Network Protocol Information

UDP Header

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

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

1. Source Port (16 bits)
2. Destination Port (16 bits)
3. Length (16 bits)
4. 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:

1. Source Port (16 bits)
2. Destination Port (16 bits)
3. Sequence Number (32 bits)
4. Acknowledgment Number (32 bits)
5. Data Offset (4 bits)
6. Reserved (3 bits)
7. Flags (9 bits)
8. Window Size (16 bits)
9. Checksum (16 bits)
10. Urgent Pointer (16 bits)
11. Options (variable length)

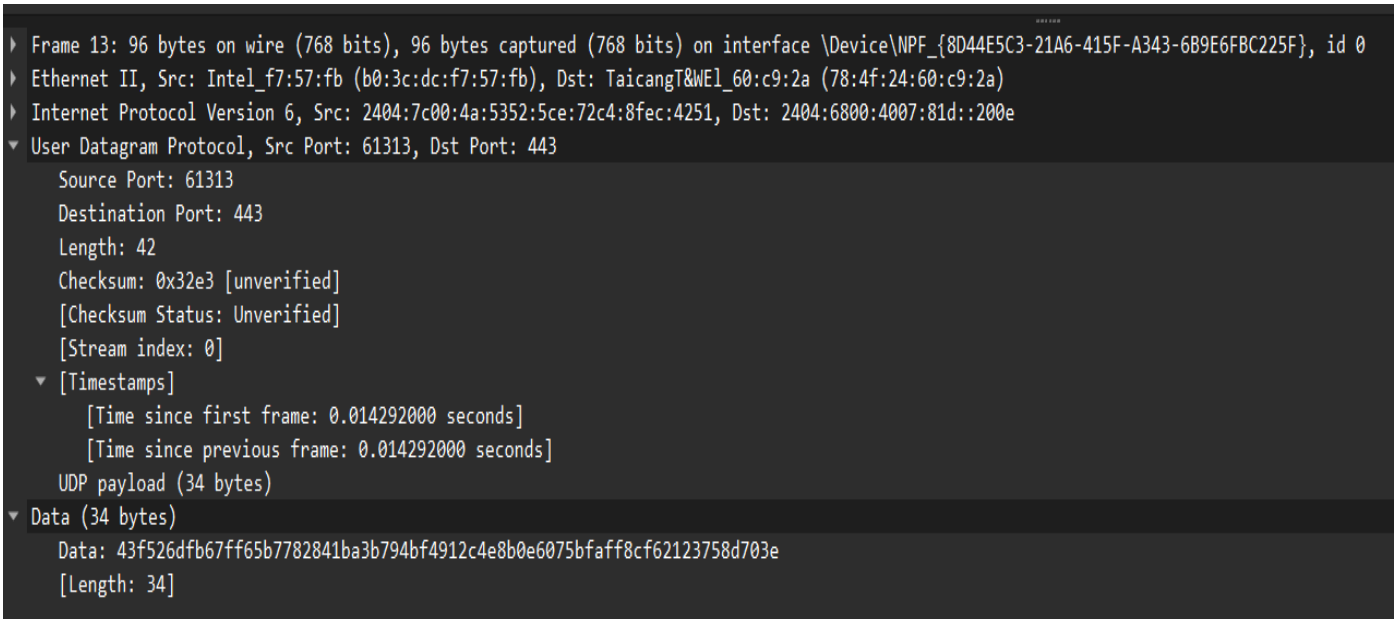
Question 6: Describe the fields in the TCP header.

1. Source Port (16 bits):The port number of the sending process.
2. Destination Port (16 bits):The port number of the receiving process.
3. Sequence Number (32 bits):The sequence number of the first byte of data in this segment.
4. 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.
5. Data Offset (4 bits):The size of the TCP header in 32-bit words.
6. Reserved (3 bits):Reserved for future use and should be set to zero.
7. Flags (9 bits):Control flags such as URG, ACK, PSH, RST, SYN, and FIN.
8. Window Size (16 bits):The size of the receive window, which specifies the number of bytes that the sender is willing to receive.
9. Checksum (16 bits):Used for error-checking of the header and data.
10. Urgent Pointer (16 bits):If the URG flag is set, this field points to the sequence number of the byte following urgent data.
11. 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.

