**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’

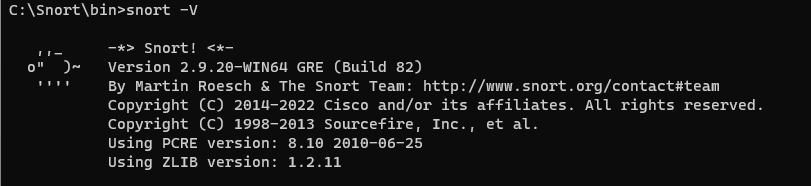
**Conclusion:**

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:**

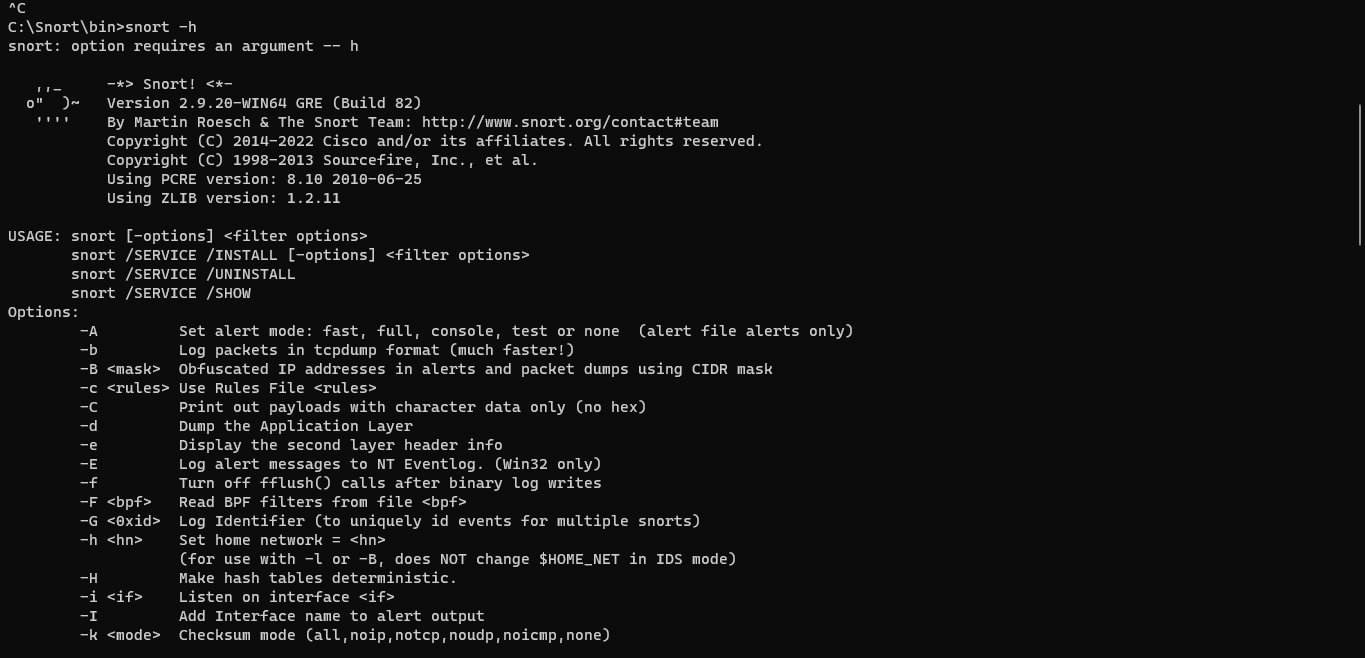
1. “Snort User’s Manual 2.9.16”, <https://snort.org/>
2. Bart Lenaerts-Bergmans , “SNORT AND SNORT RULES EXPLAINED”, <https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/snort-rules/>
3. “Basic snort rules syntax and usage”, <https://resources.infosecinstitute.com/topics/penetration-testing/snort-rules-workshop-part-one/>
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

