Wireshark Lab 5

UDP

Suraj Durgesht

(16EC06)

Instructor: Dr. Rajendra Hegadi

Que1. Select *one* UDP packet from your trace. From this packet, determine how many

fields there are in the UDP header. Name these fields.

Solution:

There are four fields in the header: source port, destination port, Length, and checksum.

Que2. By consulting the displayed information in Wireshark’s packet content field for

this packet, determine the length (in bytes) of each of the UDP header fields.

Solution: Each of the UDP header fields is 2 bytes long.

Que3. The value in the Length field is the length of what? Verify your claim with your captured UDP packet.

Solution:

The value in the length field, in the example below it is 46, is the sum of the 8 header bytes and the remaining data bytes encapsulated in the packet.

Que4. What is the maximum number of bytes that can be included in a UDP payload?

Solution:

The maximum number of bytes that can be in the payload is 2^16- the bytes already being used by the header field (8). Therefore, the maximum payload is 65535-8= 65527 bytes.

Que5. What is the largest possible source port number?

Solution: The largest possible source port number is 2^16 or 65535.

Que6. What is the protocol number for UDP? Give your answer in both hexadecimal and

decimal notation. To answer this question, you’ll need to look into the Protocol

field of the IP datagram containing this UDP segment.

Solution:

The protocol number for UDP is 17 in decimal notation which in hexadecimal notation is 0x11.

Que7. Examine a pair of UDP packets in which your host sends the first UDP packet and

the second UDP packet is a reply to this first UDP packet. Describe the relationship between the port numbers in the two packets.

Solution:



