### **UDP Header Information**

**Question 1: What is the size of the UDP header?**

* The size of the UDP header is 8 bytes (64 bits).

**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.**

1. **Source Port (16 bits)**
   * Identifies the sender's port.
   * Optional, if not used, set to zero.
2. **Destination Port (16 bits)**
   * Identifies the receiver's port.
3. **Length (16 bits)**
   * Specifies the length of the UDP header and data.
   * Minimum value is 8 bytes (header only).
4. **Checksum (16 bits)**
   * Used for error-checking of the header and data.
   * Optional in IPv4 but mandatory in IPv6.

### **TCP Header Information**

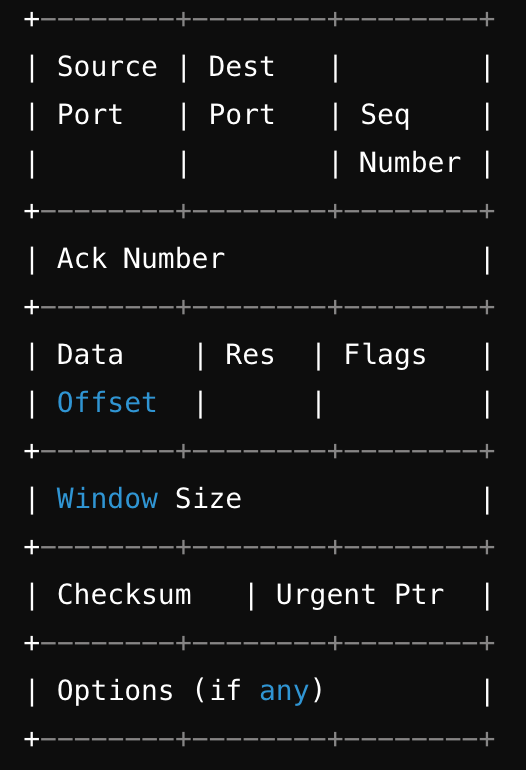
**Question 4: What is the size of the TCP header?**

* The minimum size of the TCP header is 20 bytes (160 bits), but it can be larger if options are included.

**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.**

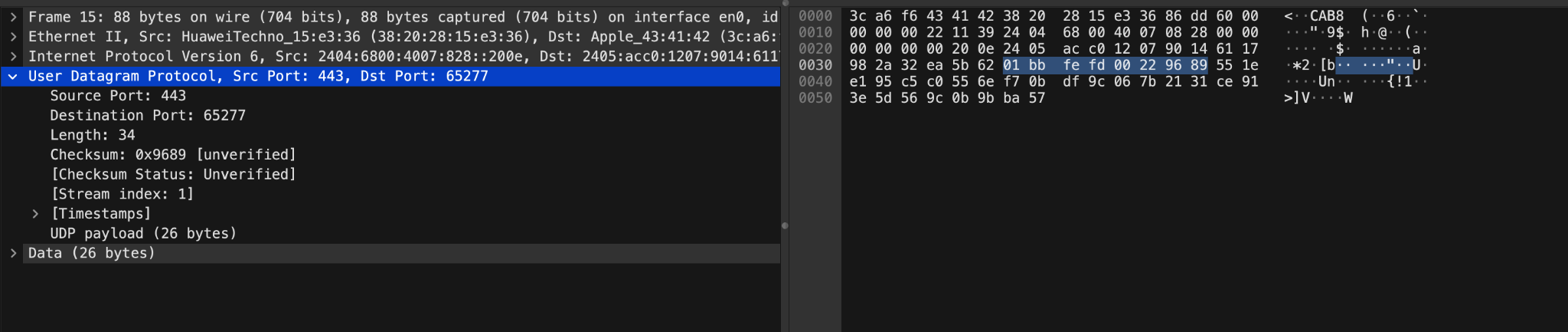
1. **Source Port (16 bits)**
   * Identifies the sender's port.
2. **Destination Port (16 bits)**
   * Identifies the receiver's port.
3. **Sequence Number (32 bits)**
   * Indicates the sequence number of the first byte in the segment.
4. **Acknowledgment Number (32 bits)**
   * If the ACK flag is set, this field contains the value of the next sequence number that the sender is expecting to receive.
5. **Data Offset (4 bits)**
   * Specifies the size of the TCP header in 32-bit words.
   * Indicates where the data begins.
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)**
   * Specifies the size of the sender's receive window (flow control).
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 is an offset from the sequence number indicating the last urgent data byte.
11. **Options (variable length)**
    * Used for various TCP options.
    * The length of the options is variable and affects the total size of the TCP header.