**a. Snort –V:**

****

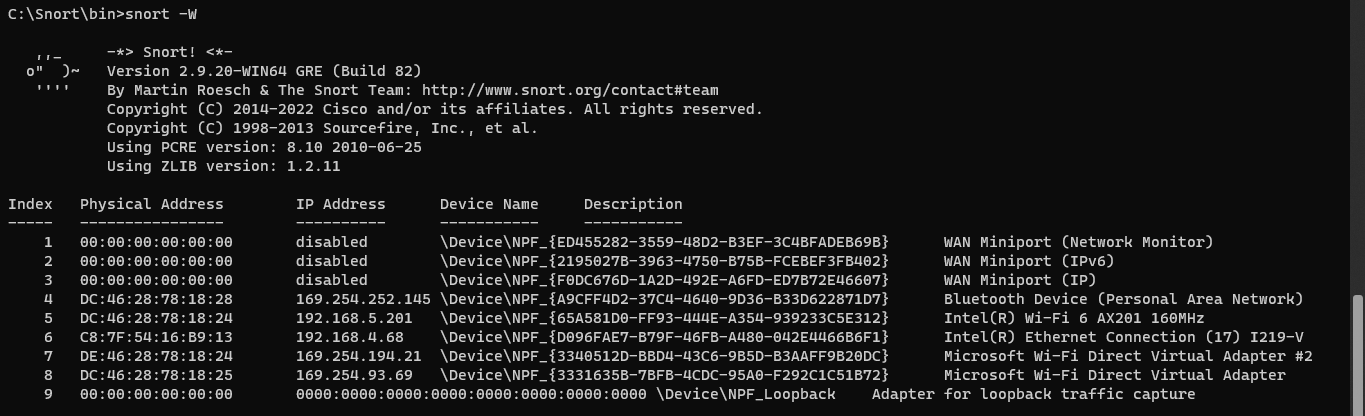
We see that this command displays the version of Snort installed on the system. This output includes essential information such as the version number, the build date, and the copyright details. Knowing the version is crucial for ensuring that the latest features and security patches are implemented.

**b. Snort -h:**

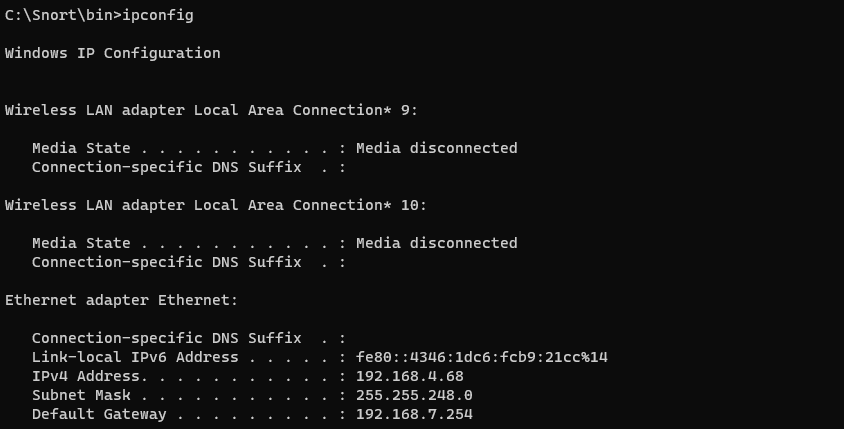


snort -h displays the help information for Snort. This includes a list of command-line options and parameters available for configuration, providing guidance on how to use Snort effectively. It serves as a quick reference for users who need assistance with command syntax or available features.

