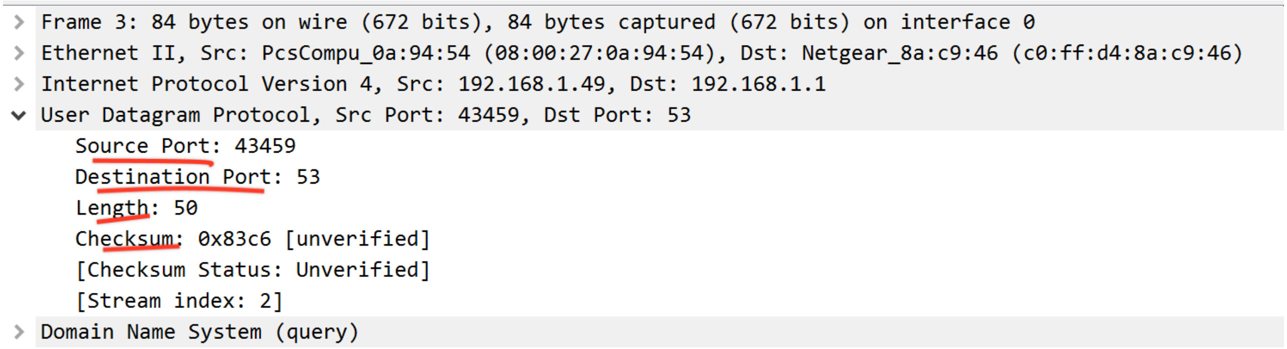
Joel Benjamin Castillo (jc5383)
CS6843 - Computer Networking
Prof. Rafail Portnoy

Wireshark Lab - UDP

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. Fields

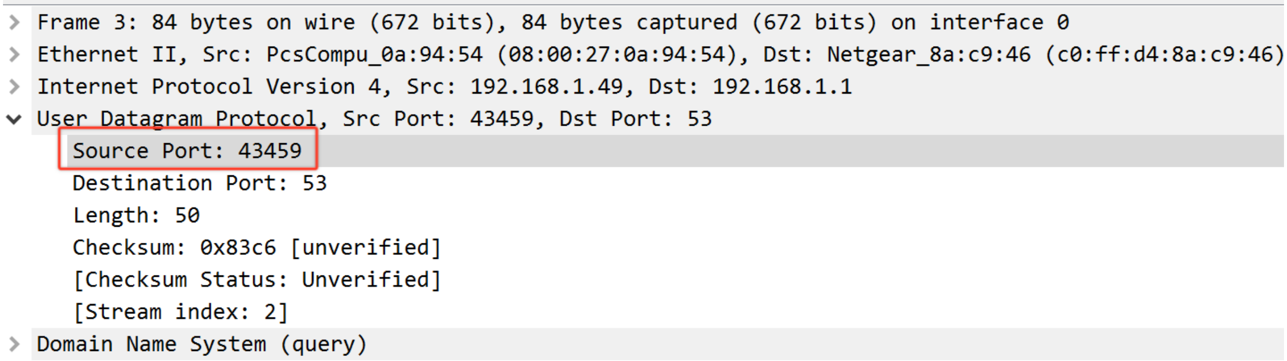
- Source Port
- Destination Port
- Length
- Checksum



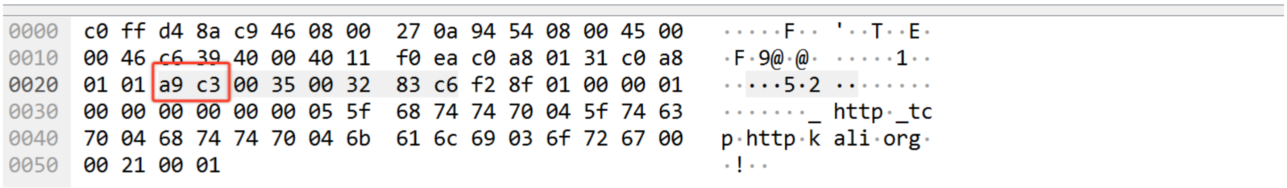
```
> Frame 3: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
> Ethernet II, Src: PcsCompu_0a:94:54 (08:00:27:0a:94:54), Dst: Netgear_8a:c9:46 (c0:ff:d4:8a:c9:46)
> Internet Protocol Version 4, Src: 192.168.1.49, Dst: 192.168.1.1
v User Datagram Protocol, Src Port: 43459, Dst Port: 53
     Source Port: 43459
     Destination Port: 53
     Length: 50
     Checksum: 0x83c6 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 2]
> Domain Name System (query)
```

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.

