

Questions

All Answers can be seen in Figure 1 for Q1-Q5

1. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.

UDP header contains 4 fields. Source port, destination port, length, checksum.

2. 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.

The UDP header has a fixed length of 8 bytes. Each of these 4 header fields is 2 bytes long.

3. The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.

Length gives number of bytes in UDP segment. This contains the header + the data. Length is needed since the size of the data may differ from each segment.

The length of the UDP for selected packet is $48 - 8 = 40$ bytes.

4. What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your answer to 2. above)

The maximum number of bytes that can be included in a UDP payload is $(2^{16} - 1)$ bytes plus the header bytes. This gives $65535 \text{ bytes} - 8 \text{ bytes} = 65527 \text{ bytes}$.

5. What is the largest possible source port number? (Hint: see the hint in 4.)

The largest possible source port number is $(2^{16} - 1) = 65535$.

6. 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 (see Figure 4.13 in the text, and the discussion of IP header fields).

The IP protocol number for UDP is 0x11 hex, which is 17 in decimal value. (Figure 2).

7. 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. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). Describe the relationship between the port numbers in the two packets.

The source port of the UDP packet sent by the host is the same as the destination port of the reply packet, and inversely the destination port of the UDP packet sent by the host is the same as the source port of the reply packet. (Shown In Figures 3 & 4)

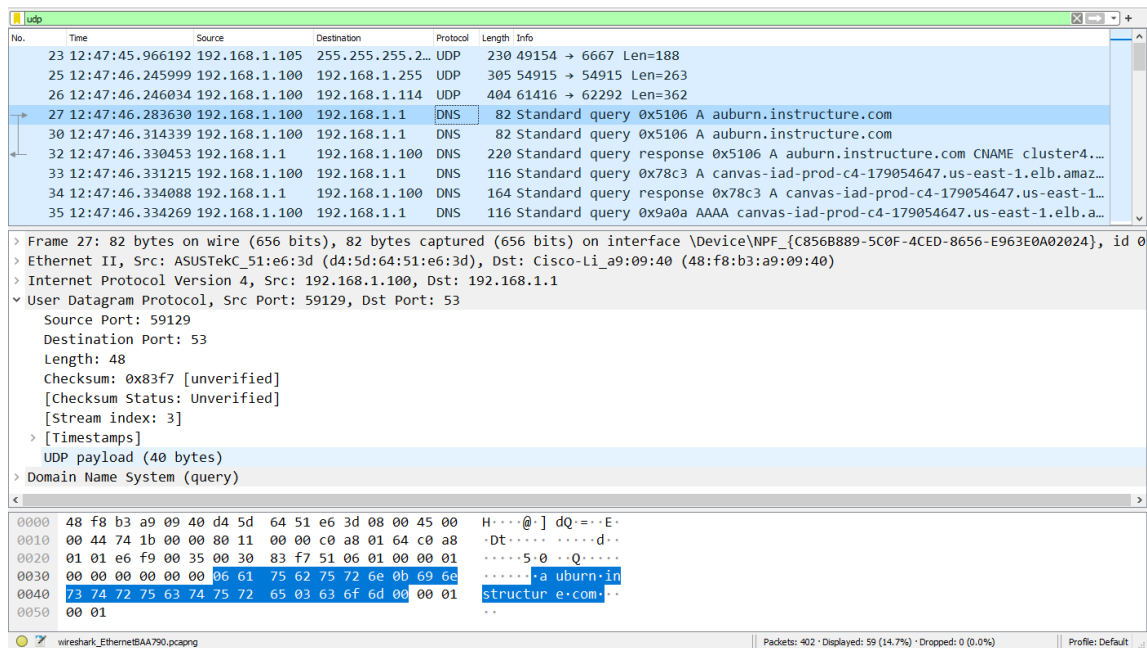


Figure 1

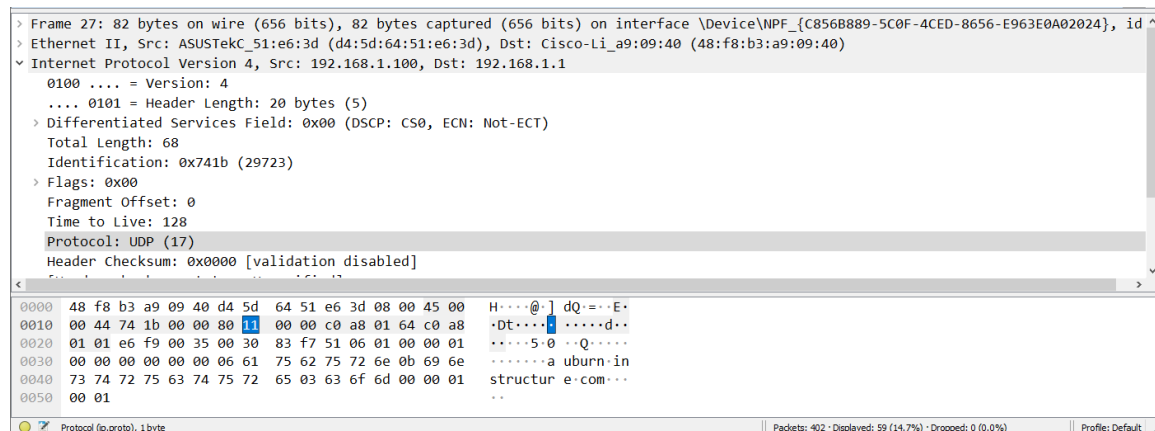


Figure 2

```

> Frame 27: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{C856B889-5C0F-4CED-8656-E963E0A02024}, id 0
> Ethernet II, Src: ASUSTekC_51:e6:3d (d4:5d:64:51:e6:3d), Dst: Cisco-Li_a9:09:40 (48:f8:b3:a9:09:40)
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.1
  User Datagram Protocol, Src Port: 59129, Dst Port: 53
    Source Port: 59129
    Destination Port: 53
    Length: 48
    Checksum: 0x83f7 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
    > [Timestamps]
      UDP payload (40 bytes)
    > Domain Name System (query)

```

Figure 3

```

> Frame 32: 220 bytes on wire (1760 bits), 220 bytes captured (1760 bits) on interface \Device\NPF_{C856B889-5C0F-4CED-8656-E963E0A02024},
> Ethernet II, Src: Cisco-Li_a9:09:40 (48:f8:b3:a9:09:40), Dst: ASUSTekC_51:e6:3d (d4:5d:64:51:e6:3d)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.100
  User Datagram Protocol, Src Port: 53, Dst Port: 59129
    Source Port: 53
    Destination Port: 59129
    Length: 186
    Checksum: 0x86b2 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
    > [Timestamps]
      UDP payload (178 bytes)
    > Domain Name System (response)

```

Figure 4