**c. Snort –W**

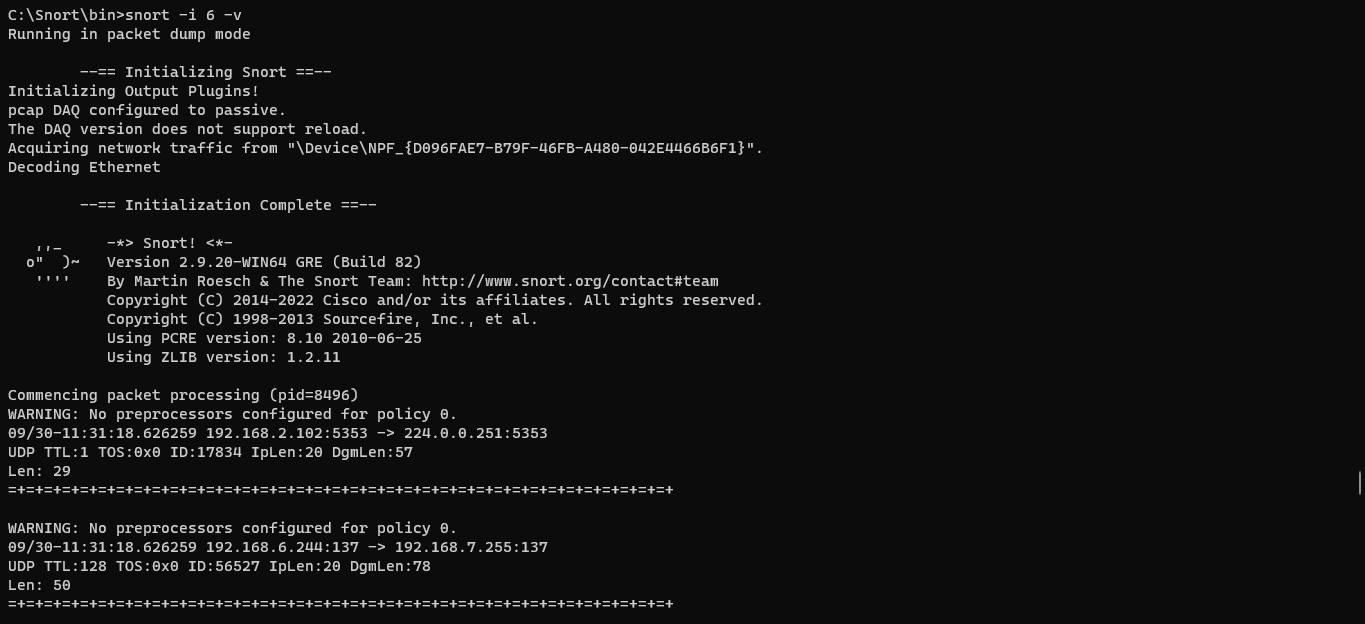


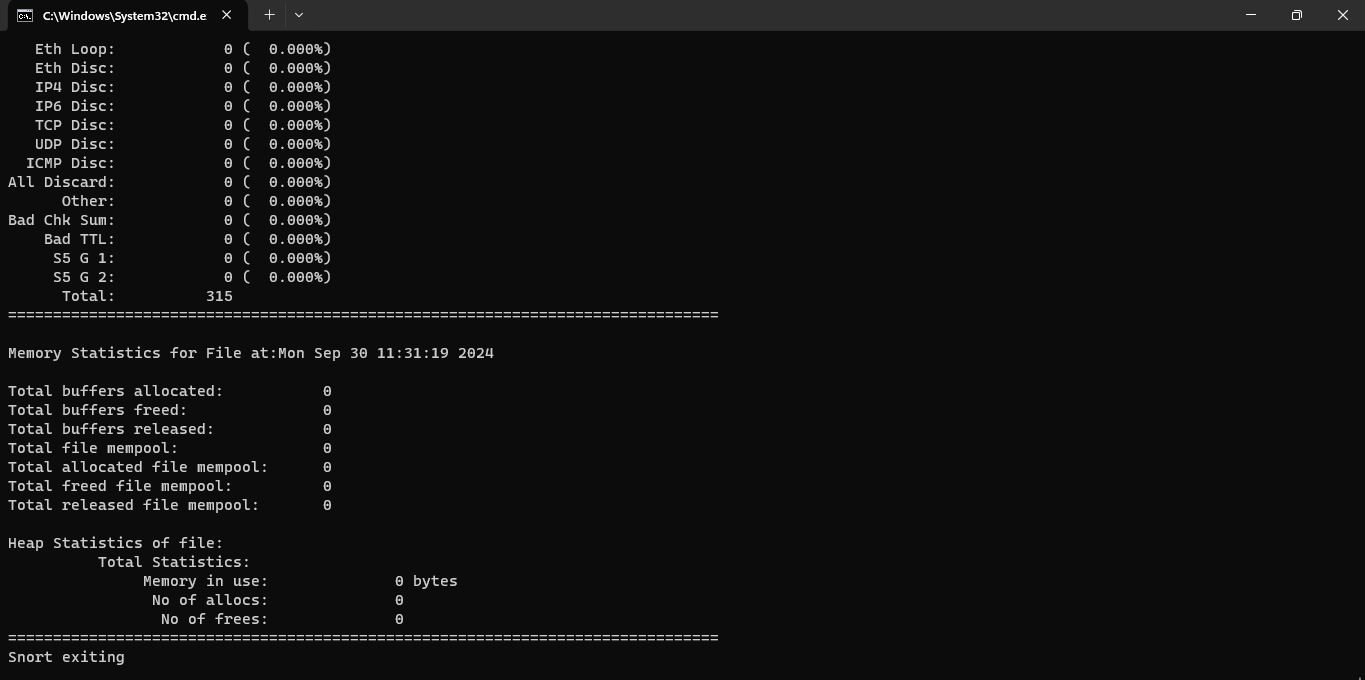
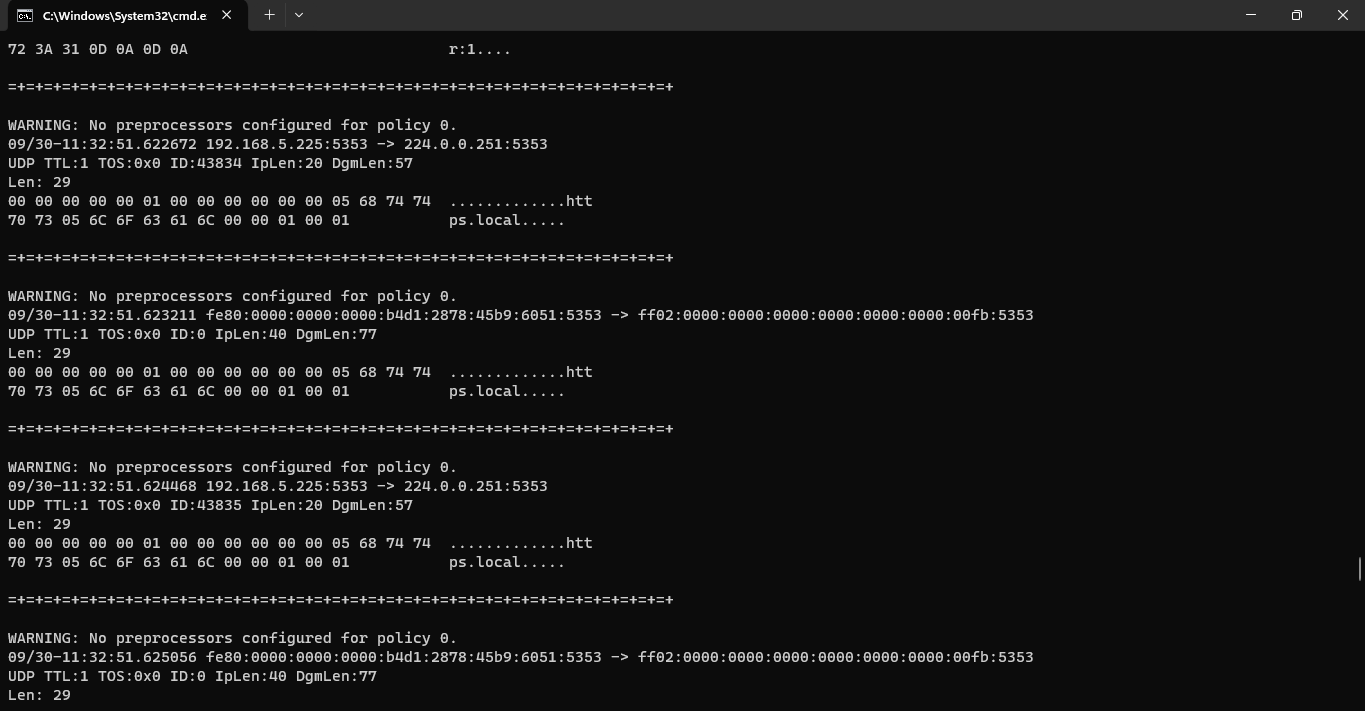
The command snort -W lists the available network interfaces on which Snort can operate. This output includes the interface names, their respective indices, and their operational status. Identifying the correct interface is essential for configuring Snort to monitor the appropriate network traffic.



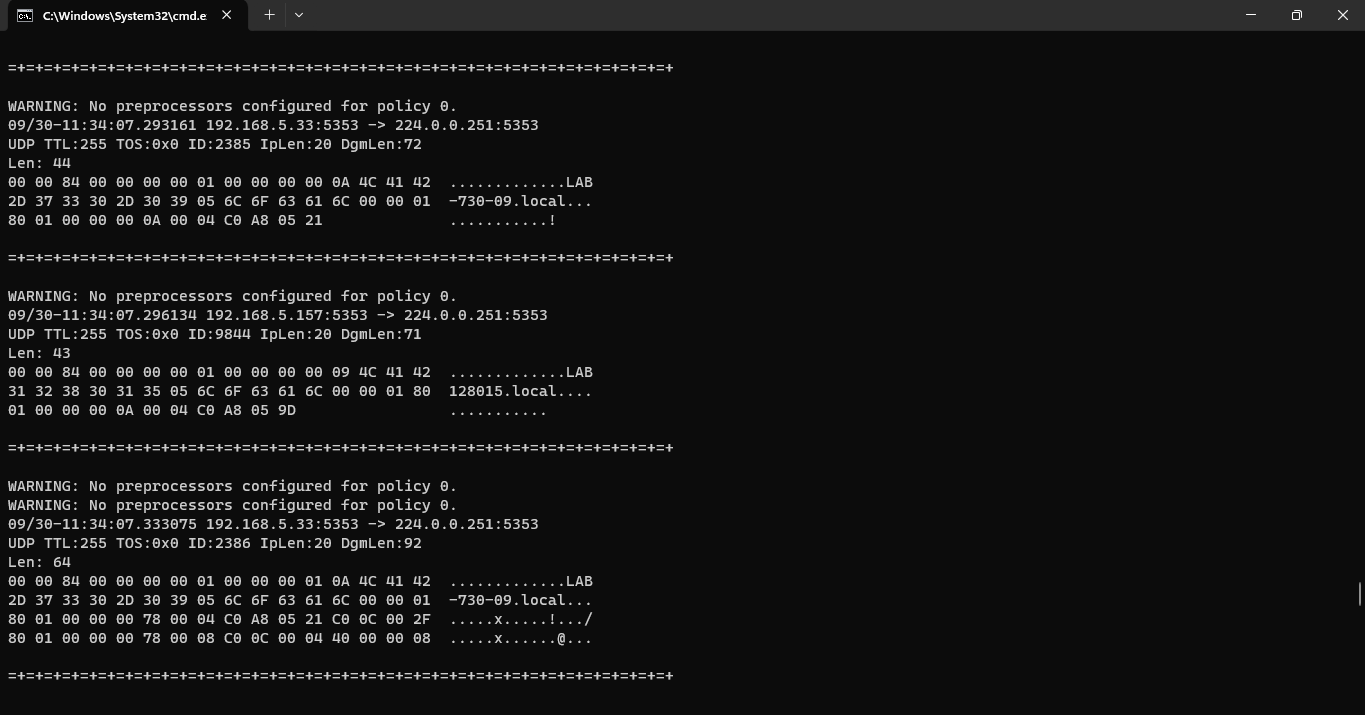
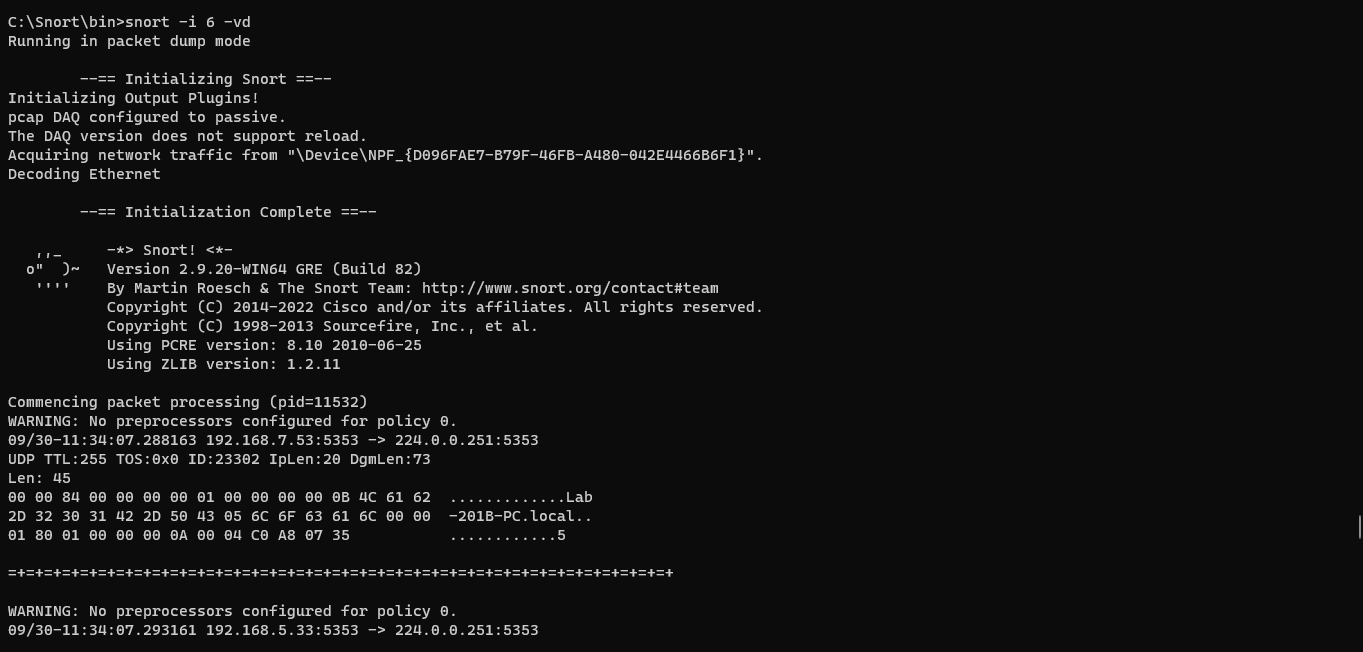
The ipconfig command is used to retrieve the ip address of the computer.

