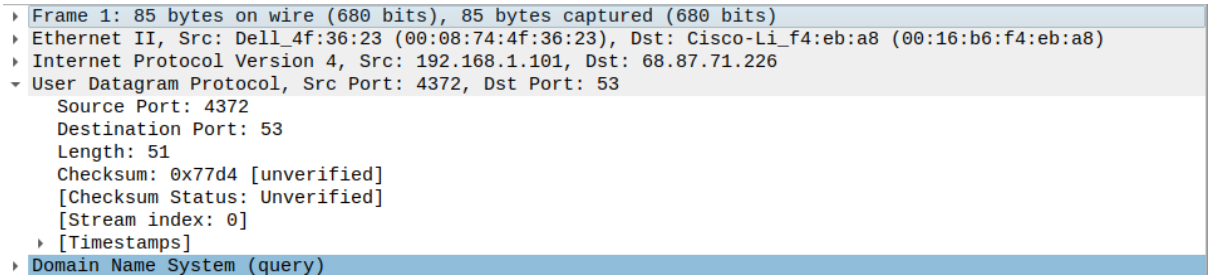
Lab_3a_Wireshark_UDP_v8.0

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.

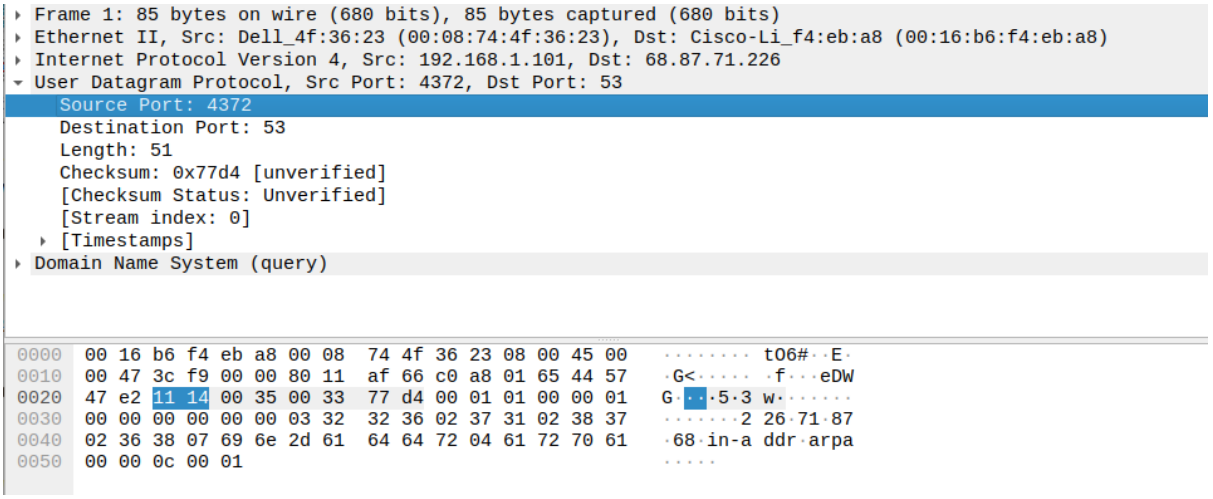
Answer:



The header only contains 4 fields: the source port, destination port, length, and 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

Answer:



Each of the UDP 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.

Answer:

The value in the length field is 51, is the sum of the 8 header bytes and the remaining data bytes encapsulated in the packet (43+8)

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)

Answer:

The maximum number of bytes that can be in the payload is 2^16-1 the bytes already being used by the header field (8). Therefore the maximum payload is 65535-8= 65527 bytes.

