Capturing and analyzing IP, TCP protocols using Wireshark

Name: Bhargav Surisetti
Date on : July -02,2025

Objectives:

1. Accessing a website in web browser while capturing the network traffic using Wireshark.
2. Filtering the relevant packets of the conversation with the particular website in the captured file.
3. Analyzing the IPV4, TCP header fields and TCP three way handshake procedure in establishing and releasing the connections.

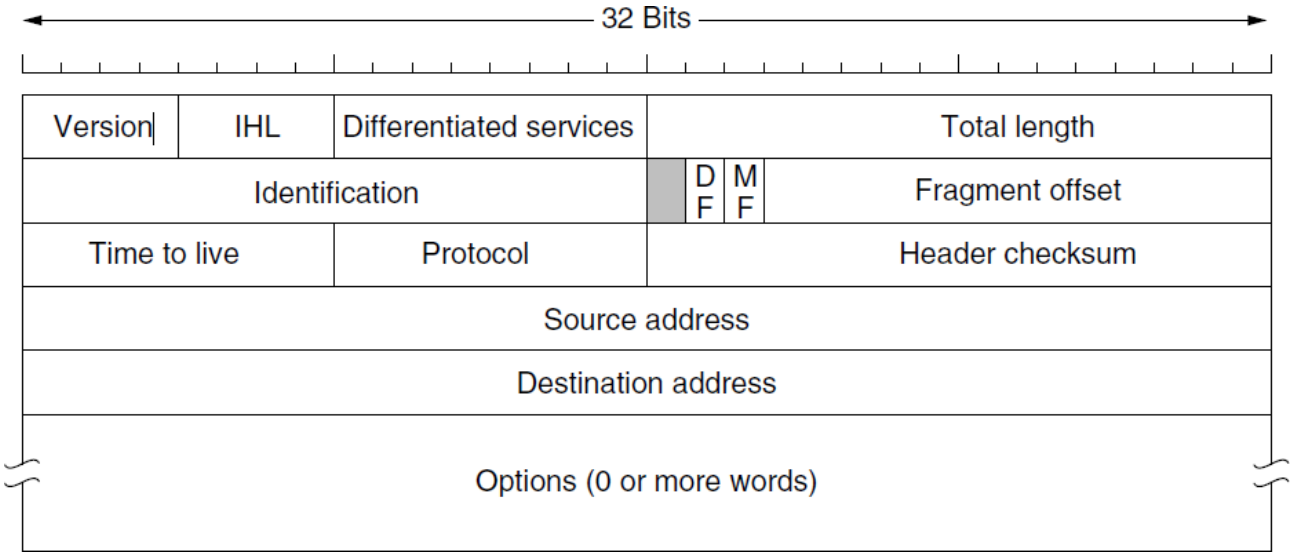
Tool(s) required:

- Wireshark Network Analyzer
- OS: macOS
- Internet Browser / Application (used to generate traffic)

About IPV4 protocol:

- It is a fundamental protocol that routes data packets across the internet, using a 32-bit address system to identify devices and ensure data reaches the correct destination in the presence of multiple networks.
- It is a core protocol that enables communication across the internet and other packet-switched networks.
- Its primary function is to provide a way to identify and locate devices on a network, allowing data packets to be routed from one device to another.
- IPv4 uses a 32-bit address system, which is represented as four sets of numbers (0-255) separated by periods (e.g., 192.168.1.1).
- When a device sends data, it's broken down into packets, each containing the source and destination IP addresses. Routers then use these addresses to forward the packets along the network until they reach their destination.

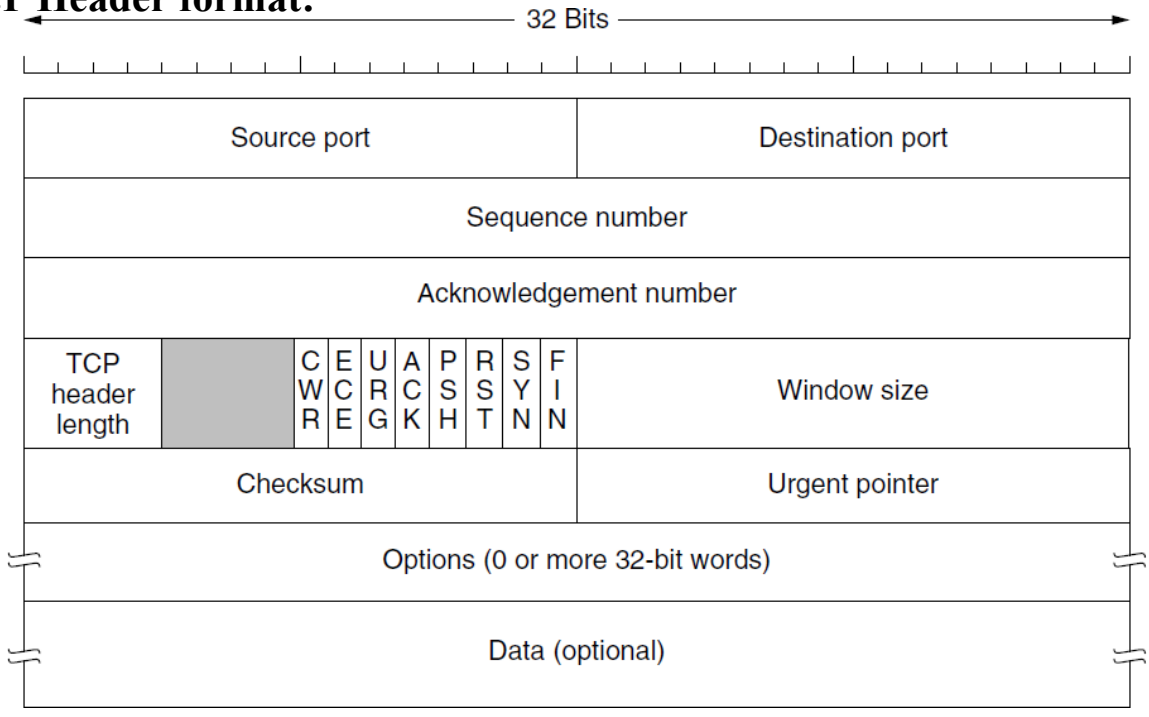
IPV4 Header format:



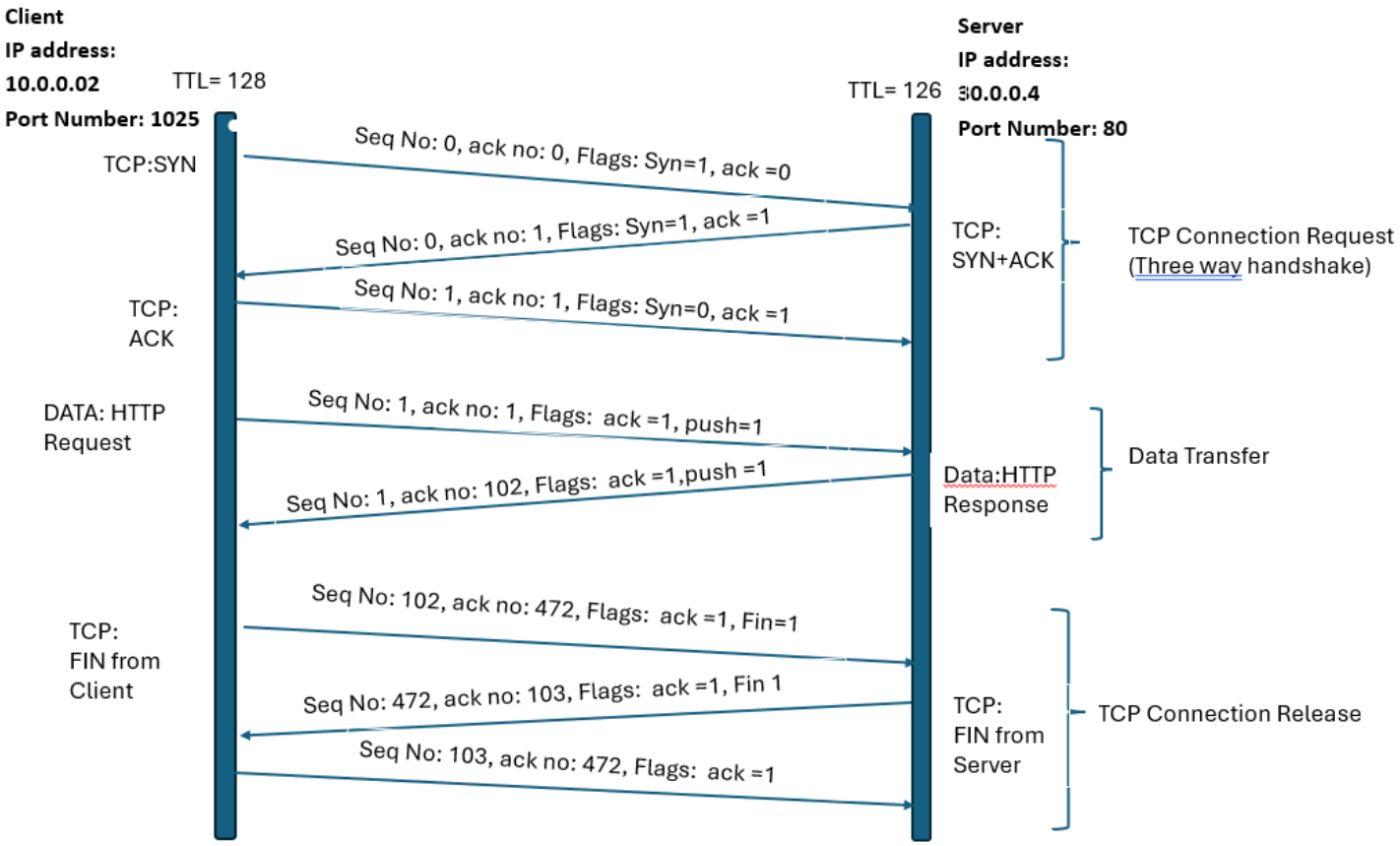
About TCP Protocol:

- TCP (Transmission Control Protocol) is a connection-oriented, reliable protocol that ensures data delivery by using features like a three-way handshake, flow control, and error checking with retransmission, all while maintaining the order of data packets.
- TCP establishes a connection between the sender and receiver before data transmission, using a three-way handshake (SYN, SYN-ACK, ACK) to ensure both parties are ready.
- TCP guarantees reliable data delivery by using sequence numbers, acknowledgements (ACKs), and retransmission mechanisms to handle lost or corrupted packets.
- TCP uses a windowing mechanism to prevent the sender from overwhelming the receiver with data, ensuring efficient and reliable data transfer.

TCP Header format:



TCP three way handshake:



TCP 3-Way Handshake

The TCP 3-way handshake is the process used to establish a reliable connection between a client and server. It involves three steps:

1. SYN – The client sends a synchronize (SYN) packet to initiate the connection.
2. SYN-ACK – The server responds with a synchronize-acknowledgment (SYN-ACK) packet.
3. ACK – The client replies with an acknowledgment (ACK) packet, completing the connection setup.