**d. Snort –i interface number -v**



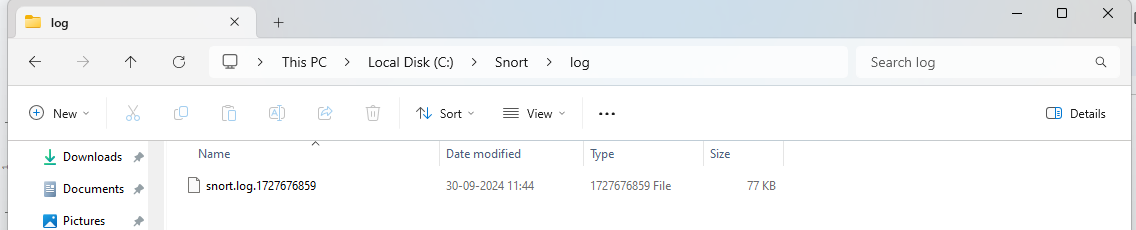


The command snort -i interface number -vd operates Snort on the specified interface while providing additional verbosity. This mode outputs even more detailed packet information, including the payload data in human-readable format. Such in-depth analysis is invaluable for security professionals who need to scrutinize the contents of network packets for potential threats.

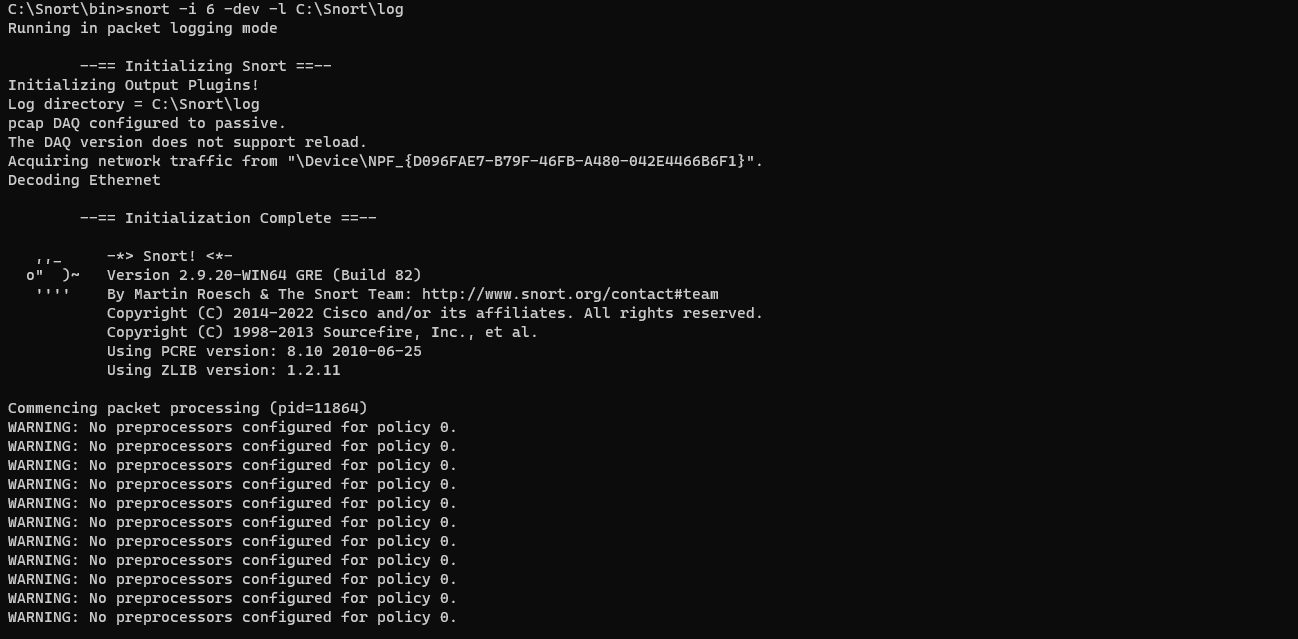
**e. Snort –i interface number -vd**

The command snort -i interface number -vd operates Snort on the specified interface while providing additional verbosity. This mode outputs even more detailed packet information, including the payload data in human-readable format. Such in-depth analysis is invaluable for security professionals who need to scrutinize the contents of network packets for potential threats.

