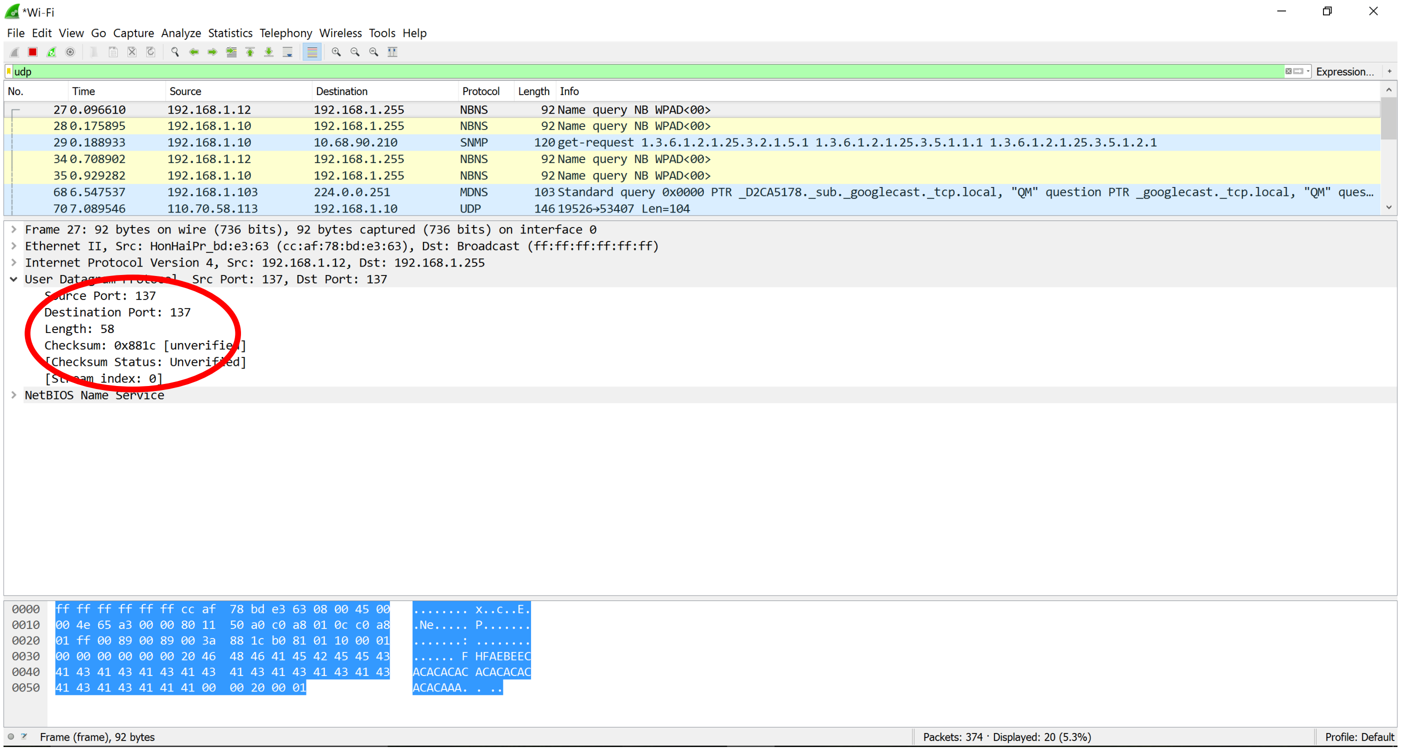
Wireshark UDP

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.**

   The header contains 4 fields; source port, destination port, lengh, checksum.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
Expression...

```
No.   Time      Source         Destination    Protocol  Length Info
   27 0.096610  192.168.1.12   192.168.1.255  NBNS          92 Name query NB WPAD<00>
   28 0.175895  192.168.1.10   192.168.1.255  NBNS          92 Name query NB WPAD<00>
   29 0.188933  192.168.1.10   10.68.90.210   SNMP         120 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1
   34 0.708902  192.168.1.12   192.168.1.255  NBNS          92 Name query NB WPAD<00>
   35 0.929282  192.168.1.10   192.168.1.255  NBNS          92 Name query NB WPAD<00>
   68 6.547537  192.168.1.103  224.0.0.251    MDNS         103 Standard query 0x0000 PTR _D2CA5178._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" ques…
   70 7.089546  110.70.58.113  192.168.1.10   UDP          146 19526→53407 Len=104
```

```
> Frame 27: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
> Ethernet II, Src: HonHaiPr_bd:e3:63 (cc:af:78:bd:e3:63), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.1.12, Dst: 192.168.1.255
v User Datagram Protocol, Src Port: 137, Dst Port: 137
