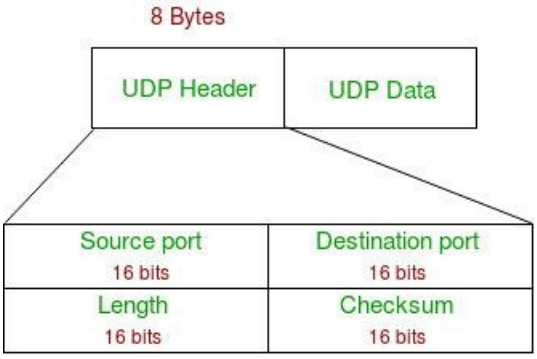
1)What is the size of UDP header? What are the different fields? Describe its fields ?

The size of udp header is 8 bytes long.
The different fields of UDP header along with description is shown below:

1)Source Port (16 bits): Identifies the port number of the application or process on the sender's host that originated the message

2)Destination Port (16 bits): Identifies the port number of the application or process on the receiver's host that is intended to receive the message.



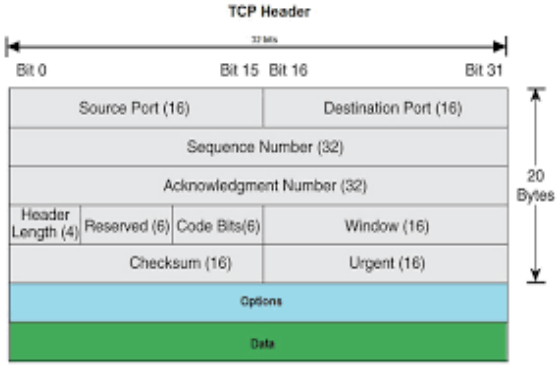
3)Length (16 bits): Specifies the total length of the UDP datagram, including both the UDP header and the data. The minimum value is 8 (header only), and the maximum is 65,535.

4)Checksum (16 bits): Used for error detection. It is a calculation based on the contents of the UDP header and data. The receiver recalculates the checksum and compares it to the one in the header. If they match, the data is assumed to be valid.

2)What is the size of TCP header ? What are the different fields .Describe each field.

The size of TCP header ranges from 20 byte(min) to 60 byte(max).

The different fields of TCP header along with description is shown below:



Source Port (16 bits): Identifies the port number of the application or process on the sender's host that originated the message.

Destination Port (16 bits): Identifies the port number of the application or process on the receiver's host that is intended to receive the message.

Sequence Number (32 bits): Identifies the position of the first data byte in the TCP segment within the overall byte stream of the connection.

Acknowledgment Number (32 bits): If the ACK control bit is set, this field indicates the next sequence number that the sender of the ACK is expecting. It acknowledges receipt of all prior bytes.

Data Offset (4 bits): Specifies the size of the TCP header in 32-bit words. The minimum size header is 5 words (20 bytes), and the maximum is 15 words (60 bytes).

Reserved (6 bits): Reserved for future use and should be set to zero.

Control Bits (6 bits): These flags control various aspects of the TCP connection:

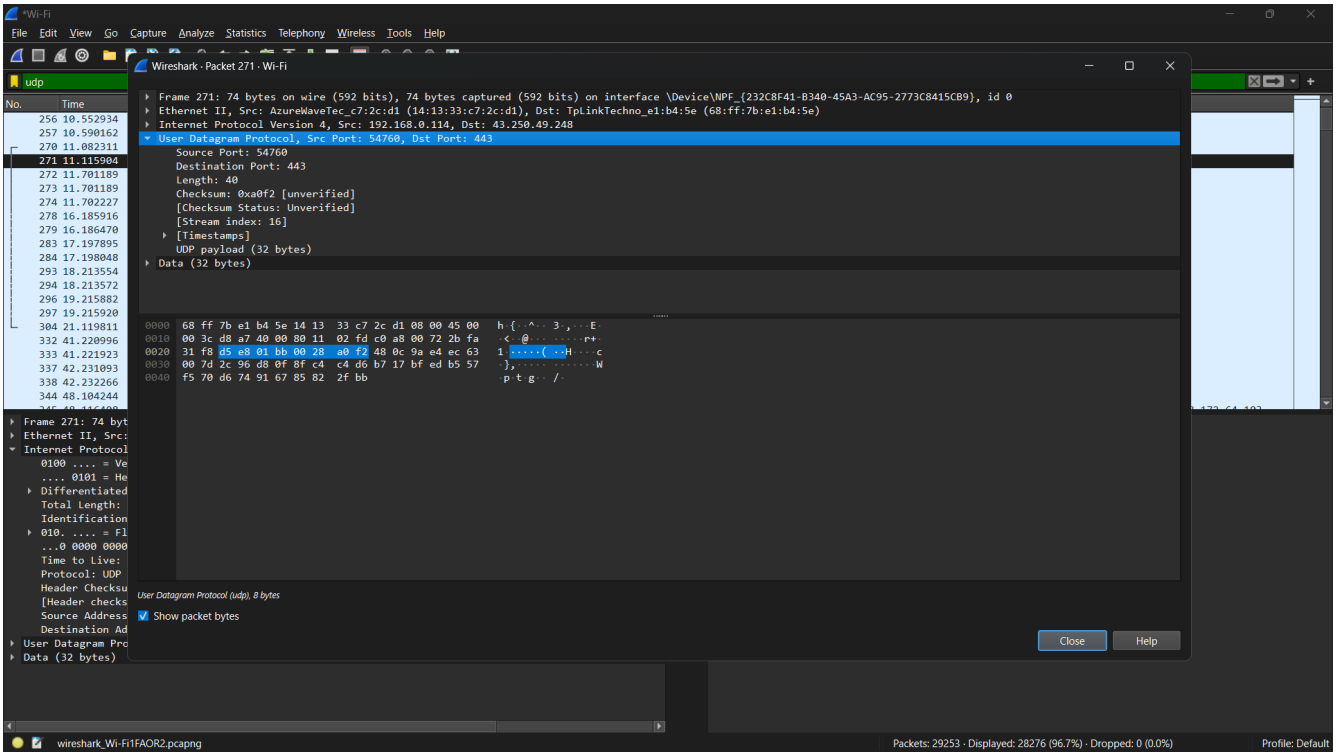
URG: Urgent Pointer field significant
ACK: Acknowledgment field significant
PSH: Push function
RST: Reset the connection
SYN: Synchronize sequence numbers
FIN: No more data from sender

Window Size (16 bits): Specifies the number of bytes that the receiver is willing to accept beyond the acknowledged sequence number. Used for flow control.

Checksum (16 bits): Used for error detection. It's a calculation based on the contents of the TCP header and data.

Urgent Pointer (16 bits): If the URG control bit is set, this field points to the last urgent data byte in the segment.

3) Locate a UDP packet in wireshark and relate the values to the fields .

