Wireshark Lab: UDP v6.1

Vandré Leal Cândido

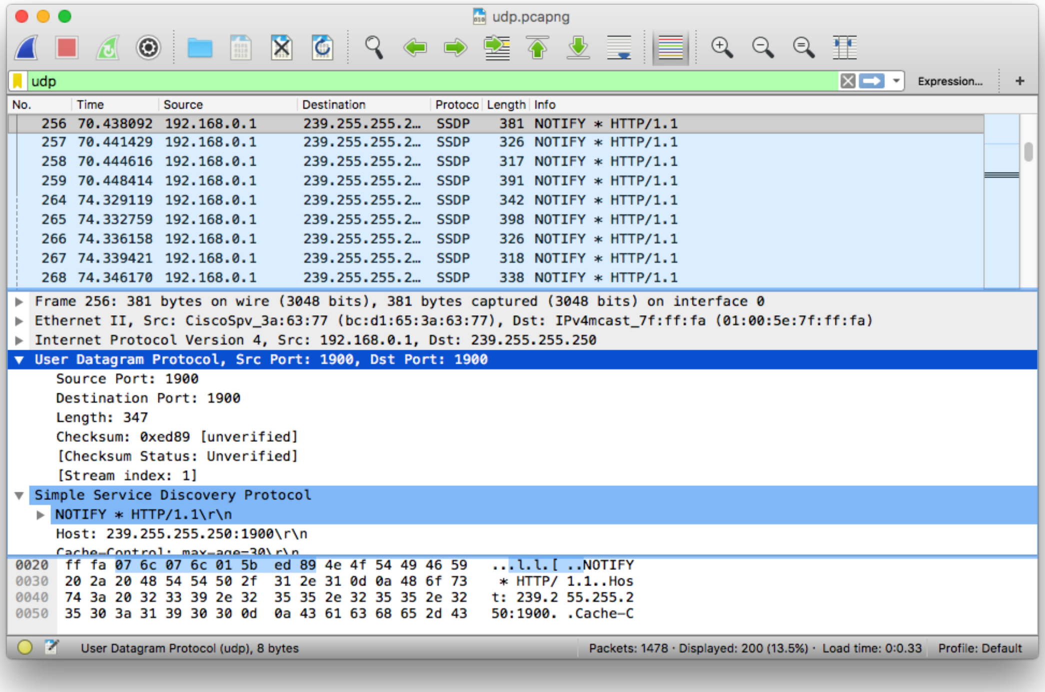
September 1, 2017

1 The Assignment

- *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.*

  There are four fields in the UDP header: **Source Port**, **Destination Port**, **Length** and **Checksum**.

Figure 1: UDP packet



No.	Time	Source	Destination	Protoco	Length	Info
256	70.438092	192.168.0.1	239.255.255.2…	SSDP	381	NOTIFY * HTTP/1.1
257	70.441429	192.168.0.1	239.255.255.2…	SSDP	326	NOTIFY * HTTP/1.1
258	70.444616	192.168.0.1	239.255.255.2…	SSDP	317	NOTIFY * HTTP/1.1
259	70.448414	192.168.0.1	239.255.255.2…	SSDP	391	NOTIFY * HTTP/1.1
264	74.329119	192.168.0.1	239.255.255.2…	SSDP	342	NOTIFY * HTTP/1.1
265	74.332759	192.168.0.1	239.255.255.2…	SSDP	398	NOTIFY * HTTP/1.1
266	74.336158	192.168.0.1	239.255.255.2…	SSDP	326	NOTIFY * HTTP/1.1
267	74.339421	192.168.0.1	239.255.255.2…	SSDP	318	NOTIFY * HTTP/1.1
268	74.346170	192.168.0.1	239.255.255.2…	SSDP	338	NOTIFY * HTTP/1.1

```
▶ Frame 256: 381 bytes on wire (3048 bits), 381 bytes captured (3048 bits) on interface 0
▶ Ethernet II, Src: CiscoSpv_3a:63:77 (bc:d1:65:3a:63:77), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
▶ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 239.255.255.250
▼ User Datagram Protocol, Src Port: 1900, Dst Port: 1900
    Source Port: 1900
    Destination Port: 1900
    Length: 347
    Checksum: 0xed89 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
▼ Simple Service Discovery Protocol
  ▶ NOTIFY * HTTP/1.1\r\n
    Host: 239.255.255.250:1900\r\n
    Cache-Control: max-age=30\r\n
```