- 2 bytes

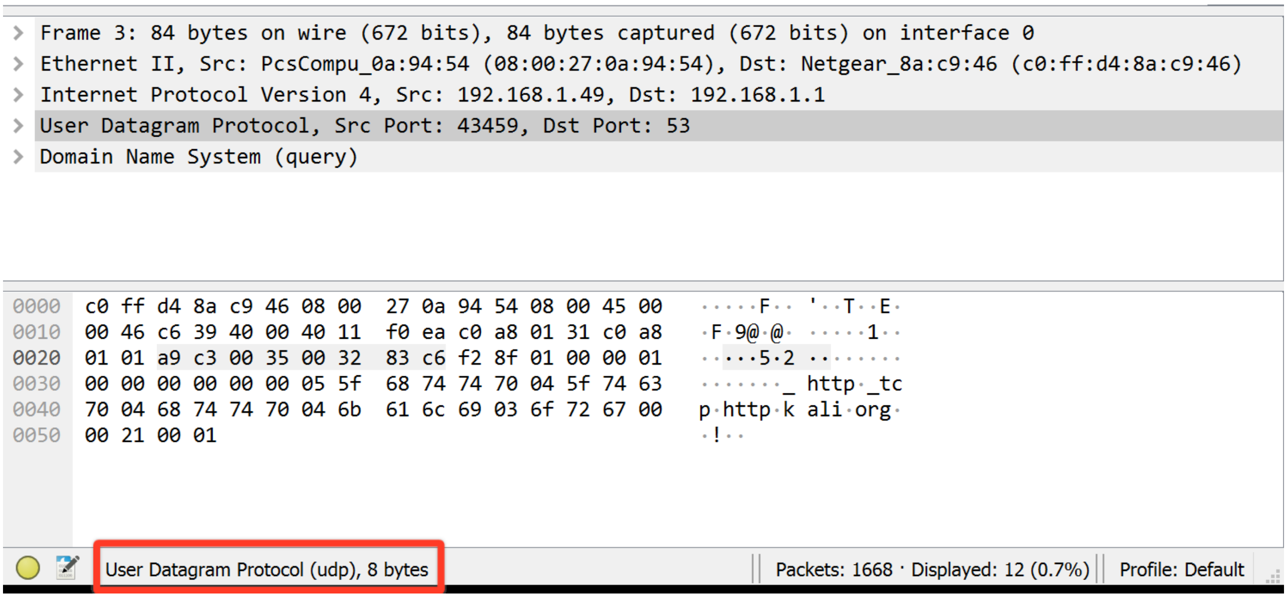


```
> Frame 3: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
> Ethernet II, Src: PcsCompu_0a:94:54 (08:00:27:0a:94:54), Dst: Netgear_8a:c9:46 (c0:ff:d4:8a:c9:46)
> Internet Protocol Version 4, Src: 192.168.1.49, Dst: 192.168.1.1
v User Datagram Protocol, Src Port: 43459, Dst Port: 53
     Source Port: 43459
     Destination Port: 53
     Length: 50
     Checksum: 0x83c6 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 2]
> Domain Name System (query)
```



```
0000  c0 ff d4 8a c9 46 08 00  27 0a 94 54 08 00 45 00   ·····F·· '··T··E·
0010  00 46 c6 39 40 00 40 11  f0 ea c0 a8 01 31 c0 a8   ·F·9@·@· ·····1··
0020  01 01 a9 c3 00 35 00 32  83 c6 f2 8f 01 00 00 01   ·····5·2 ········
0030  00 00 00 00 00 00 05 5f  68 74 74 70 04 5f 74 63   ·······_ http·_tc
0040  70 04 68 74 74 70 04 6b  61 6c 69 03 6f 72 67 00   p·http·k ali·org·
0050  00 21 00 01                                        ·!··
```