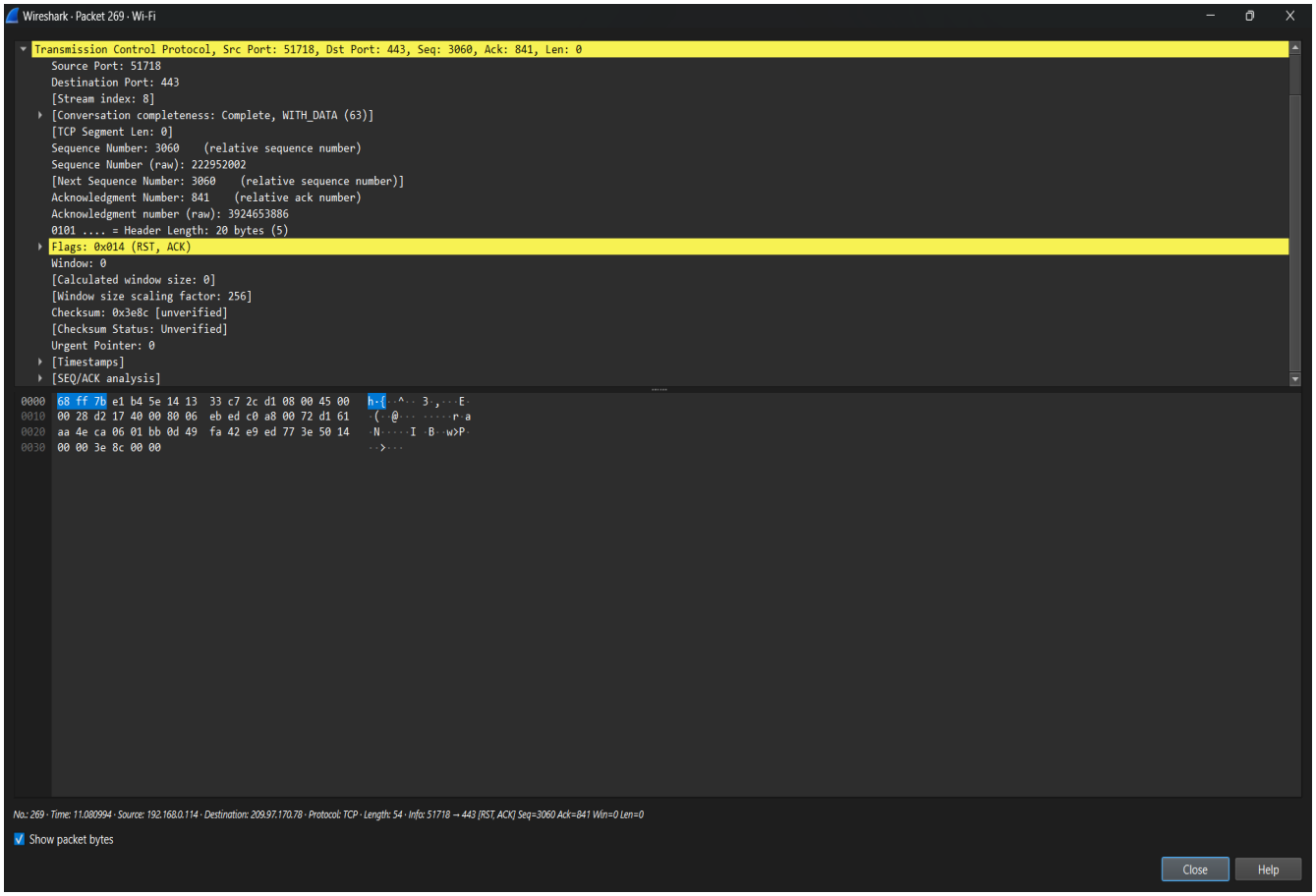


Source port :54760
This is the port number on the sender's device from which the data is being sent. Port numbers help identify the specific application or process that initiated the communication.

destination port:443
This is the port number on the receiver's device to which the data is being sent. Port 443 is the standard port for HTTPS .

Length :40
The length of UDP header it's 40 bytes, which is a relatively small amount of data.
checksum:oxaof2
It is the error checking mechanism. The checksum helps detect if any errors occurred during the transmission process.

4)locate tcp header in wireshark and relate the values to the field.Source



Port: 51716

- This is the port number on your computer that initiated the TCP connection. It's a randomly assigned ephemeral port used by client applications.

Destination Port: 443

- This is the well-known port number for HTTPS (Hypertext Transfer Protocol Secure), indicating that the communication is with a web server and the data is encrypted.

Sequence Number: 3068 (relative), 222952002 (raw)

- This represents the byte number of the first byte of data in this TCP segment. The relative number is used within the context of the current session, while the raw number is the absolute byte count since the connection began.

Acknowledgment Number: 841 (relative), 3924653886 (raw)

- This acknowledges that the sender has received all data up to byte number 840 and is expecting byte 841 next. The relative and raw numbers have the same interpretation as the sequence number.

Header Length: 20 bytes (5)

- This indicates the size of the TCP header, which is 20 bytes long or 5 32-bit words.

Flags: 0x014 (RST, ACK)

- **RST (Reset):** This flag indicates that the connection should be terminated immediately due to an error or abnormal condition.
- **ACK (Acknowledgment):** This flag confirms the receipt of previous data segments.

Window: 0

- This represents the receiver's advertised window size, which is the amount of data the receiver is willing to accept before sending another acknowledgment. In this case, a window size of 0 might indicate that the receiver is temporarily unable to receive data.

Checksum: 0x3e8c (unverified)

- This is a value calculated over the TCP header and data for error detection. Wireshark hasn't verified it yet, as indicated by the "(unverified)" status.

Urgent Pointer: 0

- This field is not used in this packet, as there is no urgent data.