**Ethical Hacking Lab**

**Module 2:**

**Scanning networks, Enumeration and sniffing**

**A. Port Scanning**

**Aim:** To identify open ports and services running on a target system

**Theory:** Port Scanning

Port scanning is a technique used to discover open ports and associated services on a networked device. Ports are endpoints for network communications and each port can be used by different services or applications.

**Command:**

**Using cmd**

**>** nmap 192.168.56.1

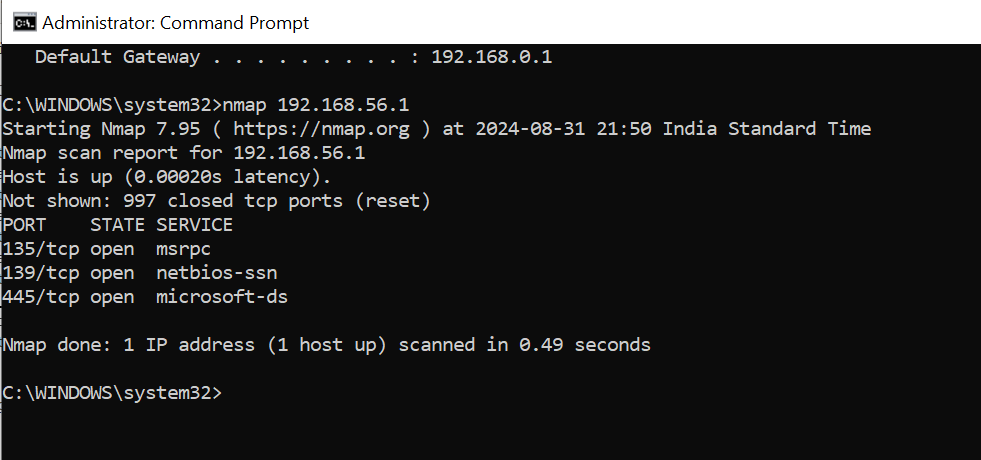
**>** nmap -p 22,80,443 192.168.56.1

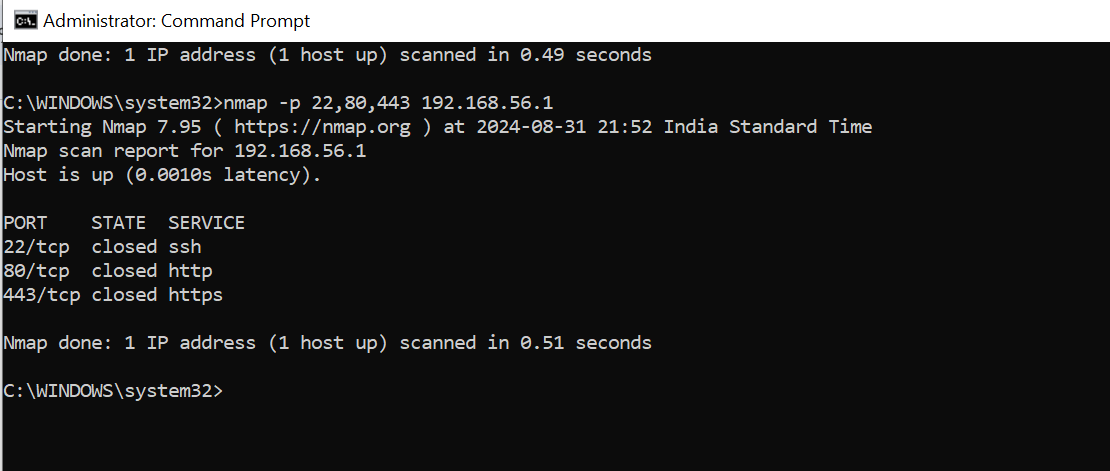
**>** nmap -p 1-65535 192.168.56.1

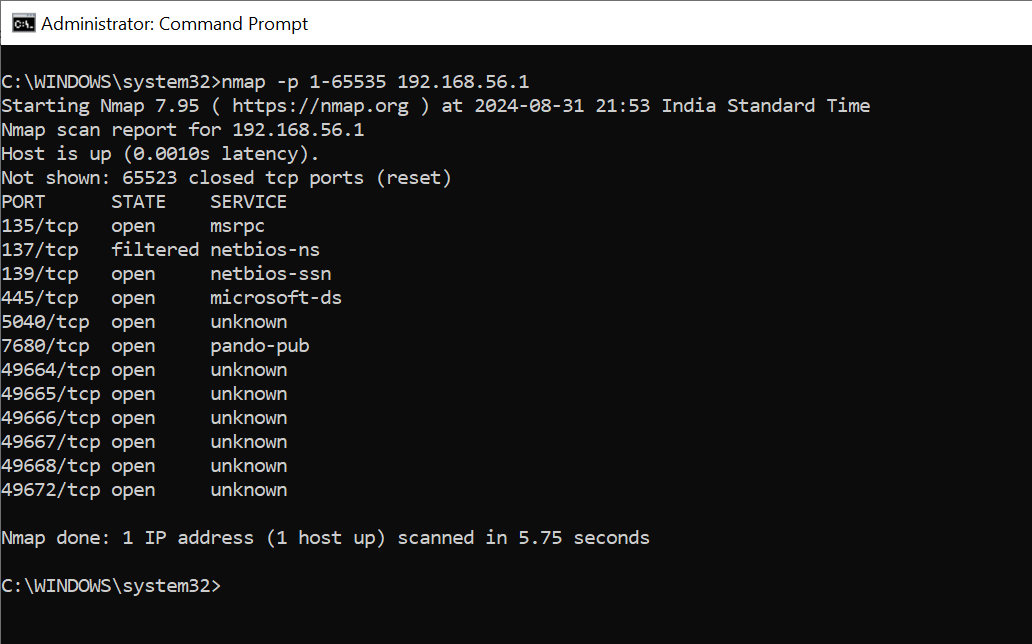
**Using Nmap - Zenmap GUI**

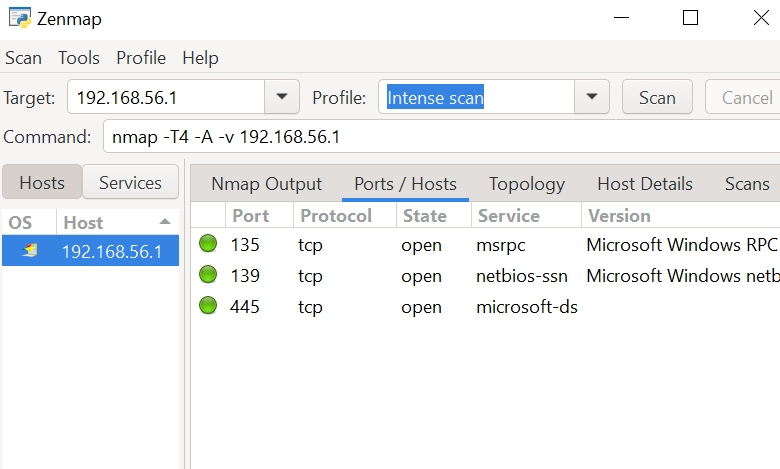
**>** nmap -T4 -A -v 192.168.56.1

**Output:**









**Download Nmap:** <https://nmap.org/download.html>

**B. Network Scanning Tools**

**IP Addresses: 45.33.49.119; 142.250.182.196 & 54.182.0.79**

**Aim:** To use network scanning tools, specifically Nmap with NPCAP, to scan multiple IP addresses for open ports and services

**Theory:** Network Scanning Tools

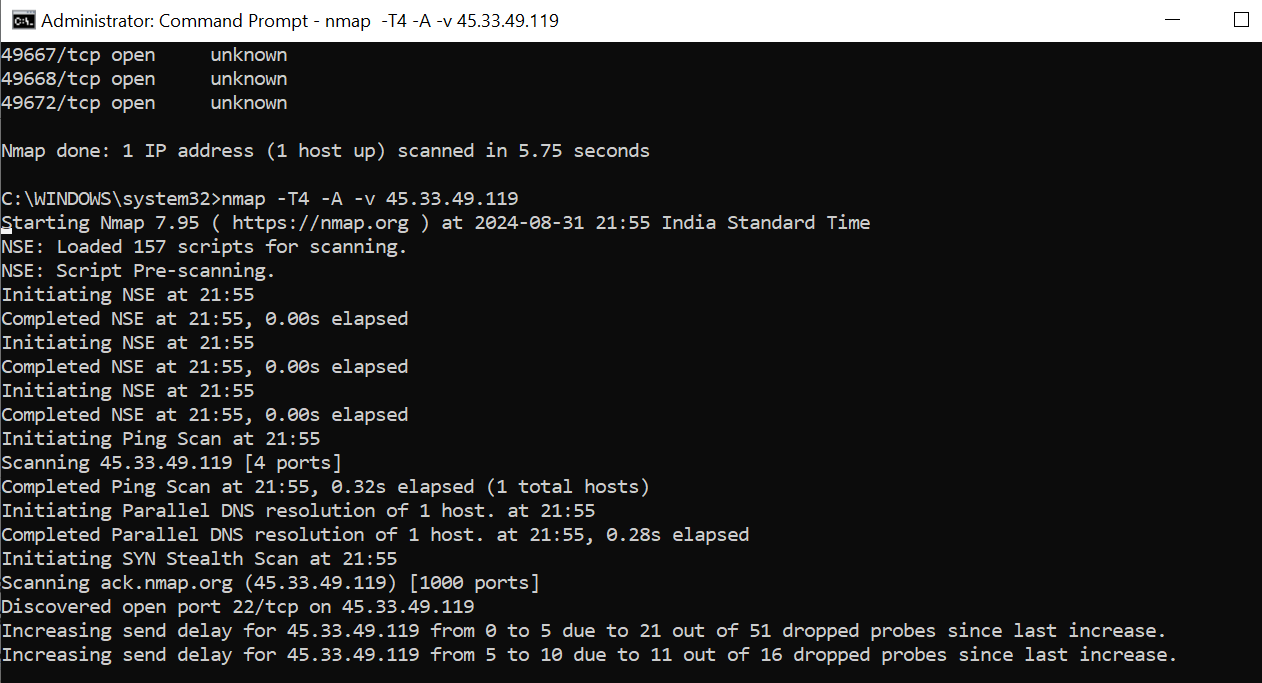
Network scanning tools like Nmap, when used with packet capture libraries such as NPCAP, are crucial for network assessment and security analysis. Nmap is used to discover hosts and services on a network by sending packets and analyzing responses. NPCAP enhances Nmap's capabilities by providing real-time packet capture on Windows systems. Scanning multiple IP addresses helps in identifying which ports are open and which services are running, offering insights into the network's security and configuration.