**Visual Representation of UDP and TCP Headers**



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

**Breakdown of the UDP Header Fields:**



1. **Source Port (16 bits)**

* Value: 443
* Position: First 2 bytes of the UDP header
* Hex: 01BB (Hex for 443)

1. **Destination Port (16 bits)**

* Value: 65277
* Position: Next 2 bytes
* Hex: FFFD (Hex for 65277)

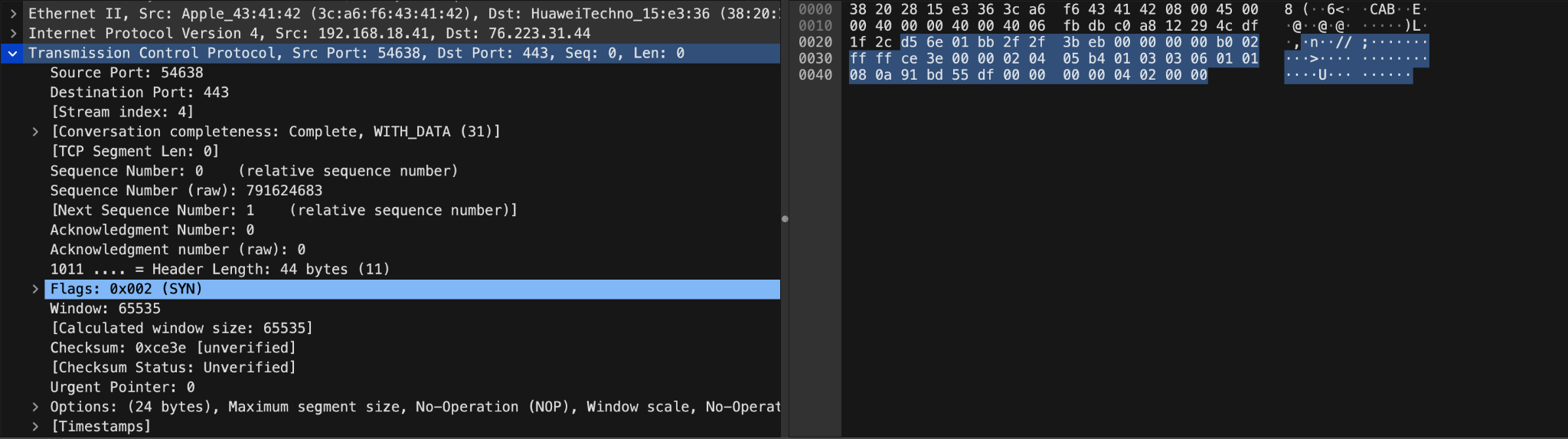
1. **Length (16 bits)**

* Value: 34
* Position: Next 2 bytes
* Hex: 0022 (Hex for 34)

1. **Checksum (16 bits)**

* Value: 0x9689 (unverified)
* Position: Next 2 bytes
* Hex: 9689

### **Question 8: Locate a TCP packet in Wireshark and explain why the fields have the values they have.**



### **TCP Header Fields Breakdown:**

1. **Source Port (16 bits)**
   * **Value**: 54638
   * **Explanation**: The port number of the sender's application.
2. **Destination Port (16 bits)**
   * **Value**: 443
   * **Explanation**: The port number of the receiver's application, commonly used for HTTPS.
3. **Sequence Number (32 bits)**
   * **Value**: 0
   * **Explanation**: Initial sequence number of the first byte of data in this segment.
4. **Acknowledgment Number (32 bits)**
   * **Value**: 0
   * **Explanation**: Indicates that this packet does not acknowledge any data (typical for SYN packets).
5. **Data Offset (4 bits)**
   * **Value**: 11 (44 bytes)
   * **Explanation**: Size of the TCP header in 32-bit words; includes options, hence 44 bytes.
6. **Reserved (3 bits)**
   * **Value**: 0
   * **Explanation**: Reserved for future use, must be set to zero.
7. **Flags (9 bits)**
   * **Value**: 0x002 (SYN)
   * **Explanation**: Indicates that this is a SYN packet, used to initiate a TCP connection.
8. **Window Size (16 bits)**
   * **Value**: 65535
   * **Explanation**: Maximum number of bytes that can be received without acknowledgment.
9. **Checksum (16 bits)**
   * **Value**: 0xce3e
   * **Explanation**: Used for error-checking the header and data.
10. **Urgent Pointer (16 bits)**
    * **Value**: 0
    * **Explanation**: Not used in this packet (typical for non-urgent data).
11. **Options (variable length)**
    * **Content**: Maximum segment size, window scale, etc.
    * **Explanation**: Additional TCP options to fine-tune the connection parameters.