    Source Port: 137
    Destination Port: 137
    Length: 58
    Checksum: 0x881c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
> NetBIOS Name Service
```

```
0000  ff ff ff ff ff ff cc af  78 bd e3 63 08 00 45 00   ........ x..c..E.
0010  00 4e 65 a3 00 00 80 11  50 a0 c0 a8 01 0c c0 a8   .Ne..... P.......
0020  01 ff 00 89 00 89 00 3a  88 1c b0 81 01 10 00 01   .......: ........
0030  00 00 00 00 00 00 20 46  48 46 41 45 42 45 45 43   ...... F HFAEBEEC
0040  41 43 41 43 41 43 41 43  41 43 41 43 41 43 41 43   ACACACAC ACACACAC
0050  41 43 41 43 41 41 41 00  00 20 00 01               ACACAAA. . ..
```

Frame (frame), 92 bytes | Packets: 374 · Displayed: 20 (5.3%) | Profile: Default

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 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.**

   The value of the length is the sum of 8 header bytes plus the encapsulated data.

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 216 – 1 less the header bytes. This gives 65535 – 8 = 65527 bytes.

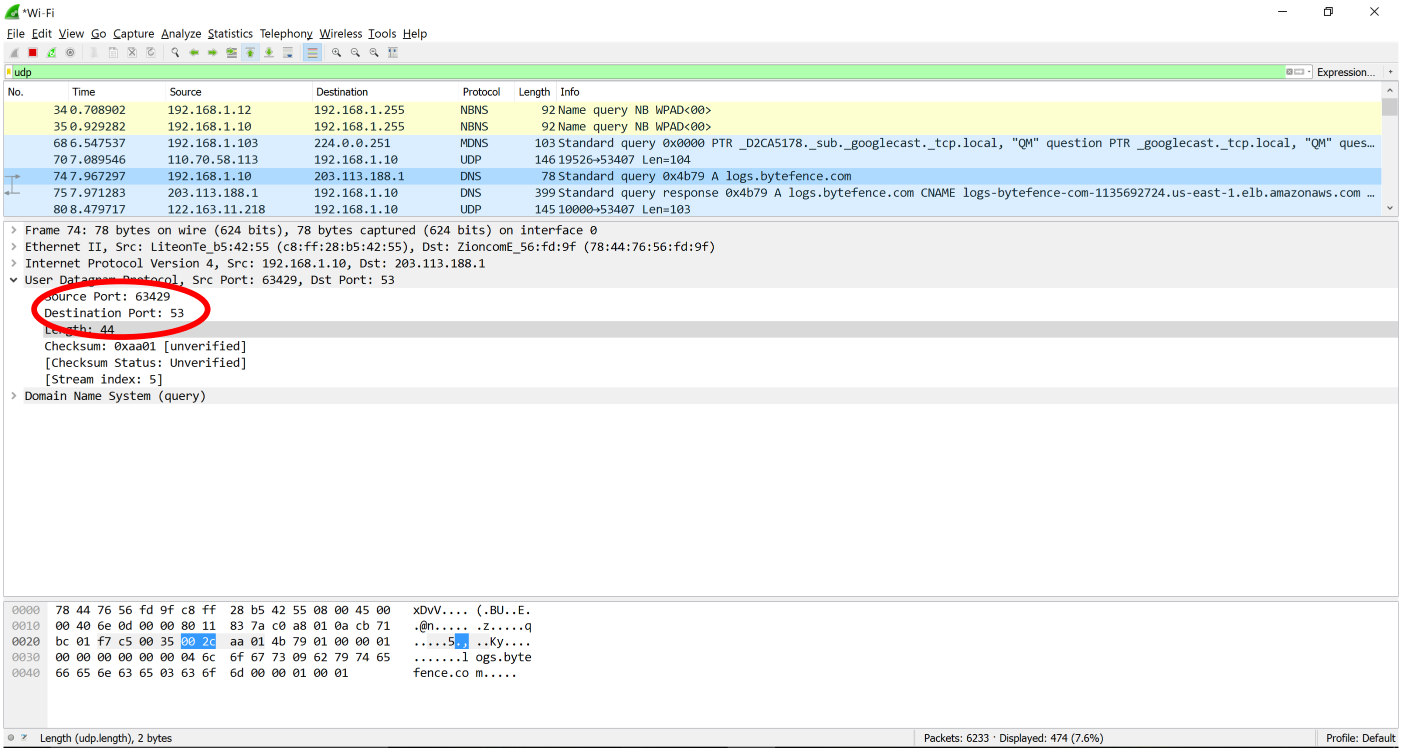
5. **What is the largest possible source port number? (Hint: see the hint in 4.)**

   The largest possible source port number is 216 – 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.