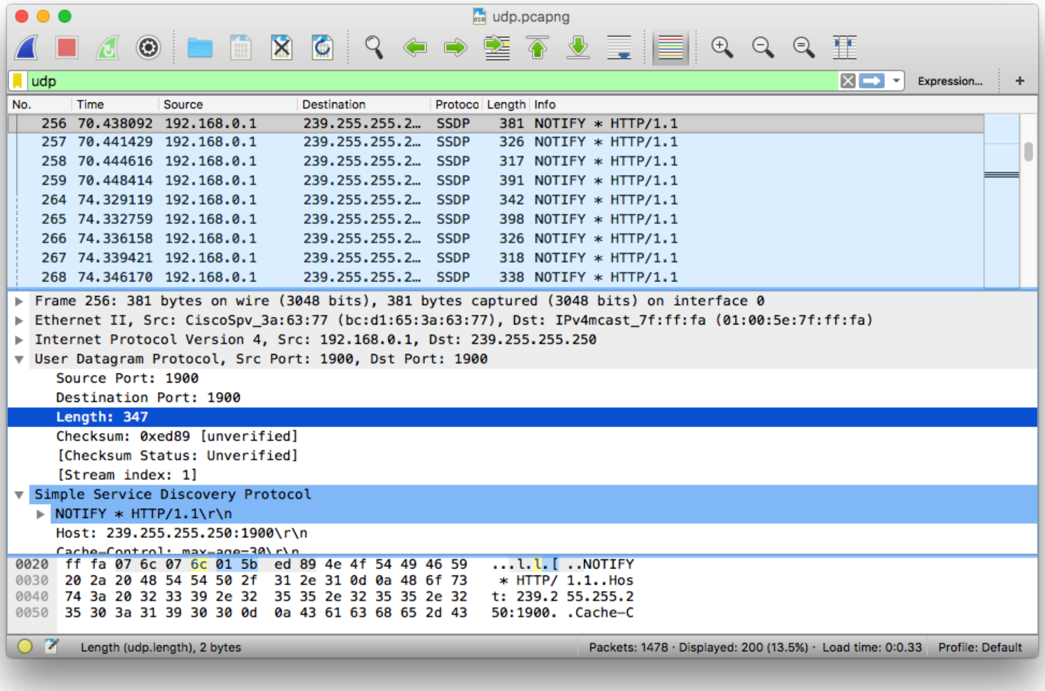
```
0020  ff fa 07 6c 07 6c 01 5b  ed 89 4e 4f 54 49 46 59   ...l.l.[ ..NOTIFY
0030  20 2a 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73    * HTTP/ 1.1..Hos
0040  74 3a 20 32 33 39 2e 32  35 35 2e 32 35 35 2e 32   t: 239.2 55.255.2
0050  35 30 3a 31 39 30 30 0d  0a 43 61 63 68 65 2d 43   50:1900. .Cache-C
```

User Datagram Protocol (udp), 8 bytes   Packets: 1478 · Displayed: 200 (13.5%) · Load time: 0:0.33   Profile: Default

- *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.*

  Each one of the fields in the UDP header is 2 bytes long.

