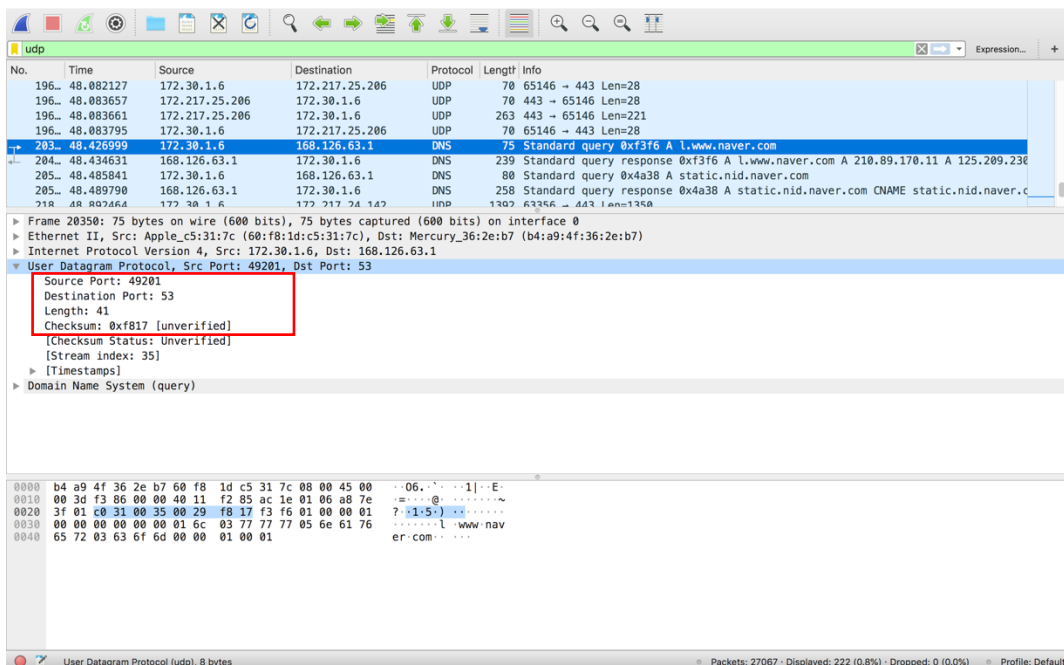


Wireshark Lab 4 (UDP)

17011599 안정연, 17011588 노하윤

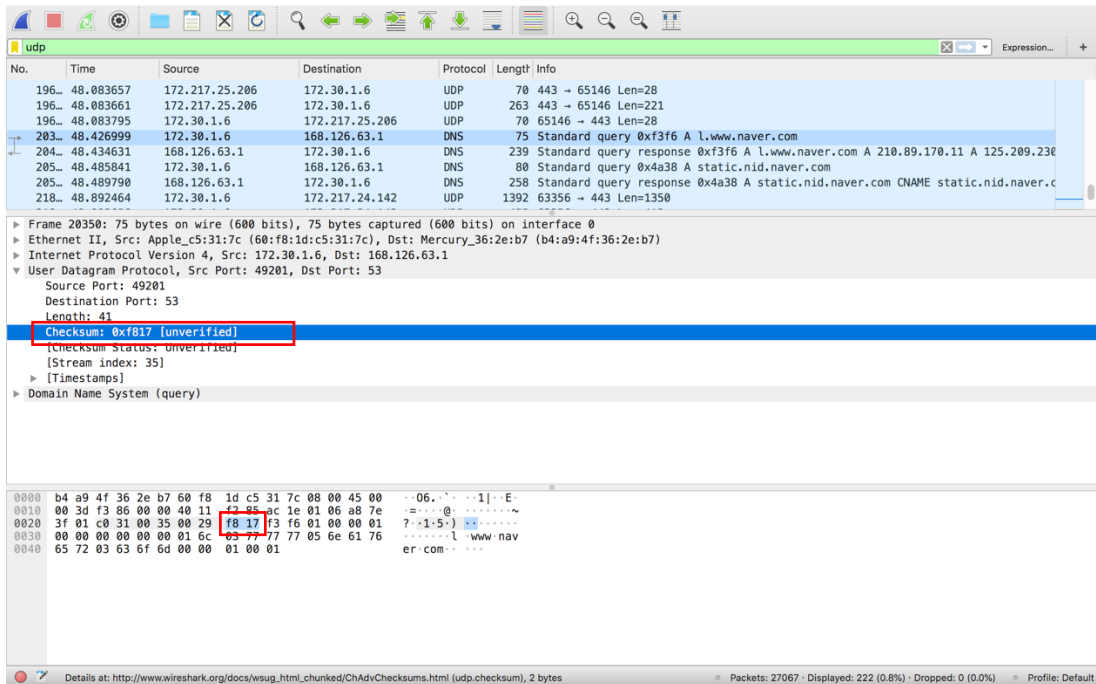
1. Select *one* UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.