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.**



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
Expression…

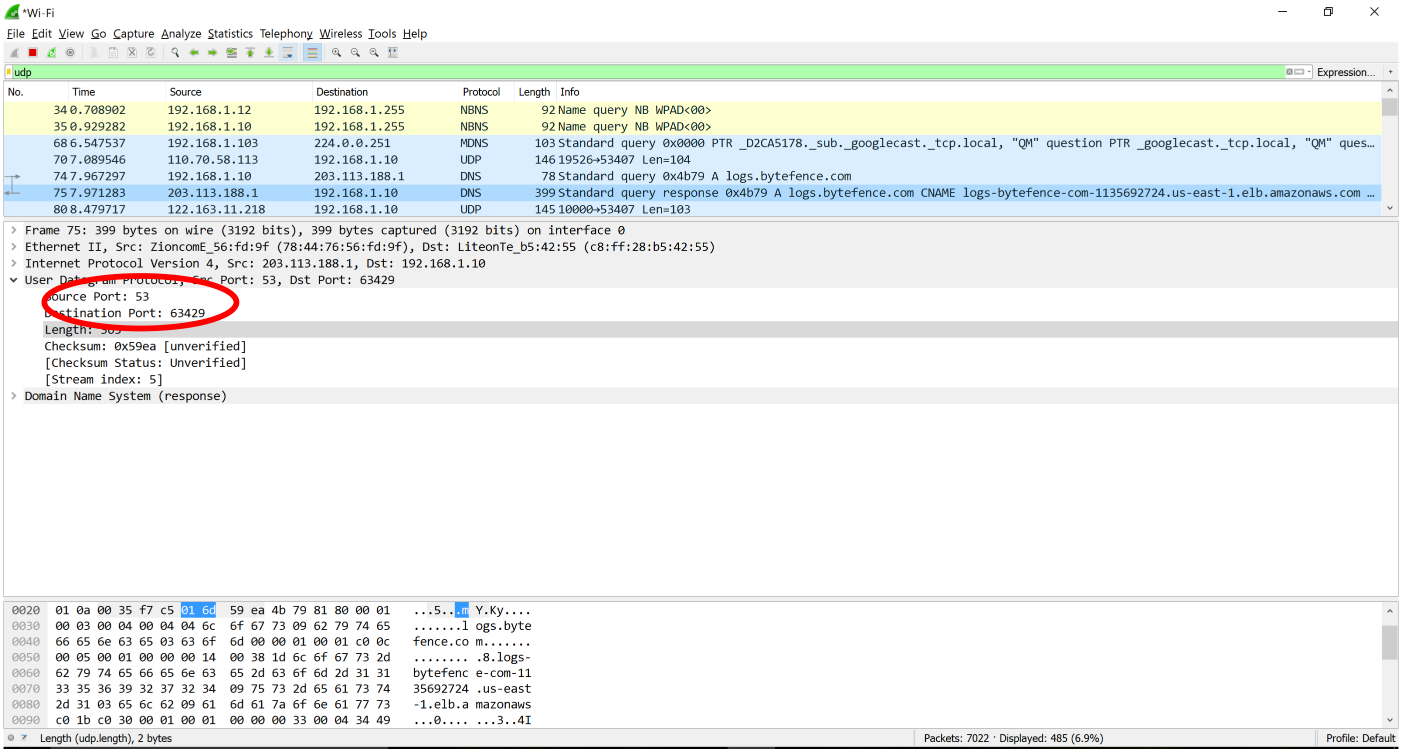
```
No.   Time       Source          Destination     Protocol Length Info
   34 0.708902   192.168.1.12    192.168.1.255   NBNS        92 Name query NB WPAD<00>
   35 0.929282   192.168.1.10    192.168.1.255   NBNS        92 Name query NB WPAD<00>
   68 6.547537   192.168.1.103   224.0.0.251     MDNS       103 Standard query 0x0000 PTR _D2CA5178._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" ques…
   70 7.089546   110.70.58.113   192.168.1.10    UDP        146 19526→53407 Len=104
   74 7.967297   192.168.1.10    203.113.188.1   DNS         78 Standard query 0x4b79 A logs.bytefence.com
   75 7.971283   203.113.188.1   192.168.1.10    DNS        399 Standard query response 0x4b79 A logs.bytefence.com CNAME logs-bytefence-com-1135692724.us-east-1.elb.amazonaws.com …
   80 8.479717   122.163.11.218  192.168.1.10    UDP        145 10000→53407 Len=103
```

```
> Frame 74: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
> Ethernet II, Src: LiteonTe_b5:42:55 (c8:ff:28:b5:42:55), Dst: ZioncomE_56:fd:9f (78:44:76:56:fd:9f)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 203.113.188.1
v User Datagram Protocol, Src Port: 63429, Dst Port: 53
    Source Port: 63429
    Destination Port: 53
    Length: 44
    Checksum: 0xaa01 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
> Domain Name System (query)
```

```
0000  78 44 76 56 fd 9f c8 ff  28 b5 42 55 08 00 45 00   xDvV.... (.BU..E.
0010  00 40 6e 0d 00 00 80 11  83 7a c0 a8 01 0a cb 71   .@n..... .z.....q
0020  bc 01 f7 c5 00 35 00 2c  aa 01 4b 79 01 00 00 01   .....5., ..Ky....
0030  00 00 00 00 00 00 04 6c  6f 67 73 09 62 79 74 65   .......l ogs.byte
0040  66 65 6e 63 65 03 63 6f  6d 00 00 01 00 01         fence.co m.....
```

```
Length (udp.length), 2 bytes          Packets: 6233 · Displayed: 474 (7.6%)          Profile: Default
```