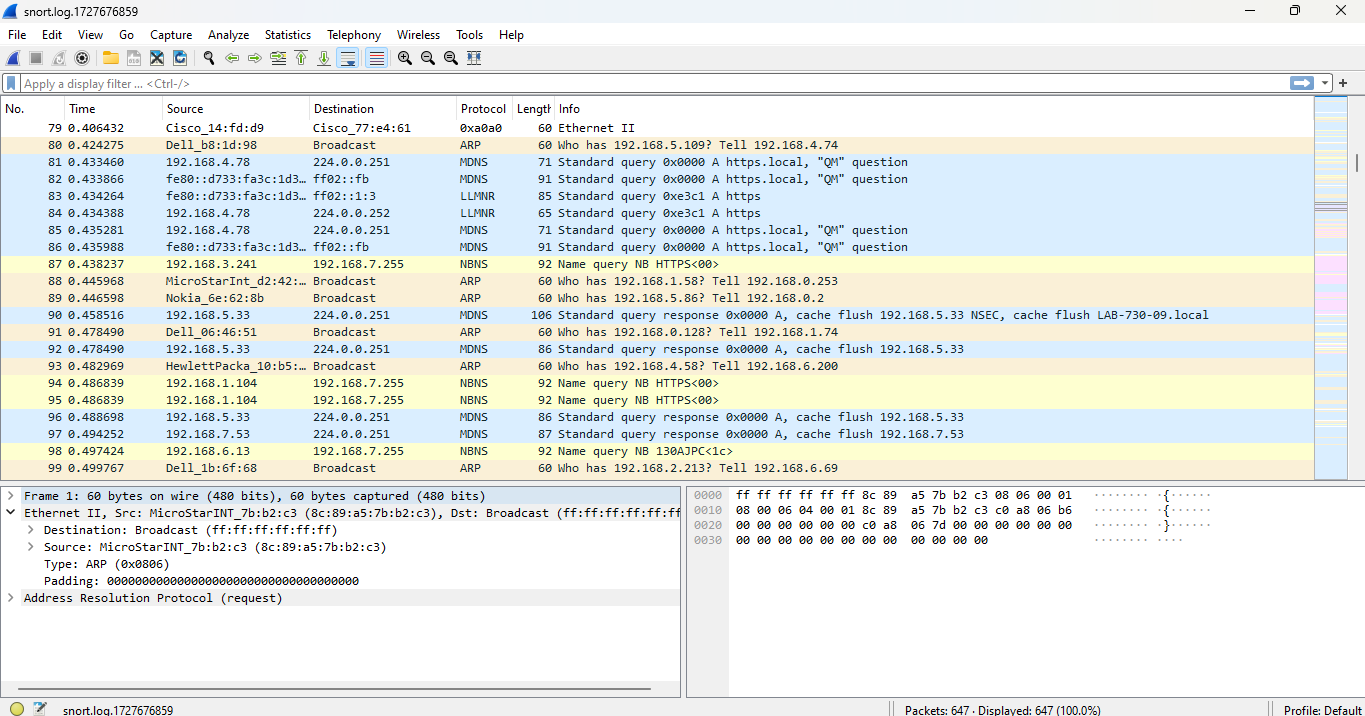
**2. Snort –i interface number -dev -1 C:\Snort\log**

****

We first open the log folder from the Snort folder in the cmd.

