Network Protocol Information

UDP Header

Question 1:
What is the size of the UDP header?
Ans: The UDP header is 8 bytes (64 bits) long.

Question 2:
What are the different fields in the UDP header?
Ans: The UDP header consists of the following fields:

- Source Port (16 bits)
- Destination Port (16 bits)
- Length (16 bits)
- Checksum (16 bits)

Question 3: Describe the fields in the UDP header.

- Source Port (16 bits): The port number of the sending process.
- Destination Port (16 bits): The port number of the receiving process.
- Length (16 bits): The length of the UDP header and data. The minimum value is 8 bytes (the size of the header).
- Checksum (16 bits): Used for error-checking of the header and data.

TCP Header

Question 4: What is the size of the TCP header?
The size of the TCP header is a minimum of 20 bytes (160 bits), but it can be larger if options are used.

Question 5: What are the different fields in the TCP header?
The TCP header consists of the following fields:

- Source Port (16 bits)
- Destination Port (16 bits)
- Sequence Number (32 bits)
- Acknowledgment Number (32 bits)
- Data Offset (4 bits)
- Reserved (3 bits)
- Flags (9 bits)
- Window Size (16 bits)
- Checksum (16 bits)
- Urgent Pointer (16 bits)
- Options (variable length)

Question 6: Describe the fields in the TCP header.

- Source Port (16 bits): The port number of the sending process.
- Destination Port (16 bits): The port number of the receiving process.
- Sequence Number (32 bits): The sequence number of the first byte of data in this segment.
- Acknowledgment Number (32 bits): If the ACK flag is set, this field contains the value of the next sequence number that the sender is expecting to receive.
- Data Offset (4 bits): The size of the TCP header in 32-bit words.
- Reserved (3 bits): Reserved for future use and should be set to zero.
- Flags (9 bits): Control flags such as URG, ACK, PSH, RST, SYN, and FIN.
- Window Size (16 bits): The size of the receive window, which specifies the number of bytes that the sender is willing to receive.
- Checksum (16 bits): Used for error-checking of the header and data.
- Urgent Pointer (16 bits): If the URG flag is set, this field points to the sequence number of the byte following urgent data.
- Options (variable length): Optional additional fields that can extend the header size.

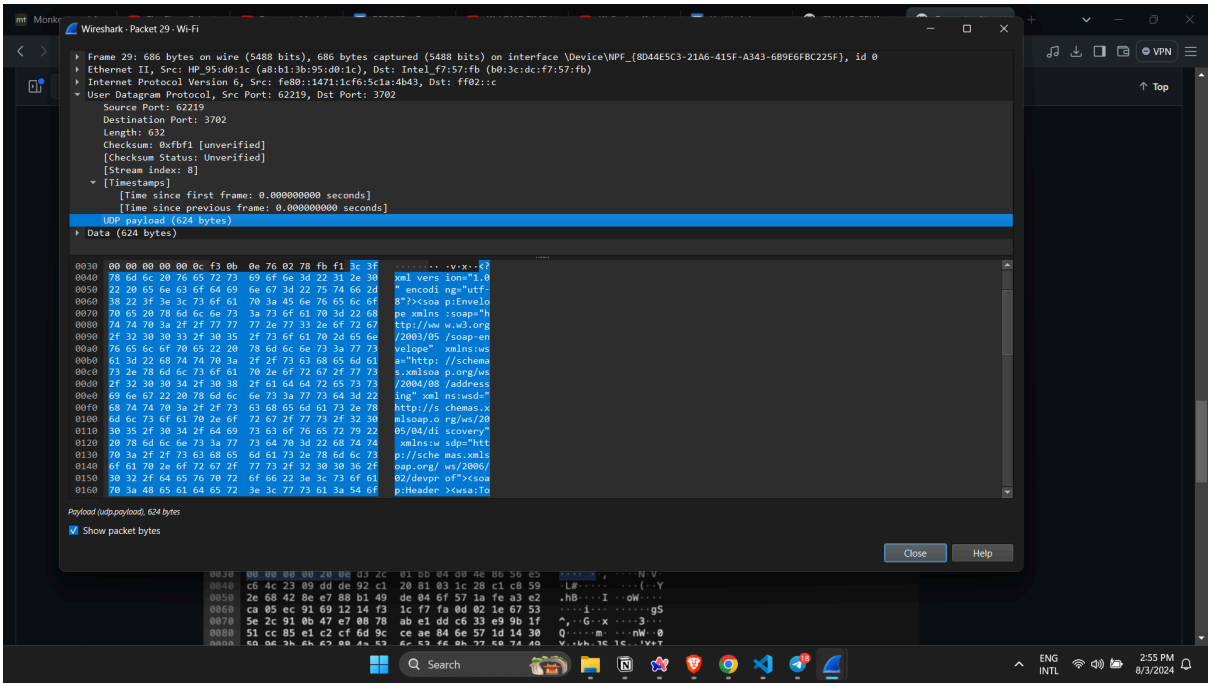
Capturing Packets in Wireshark

Question 7: Locate a UDP packet in Wireshark and relate the values to the fields.

UDP-Packets-Wireshark

Relate the values to the fields:

- Source Port: 54060 (0xd31c) - The port number of the sender.
- Destination Port: 443 (0x01bb) - The port number of the receiver.
- Length: 1232 (0x04d0) - The length of the UDP header and payload.
- Checksum: 0x4e86 - The checksum value for error-checking.
- Question 8: Locate a TCP packet in Wireshark and explain why the fields have the values they have.



TCP-Packets-Wireshark

Relate the values to the fields:

- Source Port: 443 (0x01bb) - The port number of the sender, typically a well-known port for HTTPS.
- Destination Port: 53284 (0xd024) - The port number of the receiver, typically a high-numbered ephemeral port.
- Sequence Number: 1 - The sequence number of the first byte in this segment.
- Acknowledgment Number: 26 - The next sequence number the sender expects to receive.
- Flags: 0x010 (ACK) - Control flags indicating the state of the connection.
- Window Size: 303 - The size of the sender's receive window.
- Checksum: 0xcc16 - The checksum value for error-checking.

- Urgent Pointer: 0 - Points to the sequence number of the byte following urgent data if the URG flag is set.
- Options: No-Operation (NOP), Timestamps - Optional fields used in the header.