Sent by my host.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
Expression…

```
No.   Time       Source          Destination     Protocol Length Info
   34 0.708902   192.168.1.12    192.168.1.255   NBNS        92 Name query NB WPAD<00>
   35 0.929282   192.168.1.10    192.168.1.255   NBNS        92 Name query NB WPAD<00>
   68 6.547537   192.168.1.103   224.0.0.251     MDNS       103 Standard query 0x0000 PTR _D2CA5178._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" ques…
   70 7.089546   110.70.58.113   192.168.1.10    UDP        146 19526→53407 Len=104
   74 7.967297   192.168.1.10    203.113.188.1   DNS         78 Standard query 0x4b79 A logs.bytefence.com
   75 7.971283   203.113.188.1   192.168.1.10    DNS        399 Standard query response 0x4b79 A logs.bytefence.com CNAME logs-bytefence-com-1135692724.us-east-1.elb.amazonaws.com …
   80 8.479717   122.163.11.218  192.168.1.10    UDP        145 10000→53407 Len=103
```

```
> Frame 75: 399 bytes on wire (3192 bits), 399 bytes captured (3192 bits) on interface 0
> Ethernet II, Src: ZioncomE_56:fd:9f (78:44:76:56:fd:9f), Dst: LiteonTe_b5:42:55 (c8:ff:28:b5:42:55)
> Internet Protocol Version 4, Src: 203.113.188.1, Dst: 192.168.1.10
v User Datagram Protocol, Src Port: 53, Dst Port: 63429
    Source Port: 53
    Destination Port: 63429
    Length: 365
    Checksum: 0x59ea [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
> Domain Name System (response)
```

```
0020  01 0a 00 35 f7 c5 01 6d  59 ea 4b 79 81 80 00 01   ...5...m Y.Ky....
0030  00 03 00 04 00 04 04 6c  6f 67 73 09 62 79 74 65   .......l ogs.byte
0040  66 65 6e 63 65 03 63 6f  6d 00 00 01 00 01 c0 0c   fence.co m.......
0050  00 05 00 01 00 00 00 14  00 38 1d 6c 6f 67 73 2d   ........ .8.logs-
0060  62 79 74 65 66 65 6e 63  65 2d 63 6f 6d 2d 31 31   bytefenc e-com-11
0070  33 35 36 39 32 37 32 34  09 75 73 2d 65 61 73 74   35692724 .us-east
0080  2d 31 03 65 6c 62 09 61  6d 61 7a 6f 6e 61 77 73   -1.elb.a mazonaws
0090  c0 1b c0 30 00 01 00 01  00 00 00 33 00 04 34 49   ...0.... ...3..4I
```

```
Length (udp.length), 2 bytes          Packets: 7022 · Displayed: 485 (6.9%)          Profile: Default
```

Reply to host.

The source port of the UDP packet sent by the host is the same as the destination port of the reply packet, and conversely the destination port of the UDP packet sent by the host is the same as the source port of the reply packet.