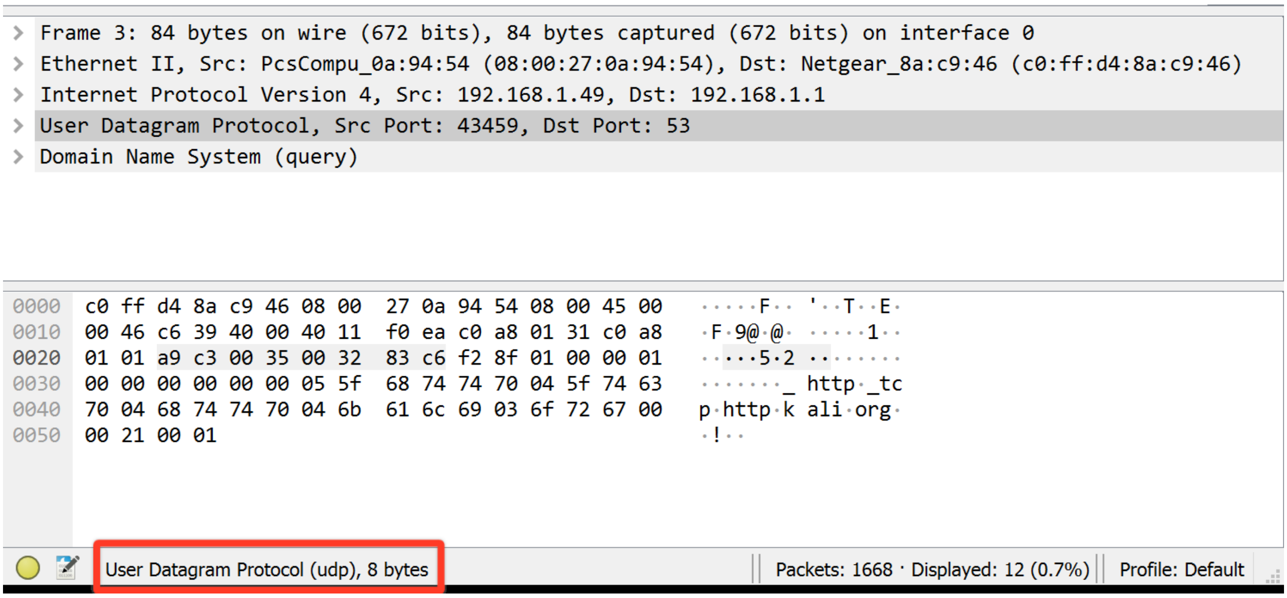
3. The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet. Specifies the length in bytes of the UDP header + data. As shown in the screenshot, there are 8 bytes in the UDP header + 42 bytes in the DNS data, totaling 50 bytes in the UDP Data + Header (the length field.)



```
> Frame 3: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
> Ethernet II, Src: PcsCompu_0a:94:54 (08:00:27:0a:94:54), Dst: Netgear_8a:c9:46 (c0:ff:d4:8a:c9:46)
> Internet Protocol Version 4, Src: 192.168.1.49, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 43459, Dst Port: 53
> Domain Name System (query)

0000  c0 ff d4 8a c9 46 08 00  27 0a 94 54 08 00 45 00   ·····F·· '··T··E·
0010  00 46 c6 39 40 00 40 11  f0 ea c0 a8 01 31 c0 a8   ·F·9@·@· ·····1··
0020  01 01 a9 c3 00 35 00 32  83 c6 f2 8f 01 00 00 01   ·····5·2 ········
0030  00 00 00 00 00 00 05 5f  68 74 74 70 04 5f 74 63   ·······_ http·_tc
0040  70 04 68 74 74 70 04 6b  61 6c 69 03 6f 72 67 00   p·http·k ali·org·
0050  00 21 00 01                                        ·!··
```

User Datagram Protocol (udp), 8 bytes | Packets: 1668 · Displayed: 12 (0.7%) | Profile: Default



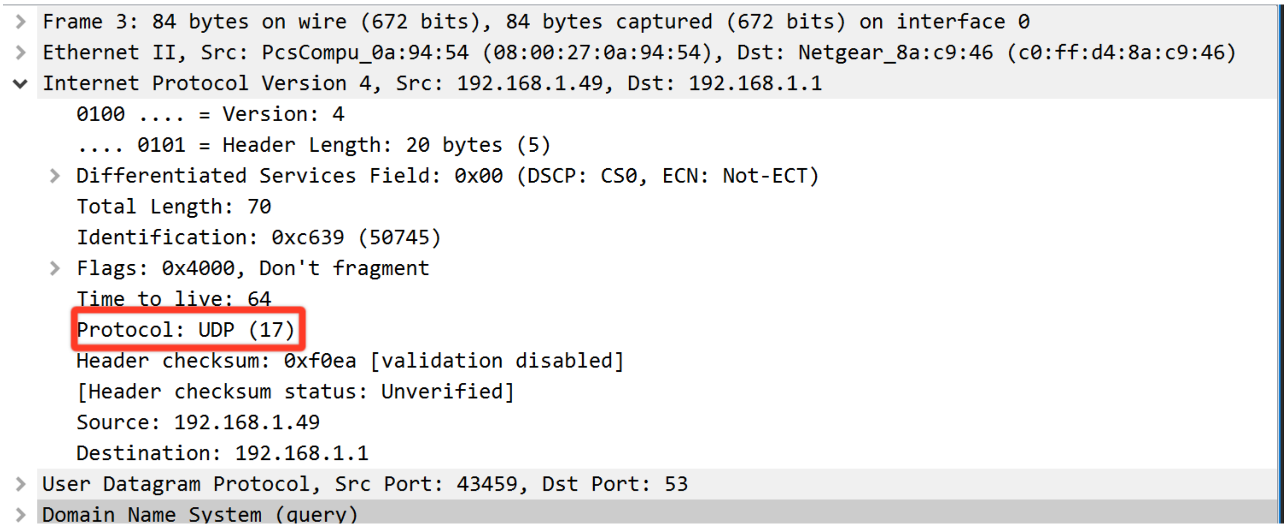
```
> Frame 3: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
> Ethernet II, Src: PcsCompu_0a:94:54 (08:00:27:0a:94:54), Dst: Netgear_8a:c9:46 (c0:ff:d4:8a:c9:46)
> Internet Protocol Version 4, Src: 192.168.1.49, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 43459, Dst Port: 53
> Domain Name System (query)

0000  c0 ff d4 8a c9 46 08 00  27 0a 94 54 08 00 45 00   ·····F·· '··T··E·
0010  00 46 c6 39 40 00 40 11  f0 ea c0 a8 01 31 c0 a8   ·F·9@·@· ·····1··
0020  01 01 a9 c3 00 35 00 32  83 c6 f2 8f 01 00 00 01   ·····5·2 ········
0030  00 00 00 00 00 00 05 5f  68 74 74 70 04 5f 74 63   ·······_ http·_tc
0040  70 04 68 74 74 70 04 6b  61 6c 69 03 6f 72 67 00   p·http·k ali·org·
0050  00 21 00 01                                        ·!··
```