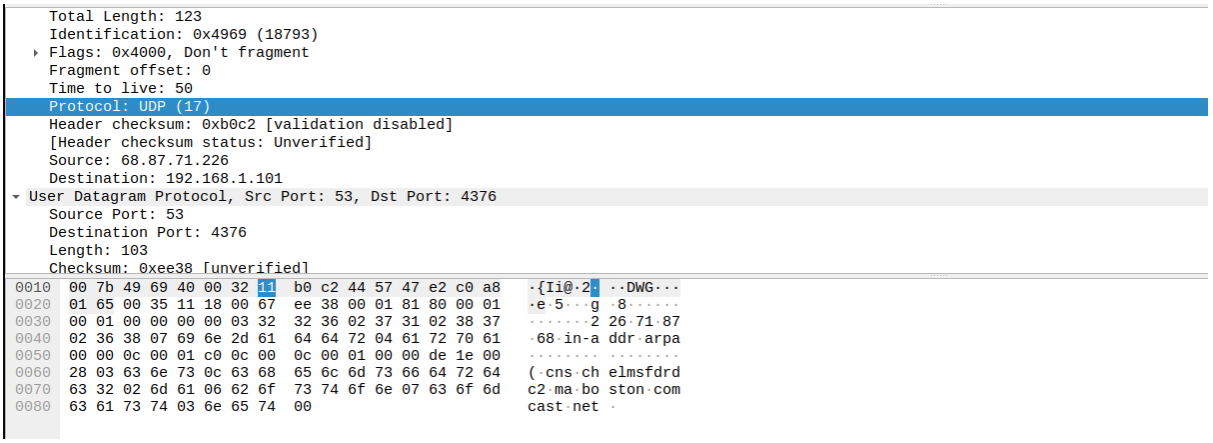
5.What is the largest possible source port number? (Hint: see the hint in 4.)

Answer:

The largest possible source port number is 2^16-1 or 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).

Answer:

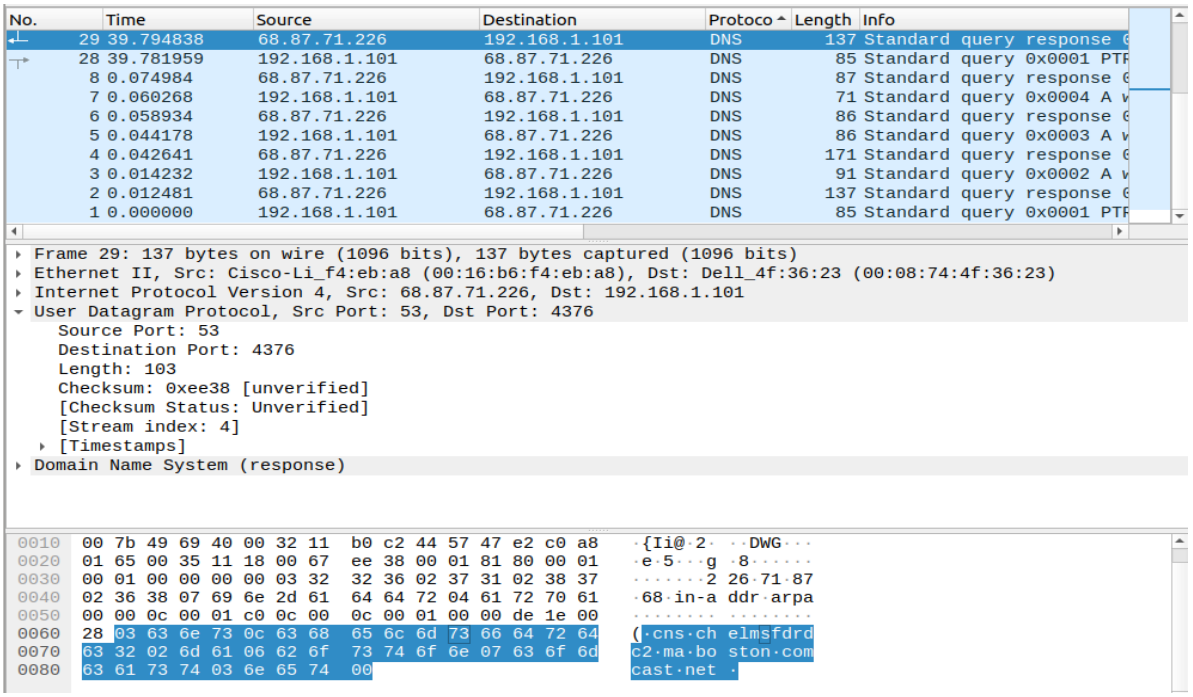


The protocol number for UDP is 17 in decimal notation which in hexadecimal notation is 0x11.