Figure 2: Field size example (length)



```
No.   Time       Source        Destination      Protoco Length Info
  256 70.438092  192.168.0.1   239.255.255.2…   SSDP     381 NOTIFY * HTTP/1.1
  257 70.441429  192.168.0.1   239.255.255.2…   SSDP     326 NOTIFY * HTTP/1.1
  258 70.444616  192.168.0.1   239.255.255.2…   SSDP     317 NOTIFY * HTTP/1.1
  259 70.448414  192.168.0.1   239.255.255.2…   SSDP     391 NOTIFY * HTTP/1.1
  264 74.329119  192.168.0.1   239.255.255.2…   SSDP     342 NOTIFY * HTTP/1.1
  265 74.332759  192.168.0.1   239.255.255.2…   SSDP     398 NOTIFY * HTTP/1.1
  266 74.336158  192.168.0.1   239.255.255.2…   SSDP     326 NOTIFY * HTTP/1.1
  267 74.339421  192.168.0.1   239.255.255.2…   SSDP     318 NOTIFY * HTTP/1.1
  268 74.346170  192.168.0.1   239.255.255.2…   SSDP     338 NOTIFY * HTTP/1.1
```

```
▶ Frame 256: 381 bytes on wire (3048 bits), 381 bytes captured (3048 bits) on interface 0
▶ Ethernet II, Src: CiscoSpv_3a:63:77 (bc:d1:65:3a:63:77), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
▶ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 239.255.255.250
▼ User Datagram Protocol, Src Port: 1900, Dst Port: 1900
    Source Port: 1900
    Destination Port: 1900
    Length: 347
    Checksum: 0xed89 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
▼ Simple Service Discovery Protocol
  ▶ NOTIFY * HTTP/1.1\r\n
    Host: 239.255.255.250:1900\r\n
    Cache-Control: max-age=30\r\n
```

```
0020  ff fa 07 6c 07 6c 01 5b  ed 89 4e 4f 54 49 46 59   ...l.l.[ ..NOTIFY
0030  20 2a 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73    * HTTP/ 1.1..Hos
0040  74 3a 20 32 33 39 2e 32  35 35 2e 32 35 35 2e 32   t: 239.2 55.255.2
0050  35 30 3a 31 39 30 30 0d  0a 43 61 63 68 65 2d 43   50:1900. .Cache-C
```

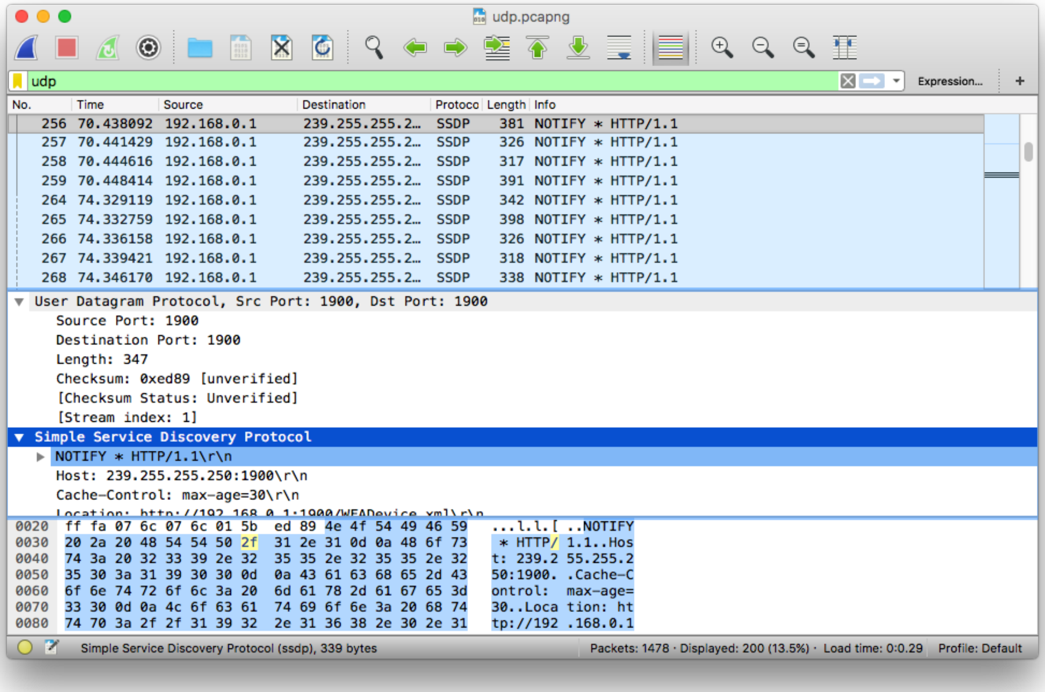
Length (udp.length), 2 bytes

Packets: 1478 · Displayed: 200 (13.5%) · Load time: 0:0.33 | Profile: Default

- *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 in the length field (347 bytes) is the sum of the header length (8 bytes) plus the SSDP data (339 bytes).