User Datagram Protocol (udp), 8 bytes | Packets: 1668 · Displayed: 12 (0.7%) | Profile: Default

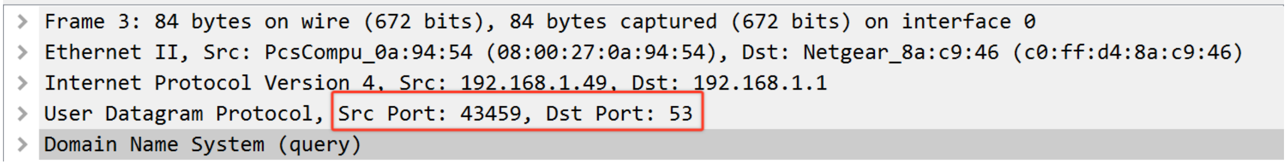
4. What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your answer to 2. above) Since the length header field can only store 2 bytes, the largest number that can be represented by that is 1111111111111111 (in binary), or 65535 (in base 10).
5. What is the largest possible source port number? (Hint: see the hint in 4.) Since the source port number header field can only store 2 bytes, the largest number that can be represented by that is 1111111111111111 (in binary), or 65535 (in base 10).
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). UDP - 17 (0x11)

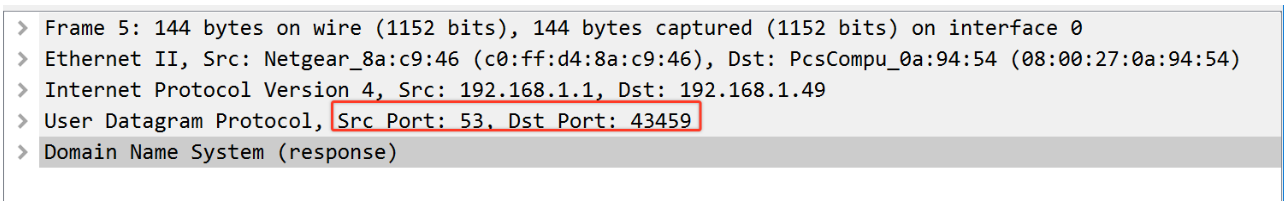


```
> Frame 3: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
> Ethernet II, Src: PcsCompu_0a:94:54 (08:00:27:0a:94:54), Dst: Netgear_8a:c9:46 (c0:ff:d4:8a:c9:46)
v Internet Protocol Version 4, Src: 192.168.1.49, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 70
    Identification: 0xc639 (50745)
  > Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0xf0ea [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.49
    Destination: 192.168.1.1
> User Datagram Protocol, Src Port: 43459, Dst Port: 53
> Domain Name System (query)
```

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 from the original packet is the destination port in the second packet. The client opens the port and waits for a response on it to close the connection.



```
> Frame 3: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
> Ethernet II, Src: PcsCompu_0a:94:54 (08:00:27:0a:94:54), Dst: Netgear_8a:c9:46 (c0:ff:d4:8a:c9:46)
> Internet Protocol Version 4, Src: 192.168.1.49, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 43459, Dst Port: 53
> Domain Name System (query)
```



```
> Frame 5: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface 0
> Ethernet II, Src: Netgear_8a:c9:46 (c0:ff:d4:8a:c9:46), Dst: PcsCompu_0a:94:54 (08:00:27:0a:94:54)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.49
> User Datagram Protocol, Src Port: 53, Dst Port: 43459
> Domain Name System (response)
```