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.

Answer:

UDP Sent

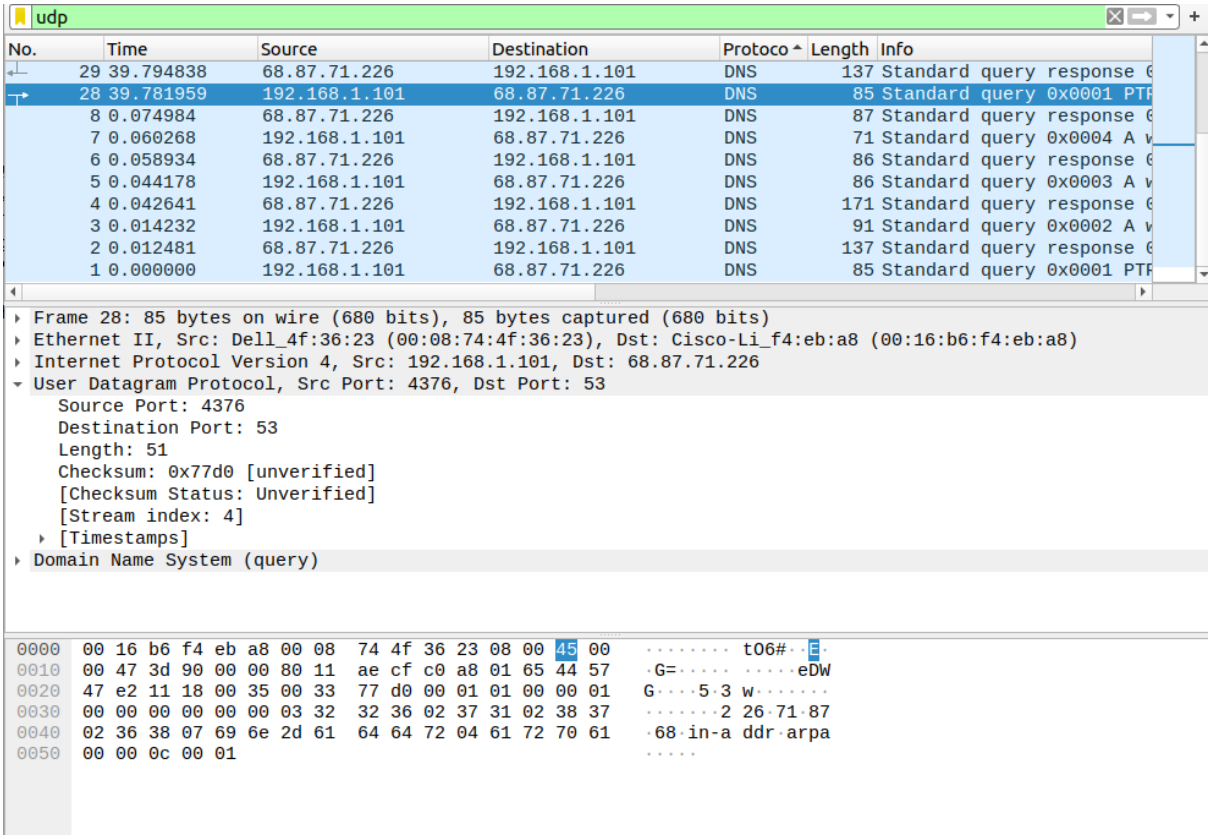


No.	Time	Source	Destination	Protoco	Length	Info
29	39.794838	68.87.71.226	192.168.1.101	DNS	137	Standard query response 0
28	39.781959	192.168.1.101	68.87.71.226	DNS	85	Standard query 0x0001 PTR
8	0.074984	68.87.71.226	192.168.1.101	DNS	87	Standard query response 0
7	0.060268	192.168.1.101	68.87.71.226	DNS	71	Standard query 0x0004 A w
6	0.058934	68.87.71.226	192.168.1.101	DNS	86	Standard query response 0
5	0.044178	192.168.1.101	68.87.71.226	DNS	86	Standard query 0x0003 A w
4	0.042641	68.87.71.226	192.168.1.101	DNS	171	Standard query response 0
3	0.014232	192.168.1.101	68.87.71.226	DNS	91	Standard query 0x0002 A w
2	0.012481	68.87.71.226	192.168.1.101	DNS	137	Standard query response 0
1	0.000000	192.168.1.101	68.87.71.226	DNS	85	Standard query 0x0001 PTR

```
▸ Frame 29: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits)
▸ Ethernet II, Src: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
▸ Internet Protocol Version 4, Src: 68.87.71.226, Dst: 192.168.1.101
▾ User Datagram Protocol, Src Port: 53, Dst Port: 4376
    Source Port: 53
    Destination Port: 4376
    Length: 103
    Checksum: 0xee38 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  ▸ [Timestamps]
▸ Domain Name System (response)
```

```
0010  00 7b 49 69 40 00 32 11  b0 c2 44 57 47 e2 c0 a8   ·{Ii@·2· ··DWG···
0020  01 65 00 35 11 18 00 67  ee 38 00 01 81 80 00 01   ·e·5···g ·8······
0030  00 01 00 00 00 00 03 32  32 36 02 37 31 02 38 37   ·······2 26·71·87
0040  02 36 38 07 69 6e 2d 61  64 64 72 04 61 72 70 61   ·68·in-a ddr·arpa
0050  00 00 0c 00 01 c0 0c 00  0c 00 01 00 00 de 1e 00   ········ ········
0060  28 03 63 6e 73 0c 63 68  65 6c 6d 73 66 64 72 64   (·cns·ch elmsfdrd
0070  63 32 02 6d 61 06 62 6f  73 74 6f 6e 07 63 6f 6d   c2·ma·bo ston·com
0080  63 61 73 74 03 6e 65 74  00                       cast·net ·