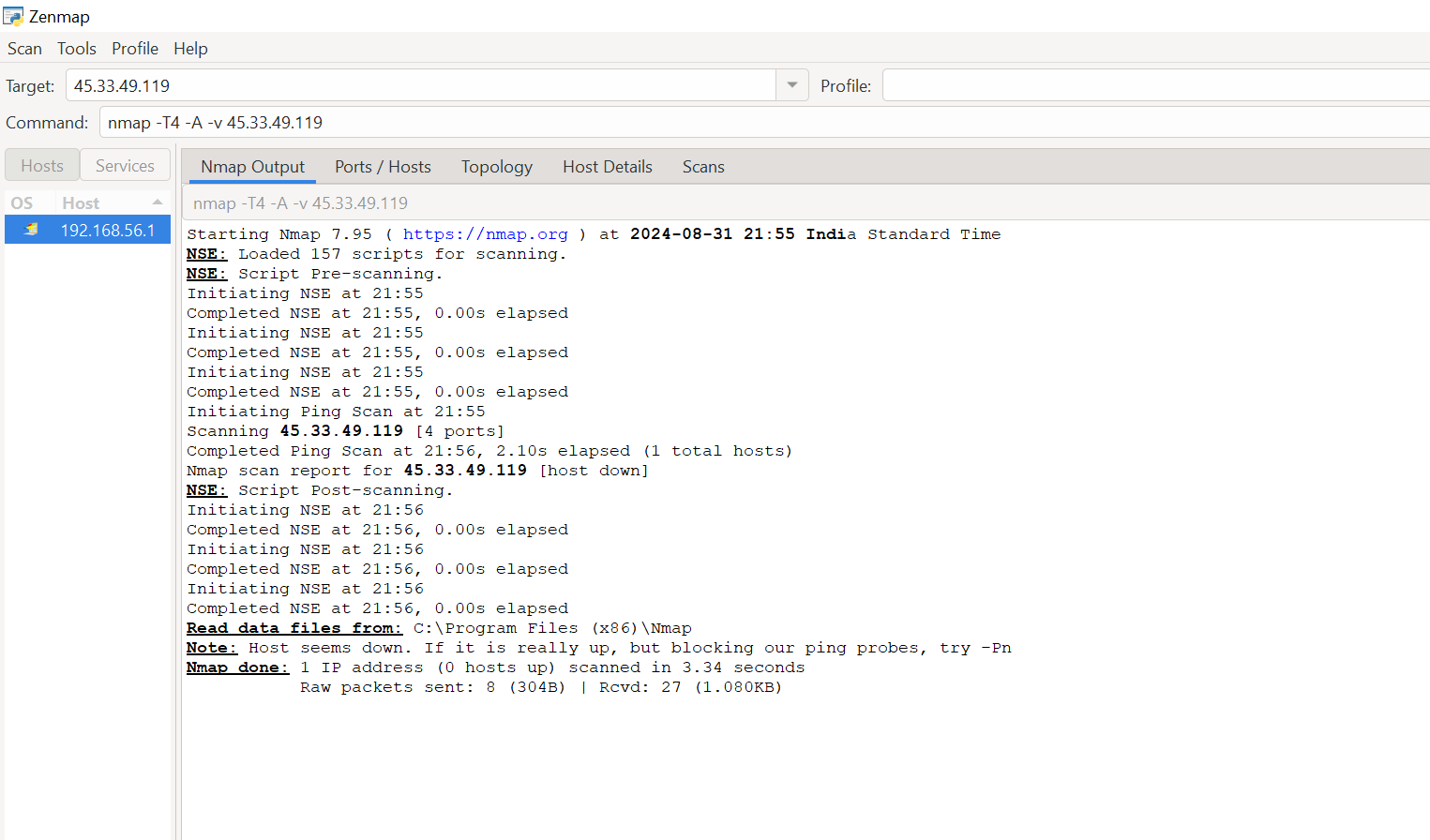
**Command:**

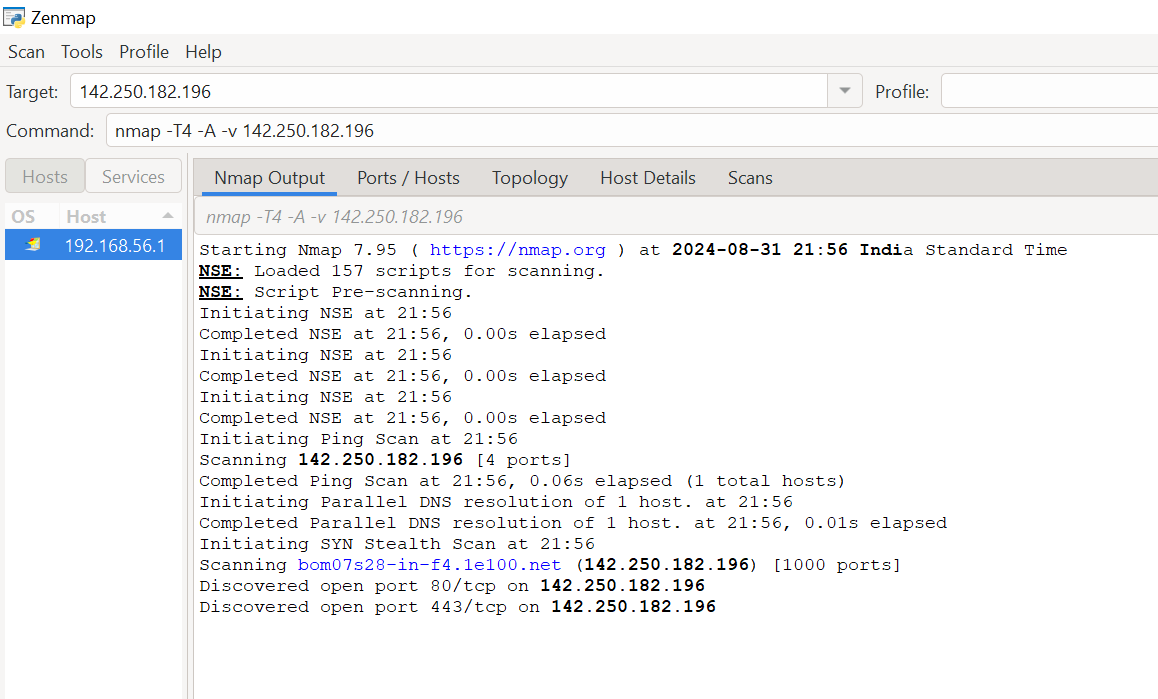
**Using Nmap - Zenmap GUI**

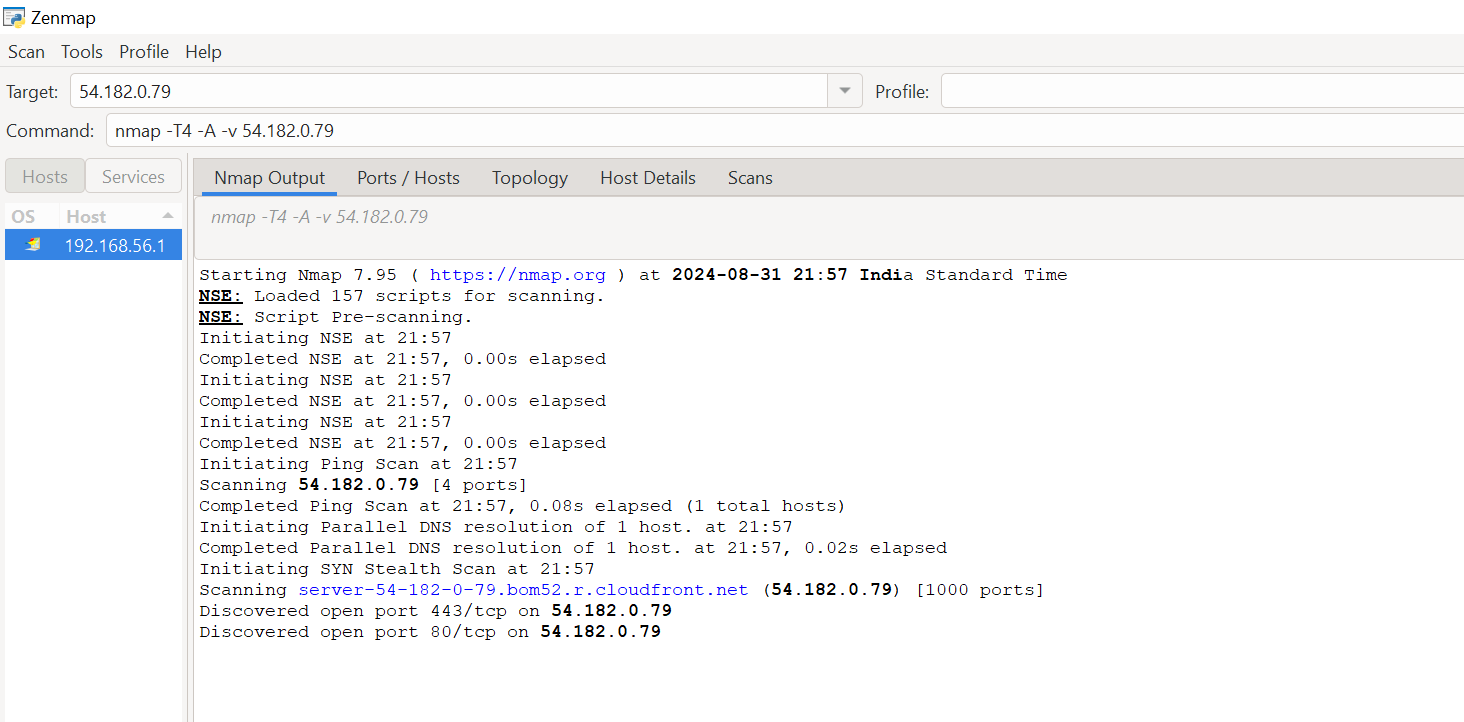
**>** nmap -T4 -A -v 45.33.49.119 | **>** nmap -T4 -A -v 142.250.182.196 | **>** nmap -T4 -A -v 54.182.0.79

**Output:**

****

****





**C. IDS Tool**

**Aim:** To deploy and configure an Intrusion Detection System (IDS) tool for monitoring and detecting potential security breaches in a network

**Theory:** IDS Tool

An Intrusion Detection System (IDS) is a crucial security tool used to monitor network traffic for suspicious activities and potential threats. IDS tools analyze the incoming and outgoing traffic and compare it against known attack patterns or signatures. When an anomaly or a match is detected, the IDS generates alerts, enabling administrators to take appropriate action to mitigate risks. IDS can be categorized into two types: Network-based IDS (NIDS) and Host-based IDS (HIDS). NIDS monitors traffic across an entire network segment, while HIDS focuses on individual host activities. IDS systems can operate in real-time, providing timely alerts, and are an integral part of a comprehensive cybersecurity strategy, helping organizations safeguard against unauthorized access, data breaches, and other malicious activities.

**Steps to be followed:**

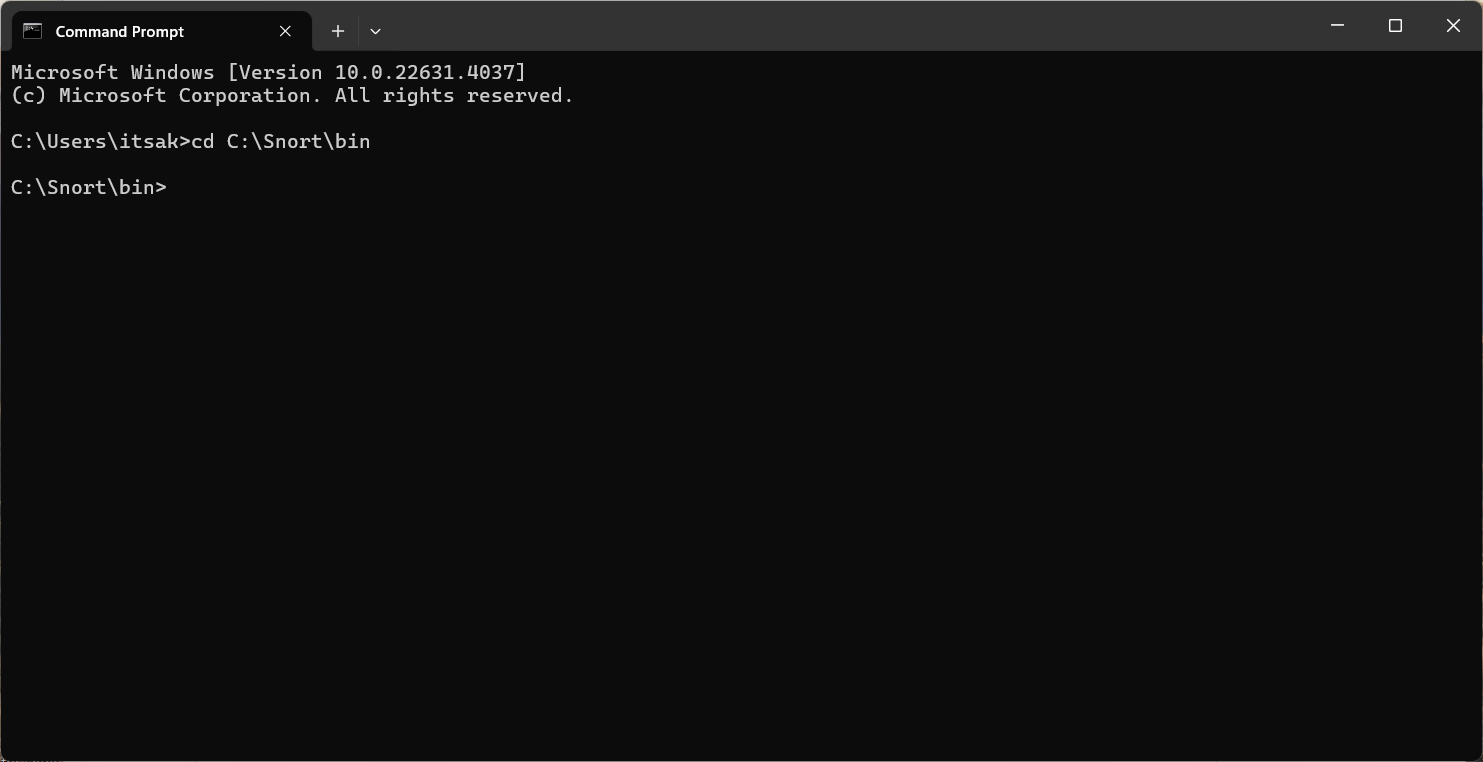
1. **Download Snort** from the **snort.org** website.
2. **Download Rules** from the snort.org website. You must **register** to get the rules (you should download these often): **snortrules-snapshot-29200.tar.gz**
3. **Install Snort**. Double-click the .exe file to install Snort. This will install Snort in the C:\Snort folder. It is important to have **npcap** or WinPcap installed.
4. **Extract** the Rules file. You will need WinRAR for the .gz file.
5. **Copy all files** from the **rules folder** of the extracted folder. Now **paste** the rules into the **C:\Snort\rules folder**.
6. **Copy the snort.conf file** from the etc folder of the extracted folder. **Paste it** into the **C:\Snort\etc folder**. Overwrite any existing file. Remember, if you modify your snort.conf file and download a new one, you must modify it for Snort to work.
7. **Open a command prompt** (cmd.exe) and navigate to the C:\Snort\bin folder. (At the prompt, type cd\snort\bin)
8. To start (execute) Snort in **sniffer mode**, use the following command: **snort -dev -i 7**
   1. **-i** interface specifies which interface Snort should listen on. This option is used on machines that have more than one network interface card or different kinds of interfaces besides Ethernet.
   2. **-dev** is used to run Snort to capture packets on your network.
9. To **check the interface list**, use the following command: **snort -W**
10. You can tell which interface to use by looking at the Index number and finding Microsoft. As you can see in the example, the other interfaces are for VMware.
11. To run Snort in **IDS mode**, you will need to **configure the snort.conf** file according to your network environment.
12. To specify the network address that you want to protect in the snort.conf file, look for the following line: **var HOME\_NET 192.168.1.0/24** (You will normally see any here). Find **your system IP Address**.
13. You may also want to set the **addresses of DNS\_SERVERS** if you have some on your network. Example:
14. **Change the RULE\_PATH variable** to the path of the rules folder: **var RULE\_PATH c:\snort\rules**
15. Change the path of all library files with the name and path on your system. You must change the **path of the snort\_dynamicpreprocessor variable**: **C:\Snort\lib\snort\_dynamicpreprocessor**. You need to do this to all library files in the **C:\Snort\lib** folder. The old path might be: **/usr/local/lib/....** You will need to replace that path with your system path using **C:\Snort\lib**.
16. Change the path of the **dynamicengine** variable value in the **snort.conf** file. Example: **dynamicengine C:\Snort\lib\snort\_dynamicengine\sf\_engine.dll**
17. Add the paths for **include classification.config** and **include reference.config** files
    1. include c:\Snort\etc\classification.config
    2. include c:\Snort\etc\reference.config
18. **Remove the comment (#)** on the line to **allow ICMP rules**, if it is commented with a #:
    1. **include $RULE\_PATH/icmp.rules**
19. You can also remove the comment on **ICMP-info rules** if it is commented:
    1. **include $RULE\_PATH/icmp-info.rules**
20. To **add log files** to store alerts generated by Snort, **search** for the **output log test** in **snort.conf** and add the following line:
    1. **output alert\_fast: snort-alerts.ids**
21. **Comment** (add a #) to the whitelist: **$WHITE\_LIST\_PATH/white\_list.rules** and the blacklist. **Change** the nested\_ip inner , \ to nested\_ip inner #, \
22. **Comment out** (#) the following lines:
    1. **#preprocessor normalize\_ip4**
    2. **#preprocessor normalize\_tcp: ips ecn stream**
    3. **#preprocessor normalize\_icmp4**
    4. **#preprocessor normalize\_ip6**
    5. **#preprocessor normalize\_icmp6**
23. **Save** the **snort.conf file**.
24. To start Snort in **IDS mode**, run the following command:
    1. **snort -c c:\snort\etc\snort.conf -l c:\snort\log -i 3**
    2. If a log is created, select the appropriate program to open it. You can use WordPad or Notepad++ to read the file. If you encounter an error on line 324, comment decompress\_swf { deflate lzma } \ and replace it with decompress\_swf { deflate } \ and decompress\_pdf { deflate }.

