A logo of a graduation cap

Description automatically generated

Lab Number: 15 Date: 2082-05-15

Title: Packet Capture and Header Analysis by Wire shark

**Theory**

**Wireshark**

Wireshark is an open-source network protocol analyser used for capturing and analysing real-time traffic. It helps in troubleshooting, monitoring performance, and detecting security issues by decoding various protocols and presenting detailed packet information in a graphical interface.

**TCP (Transmission Control Protocol):** A reliable, connection-oriented protocol that ensures accurate, ordered, and error-checked delivery of data. It establishes a connection before data transfer begins, incorporates error checking mechanisms, and guarantees that data packets are delivered in sequence and without duplication. It is commonly used in web browsing, emails, and file transfers.

**UDP (User Datagram Protocol):** A fast, connectionless protocol that does not guarantee delivery or order of packets. It is suitable for applications like video streaming, gaming, and VoIP, where speed is more important than reliability.

**Internet Protocol (IP):** A network layer protocol responsible for addressing and routing packets between devices. It works with TCP and UDP to enable communication across the internet.

**Network Interface Selection and Traffic Filtering**

**Steps:**

1. Open Wireshark and select the network interface (Wi-Fi or Ethernet) where traffic is to be captured.
2. Click the start button to begin capturing live traffic.
3. Apply a filter to focus on specific traffic, such as tcp for TCP traffic, udp for UDP, or ip for general IP traffic.

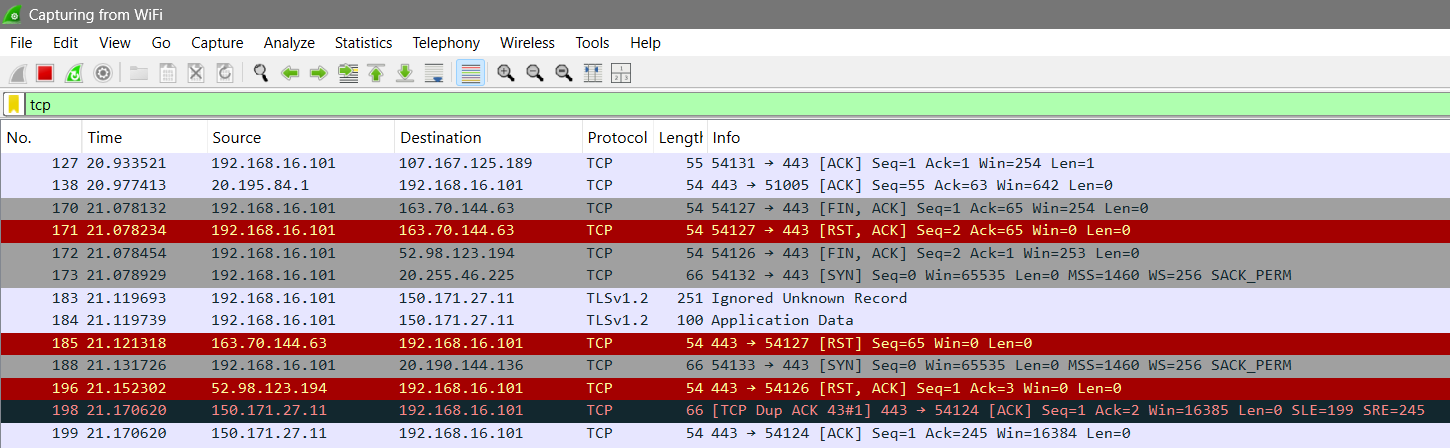


Fig: Traffic Filtering

**TCP Header Analysis**

After capturing TCP traffic, select a TCP packet to view its header details, which include:

* **Source Port:** Identifies the port on the sender's machine (e.g., port 443 for HTTPS).
* **Destination Port:** Specifies the port on the recipient's machine.
* **Sequence Number:** Keeps track of the packet's position in the communication stream.
* **Acknowledgment Number:** Confirms the receipt of previous packets.
* **Flags:** Control bits (e.g., SYN, ACK, FIN) used to manage the connection's state.