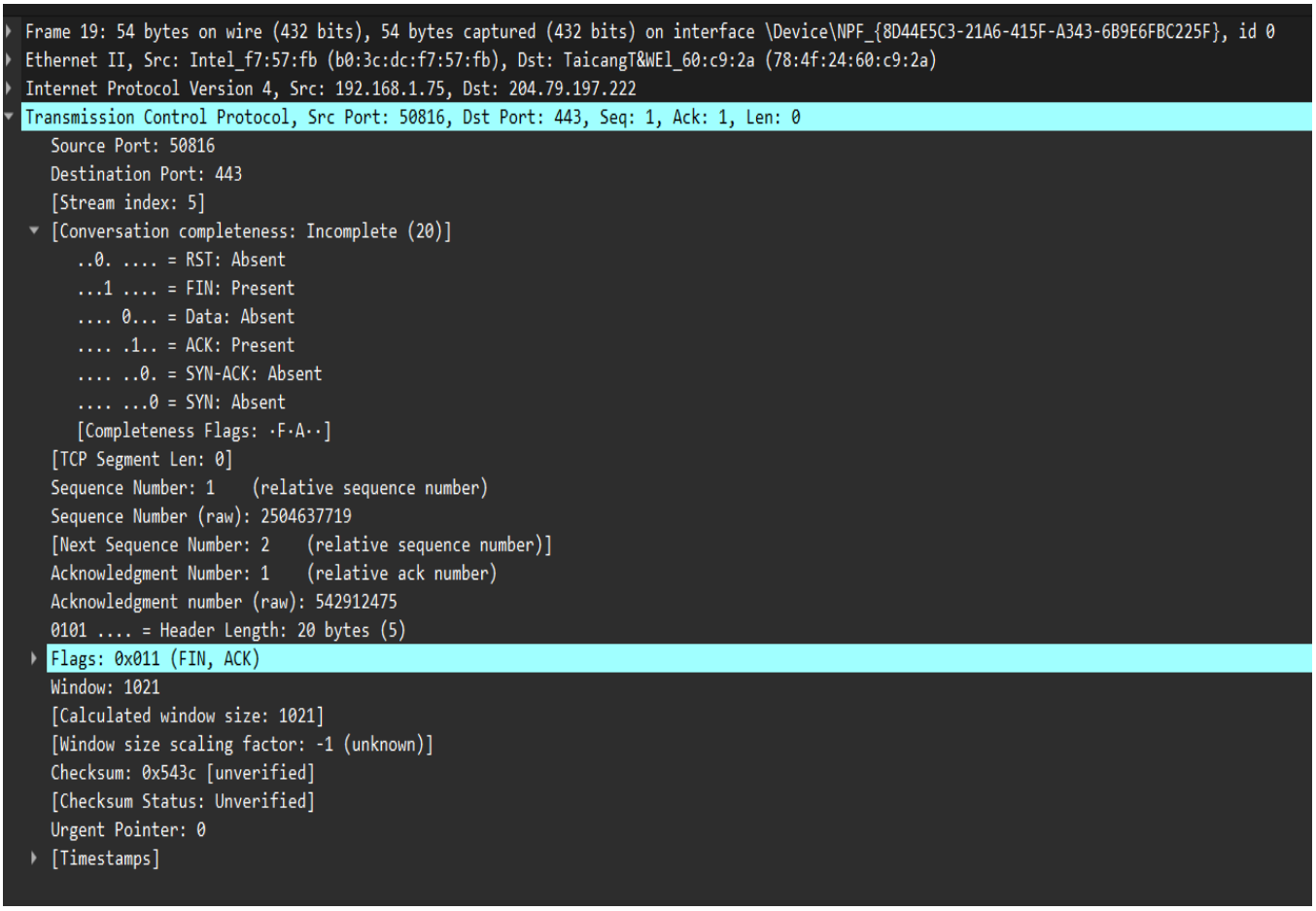
UDP-Packets-Wireshark



Relate the values to the fields:

1. Source Port: 54060 (0xd31c) - The port number of the sender.
2. Destination Port: 443 (0x01bb) - The port number of the receiver.
3. Length: 1232 (0x04d0) - The length of the UDP header and payload.
4. 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



Explain the fields:

1. Source Port: 443 (0x01bb) - The port number of the sender, typically a well-known port for HTTPS.
2. Destination Port: 53284 (0xd024) - The port number of the receiver, typically a high-numbered ephemeral port.
3. Sequence Number: 1 - The sequence number of the first byte in this segment.
4. Acknowledgment Number: 26 - The next sequence number the sender expects to receive.
5. Flags: 0x010 (ACK) - Control flags indicating the state of the connection.
6. Window Size: 303 - The size of the sender's receive window.
7. Checksum: 0xcc16 - The checksum value for error-checking.
8. Urgent Pointer: 0 - Points to the sequence number of the byte following urgent data if the URG flag is set.
9. Options: No-Operation (NOP), Timestamps - Optional fields used in the header.