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

➔ The UDP (User Datagram Protocol) header is 8 bytes (64 bits) in size.

Fields in the UDP Header

The UDP header consists of four fields, each of which is 2 bytes (16 bits) long:

1. **Source Port (16 bits)**:
    - **Purpose**: Identifies the port number of the sending application. This field is optional and can be set to zero if the source port is not specified.

2. **Destination Port (16 bits)**:
    - **Purpose**: Identifies the port number of the receiving application. This field is mandatory and specifies the endpoint for the data.

3. **Length (16 bits)**:
    - **Purpose**: Specifies the total length of the UDP datagram, including the header and the data. The minimum value is 8 bytes (only the header without data).

4. **Checksum (16 bits)**:
    - **Purpose**: Provides error-checking for the header and data. This field is optional in IPv4 but mandatory in IPv6. It ensures data integrity by allowing the receiver to verify that the datagram has not been corrupted in transit.

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

➔ The standard TCP header size is 20 bytes (160 bits) without any options. However, it can be extended up to 60 bytes (480 bits) with optional fields.

The TCP header contains several fields, each serving a specific purpose. Here are the main fields in the order they appear:

1. **Source Port (16 bits)**: The port number of the sender.

2. **Destination Port (16 bits)**: The port number of the receiver.

3. **Sequence Number (32 bits)**: This field is used to track the order of bytes sent from the sender to the receiver. It indicates the position of the first byte of data in the segment in the sender's byte stream.

4. **Acknowledgment Number (32 bits)**: When the ACK flag is set, this field contains the value of the next sequence number that the receiver is expecting. It is used to acknowledge the successful receipt of data.

5. **Data Offset (4 bits)**: Also known as the header length, this field specifies the length of the TCP header in 32-bit words. It indicates where the data starts and helps to determine the start of the payload.

6. **Reserved (3 bits)**: Reserved for future use and should be set to zero.

7. **Flags (9 bits)**: Various control flags that manage the state of the connection. These include:
    - **NS (1 bit)**: ECN-nonce concealment protection.
    - **CWR (1 bit)**: Congestion Window Reduced.
    - **ECE (1 bit)**: ECN-Echo.
    - **URG (1 bit)**: Urgent pointer field significant.
    - **ACK (1 bit)**: Acknowledgment field significant.
    - **PSH (1 bit)**: Push function.
    - **RST (1 bit)**: Reset the connection.
    - **SYN (1 bit)**: Synchronize sequence numbers.
    - **FIN (1 bit)**: No more data from sender.

8. **Window Size (16 bits)**: Specifies the size of the sender's receive window (the amount of data the sender is willing to accept), which controls the flow of data.