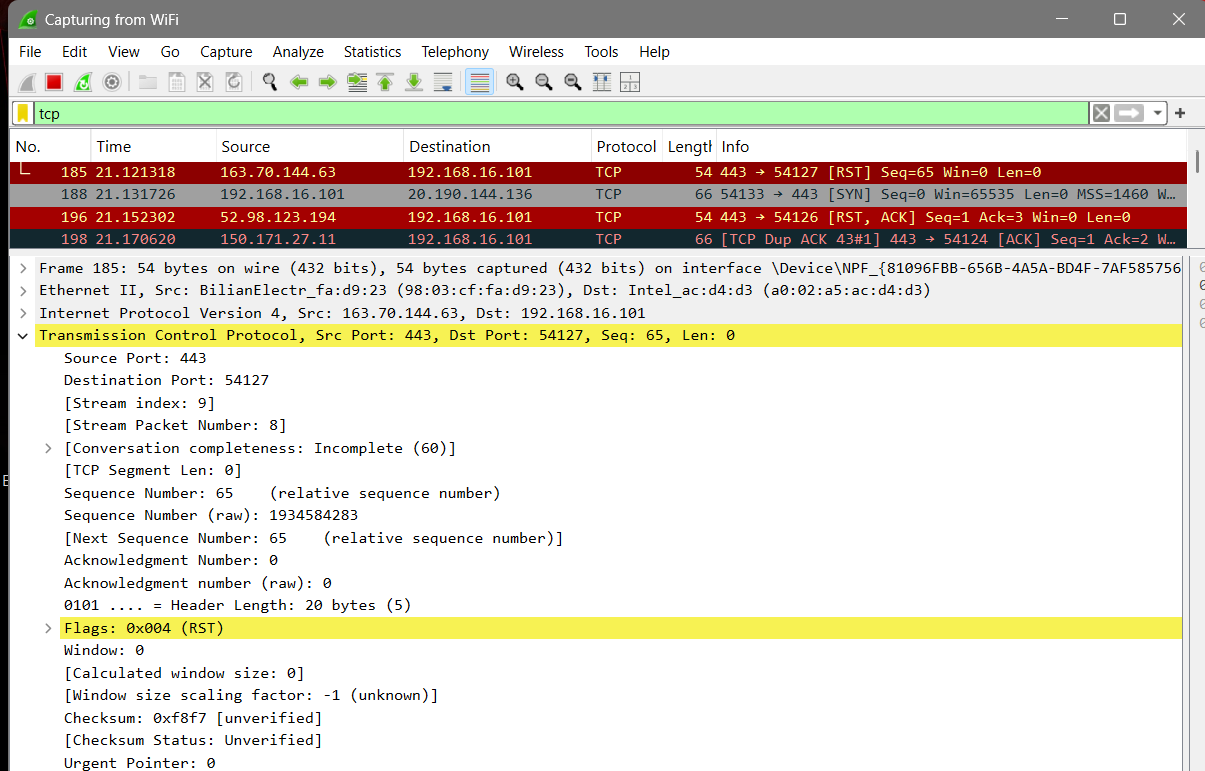


Fig: TCP header analysis of selected packet

**TCP Header Analysis Result:**

From above figure of TCP header analysis, we can deduce the following details for the website youtube.com

| **SN** | **Parameters** | **Details** |
| --- | --- | --- |
| 1 | Source Port | 443 |
| 2 | Destination Port | 54127 |
| 3 | Sequence Number | 65 |
| 4 | Acknowledgment Number | 0 |
| 5 | Flags | RST |

Fig: TCP header analysis details table

**UDP Header Analysis**

Select a UDP packet and analyse its header:

**Source Port**: The port on the sender's side.

**Destination Port**: The port on the receiver's side.

**Length**: Indicates the size of the UDP packet, including the header and data.

**Checksum**: A verification field for ensuring data integer.

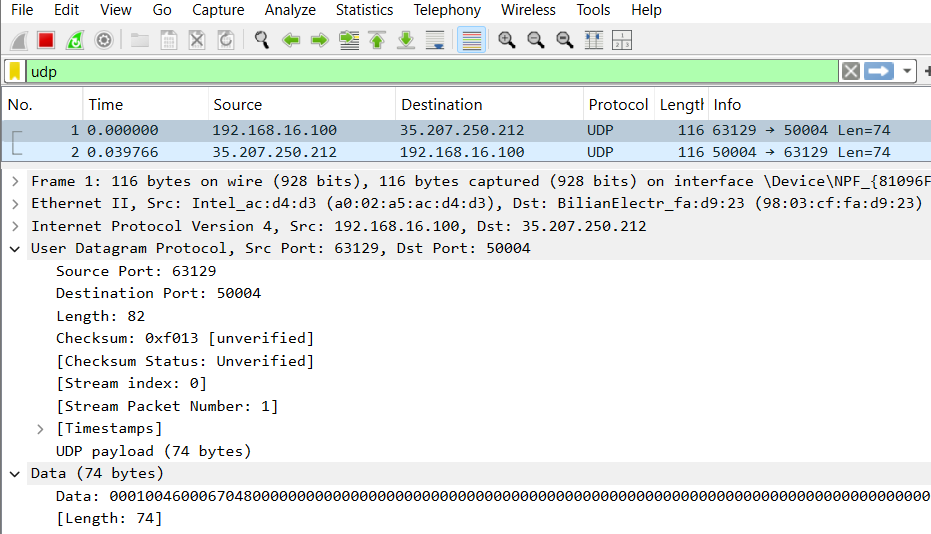


Fig: UDP header analysis of selected packet

**UDP Header Analysis Result:**

From above figure of UDP header analysis, we can deduce the following details for the website youtube.com.

| **SN** | **Parameters** | **Details** |
| --- | --- | --- |
| 1 | Source Port | 63129 |
| 2 | Destination Port | 50004 |
| 3 | Length | 82 |
| 4 | Checksum | 0Xf013 |
| 5 | Stream Index | 0 |
| 6 | Stream Packet Number | 1 |

Fig: UDP header analysis details table

**IP Header Analysis**

**Source IP:** The sender's IP address.

**Destination IP:** The receiver's IP address.

**Header Length:** Indicates the size of the IP header.

**TTL (Time to Live):** Limits the lifespan of the packet, decremented by each router.

**Protocol:** Specifies whether TCP, UDP, or another protocol is being used.

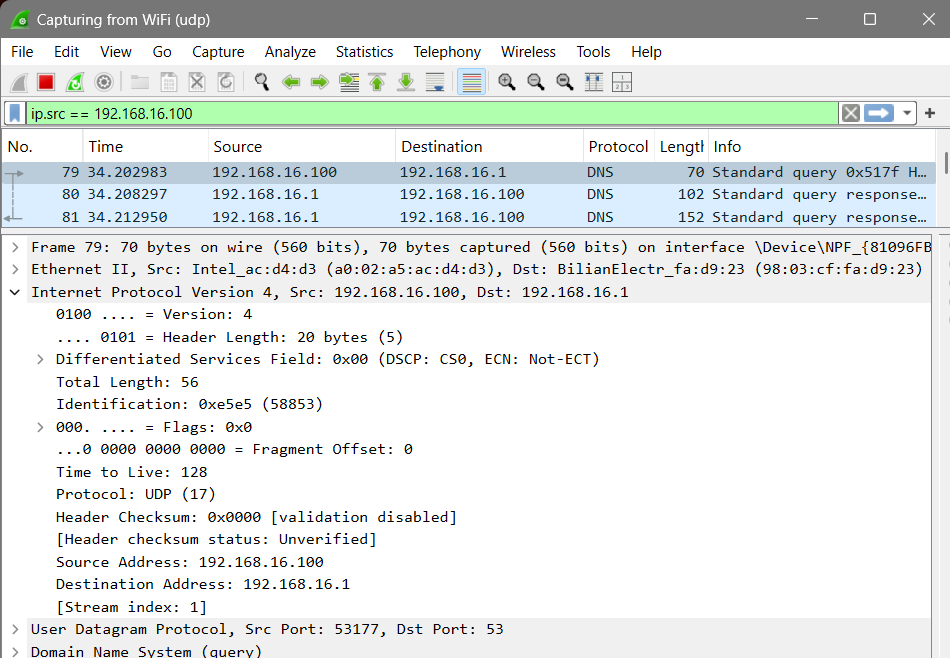


Fig: IP header analysis of selected packet.

**IP Header Analysis Result:**  
From above figure of IP header analysis, we can deduce the following details for the website youtube.com.

| **SN** | **Parameters** | **Details** |
| --- | --- | --- |
| 1 | Source IP | 192.168.16.100 |
| 2 | Destination IP | 192.168.16.1 |
| 3 | Header Length | 20 bytes |
| 4 | TTL (Time to live) | 128 |
| 5 | Protocol | UDP |

Fig: IP header analysis details table

**Conclusion**  
In this lab, we used Wireshark to capture and analyse network packets, focusing on TCP, UDP, and IP protocols. By examining packet headers in real time, we understood how data is transmitted and managed across networks. This practical exercise highlighted the importance of packet analysis for troubleshooting, performance optimization, and strengthening network security.