Figure 3: SSDP data length



udp.pcapng

udp

```
No.    Time       Source          Destination       Protoco  Length  Info
  256  70.438092  192.168.0.1     239.255.255.2…    SSDP     381  NOTIFY * HTTP/1.1
  257  70.441429  192.168.0.1     239.255.255.2…    SSDP     326  NOTIFY * HTTP/1.1
  258  70.444616  192.168.0.1     239.255.255.2…    SSDP     317  NOTIFY * HTTP/1.1
  259  70.448414  192.168.0.1     239.255.255.2…    SSDP     391  NOTIFY * HTTP/1.1
  264  74.329119  192.168.0.1     239.255.255.2…    SSDP     342  NOTIFY * HTTP/1.1
  265  74.332759  192.168.0.1     239.255.255.2…    SSDP     398  NOTIFY * HTTP/1.1
  266  74.336158  192.168.0.1     239.255.255.2…    SSDP     326  NOTIFY * HTTP/1.1
  267  74.339421  192.168.0.1     239.255.255.2…    SSDP     318  NOTIFY * HTTP/1.1
  268  74.346170  192.168.0.1     239.255.255.2…    SSDP     338  NOTIFY * HTTP/1.1
```

```
▼ User Datagram Protocol, Src Port: 1900, Dst Port: 1900
    Source Port: 1900
    Destination Port: 1900
    Length: 347
    Checksum: 0xed89 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
▼ Simple Service Discovery Protocol
  ▶ NOTIFY * HTTP/1.1\r\n
    Host: 239.255.255.250:1900\r\n
    Cache-Control: max-age=30\r\n
    Location: http://192.168.0.1:1900/WFADevice.xml\r\n
```

```
0020  ff fa 07 6c 07 6c 01 5b  ed 89 4e 4f 54 49 46 59   ...l.l.[ ..NOTIFY
0030  20 2a 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73    * HTTP/ 1.1..Hos
0040  74 3a 20 32 33 39 2e 32  35 35 2e 32 35 35 2e 32   t: 239.2 55.255.2
0050  35 30 3a 31 39 30 30 0d  0a 43 61 63 68 65 2d 43   50:1900. .Cache-C
0060  6f 6e 74 72 6f 6c 3a 20  6d 61 78 2d 61 67 65 3d   ontrol:  max-age=
0070  33 30 0d 0a 4c 6f 63 61  74 69 6f 6e 3a 20 68 74   30..Loca tion: ht
0080  74 70 3a 2f 2f 31 39 32  2e 31 36 38 2e 30 2e 31   tp://192 .168.0.1
```

Simple Service Discovery Protocol (ssdp), 339 bytes   Packets: 1478 · Displayed: 200 (13.5%) · Load time: 0:0.29   Profile: Default

- *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} minus the number of bytes in the header (8). Therefore, $65535 - 8 =$ **65527** bytes.