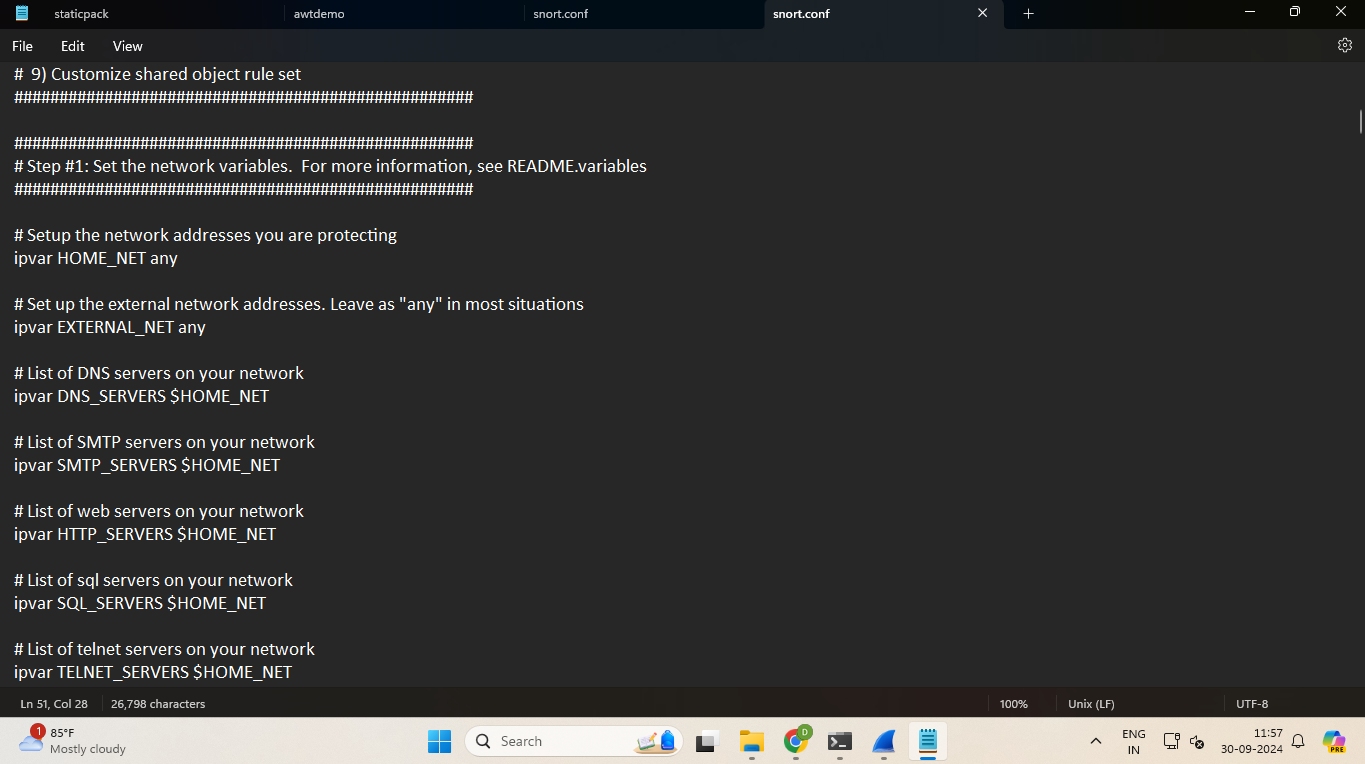
****

This command configures Snort to capture and analyze network traffic in a detailed manner, while also organizing the logs for easy access and review.

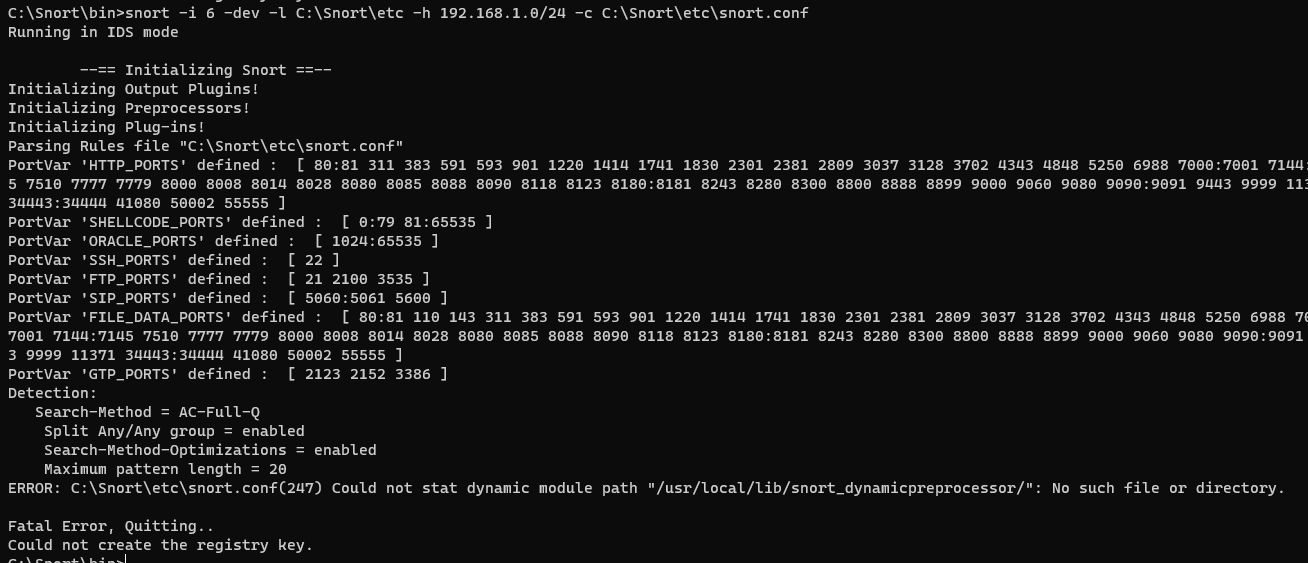
****

We open this folder in wireshark to check the packets. Wireshark provides a graphical interface to view packet details, filter specific protocols, and examine communication flows for further insights into the network activity.

**3. Snort IDS Initialization Command**

****

Use a text editor appropriate for your operating system—like Notepad on Windows or nano/vim on Linux—to access the configuration file. Opening the file allows users to view the current settings and rules defined for Snort, serving as the foundation for customization.

****

The command Snort –i interface number -dev -l C:\Snort\log -h 192.168.1.0/24 -c snort.conf is used to run Snort as an Intrusion Detection System (IDS) on a specified network interface. The -dev flag enables verbose output, providing detailed information during packet analysis, while -l specifies the log directory for captured traffic.