Lab Number: 15 **Date: 2025/08/30**

Title: Packet Capture and Header Analysis by Wireshark (TCP, UDP, IP)

Theory:

a. Wireshark: Wireshark is a powerful open-source network protocol analyzer that enables real-time capture and analysis of network traffic. Wireshark helps identify issues such as network congestion, security vulnerabilities, misconfigurations, and protocol errors. By allowing users to visualize traffic patterns and analyze the behavior of network protocols, it aids in diagnosing problems efficiently and ensuring optimal network performance. Its ability to capture and decode a wide range of protocols makes it invaluable in both network administration and cybersecurity.

b. **TCP, UDP, IP**

TCP (Transmission Control Protocol) is a connection-oriented protocol designed to ensure reliable data transmission between devices. It establishes a connection before data transfer begins, incorporates error checking mechanisms, and guarantees that data packets are delivered in sequence and without duplication. TCP is widely utilized in applications such as web browsing (HTTP/HTTPS) and email.

UDP (User Datagram Protocol) is a connectionless protocol that prioritizes speed over reliability. It transmits data packets without establishing a connection or ensuring delivery, making it ideal for applications like video streaming, online gaming, and VoIP, where low latency is crucial and some data loss is tolerable.

Internet Protocol (IP) is the primary protocol for routing packets across networks. Operating at the network layer, it assigns IP addresses to devices and ensures that data packets reach their destinations through routing, working alongside both TCP and UDP for end-to-end communication over the Internet.

Implementation

a. Capture the Network Interface of Choice and Filter the traffic

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.

b. TCP Header Analysis

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

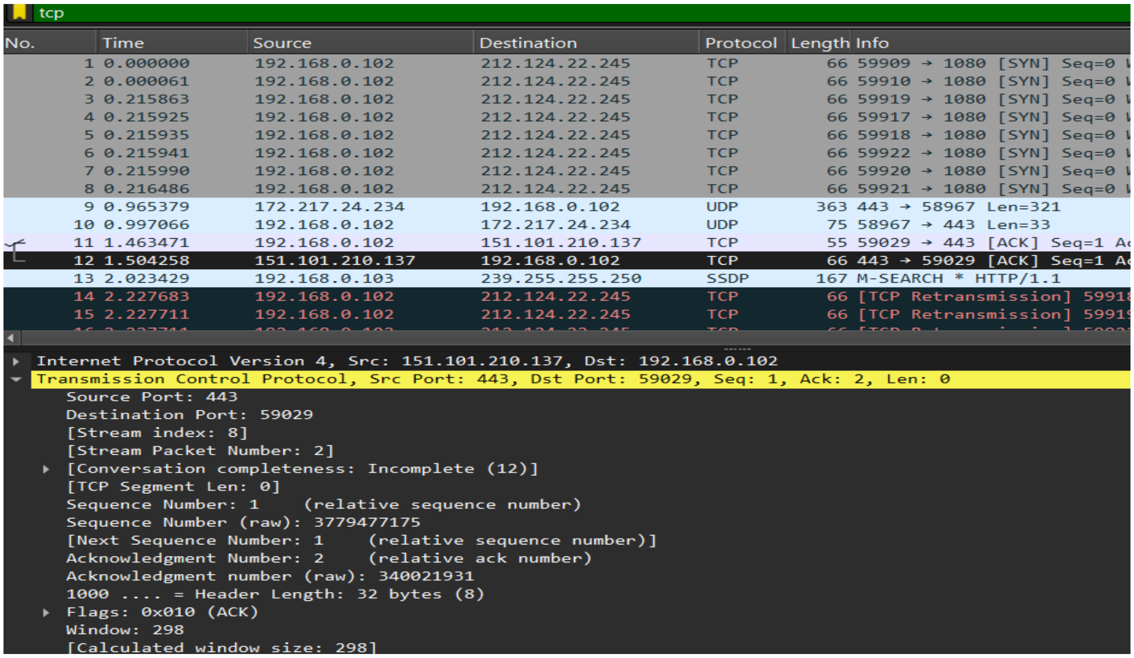
Source Port: Identifies the port on the sender's machine (e.g., port 443 for HTTPS).

Destination Port: Specifies the port on the recipient's machine.

Sequence Number: Keeps track of the packet's position in the communication stream.

Acknowledgement Number: Confirms the receipt of previous packets.