The header 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.

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.

The value in the length field, in the example below it is 41, is the sum of the 8 header bytes and the remaining data bytes encapsulated in the packet.

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 in the payload is 2^{16} - 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.)

he largest possible source port number is 2^{16} 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).

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

The image shows a Wireshark packet capture of a DNS query and response. The first packet (No. 203) is a DNS query from source 172.30.1.6 to destination 168.126.63.1. The second packet (No. 204) is a DNS response from source 168.126.63.1 to destination 172.30.1.6. The response contains the IP address 210.89.170.11 for l.www.naver.com. The packet details pane shows the User Datagram Protocol (UDP) and Domain Name System (query) fields. The packet bytes pane shows the raw data in hexadecimal and ASCII.

- 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.

UDP Sent by my host

The image shows a Wireshark packet capture of a DNS query and response. The first packet (No. 203) is a DNS query from source 172.30.1.6 to destination 168.126.63.1. The second packet (No. 204) is a DNS response from source 168.126.63.1 to destination 172.30.1.6. The response contains the IP address 210.89.170.11 for l.www.naver.com. The packet details pane shows the User Datagram Protocol (UDP) and Domain Name System (query) fields. The packet bytes pane shows the raw data in hexadecimal and ASCII.

UDP Reply to Host

udp

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
196...	48.083657	172.217.25.206	172.30.1.6	UDP	70	443 → 65146 Len=28
196...	48.083661	172.217.25.206	172.30.1.6	UDP	263	443 → 65146 Len=221
196...	48.083795	172.30.1.6	172.217.25.206	UDP	70	65146 → 443 Len=28
203...	48.426999	172.30.1.6	168.126.63.1	DNS	75	Standard query 0xf3f6 A l.www.naver.com
204...	48.424531	168.126.63.1	172.30.1.6	DNS	239	Standard query response 0xf3f6 A l.www.naver.com A 210.89.170.11 A 125.209.236
205...	48.485041	172.30.1.6	168.126.63.1	DNS	80	Standard query 0x4a38 A static.nid.naver.com
205...	48.489790	168.126.63.1	172.30.1.6	DNS	258	Standard query response 0x4a38 A static.nid.naver.com CNAME static.nid.naver.c
218...	48.892464	172.30.1.6	172.217.24.142	UDP	1392	63356 → 443 Len=1350
218...	48.892656	172.30.1.6	172.217.24.142	UDP	455	63356 → 443 Len=413

▶ Frame 20459: 239 bytes on wire (1912 bits), 239 bytes captured (1912 bits) on interface 0

▶ Ethernet II, Src: Mercury_36:2e:b7 (b4:a9:4f:36:2e:b7), Dst: Apple_c5:31:7c (60:f8:1d:c5:31:7c)

▶ Internet Protocol Version 4, Src: 168.126.63.1, Dst: 172.30.1.6

▼ User Datagram Protocol, Src Port: 53, Dst Port: 49201

Source Port: 53

Destination Port: 49201

Length: 205

Checksum: 0x4cdb [unverified]

[Checksum Status: Unverified]

[Stream index: 35]

▶ [Timestamps]

▶ Domain Name System (response)

0020 01 06 00 35 c0 31 00 cd 4c db f3 f6 01 00 00 01 ...5.1... L.....

0030 00 06 00 02 00 02 01 6c 03 77 77 77 05 6e 61 76l www nav

0040 65 72 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00er.com.....

0050 01 00 00 00 d7 00 04 d2 59 aa 0b c0 0c 00 01 00Y.....

0060 01 00 00 00 d7 00 04 7d d1 eb c3 c0 0c 00 01 00}.....

0070 01 00 00 00 d7 00 04 d2 59 ab 8b c0 0c 00 01 00Y.....

0080 01 00 00 00 d7 00 04 d2 59 ac 09 c0 0c 00 01 00Y.....

0090 01 00 00 00 d7 00 04 d2 59 ab 0b c0 0c 00 01 00Y.....

00a0 01 00 00 00 d7 00 04 7d d1 da 4f c0 12 00 02 00}...0.....

00b0 01 00 00 ff 59 00 06 03 6e 73 32 c0 12 c0 12 00Y...ns2....

00c0 02 00 01 00 00 ff 59 00 06 03 6e 73 31 c0 12 c0Y...ns1....

00d0 9f 00 01 00 01 00 00 ed 53 00 04 7d d1 f8 06 c0S...}....

00e0 8d 00 01 00 01 00 00 ed 54 00 04 7d d1 f9 06T...}....

Source Port (udp.srcport), 2 bytes

Packets: 27067 · Displayed: 222 (0.8%) · Dropped: 0 (0.0%) · Profile: Default