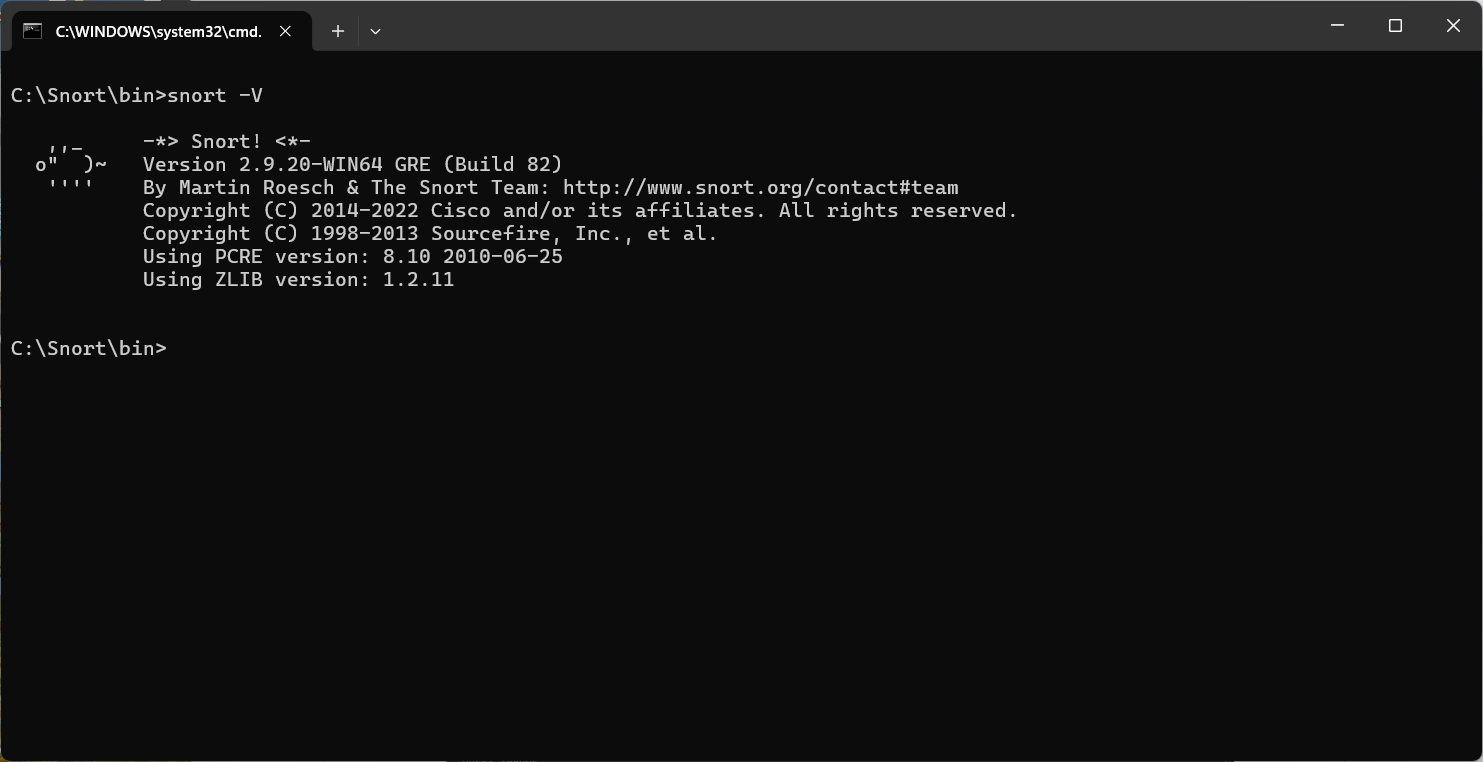
**Command:**

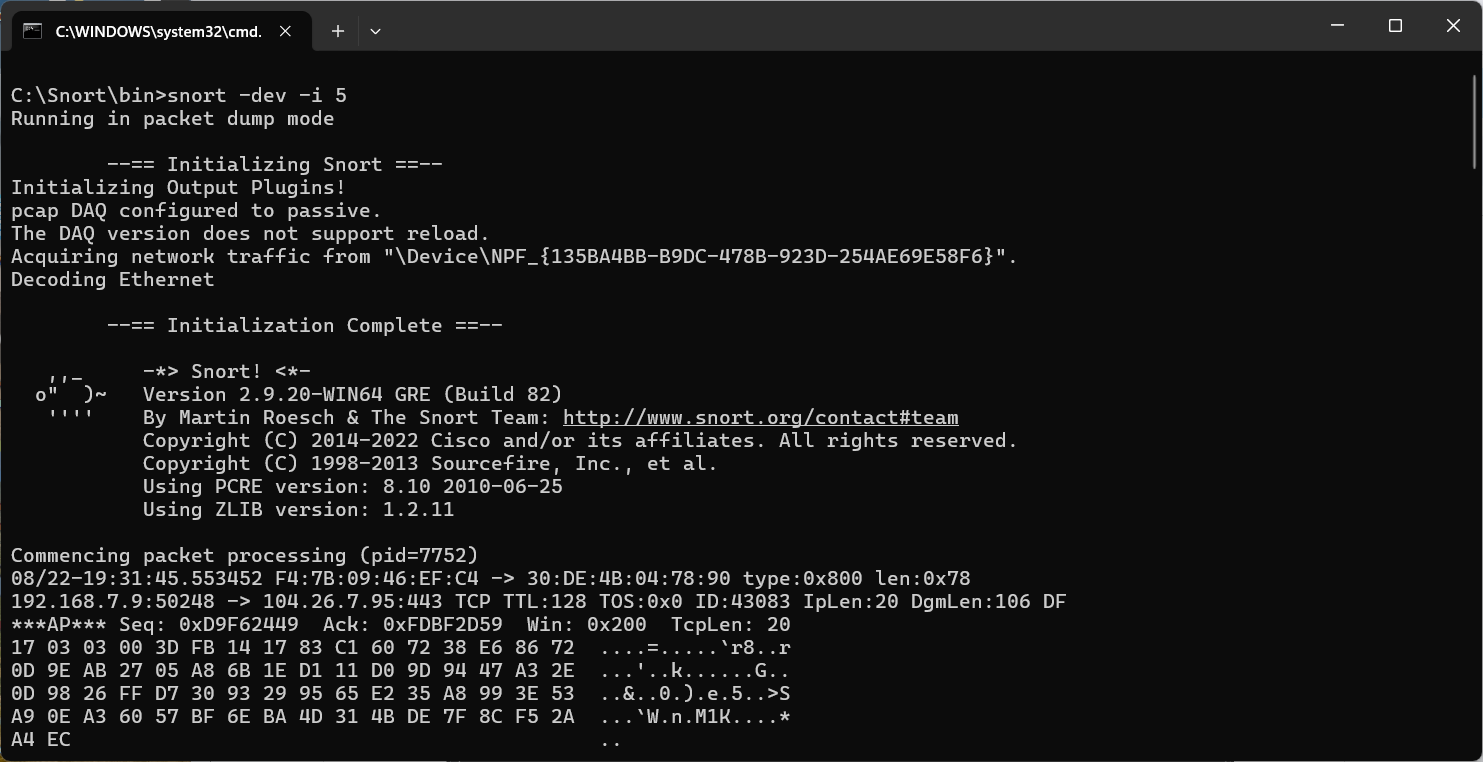
**C:\Snort\bin>**

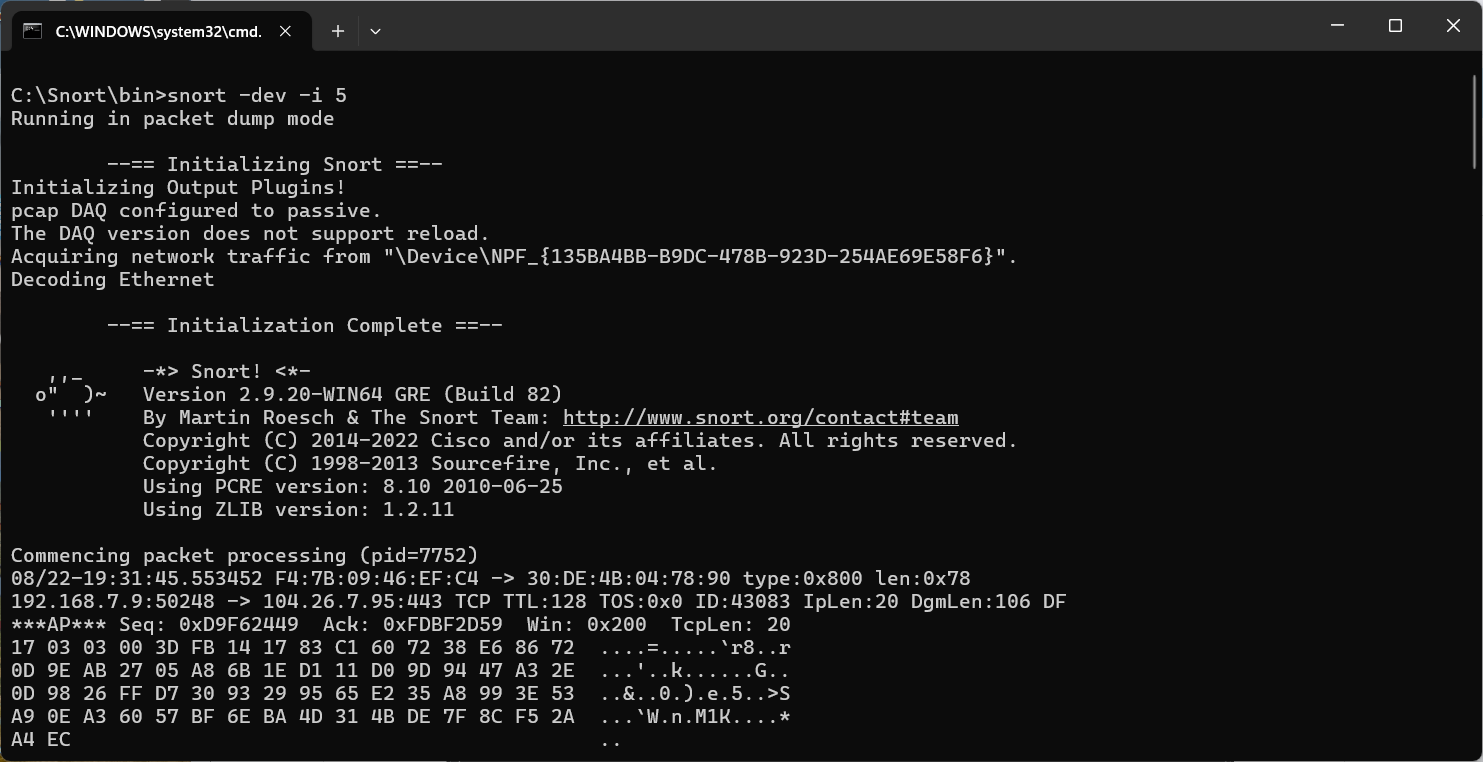
**>** cd C:\Snort\bin | **>** snort -V | **>** snort -dev -i 5 | **>** snort -W | **>** snort -i 5 -c C:\Snort\etc\snort.conf -T