```

UDP Reply



No.	Time	Source	Destination	Protoco	Length	Info
29	39.794838	68.87.71.226	192.168.1.101	DNS	137	Standard query response 0
28	39.781959	192.168.1.101	68.87.71.226	DNS	85	Standard query 0x0001 PTR
8	0.074984	68.87.71.226	192.168.1.101	DNS	87	Standard query response 0
7	0.060268	192.168.1.101	68.87.71.226	DNS	71	Standard query 0x0004 A w
6	0.058934	68.87.71.226	192.168.1.101	DNS	86	Standard query response 0
5	0.044178	192.168.1.101	68.87.71.226	DNS	86	Standard query 0x0003 A w
4	0.042641	68.87.71.226	192.168.1.101	DNS	171	Standard query response 0
3	0.014232	192.168.1.101	68.87.71.226	DNS	91	Standard query 0x0002 A w
2	0.012481	68.87.71.226	192.168.1.101	DNS	137	Standard query response 0
1	0.000000	192.168.1.101	68.87.71.226	DNS	85	Standard query 0x0001 PTR

```
▸ Frame 28: 85 bytes on wire (680 bits), 85 bytes captured (680 bits)
▸ Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
▸ Internet Protocol Version 4, Src: 192.168.1.101, Dst: 68.87.71.226
▾ User Datagram Protocol, Src Port: 4376, Dst Port: 53
    Source Port: 4376
    Destination Port: 53
    Length: 51
    Checksum: 0x77d0 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  ▸ [Timestamps]
▸ Domain Name System (query)
```

```
0000  00 16 b6 f4 eb a8 00 08  74 4f 36 23 08 00 45 00   ········ tO6#··E·
0010  00 47 3d 90 00 00 80 11  ae cf c0 a8 01 65 44 57   ·G=····· ·····eDW
0020  47 e2 11 18 00 35 00 33  77 d0 00 01 01 00 00 01   G····5·3 w·······
0030  00 00 00 00 00 00 03 32  32 36 02 37 31 02 38 37   ·······2 26·71·87
0040  02 36 38 07 69 6e 2d 61  64 64 72 04 61 72 70 61   ·68·in-a ddr·arpa
0050  00 00 0c 00 01                                     ·····
```

The relationship between port numbers is that the source port on the send message is the destination port of the receive message. The destination port for the send message is also the source port for the receive message.