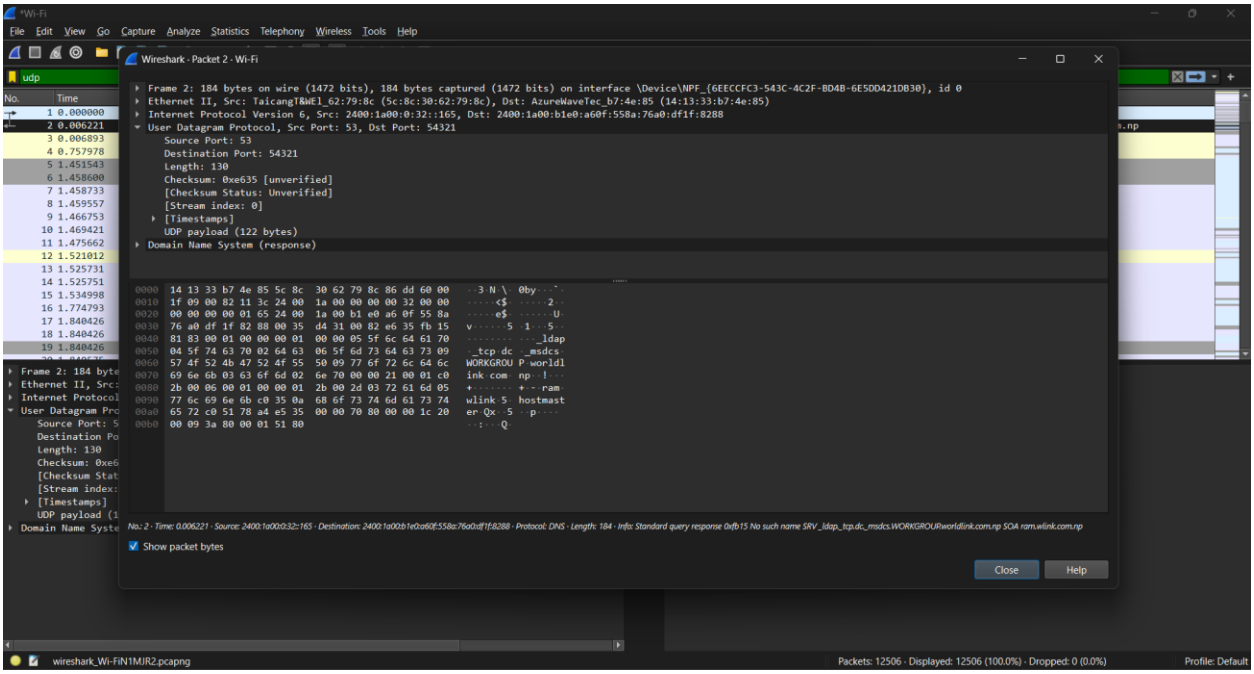
9. **Checksum (16 bits)**: Used for error-checking the header and data. It ensures data integrity by allowing the receiver to detect errors in the transmitted segment.

10) **Urgent Pointer (16 bits)**: When the URG flag is set, this field points to the sequence number of the byte following urgent data. It indicates the end of urgent data and is used to prioritize certain data in the stream.

11)**Options (variable, up to 40 bytes)**: May contain various optional parameters to extend the capabilities of the TCP header. Common options include Maximum Segment Size (MSS), Window Scale, and Timestamps.

12)**Padding (variable)**: Ensures that the TCP header ends on a 32-bit boundary. It is added if needed to make the header length a multiple of 32 bits.

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



Source Port: 53

- UDP often uses dynamic ports for client-server communications. The client typically chooses a high-numbered port, while the server may use a well-known port or a dynamic one as well.
- Port 53 is the well-known port for DNS (Domain Name System) services. This indicates that this packet is a DNS response from a DNS server.

Destination Port: 54321

➢ This is the port number on the destination device. It appears to be a high-numbered ephemeral port, typically used for the client side of a connection.