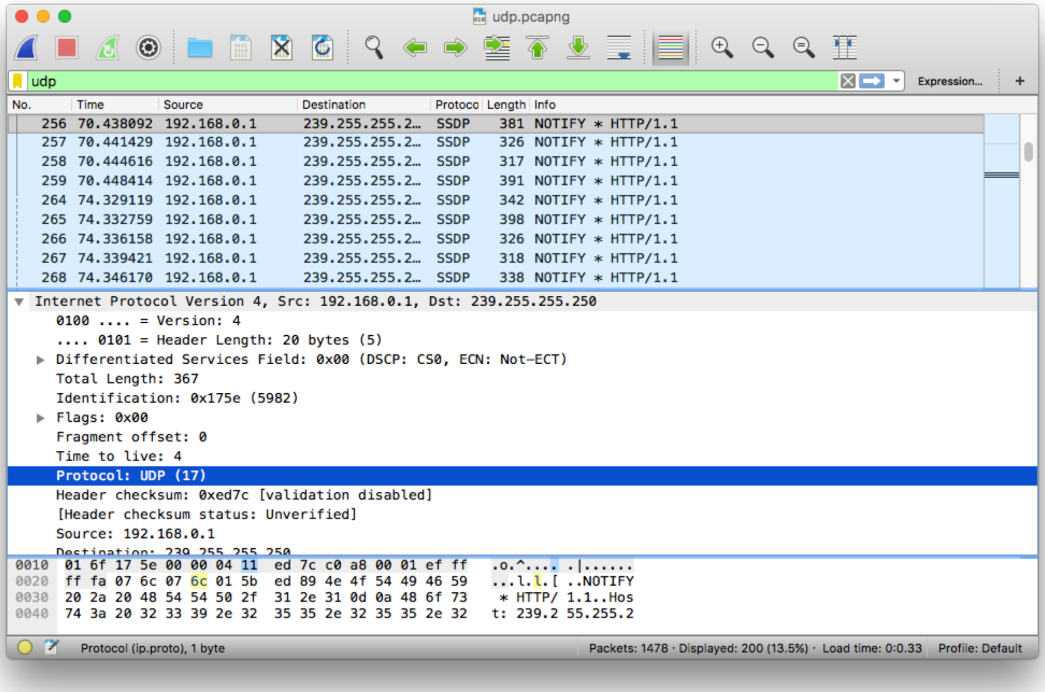
- *What is the largest possible source port number? (Hint: see the hint in 4.)*

  The largest possible source port number is $2^{16} =$ **65527**.

- *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 protocol number for UDP is 0x11 hex, which translates to 17 in decimal.

Figure 4: UDP protocol number



udp.pcapng

udp

```
No.   Time       Source         Destination       Protoco Length Info
  256 70.438092  192.168.0.1    239.255.255.2…    SSDP    381    NOTIFY * HTTP/1.1
  257 70.441429  192.168.0.1    239.255.255.2…    SSDP    326    NOTIFY * HTTP/1.1
  258 70.444616  192.168.0.1    239.255.255.2…    SSDP    317    NOTIFY * HTTP/1.1
  259 70.448414  192.168.0.1    239.255.255.2…    SSDP    391    NOTIFY * HTTP/1.1
  264 74.329119  192.168.0.1    239.255.255.2…    SSDP    342    NOTIFY * HTTP/1.1
  265 74.332759  192.168.0.1    239.255.255.2…    SSDP    398    NOTIFY * HTTP/1.1
  266 74.336158  192.168.0.1    239.255.255.2…    SSDP    326    NOTIFY * HTTP/1.1
  267 74.339421  192.168.0.1    239.255.255.2…    SSDP    318    NOTIFY * HTTP/1.1
  268 74.346170  192.168.0.1    239.255.255.2…    SSDP    338    NOTIFY * HTTP/1.1
```

```
▼ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 239.255.255.250
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 367
    Identification: 0x175e (5982)
  ▶ Flags: 0x00
    Fragment offset: 0
    Time to live: 4
    Protocol: UDP (17)
    Header checksum: 0xed7c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.1
    Destination: 239.255.255.250
```

```
0010  01 6f 17 5e 00 00 04 11  ed 7c c0 a8 00 01 ef ff   .o.^.... .|......
0020  ff fa 07 6c 07 6c 01 5b  ed 89 4e 4f 54 49 46 59   ...l.l.[ ..NOTIFY
0030  20 2a 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73    * HTTP/ 1.1..Hos
0040  74 3a 20 32 33 39 2e 32  35 35 2e 32 35 35 2e 32   t: 239.2 55.255.2
```

