the interface is listening on the 4th index which reflects my using pc’s IP address.Some packets in the dump mode with the information are seen.

Snort -i 4 -dev -l c:\Snort\log:

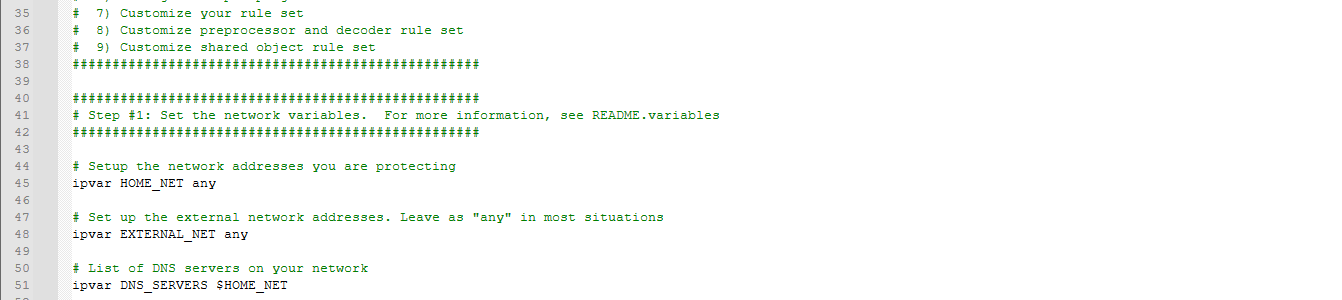
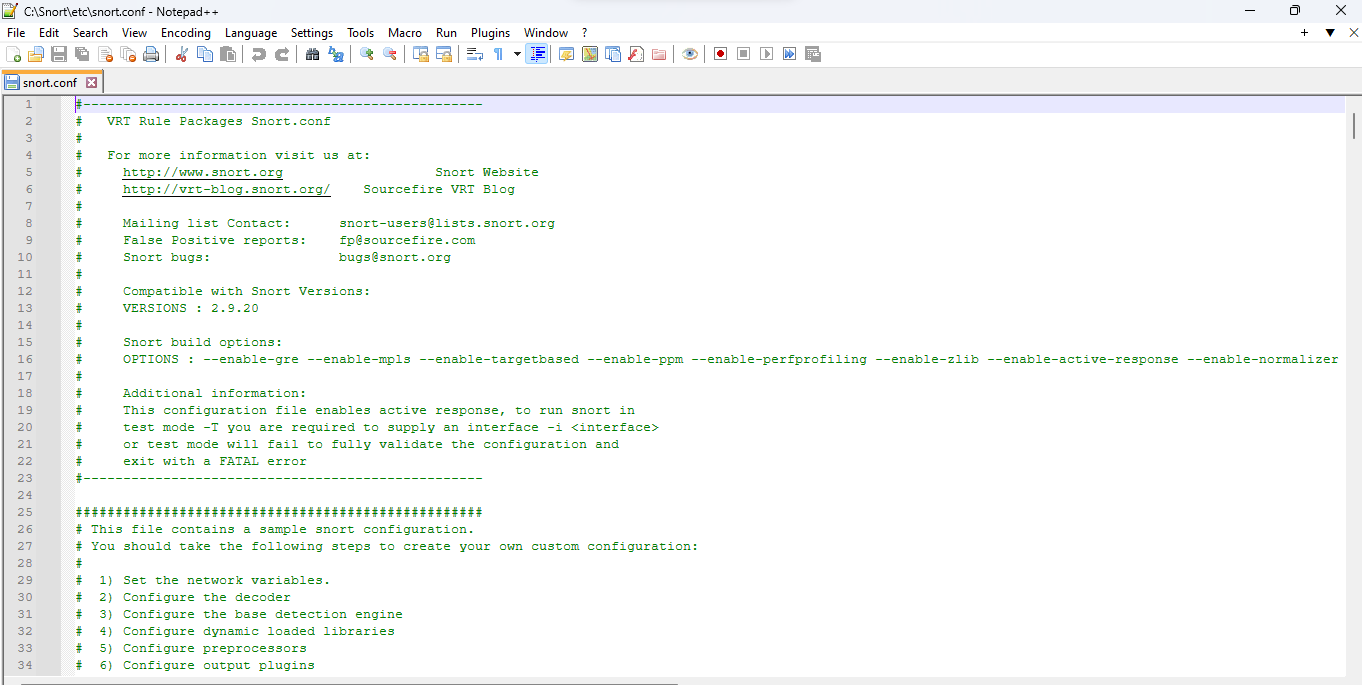
-dev provides detailed information about each captured packet, including the link-layer (Ethernet) headers, IP headers, and the packet payload.