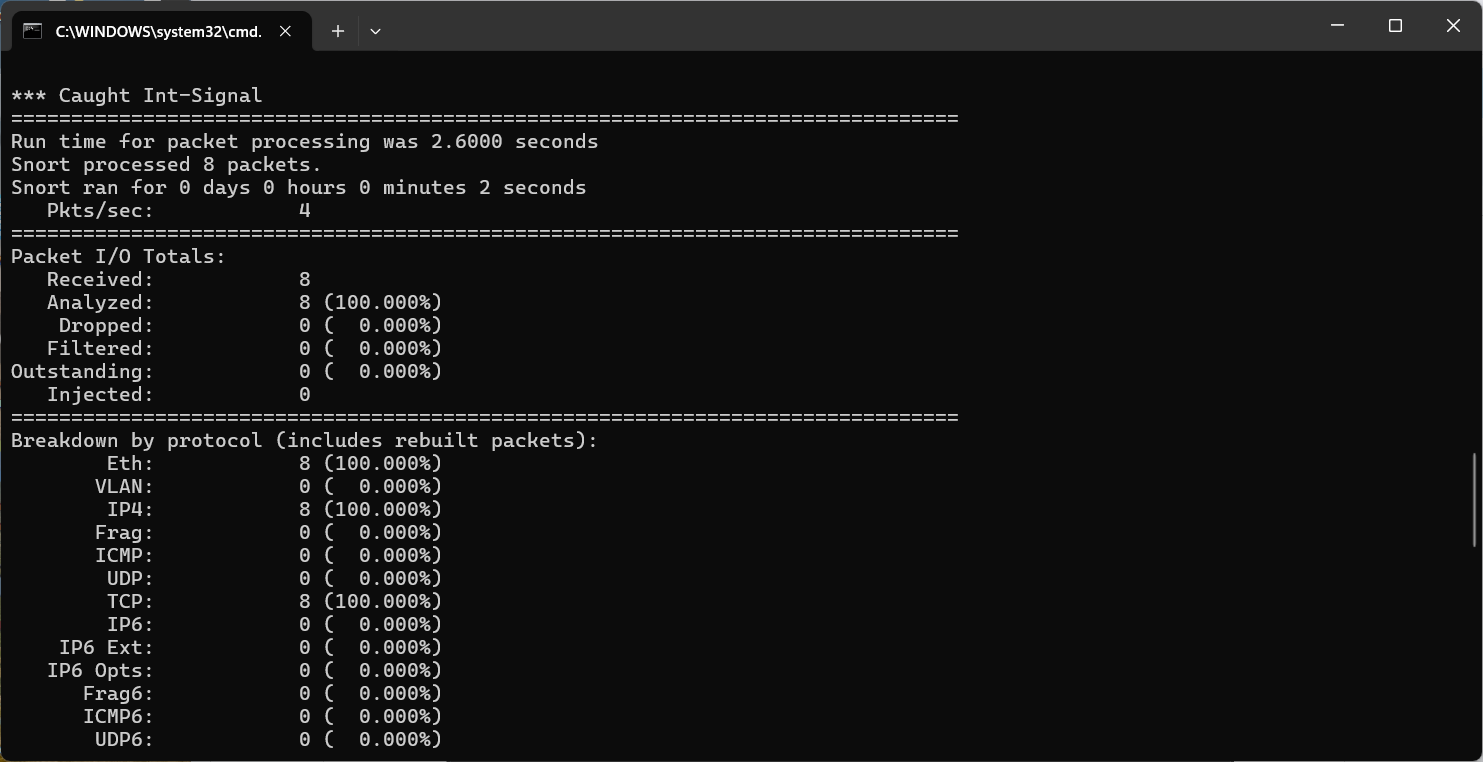
**Output:**

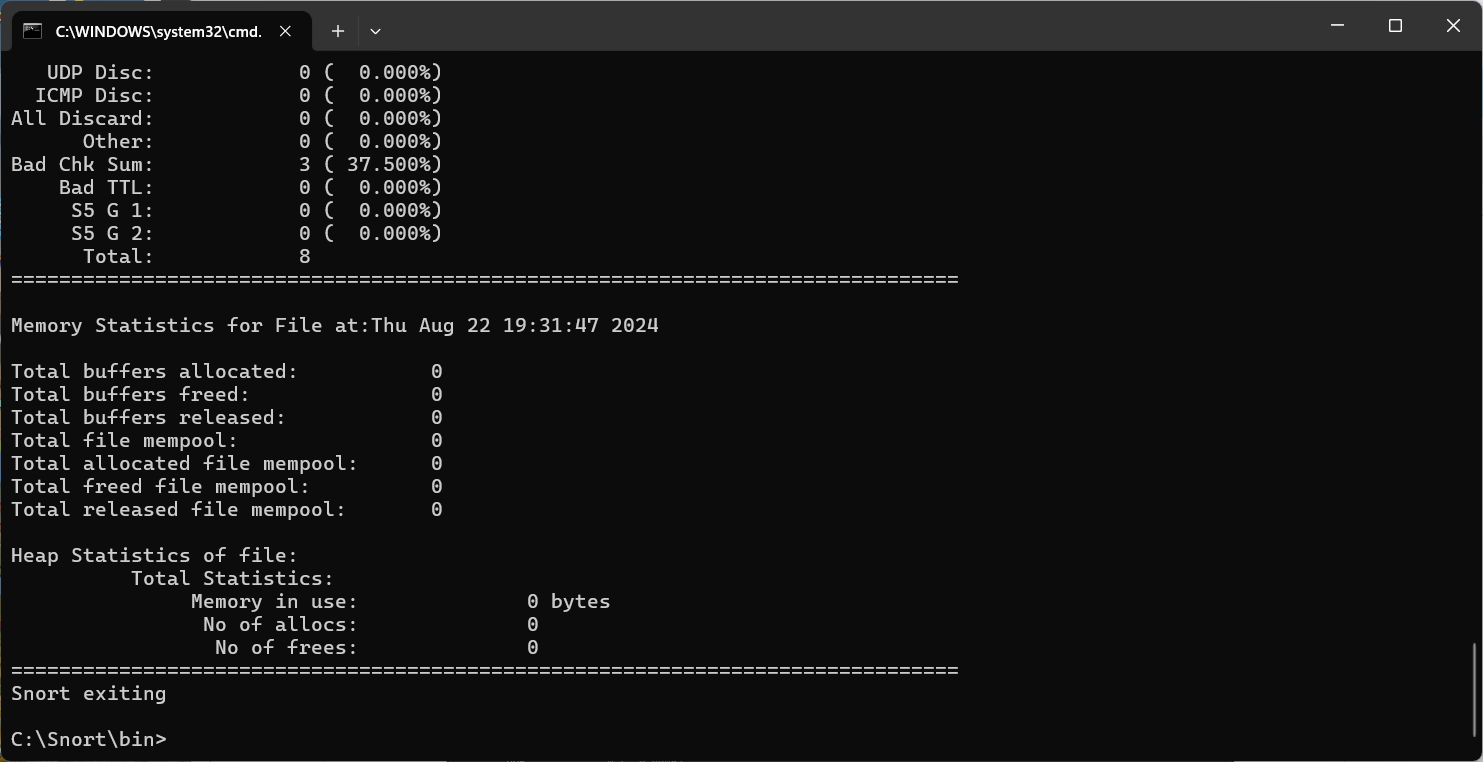


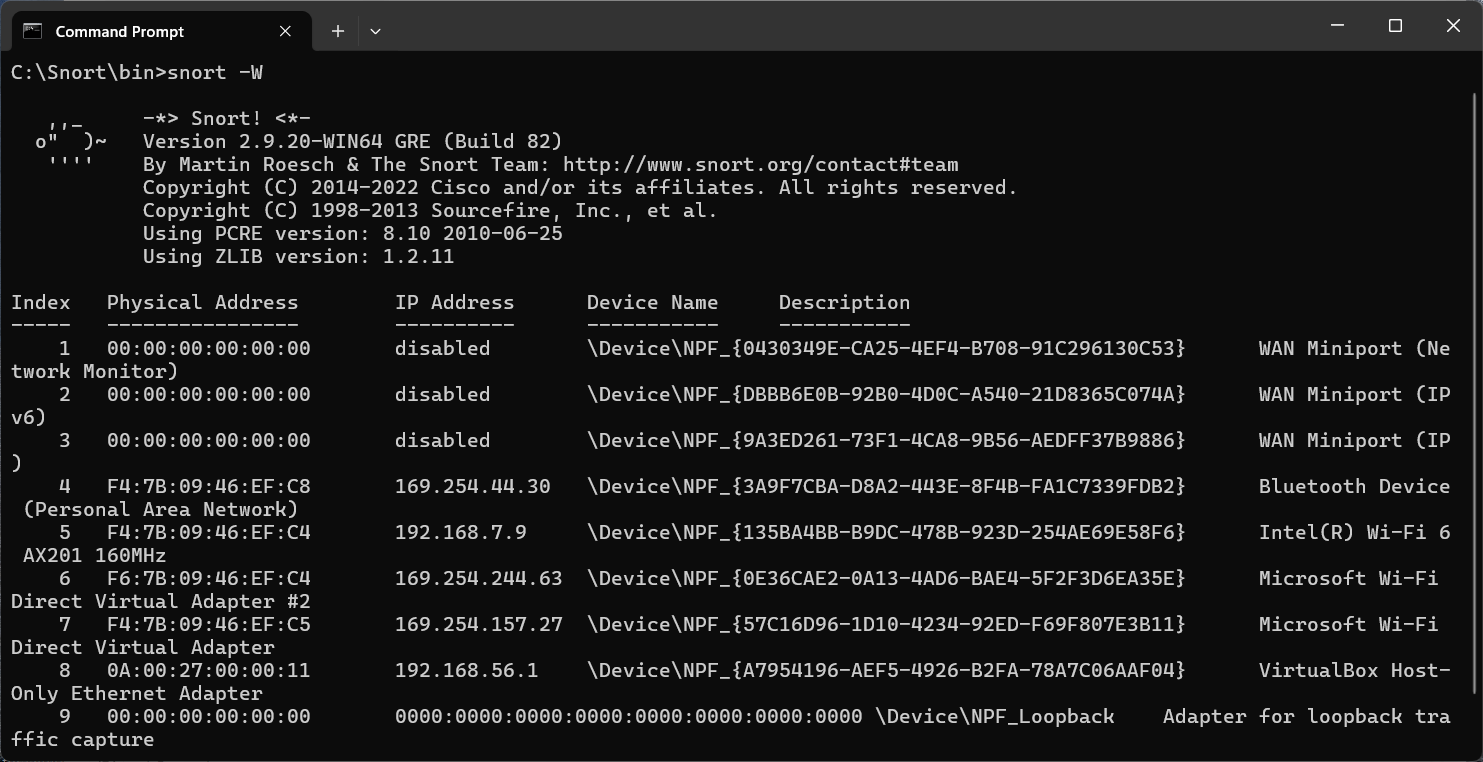


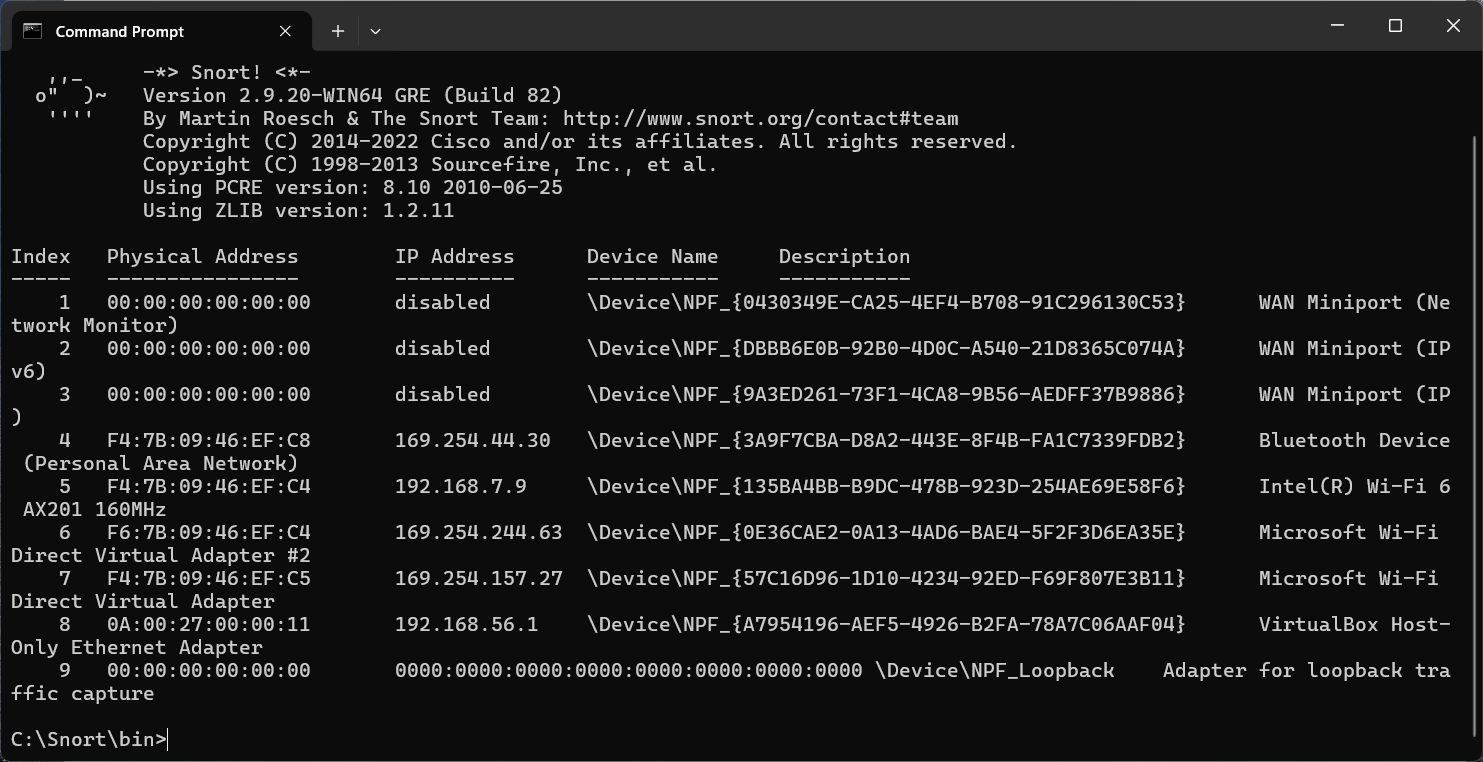


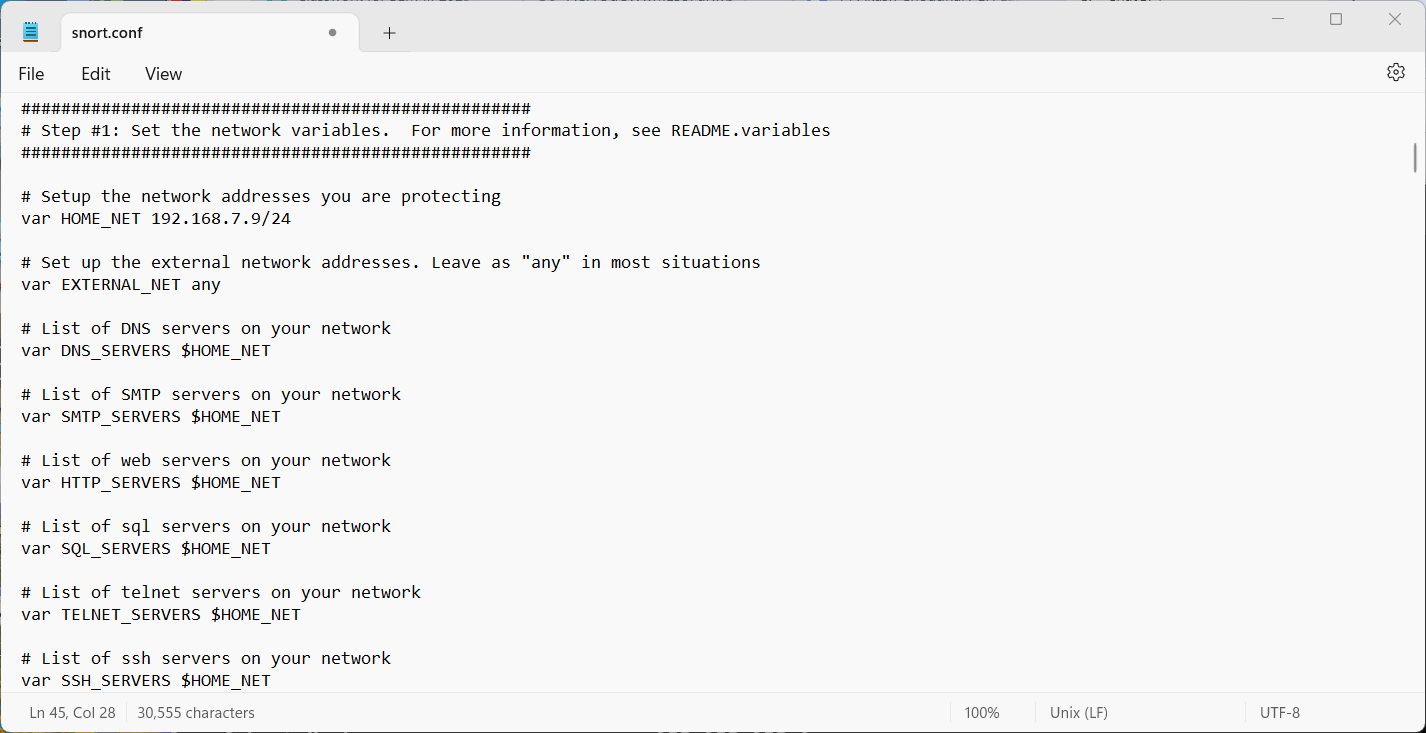


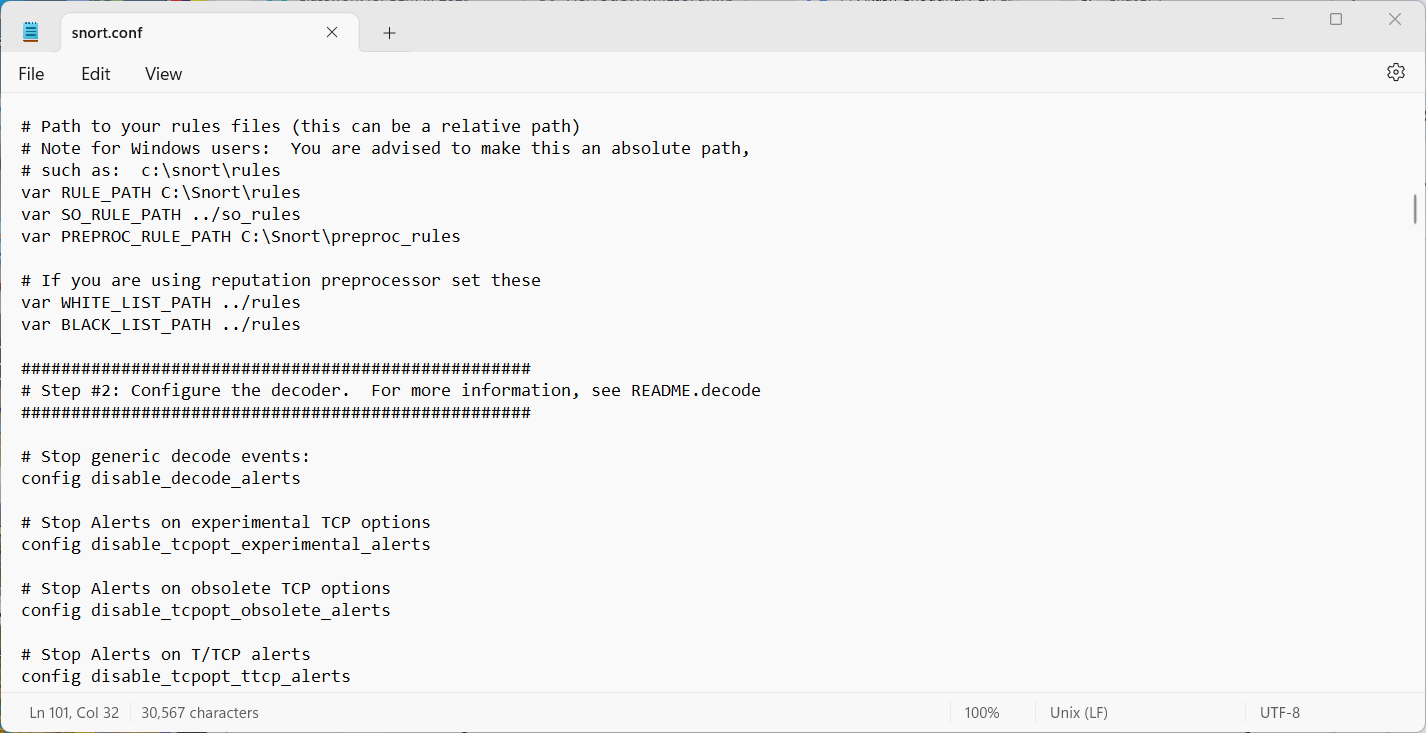


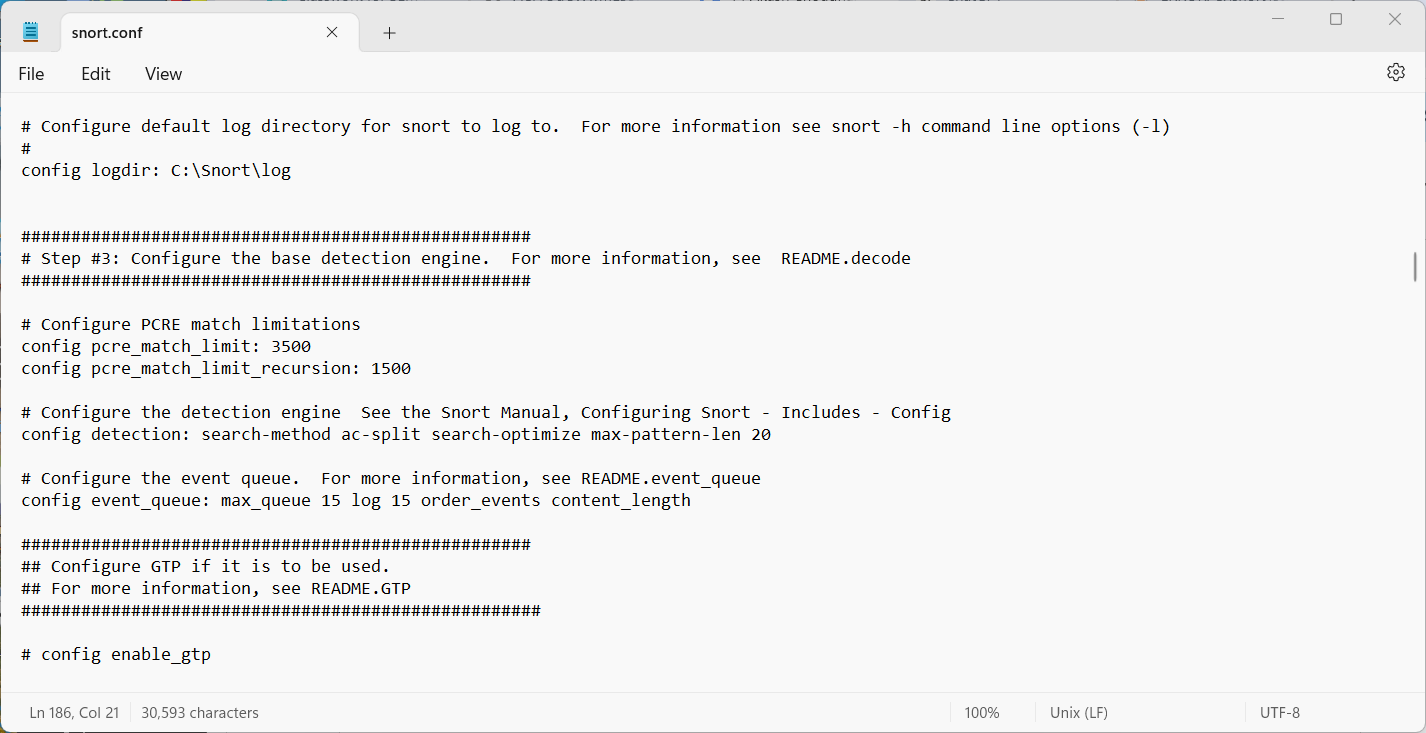


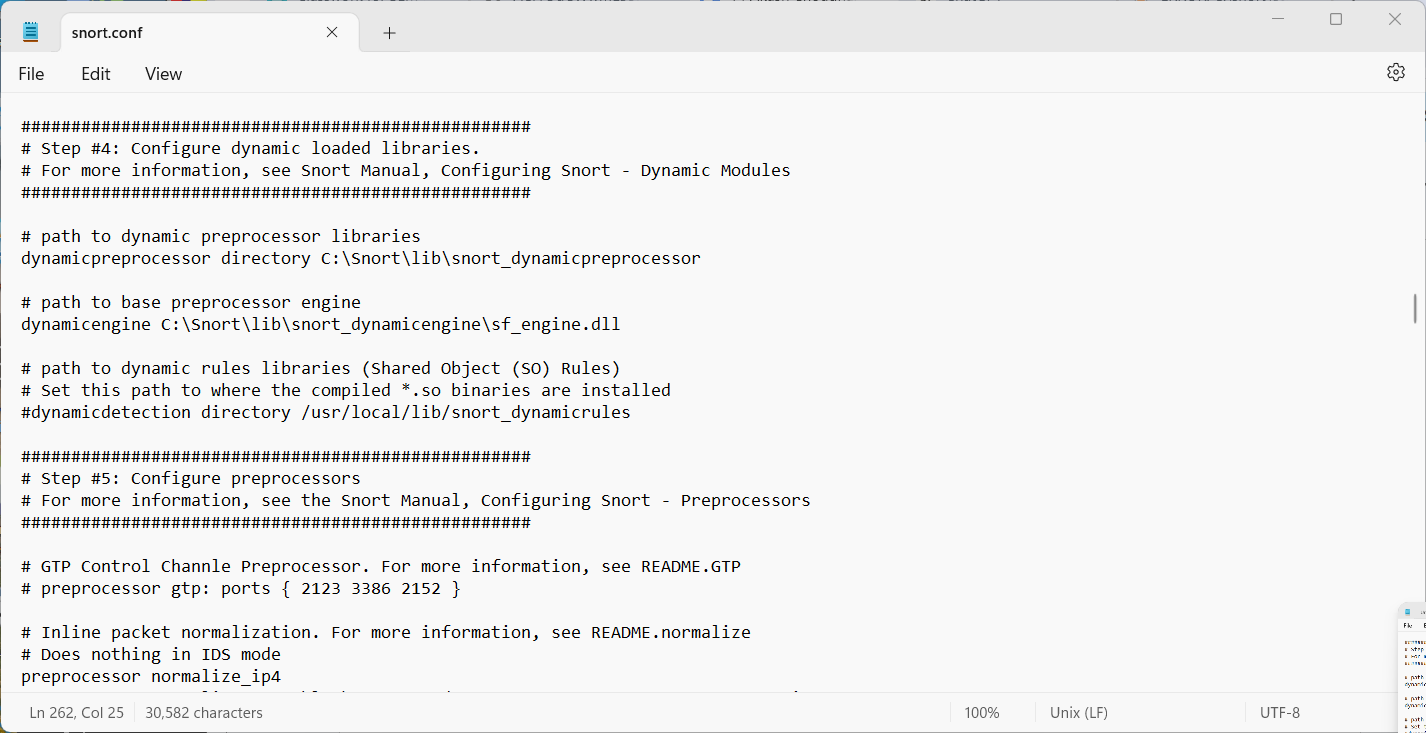


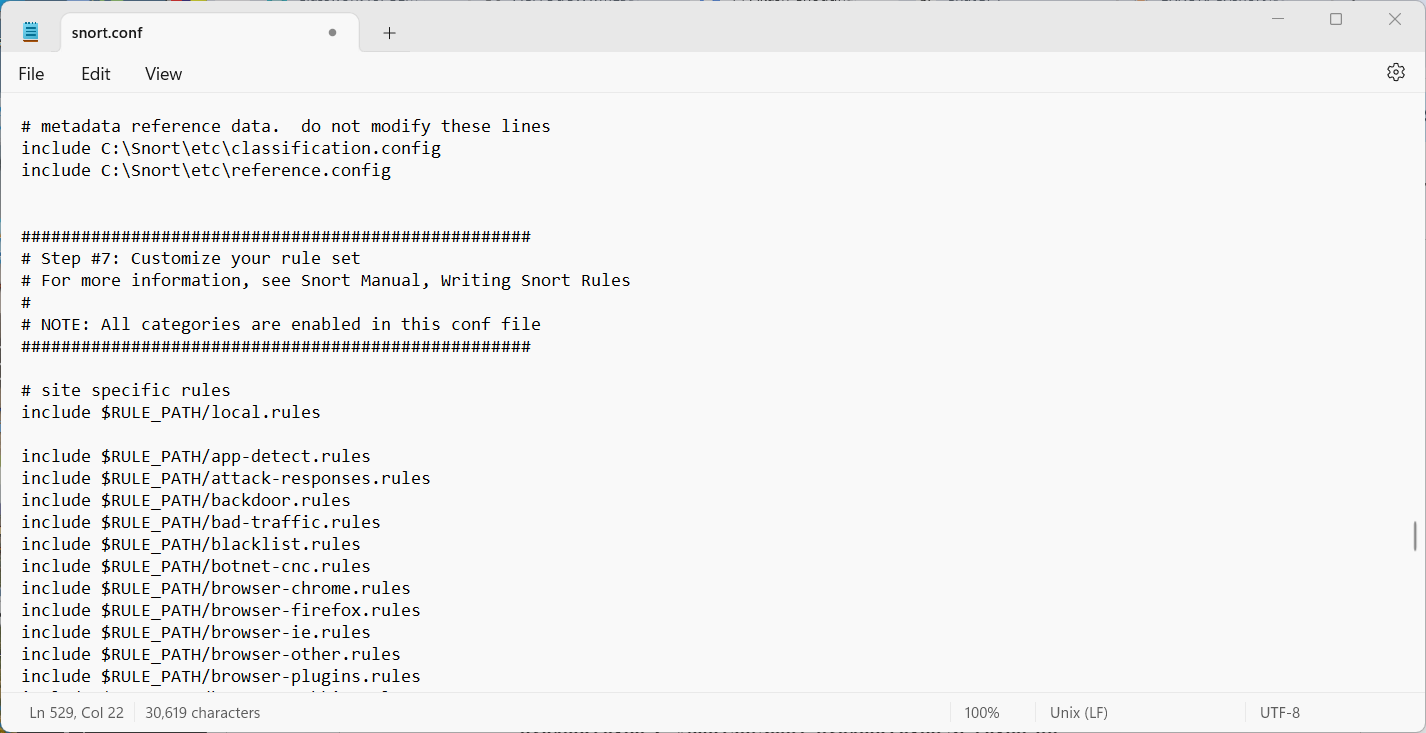


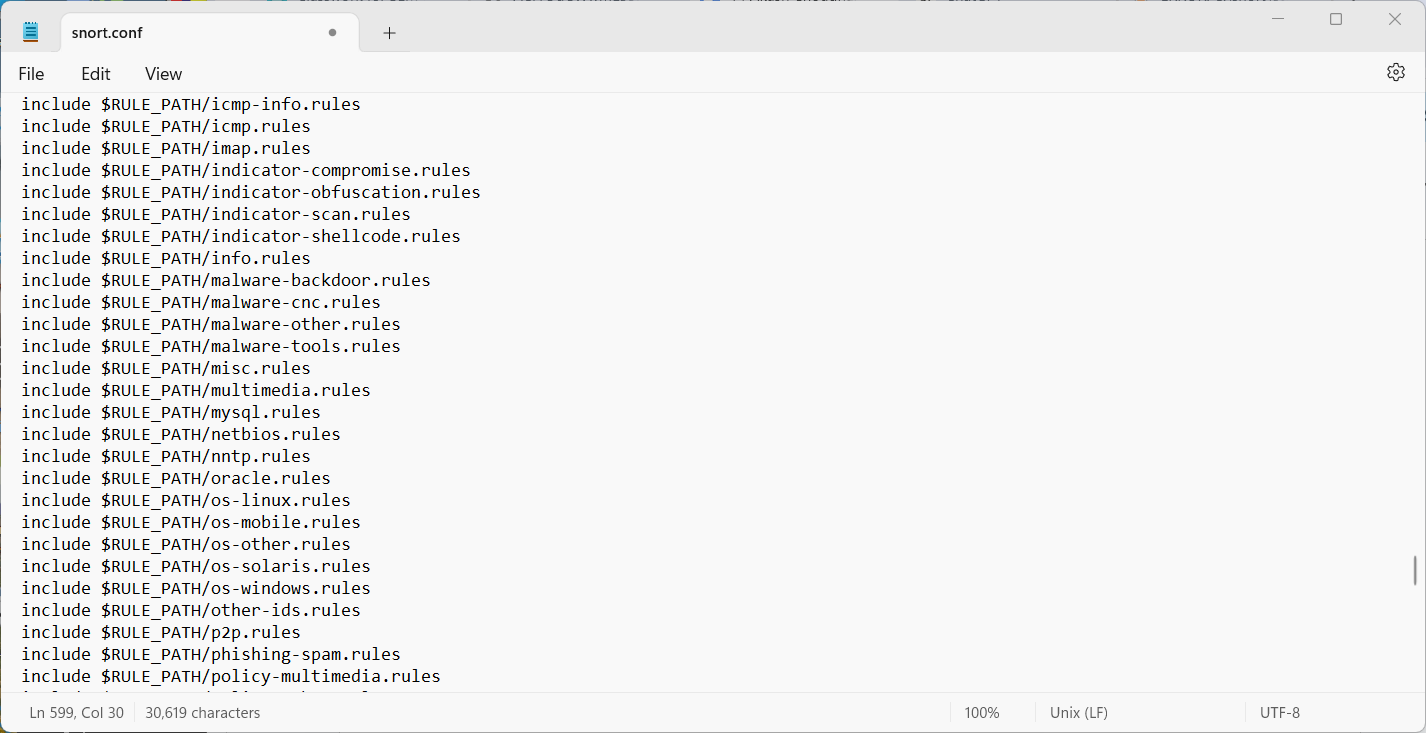


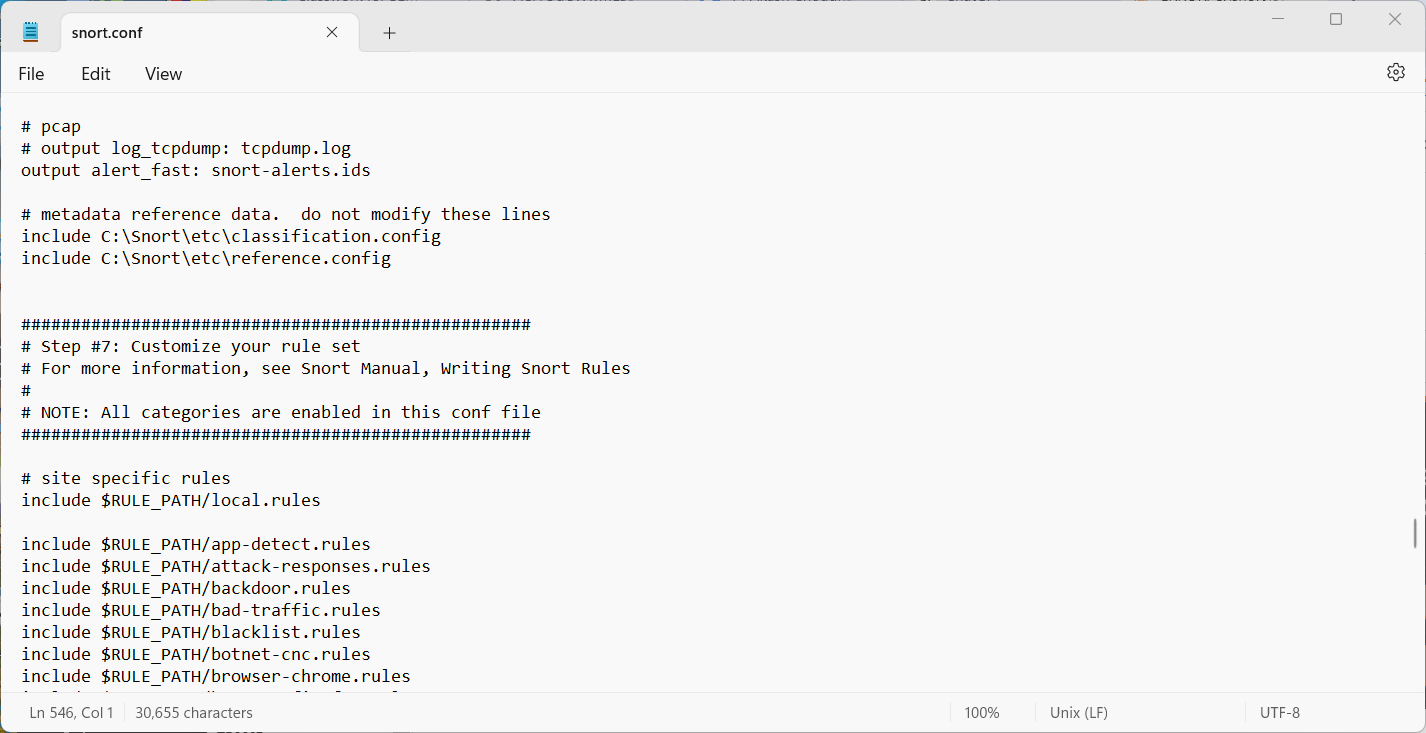


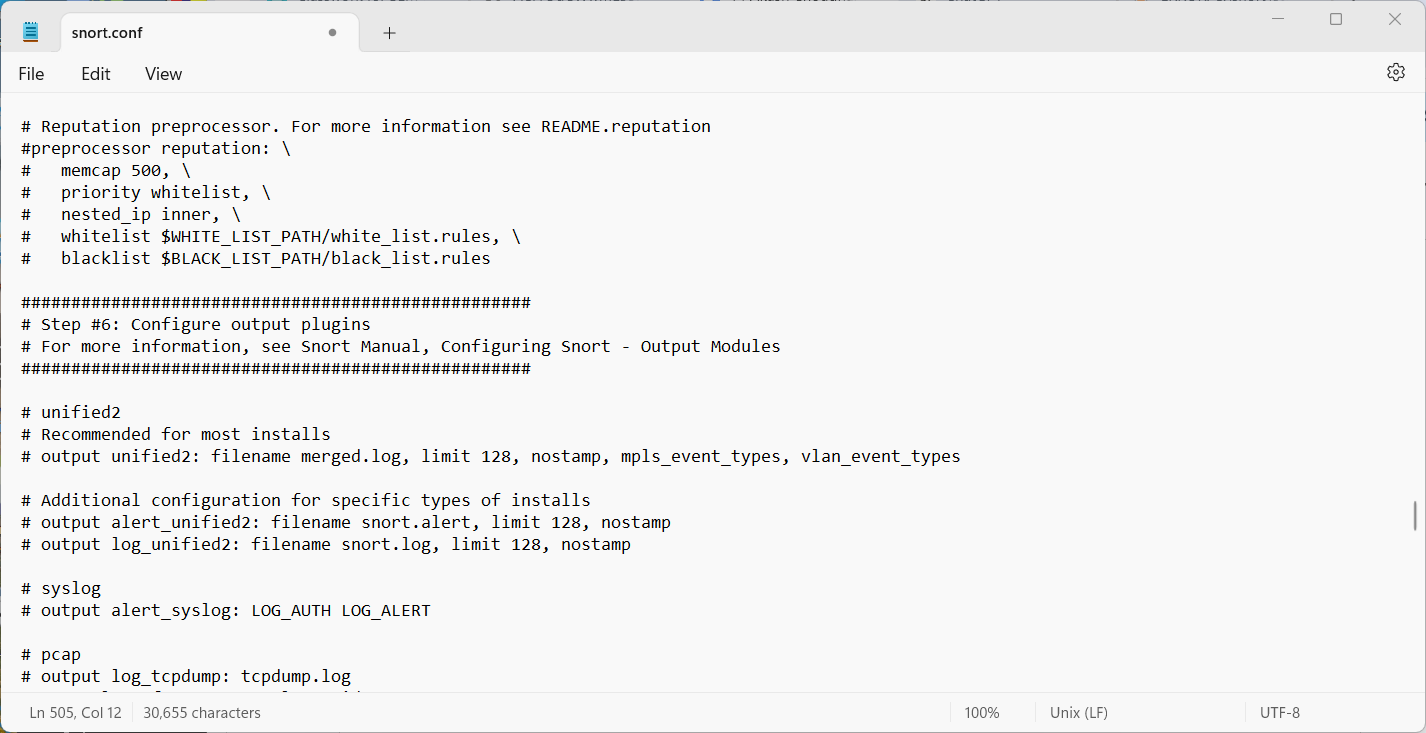


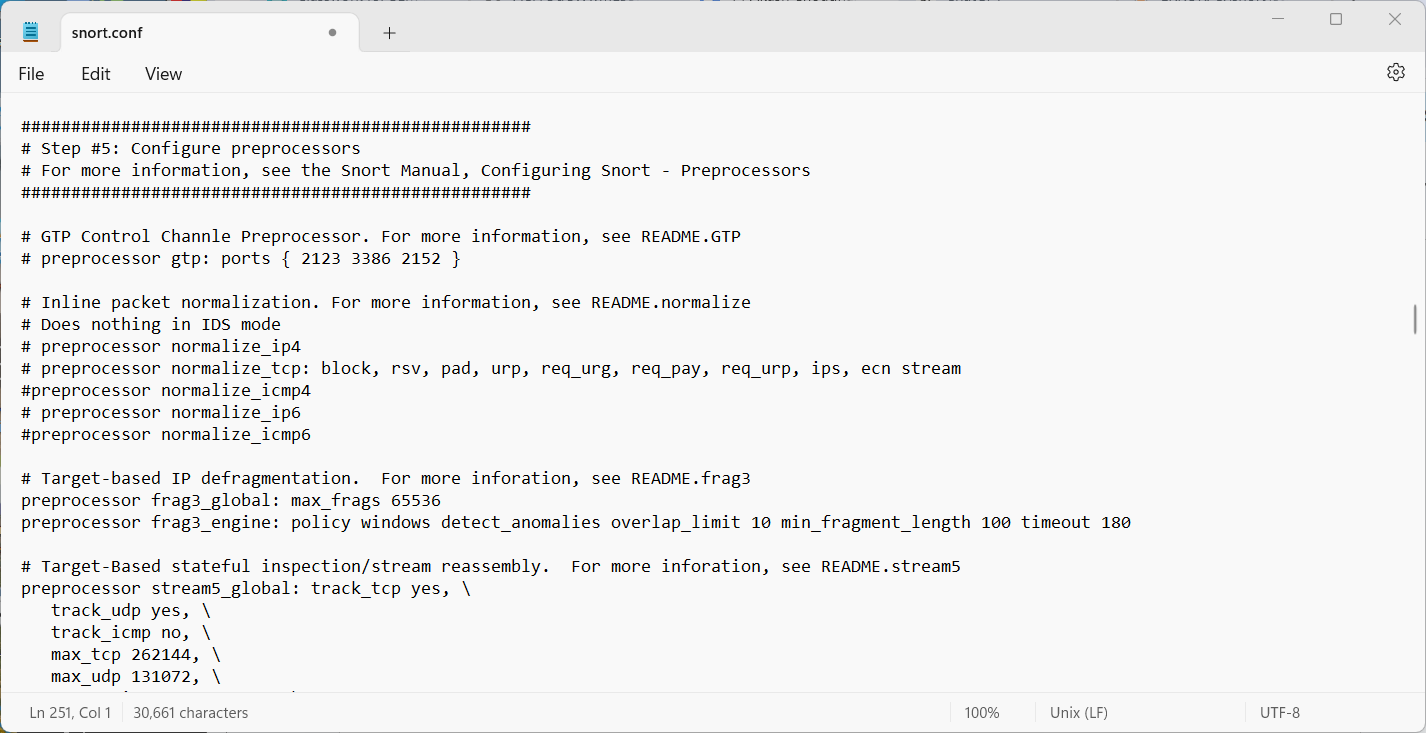


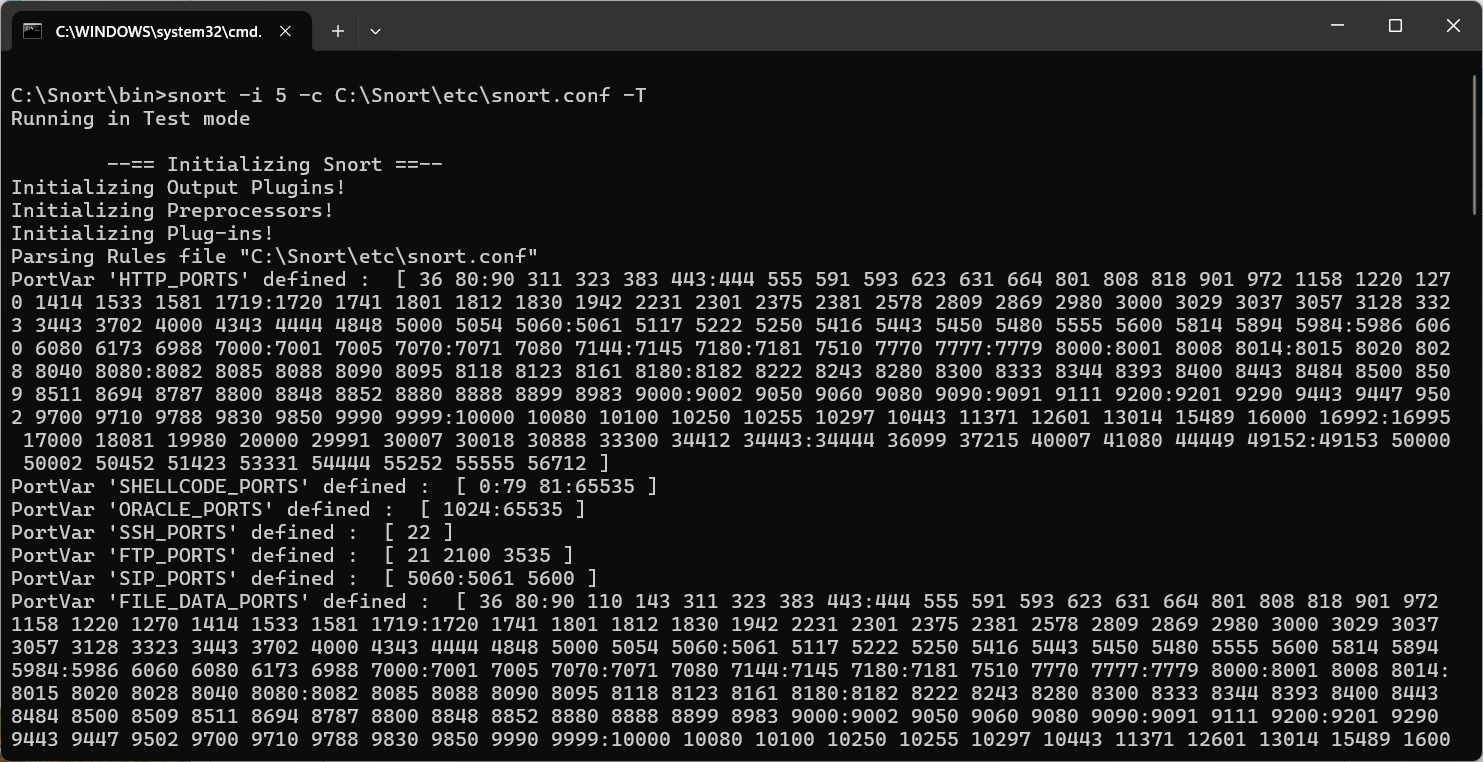


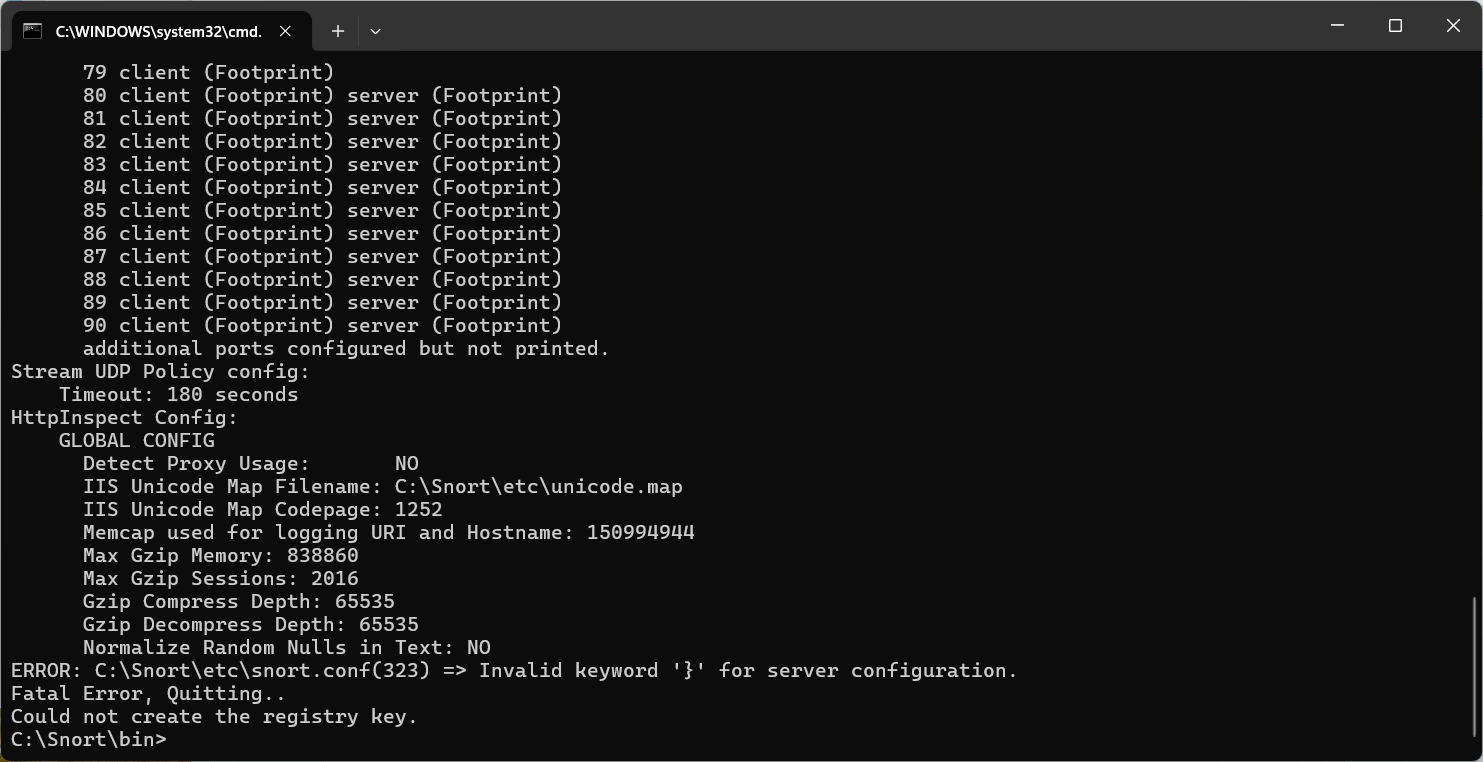


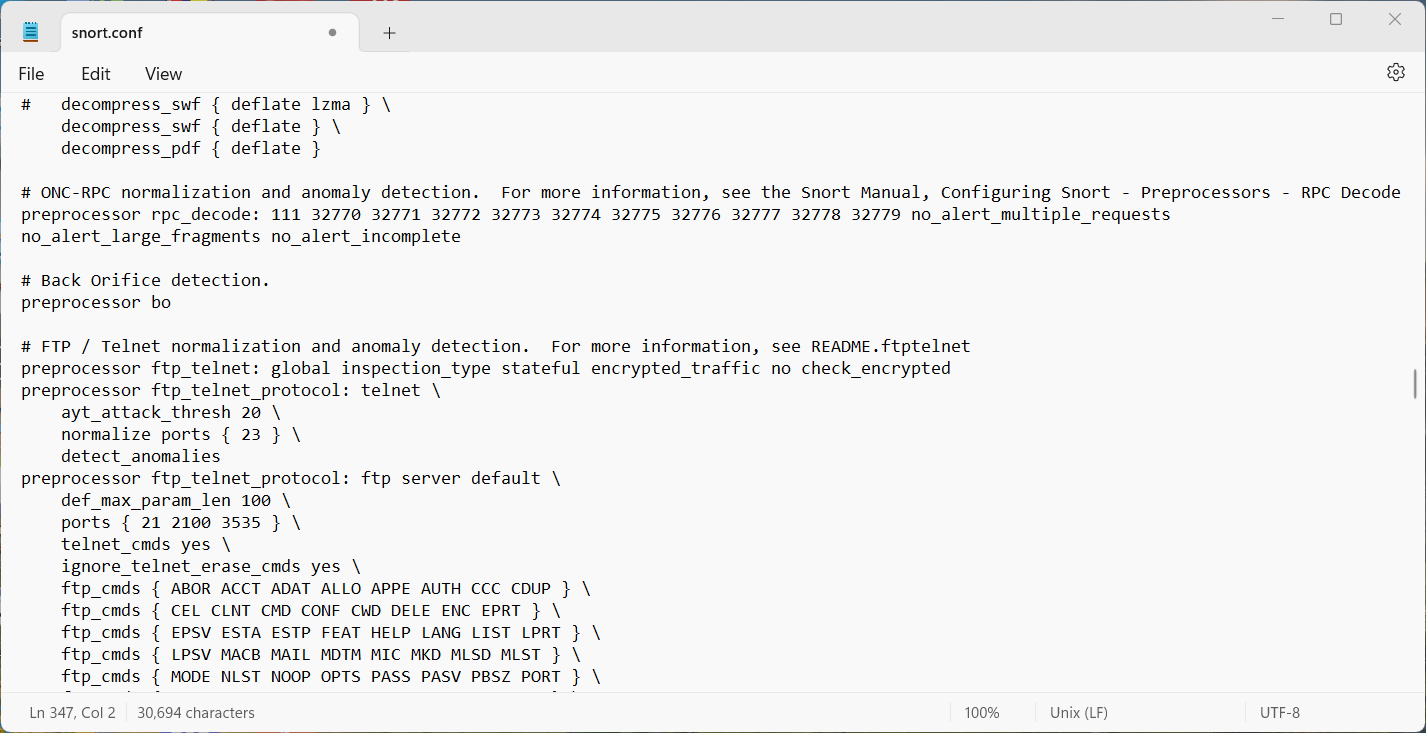