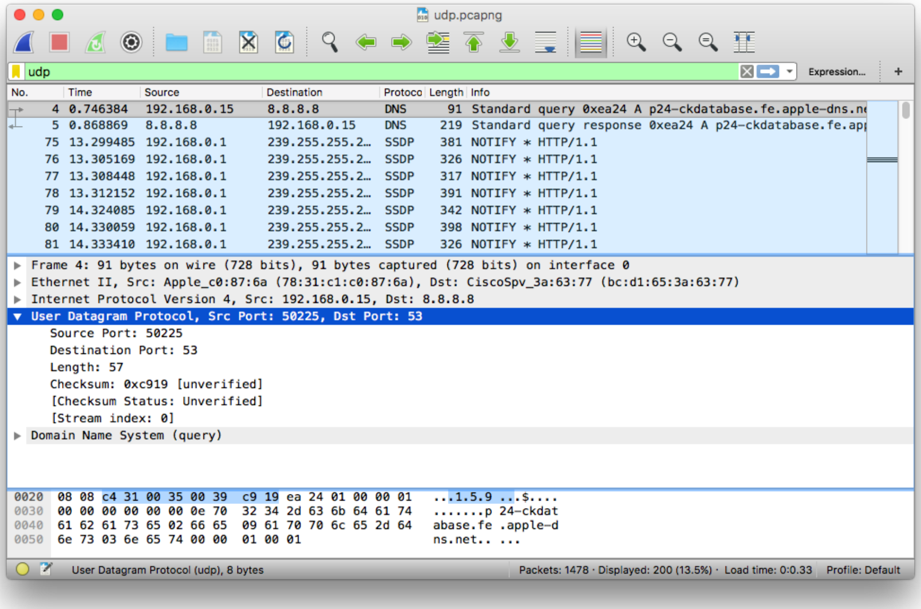
Protocol (ip.proto), 1 byte

Packets: 1478 · Displayed: 200 (13.5%) · Load time: 0:0.33   Profile: Default

- *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 first UDP packet is the same as the destination port of the reply packet. Similarly, the destination port of the UDP packet that was sent is the same as the source port of the reply packet.

Figure 5: UDP packet sent by local host



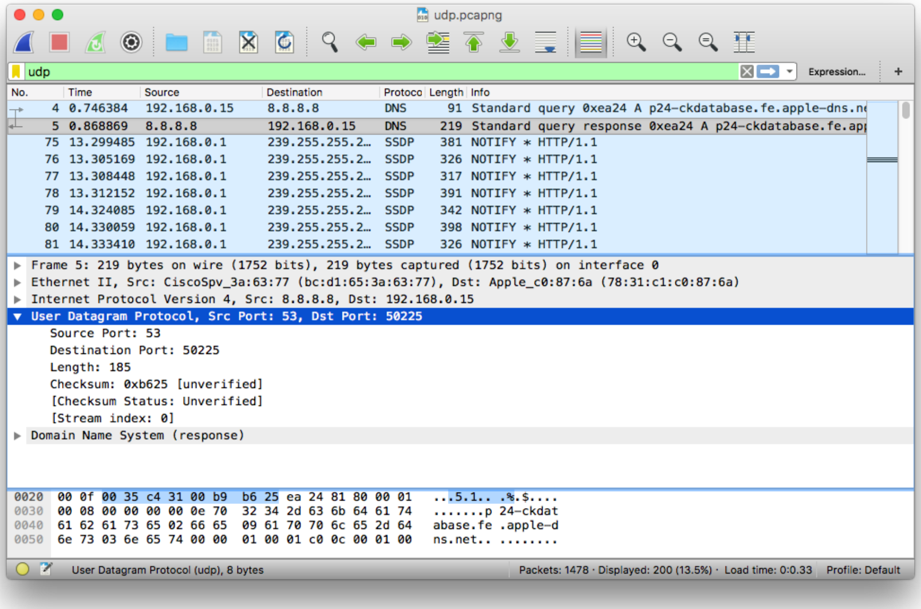
```
No.   Time       Source         Destination     Protoco Length Info
    4 0.746384   192.168.0.15   8.8.8.8         DNS       91 Standard query 0xea24 A p24-ckdatabase.fe.apple-dns.n
    5 0.868869   8.8.8.8        192.168.0.15    DNS      219 Standard query response 0xea24 A p24-ckdatabase.fe.ap
   75 13.299485  192.168.0.1    239.255.255.2…  SSDP     381 NOTIFY * HTTP/1.1
   76 13.305169  192.168.0.1    239.255.255.2…  SSDP     326 NOTIFY * HTTP/1.1
   77 13.308448  192.168.0.1    239.255.255.2…  SSDP     317 NOTIFY * HTTP/1.1
   78 13.312152  192.168.0.1    239.255.255.2…  SSDP     391 NOTIFY * HTTP/1.1
   79 14.324085  192.168.0.1    239.255.255.2…  SSDP     342 NOTIFY * HTTP/1.1
   80 14.330059  192.168.0.1    239.255.255.2…  SSDP     398 NOTIFY * HTTP/1.1
   81 14.333410  192.168.0.1    239.255.255.2…  SSDP     326 NOTIFY * HTTP/1.1
```

```
▶ Frame 4: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface 0
▶ Ethernet II, Src: Apple_c0:87:6a (78:31:c1:c0:87:6a), Dst: CiscoSpv_3a:63:77 (bc:d1:65:3a:63:77)
▶ Internet Protocol Version 4, Src: 192.168.0.15, Dst: 8.8.8.8
▼ User Datagram Protocol, Src Port: 50225, Dst Port: 53
    Source Port: 50225
    Destination Port: 53
    Length: 57
    Checksum: 0xc919 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
▶ Domain Name System (query)
```

```
0020  08 08 c4 31 00 35 00 39  c9 19 ea 24 01 00 00 01   ...1.5.9 ...$....
0030  00 00 00 00 00 00 0e 70  32 34 2d 63 6b 64 61 74   .......p 24-ckdat
0040  61 62 61 73 65 02 66 65  09 61 70 70 6c 65 2d 64   abase.fe .apple-d
0050  6e 73 03 6e 65 74 00 00  01 00 01                  ns.net.. ...
```

```
User Datagram Protocol (udp), 8 bytes     Packets: 1478 · Displayed: 200 (13.5%) · Load time: 0:0.33   Profile: Default
```

