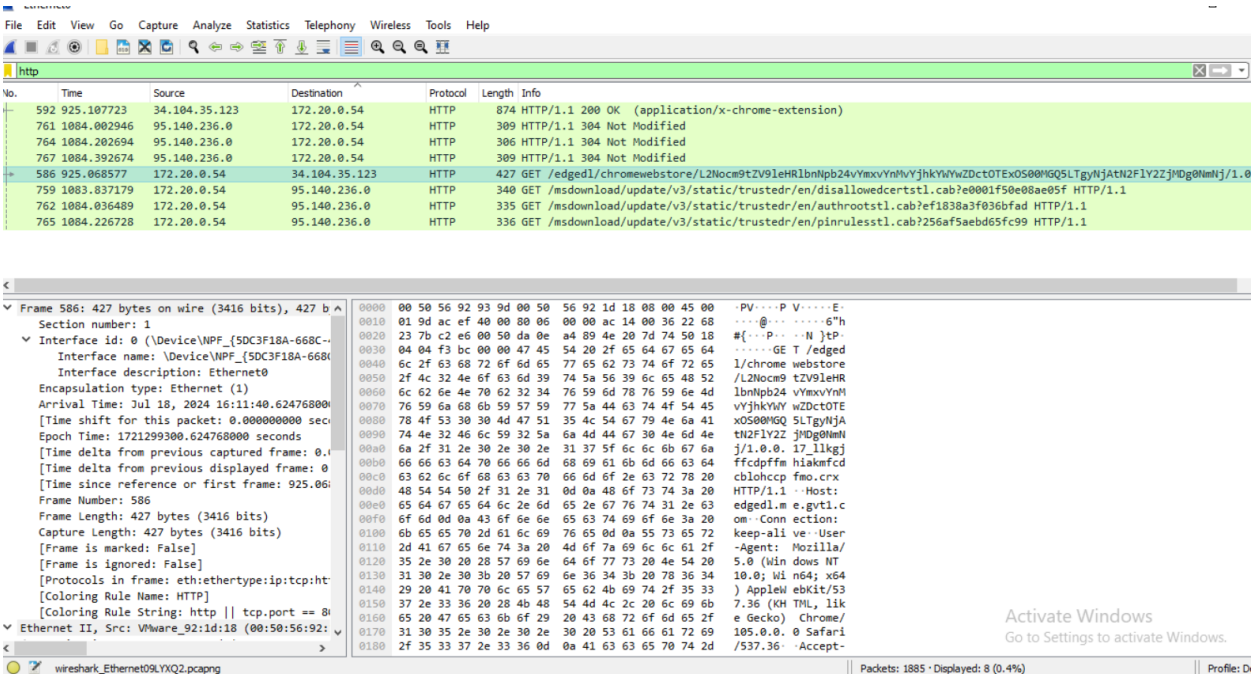
Wireshark lab1 :

Source id : 172.20.0.54

Destination id : 34.104.35.123



Overview of Wireshark
Wireshark is a widely-used network protocol analyzer that captures and interactively browses the traffic running on a computer network. It provides deep inspection of hundreds of protocols and is valuable for troubleshooting network problems, examining security issues, and developing software and protocols.

Start Wireshark : Open Wireshark and select the network interface you want to capture packets from (e.g., Ethernet, Wi-Fi).

- Start Capture : Click on the interface name and then click the green "Start" button to begin capturing packets.

- Apply Capture Filters : Optionally, apply capture filters to limit the captured packets to specific criteria (e.g., IP addresses, protocols) to focus on relevant traffic.