**Download Snort:** <https://snort.org/downloads>

**D. Sniffing Tool**

**Aim:** To use a network sniffing tool to capture and analyze network traffic for monitoring and identifying suspicious activities

**Theory:** Sniffing Tool

Network sniffing tools are designed to capture data packets as they travel across a network, allowing administrators to monitor, analyze, and troubleshoot network issues. These tools can help identify potential security threats, such as unauthorized access or data leakage, by providing insights into the type of traffic, the source and destination of packets, and the nature of the data being transmitted. Sniffing tools can operate in both passive and active modes, where passive sniffing simply monitors the traffic without interference, while active sniffing may involve injecting packets into the network. Effective use of these tools is essential in maintaining network security and ensuring the integrity of data communication.

**Steps to be followed:**

1. **Download Wireshark** from the official website of wireshark.
2. **Open Wireshark**. You will get the **following screen**.
3. **Select the network interface** you want to **sniff**. Note: for this demonstration, we are using a **wireless network connection**. If you are on a local area network, then you should select the local area network interface. **Click on the start button** as shown above.
4. **Open your web browser** and type in <http://www.techpanda.org/>
5. The **login email is admin@google.com** and the **password is Password2010**.
6. **Click** on the **submit button**.
7. A **successful logon** should give you the following **dashboard**.
8. Go **back** to **Wireshark** and **stop the live capture**.
9. **Filter for HTTP protocol** results only using the filter textbox.