Figure 6: UDP reply packet received



```
No.   Time       Source         Destination     Protoco Length Info
    4 0.746384   192.168.0.15   8.8.8.8         DNS       91 Standard query 0xea24 A p24-ckdatabase.fe.apple-dns.n
    5 0.868869   8.8.8.8        192.168.0.15    DNS      219 Standard query response 0xea24 A p24-ckdatabase.fe.ap
   75 13.299485  192.168.0.1    239.255.255.2…  SSDP     381 NOTIFY * HTTP/1.1
   76 13.305169  192.168.0.1    239.255.255.2…  SSDP     326 NOTIFY * HTTP/1.1
   77 13.308448  192.168.0.1    239.255.255.2…  SSDP     317 NOTIFY * HTTP/1.1
   78 13.312152  192.168.0.1    239.255.255.2…  SSDP     391 NOTIFY * HTTP/1.1
   79 14.324085  192.168.0.1    239.255.255.2…  SSDP     342 NOTIFY * HTTP/1.1
   80 14.330059  192.168.0.1    239.255.255.2…  SSDP     398 NOTIFY * HTTP/1.1
   81 14.333410  192.168.0.1    239.255.255.2…  SSDP     326 NOTIFY * HTTP/1.1
```

```
▶ Frame 5: 219 bytes on wire (1752 bits), 219 bytes captured (1752 bits) on interface 0
▶ Ethernet II, Src: CiscoSpv_3a:63:77 (bc:d1:65:3a:63:77), Dst: Apple_c0:87:6a (78:31:c1:c0:87:6a)
▶ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.0.15
▼ User Datagram Protocol, Src Port: 53, Dst Port: 50225
    Source Port: 53
    Destination Port: 50225
    Length: 185
    Checksum: 0xb625 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
▶ Domain Name System (response)
```

```
0020  00 0f 00 35 c4 31 00 b9  b6 25 ea 24 81 80 00 01   ...5.1.. .%.$....
0030  00 08 00 00 00 00 0e 70  32 34 2d 63 6b 64 61 74   .......p 24-ckdat
0040  61 62 61 73 65 02 66 65  09 61 70 70 6c 65 2d 64   abase.fe .apple-d
0050  6e 73 03 6e 65 74 00 00  01 00 01 c0 0c 00 01 00   ns.net.. ........
```

```
User Datagram Protocol (udp), 8 bytes     Packets: 1478 · Displayed: 200 (13.5%) · Load time: 0:0.33   Profile: Default
```