Flags: Control bits (e.g., SYN, ACK, FIN) used to manage the connection's state.



```
tcp
No.     Time        Source           Destination      Protocol Length Info
     1 0.000000    192.168.0.102    212.124.22.245   TCP        66 59909 → 1080 [SYN] Seq=0
     2 0.000061    192.168.0.102    212.124.22.245   TCP        66 59910 → 1080 [SYN] Seq=0
     3 0.215863    192.168.0.102    212.124.22.245   TCP        66 59919 → 1080 [SYN] Seq=0
     4 0.215925    192.168.0.102    212.124.22.245   TCP        66 59917 → 1080 [SYN] Seq=0
     5 0.215935    192.168.0.102    212.124.22.245   TCP        66 59918 → 1080 [SYN] Seq=0
     6 0.215941    192.168.0.102    212.124.22.245   TCP        66 59922 → 1080 [SYN] Seq=0
     7 0.215990    192.168.0.102    212.124.22.245   TCP        66 59920 → 1080 [SYN] Seq=0
     8 0.216486    192.168.0.102    212.124.22.245   TCP        66 59921 → 1080 [SYN] Seq=0
     9 0.965379    172.217.24.234   192.168.0.102    UDP       363 443 → 58967 Len=321
    10 0.997066    192.168.0.102    172.217.24.234   UDP        75 58967 → 443 Len=33
    11 1.463471    192.168.0.102    151.101.210.137  TCP        55 59029 → 443 [ACK] Seq=1 Ac
    12 1.504258    151.101.210.137  192.168.0.102    TCP        66 443 → 59029 [ACK] Seq=1 Ac
    13 2.023429    192.168.0.103    239.255.255.250  SSDP      167 M-SEARCH * HTTP/1.1
    14 2.227683    192.168.0.102    212.124.22.245   TCP        66 [TCP Retransmission] 5991
    15 2.227711    192.168.0.102    212.124.22.245   TCP        66 [TCP Retransmission] 5991

▸ Internet Protocol Version 4, Src: 151.101.210.137, Dst: 192.168.0.102
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 59029, Seq: 1, Ack: 2, Len: 0
      Source Port: 443
      Destination Port: 59029
      [Stream index: 8]
      [Stream Packet Number: 2]
    ▸ [Conversation completeness: Incomplete (12)]
      [TCP Segment Len: 0]
      Sequence Number: 1    (relative sequence number)
      Sequence Number (raw): 3779477175
      [Next Sequence Number: 1    (relative sequence number)]
      Acknowledgment Number: 2    (relative ack number)
      Acknowledgment number (raw): 340021931
      1000 .... = Header Length: 32 bytes (8)
    ▸ Flags: 0x010 (ACK)
      Window: 298
      [Calculated window size: 298]
```

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

S.N.	Parameters	Details
1	Source Port	443
2	Destination Port	59029
3	Sequence Number	1
4	Acknowledgement Number	2
5	Flags	ACK

Fig: TCP header analysis details table

c. UDP Header Analysis

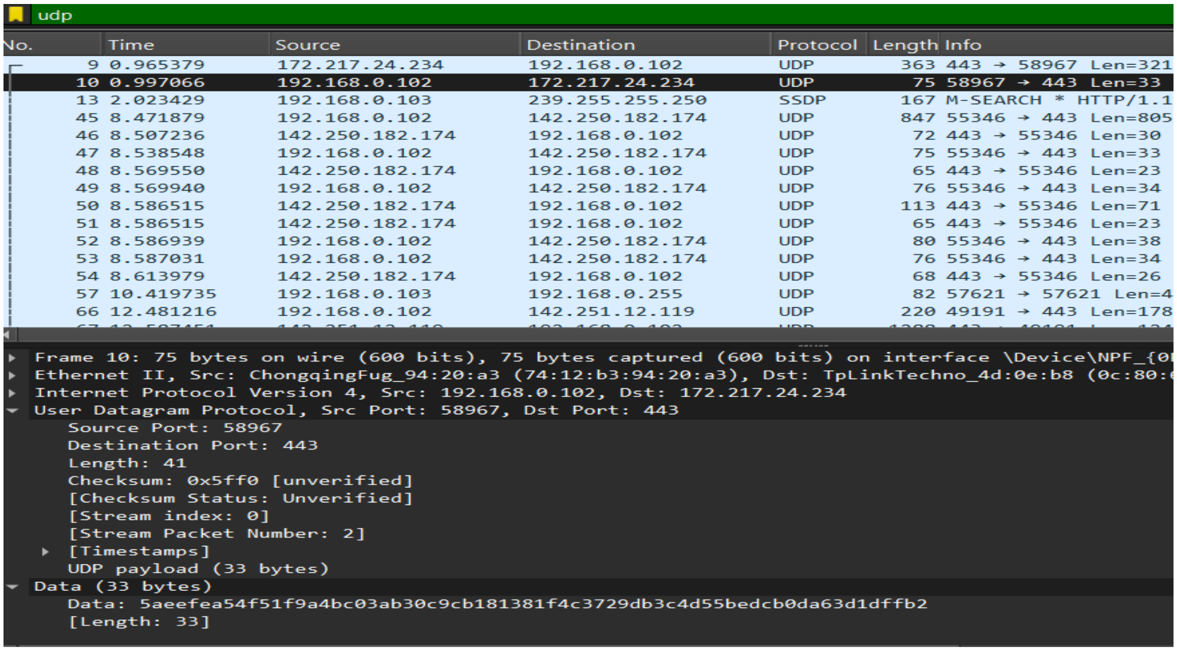
Select a UDP packet and analyze its header:

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.



```
udp
No.     Time        Source            Destination       Protocol Length Info
      9 0.965379    172.217.24.234    192.168.0.102     UDP       363 443 → 58967 Len=321
     10 0.997066    192.168.0.102     172.217.24.234    UDP        75 58967 → 443 Len=33
     13 2.023429    192.168.0.103     239.255.255.250   SSDP      167 M-SEARCH * HTTP/1.1
     45 8.471879    192.168.0.102     142.250.182.174   UDP       847 55346 → 443 Len=805
     46 8.507236    142.250.182.174   192.168.0.102     UDP        72 443 → 55346 Len=30
     47 8.538548    192.168.0.102     142.250.182.174   UDP        75 55346 → 443 Len=33
     48 8.569550    142.250.182.174   192.168.0.102     UDP        65 443 → 55346 Len=23
     49 8.569940    192.168.0.102     142.250.182.174   UDP        76 55346 → 443 Len=34
     50 8.586515    142.250.182.174   192.168.0.102     UDP       113 443 → 55346 Len=71
     51 8.586515    142.250.182.174   192.168.0.102     UDP        65 443 → 55346 Len=23
     52 8.586939    192.168.0.102     142.250.182.174   UDP        80 55346 → 443 Len=38
     53 8.587031    192.168.0.102     142.250.182.174   UDP        76 55346 → 443 Len=34
     54 8.613979    142.250.182.174   192.168.0.102     UDP        68 443 → 55346 Len=26
     57 10.419735   192.168.0.103     192.168.0.255     UDP        82 57621 → 57621 Len=4
     66 12.481216   192.168.0.102     142.251.12.119    UDP       220 49191 → 443 Len=178

▸ Frame 10: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{0
▸ Ethernet II, Src: ChongqingFug_94:20:a3 (74:12:b3:94:20:a3), Dst: TpLinkTechno_4d:0e:b8 (0c:80:
▸ Internet Protocol Version 4, Src: 192.168.0.102, Dst: 172.217.24.234
▾ User Datagram Protocol, Src Port: 58967, Dst Port: 443
     Source Port: 58967
     Destination Port: 443
     Length: 41
     Checksum: 0x5ff0 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 0]
     [Stream Packet Number: 2]
   ▸ [Timestamps]
     UDP payload (33 bytes)
▾ Data (33 bytes)
     Data: 5aeefea54f51f9a4bc03ab30c9cb181381f4c3729db3c4d55bedcb0da63d1dffb2
     [Length: 33]
```

Fig: UDP header analysis of selected packet

UDP Header Analysis Result:

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

SN	Parameters	Details
1	Source Port	58967
2	Destination Port	443
3	Length	41
4	Checksum	0x5ff0
5	Stream Index	0
6	Stream Packet Number	2