10. **Locate** the **Info column** and **look for entries** with the **HTTP verb POST** and click on it.
11. Just below the **log entries**, there is a **panel with a summary of captured data**. Look for the summary that says Line-based text data: application/x-www-form-urlencoded.

**Search:**

1. Open the website:

* Go to http://www.techpanda.org/ in your web browser.

2. Locate the login section:

* Find the fields where you can input your email and password. This is usually on the homepage or under a "Login" or "Sign In" section.

3. Enter the email:

* Click on the email field.
* Type admin@google.com.

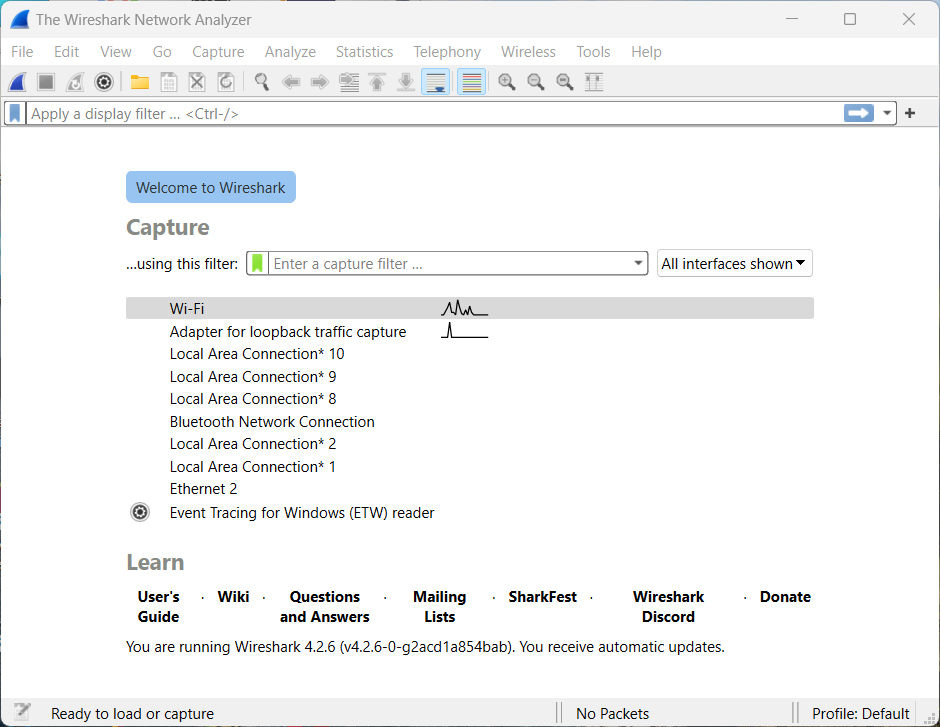
4. Enter the password:

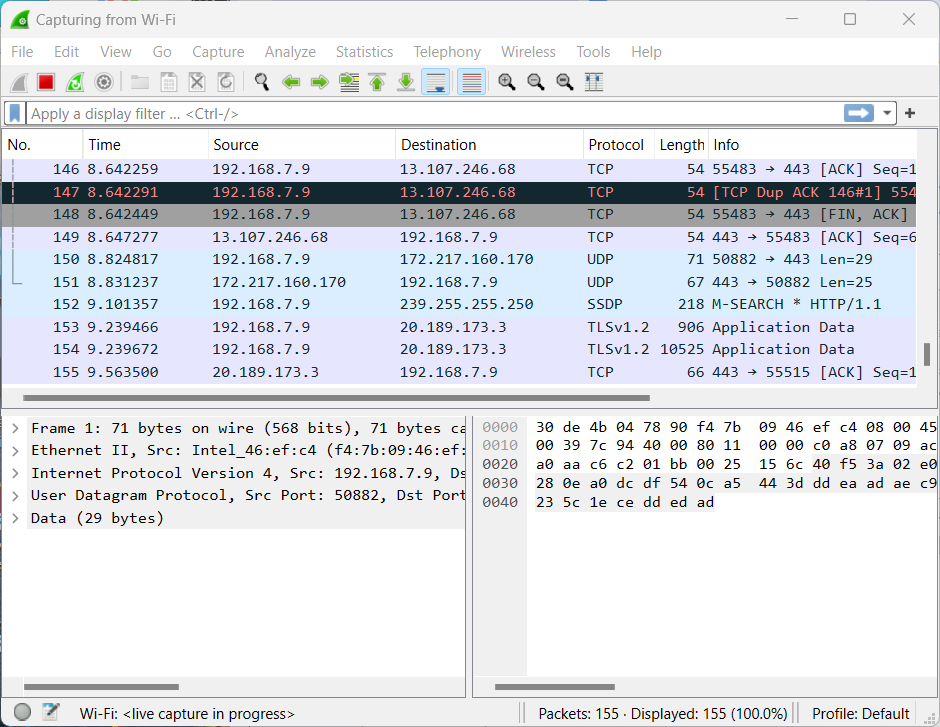
* Click on the password field.
* Type Password2010.

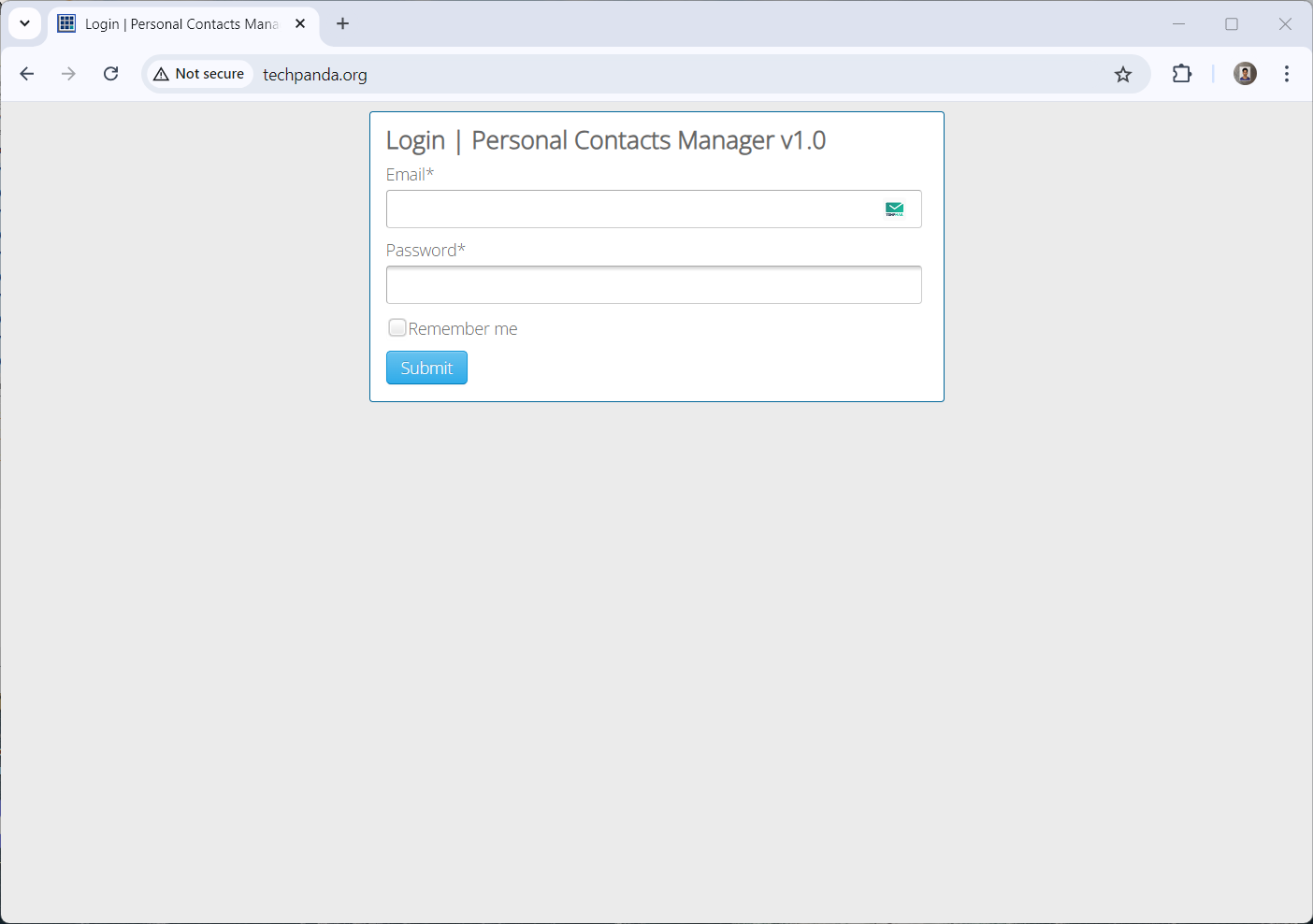
5. Submit:

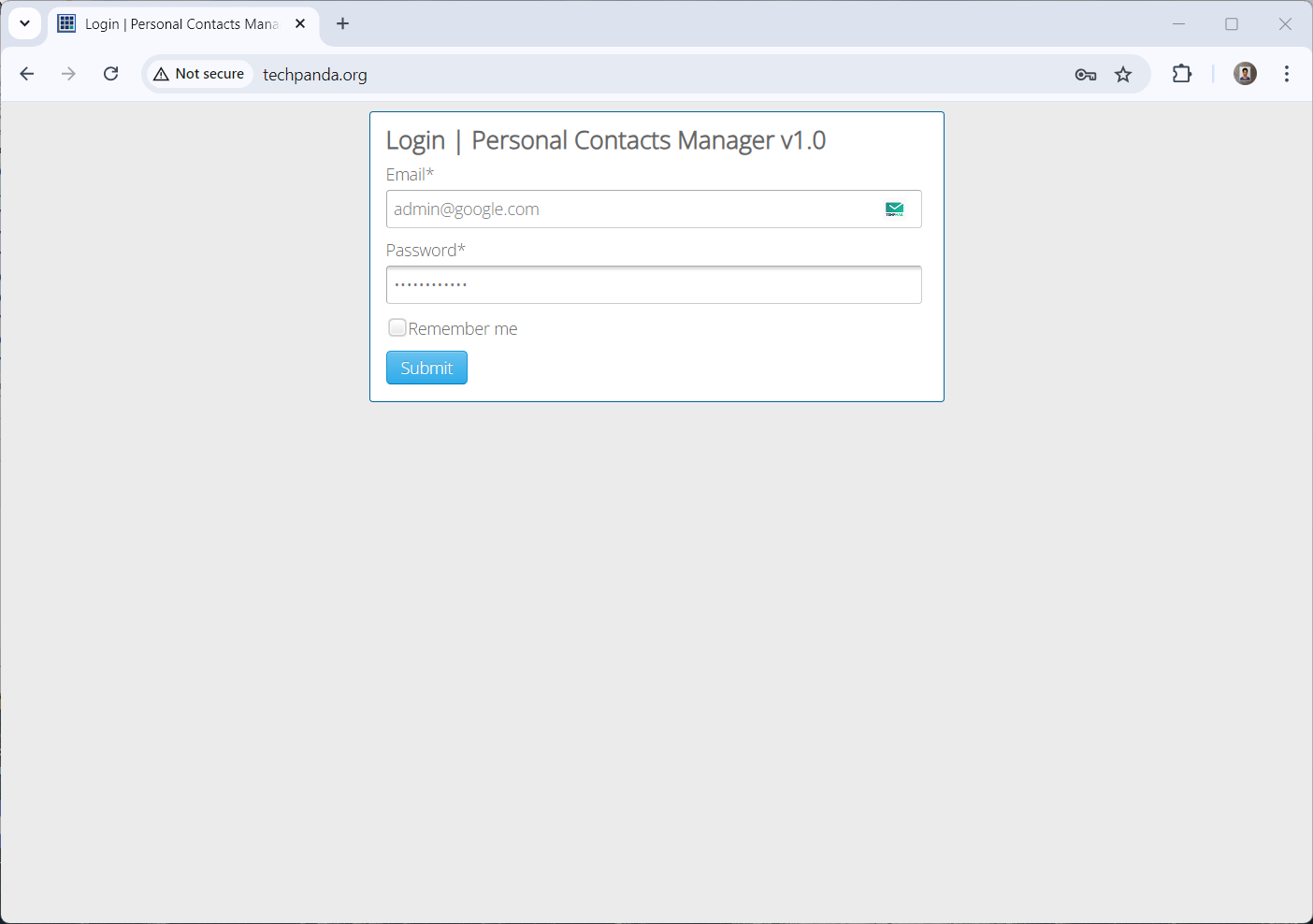
* Click the "Submit" button or the equivalent action button to log in.

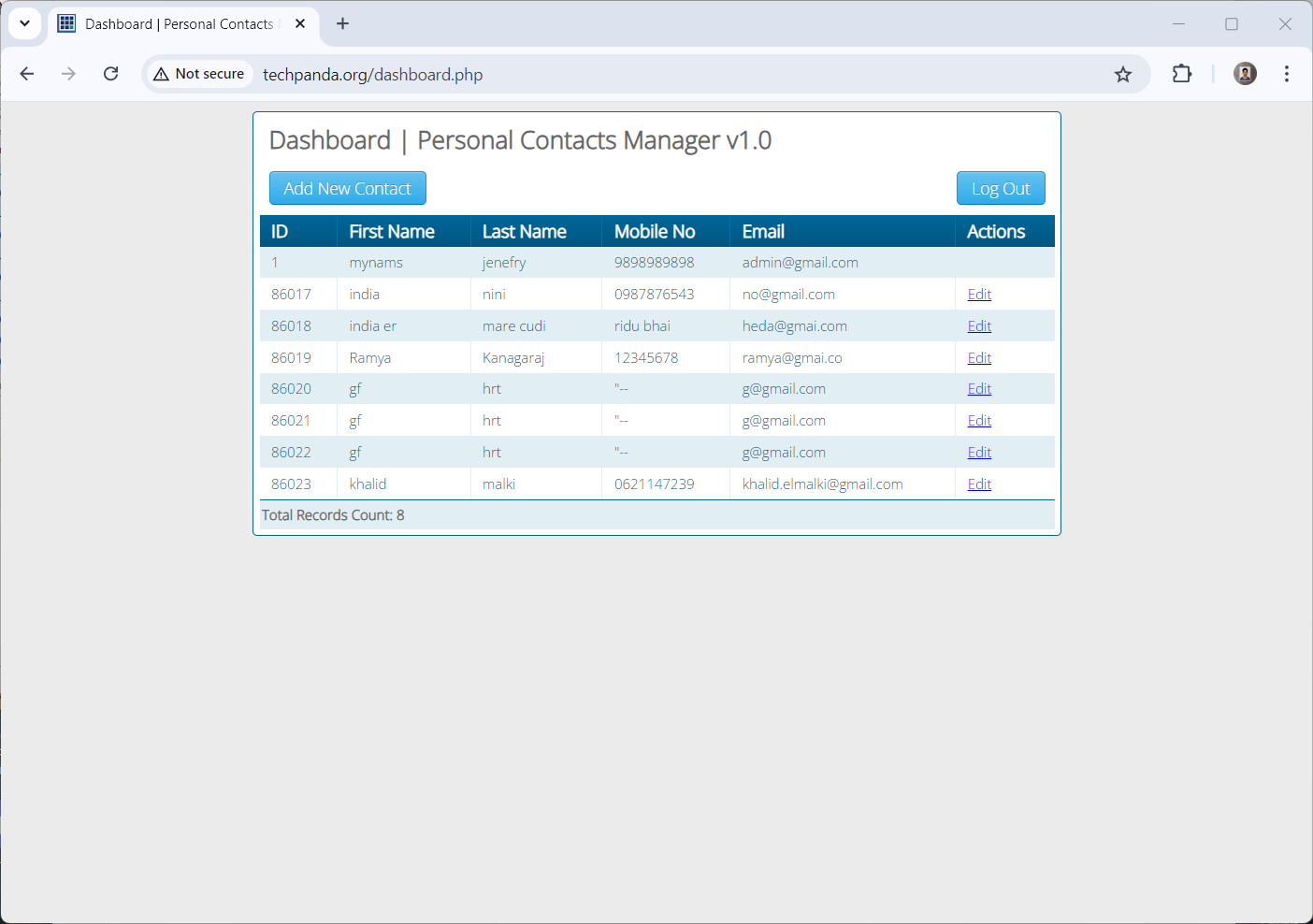
**Output:**

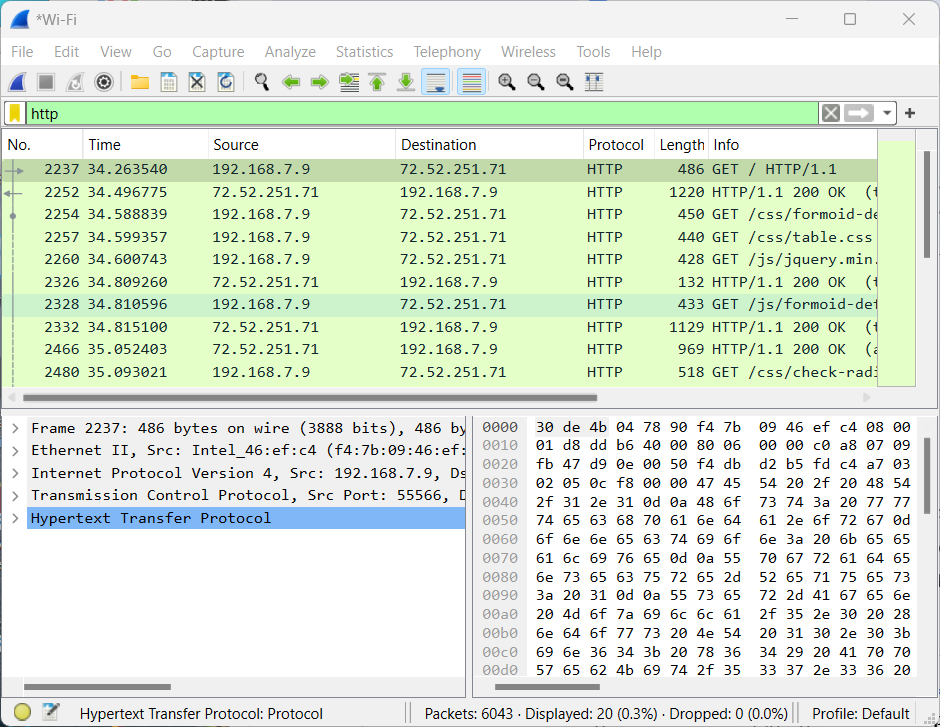


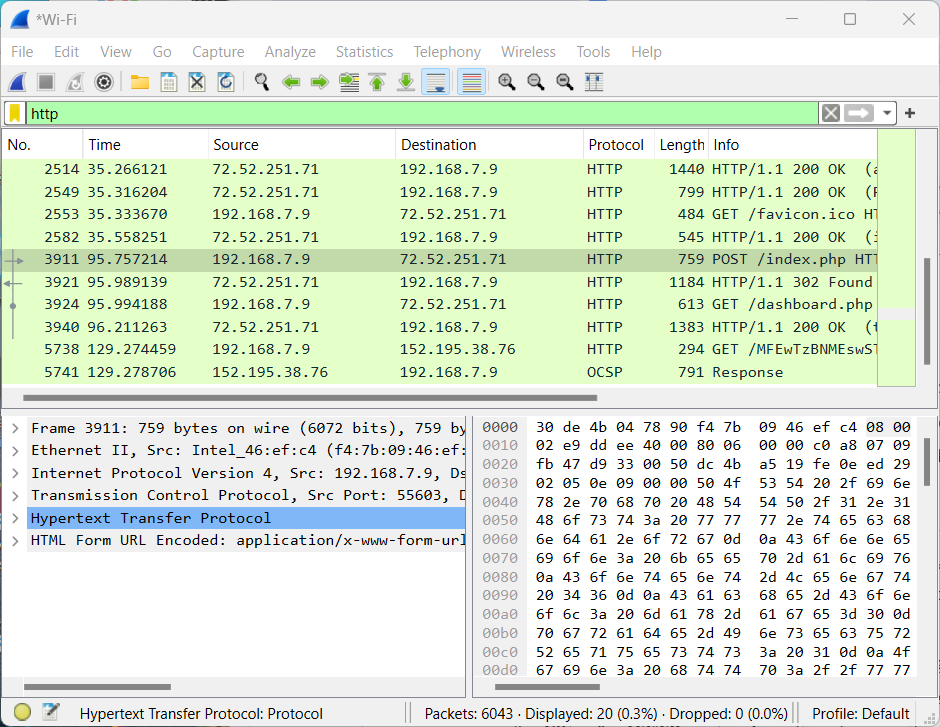


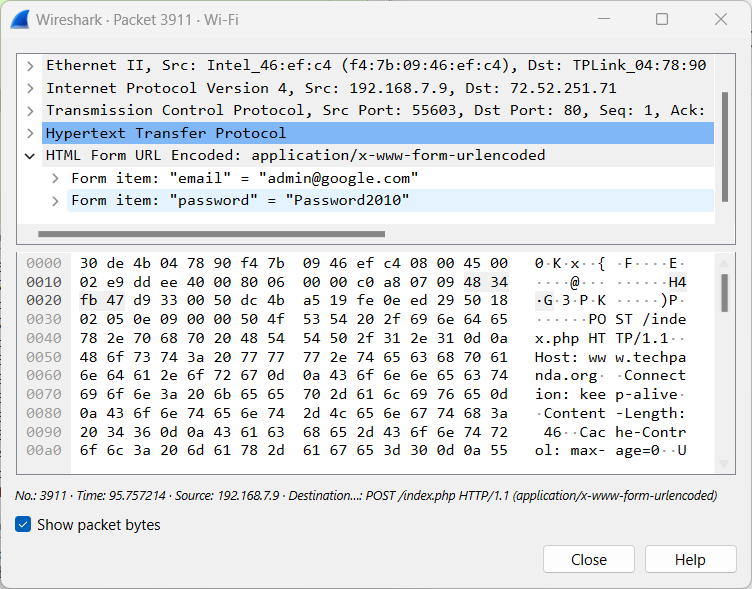












**Download Wireshark:** <https://www.wireshark.org/download.html>