-l is listing the those captured packets by creating a new file in the location specified.

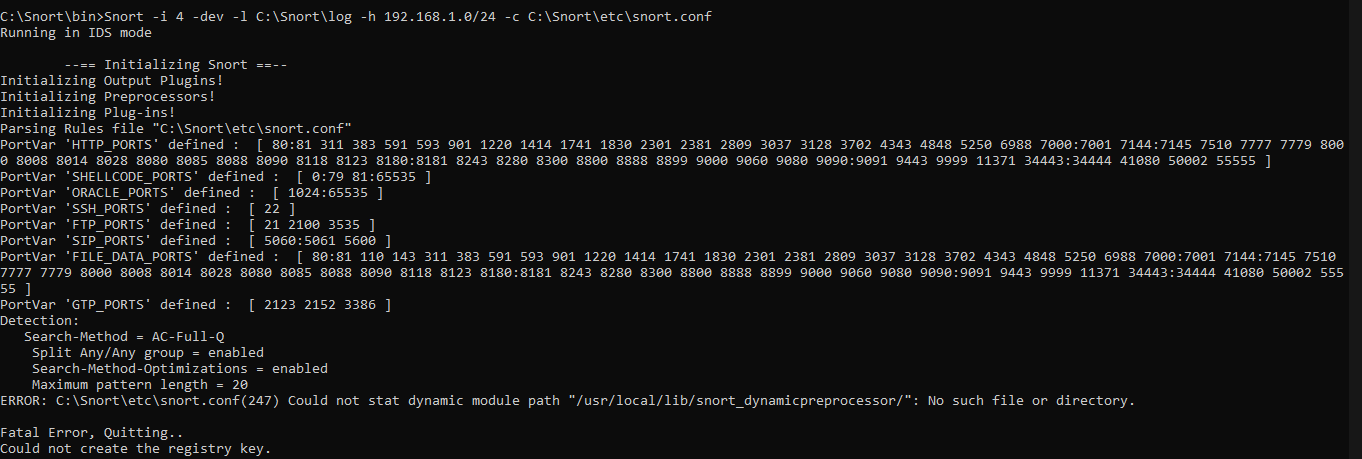
The attached snippet the snort tool is listening for packets at the interface 4 which is my pc’s ip address index,-dev is capturing the detailed information of these packets on running this command and -l is listing this information in a new file at location c:\Snort\log.The newly created file is visible in the screenshot below named as snort.log.1727676590.



On opening this file in snort snappping tool the snapped packets are visible with there source,destination,protocol used to send those packets and their length and other information related to those packets.



This is the the config file of snort that contains set of parameters that tell snort how to process and analyze network traffic defining network variables, preprocessors, rule paths, and specific Snort rules that determine what actions to take on detected traffic.



Snort –i *4* -dev -l C:\Snort\log -h 192.168.1.0/24 -c snort.conf:

In this command on the snort the the interface for scanning of packet is mentioned by the ‘ -i 4 ‘

part ,the 4 is the index at which the pc’s ip address is stored(found by ifconfig command),-dev gives detailed information about the packets capture,-l c:\snort\log is telling in which directory to store the log file of the captured packets,-h 192.168.1.0/24 is defining the home network that snort will monitor. 192.168.1.0/24 represents the entire network with IP addresses from 192.168.1.1 to 192.168.1.254.**-c snort.conf** is specifying the Snort configuration file (snort.conf) that contains Snort's detection rules, preprocessors, network variable definitions, and other configurations.

On running this command snort has captured the traffic and has processed the traffic based on the rules defined in config file and the logs are stored in the logs file.