Fig; UDP header analysis details table

d. IP Header Analysis

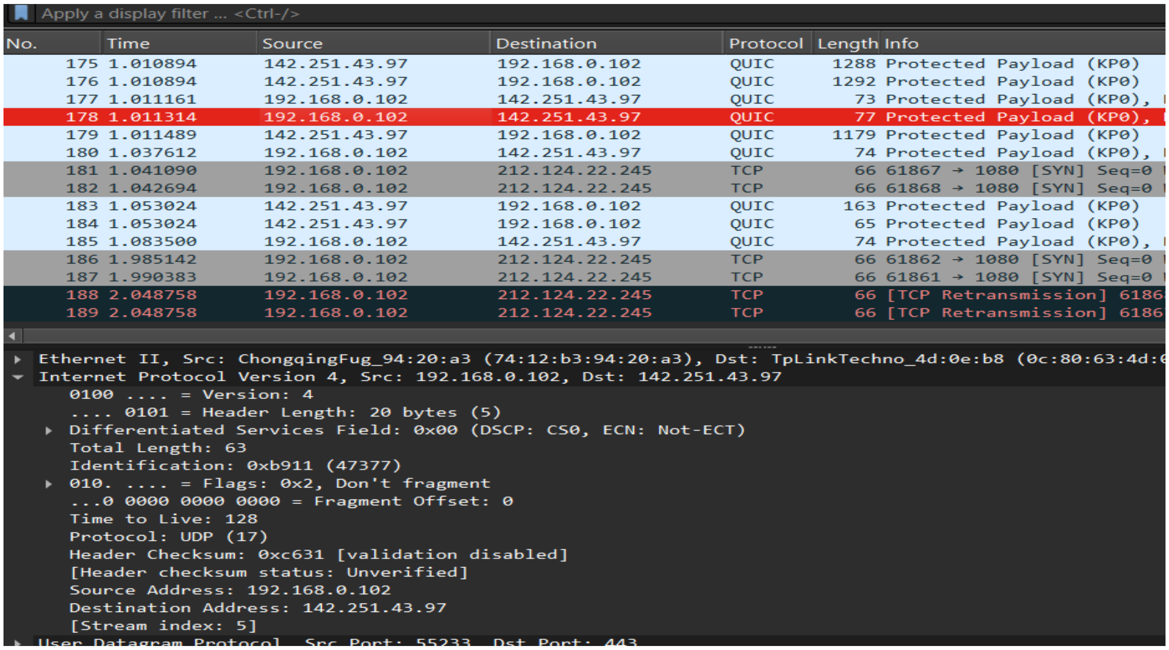
Source IP: The sender's IP address.

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.



```
Apply a display filter ... <Ctrl-/>

No.     Time        Source          Destination      Protocol Length Info
    175 1.010894    142.251.43.97   192.168.0.102    QUIC     1288 Protected Payload (KP0)
    176 1.010894    142.251.43.97   192.168.0.102    QUIC     1292 Protected Payload (KP0)
    177 1.011161    192.168.0.102   142.251.43.97    QUIC       73 Protected Payload (KP0),
    178 1.011314    192.168.0.102   142.251.43.97    QUIC       77 Protected Payload (KP0),
    179 1.011489    142.251.43.97   192.168.0.102    QUIC     1179 Protected Payload (KP0)
    180 1.037612    192.168.0.102   142.251.43.97    QUIC       74 Protected Payload (KP0),
    181 1.041090    192.168.0.102   212.124.22.245   TCP        66 61867 → 1080 [SYN] Seq=0
    182 1.042694    192.168.0.102   212.124.22.245   TCP        66 61868 → 1080 [SYN] Seq=0
    183 1.053024    142.251.43.97   192.168.0.102    QUIC      163 Protected Payload (KP0)
    184 1.053024    142.251.43.97   192.168.0.102    QUIC       65 Protected Payload (KP0)
    185 1.083500    192.168.0.102   142.251.43.97    QUIC       74 Protected Payload (KP0),
    186 1.985142    192.168.0.102   212.124.22.245   TCP        66 61862 → 1080 [SYN] Seq=0
    187 1.990383    192.168.0.102   212.124.22.245   TCP        66 61861 → 1080 [SYN] Seq=0
    188 2.048758    192.168.0.102   212.124.22.245   TCP        66 [TCP Retransmission] 6186
    189 2.048758    192.168.0.102   212.124.22.245   TCP        66 [TCP Retransmission] 6186

▸ Ethernet II, Src: ChongqingFug_94:20:a3 (74:12:b3:94:20:a3), Dst: TpLinkTechno_4d:0e:b8 (0c:80:63:4d:
▾ Internet Protocol Version 4, Src: 192.168.0.102, Dst: 142.251.43.97
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 63
    Identification: 0xb911 (47377)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xc631 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.102
    Destination Address: 142.251.43.97
    [Stream index: 5]
▸ User Datagram Protocol, Src Port: 55233, Dst Port: 443
```

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	192.168.0.102
2	Destination IP	142.251.43.97
3	Header Length	20 bytes
4	TTL (Time to live)	128
5	Protocol	UDP

Fig: IP header analysis details table

Conclusion

In conclusion, this lab provided an in-depth exploration of Packet Capture and Header Analysis using Wireshark, concentrating on essential protocols such as TCP, UDP, and IP. By capturing live network traffic and analyzing packet headers, we gained valuable insights into the mechanisms of data transmission and management across networks. This hands-on experience is crucial for understanding the functionality of different protocols, allowing us to effectively troubleshoot network issues, and enhance security through careful examination of packet-level details, including ports, IP addresses, and control flags.