Length: 130

- This value represents the total length of the UDP datagram in bytes,

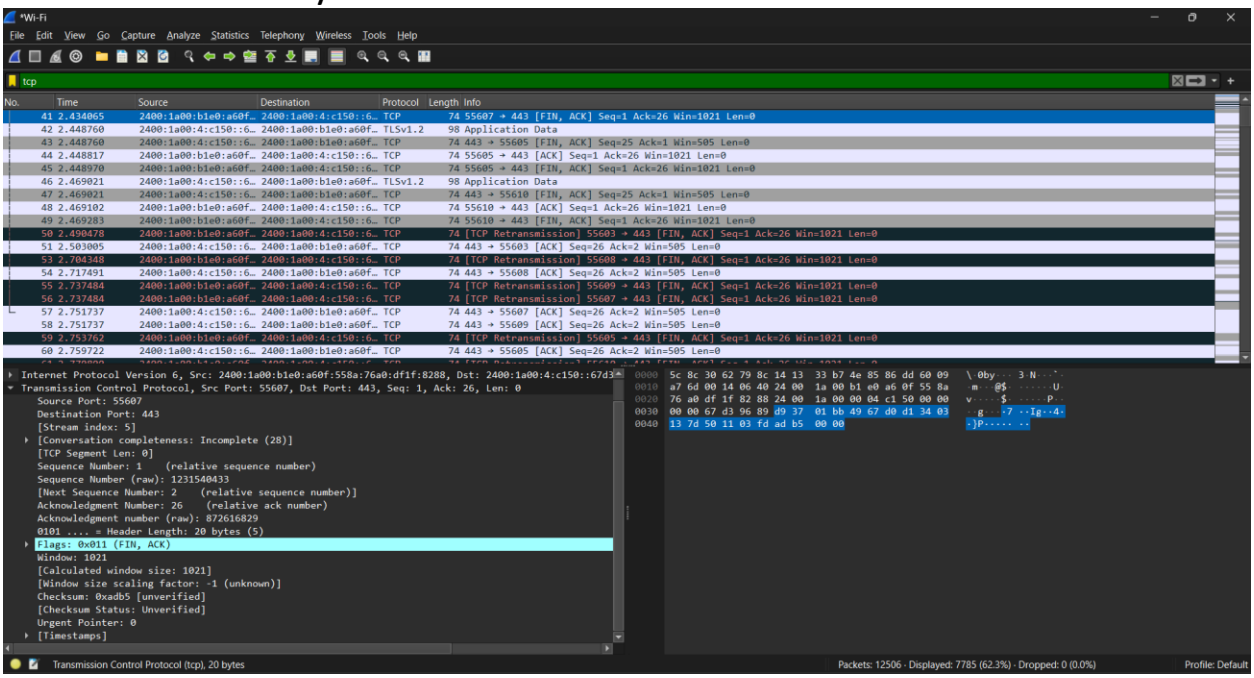
including both the header (8 bytes) and the payload (122 bytes).

- We can verify this: 8 (header) + 122 (UDP payload) = 130 bytes total.

Checksum: 0xee63 (unverified)

- The checksum is a calculated value used for error detection. It's computed over the UDP header, payload, and parts of the IP header. The "unverified" status means Wireshark hasn't re-calculated it to confirm its correctness. If the checksum were incorrect, it would indicate potential data corruption during transmission.

4).Locate a TCP package in Wireshark and explain why the field have the value that they have.



- **Source Port: 55607**

- This is the port number of the sending device. Ports are used to differentiate services or applications on the device. The source port is usually a randomly chosen high-numbered port when the device initiates a connection.

- **Destination Port: 443**
  - This is the port number of the receiving device. Port 443 is the default port for HTTPS, indicating that the packet is part of an encrypted communication over the web.

- **Sequence Number: 1**
  - The sequence number in this packet is 1, which is the first byte's number of the data segment being sent in this TCP segment.

- **Acknowledgment Number: 26**
  - The acknowledgment number indicates the next byte that the sender of the acknowledgment expects to receive. In this case, it is 26, meaning the sender has successfully received all bytes up to and including byte 25 and is expecting byte 26 next.

- **Header Length: 20 bytes (5)**
  - The header length (also known as the data offset) indicates the size of the TCP header in 32-bit words. A value of 5 means the header is 20 bytes long (5 * 4 bytes).

- **Flags: 0x011 (FIN, ACK)**
  - Flags are control bits used to manage the state of the connection. In this packet, the flags are set to 0x011:
    - **FIN**: Indicates the sender has finished sending data.
    - **ACK**: Acknowledgment field is significant.

- **Window: 1021**

    - The window size value specifies the number of bytes that the sender is willing to receive starting from the acknowledgment number. It is used for flow control.

- **Checksum: 0xad55 [unverified]**
    - The checksum is used for error-checking the header and data. It ensures the integrity of the data being sent. The value 0xad55 is calculated based on the content of the TCP header and data. It is marked as "unverified" in the capture tool, meaning the tool has not verified its correctness.

- **Urgent Pointer: 0**
    - The urgent pointer field is used when the URG flag is set to indicate a location in the data stream that requires urgent processing. Since it is set to 0, it indicates no urgent data.