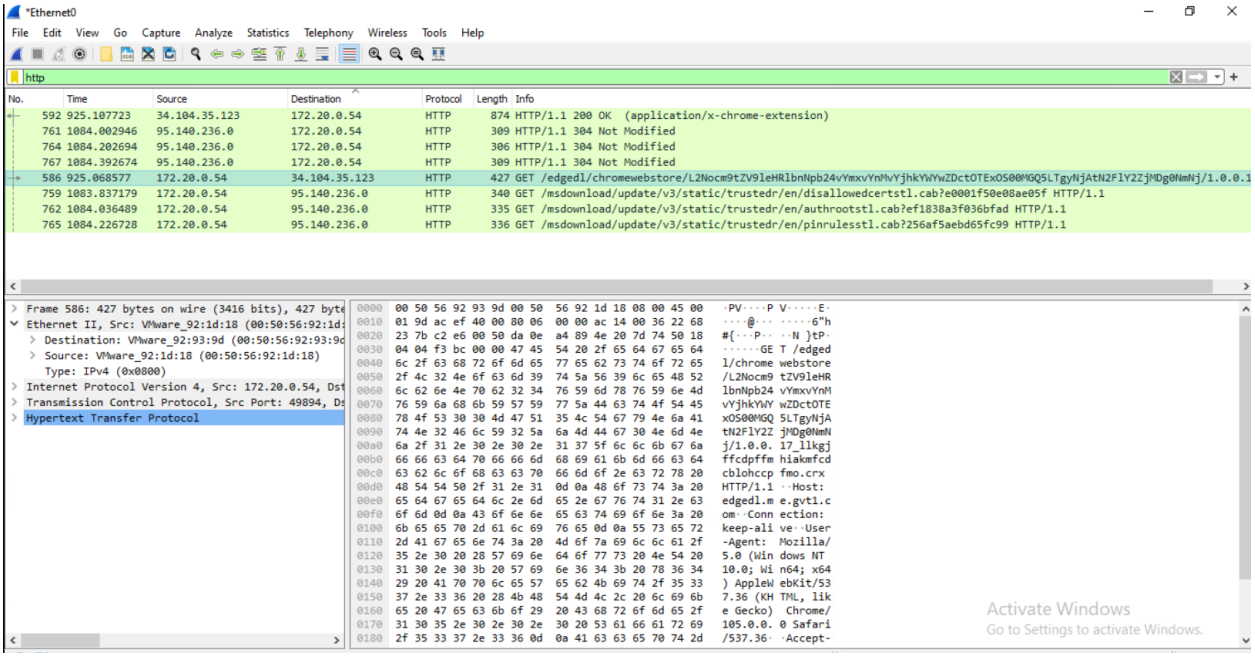
Analyzing Packets

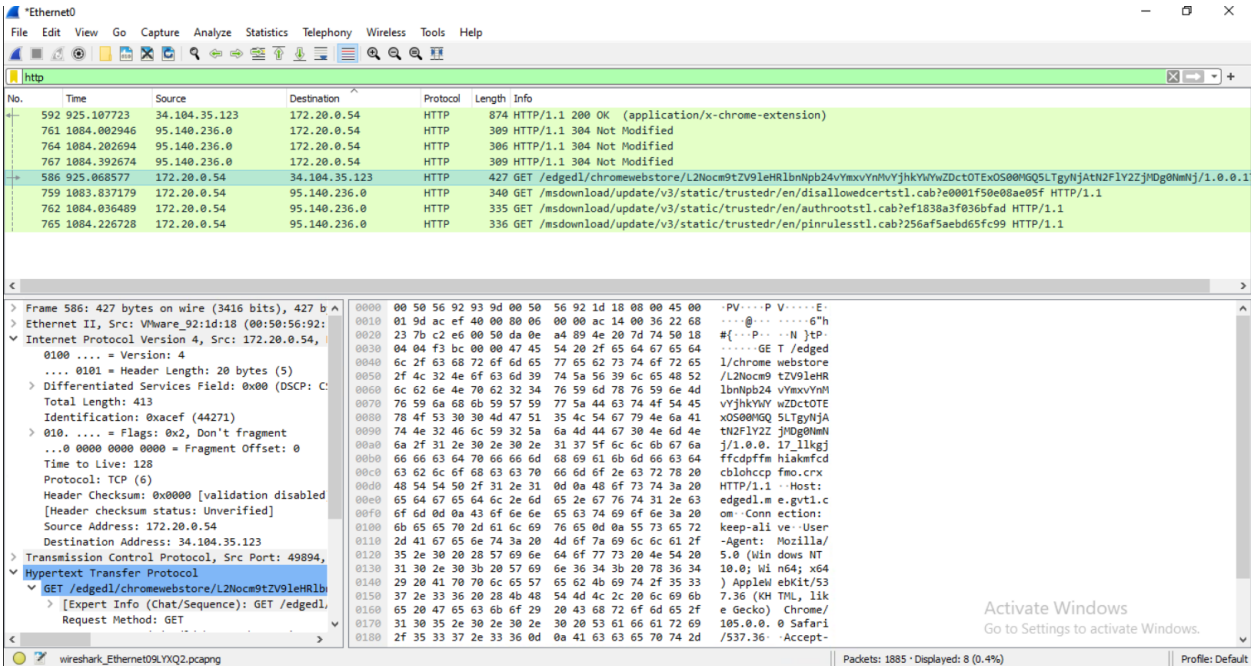
Once you've captured packets, you can analyze them in various ways:

- Packet List Pane : Displays a list of captured packets with summary information (e.g., source and destination addresses, protocols, packet length).

- Packet Details Pane : Provides a detailed view of a selected packet, showing the packet header, its raw data (hex dump), and protocol-specific information.

- Packet Bytes Pane : Shows the raw bytes of the selected packet in hexadecimal and ASCII format.

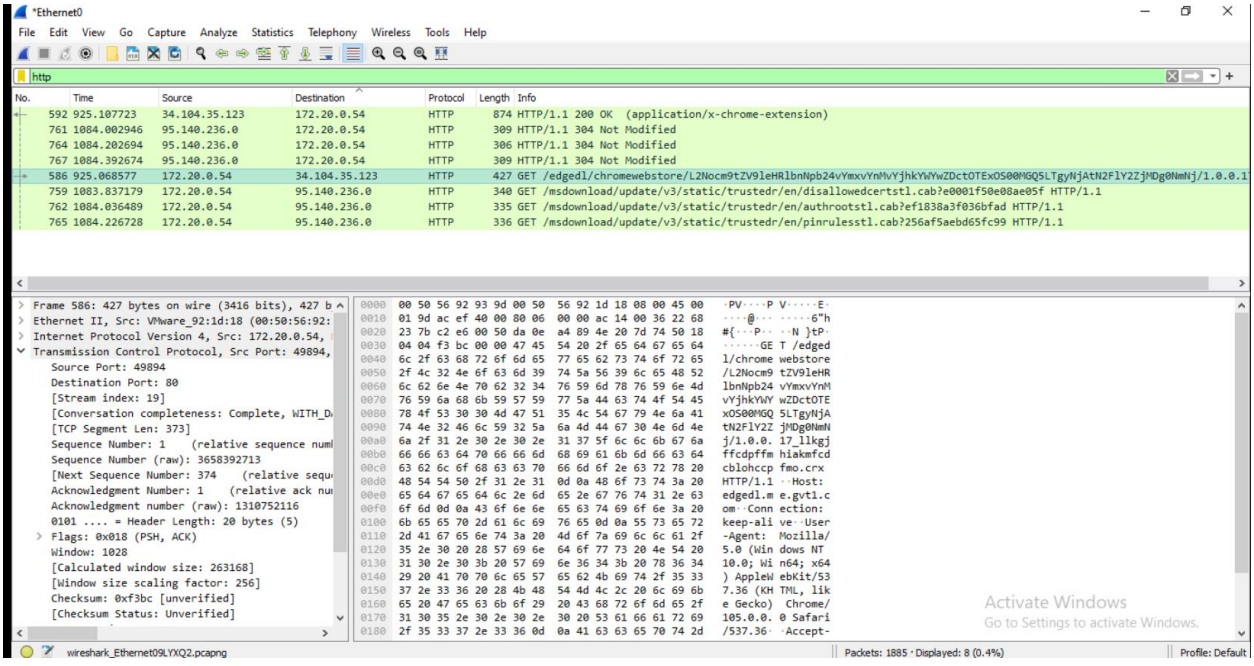


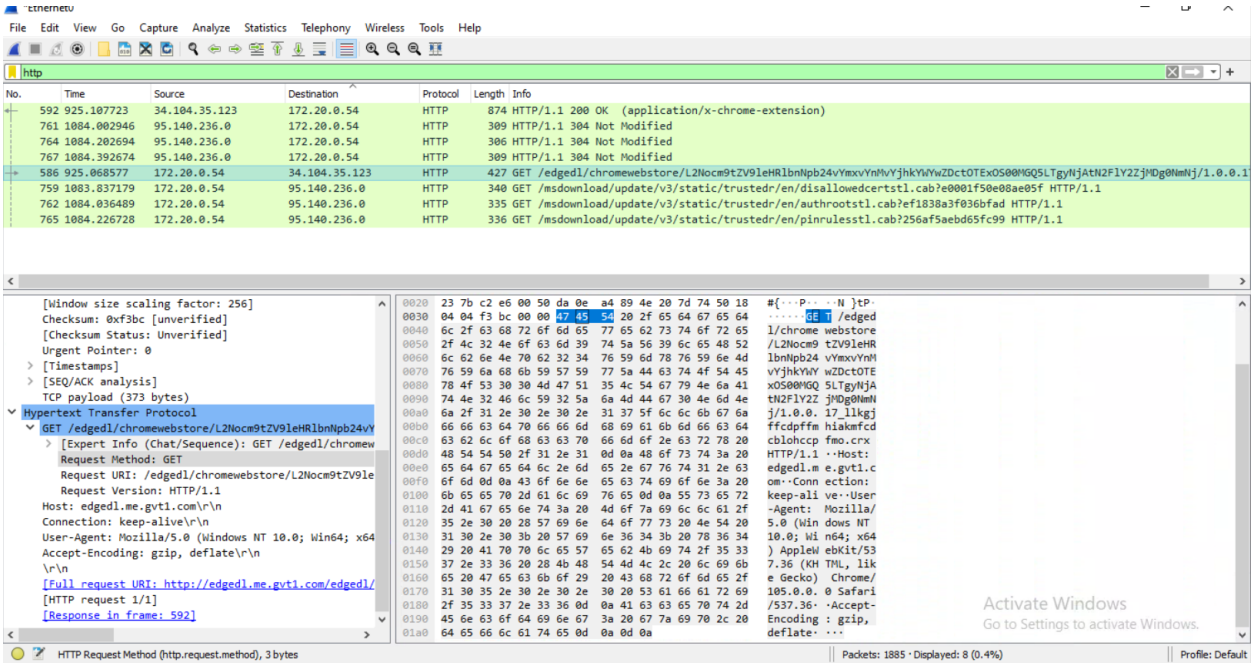


Using Filters:

Display filters (e.g., http, tcp.port == 80).
Capture filters to limit the data being captured (e.g., host 192.168.1.1).
Exporting Data:

Save capture files for later analysis or sharing.
Export specific packets or summaries to various formats (e.g., CSV, XML).





Practical Tips

Filtering: Use display filters to isolate specific traffic, such as http: tcp.port == 80, or Ip.addr == 192.168.1.1.