

# WireShark Lab: UDP

## Computer Networks

By:  
**Monil Shah**  
**mds747**

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.

Ans)

- Source Port
- Destination Port
- Length
- Checksum

The image shows a Wireshark packet capture. The packet list pane displays several packets, with packet 51 selected. The packet details pane shows the User Datagram Protocol section, which includes the following fields:

- Source Port: 50300
- Destination Port: 53
- Length: 41
- Checksum: 0x4865 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 0]

Below the User Datagram Protocol section, the Domain Name System (query) section is visible. The packet bytes pane shows the raw data in hexadecimal and ASCII.

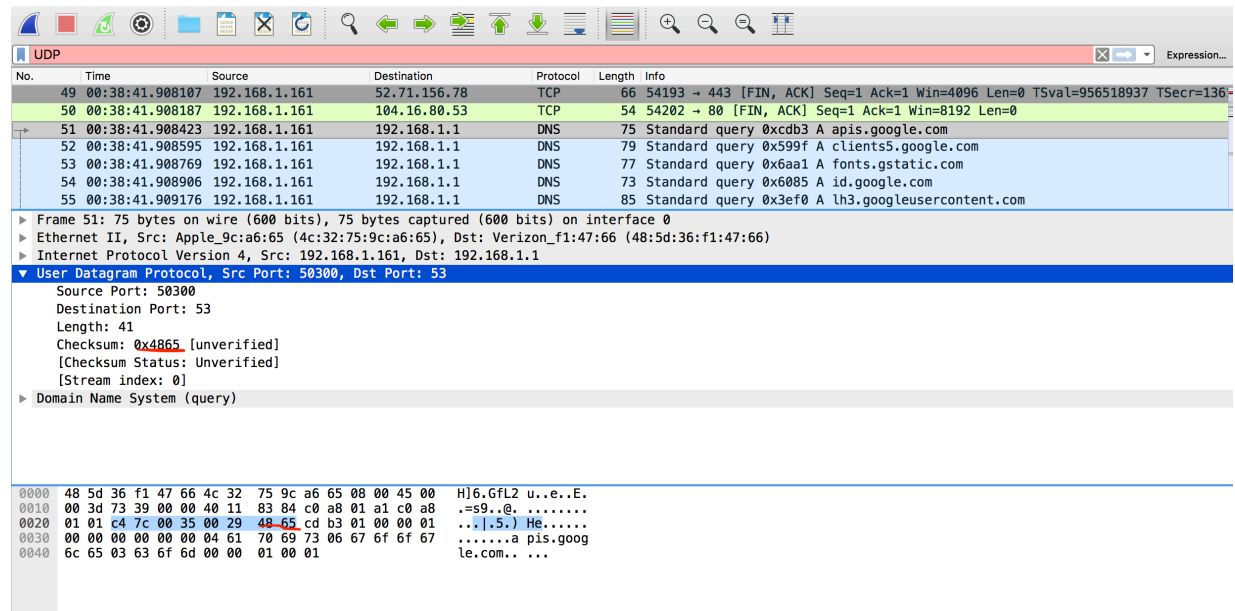
Handwritten red annotations are present on the image:

- A red arrow points from the text "A-7" to the Destination Port field (53).
- A red arrow points from the text "A-3" to the Length field (41).
- A red arrow points from the text "A-1" to the Domain Name System (query) section.

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.

Ans) Length of each UDP header fields = 2 bytes



No.	Time	Source	Destination	Protocol	Length	Info
49	00:38:41.908107	192.168.1.161	52.71.156.78	TCP	66	54193 → 443 [FIN, ACK] Seq=1 Ack=1 Win=4096 Len=0 TSval=956518937 TSecr=136...
50	00:38:41.908187	192.168.1.161	104.16.80.53	TCP	54	54202 → 80 [FIN, ACK] Seq=1 Ack=1 Win=8192 Len=0
51	00:38:41.908423	192.168.1.161	192.168.1.1	DNS	75	Standard query 0xcdb3 A apis.google.com
52	00:38:41.908595	192.168.1.161	192.168.1.1	DNS	79	Standard query 0x599f A clients5.google.com
53	00:38:41.908769	192.168.1.161	192.168.1.1	DNS	77	Standard query 0x6aa1 A fonts.gstatic.com
54	00:38:41.908906	192.168.1.161	192.168.1.1	DNS	73	Standard query 0x6085 A id.google.com
55	00:38:41.909176	192.168.1.161	192.168.1.1	DNS	85	Standard query 0x3ef0 A lh3.googleusercontent.com

User Datagram Protocol, Src Port: 50300, Dst Port: 53	
Source Port:	50300
Destination Port:	53
Length:	41
Checksum:	0x4865 [unverified]
[Checksum Status:	Unverified]
[Stream index:	0]
Domain Name System (query)	

Offset	Hex	ASCII
0000	48 5d 36 f1 47 66 4c 32 75 9c a6 65 08 00 45 00	H)6.GfL2 u...E.
0010	00 3d 73 39 00 00 40 11 83 84 c0 a8 01 a1 c0 a8	..s9..@. ....
0020	01 01 c4 7c 00 35 00 29 48 65 cd b3 01 00 00 01	...[.5.] He.....
0030	00 00 00 00 00 00 04 61 70 69 73 06 67 6f 6f 67	.....a pis.goog
0040	6c 65 03 63 6f 6d 00 00 01 00 01	le.com.. ...

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.

Ans) The value in the length field = 8 bytes(sum of header field lengths) + 33 bytes(data encapsulated in packets.) = 41 bytes

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)

Ans)  $2^{16} - 1 - 8(\text{sum of header field lengths}) = 65536 - 1 - 8 = 65527$  is the maximum number of bytes that can be included in a UDP payload.

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

Ans)  $2^{16} - 1 = 65536 - 1 = 65535$  is the largest possible source port number.

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).

Ans) 11 Hex and 17 decimal is the protocol number for UDP.

The image shows a Wireshark interface with a packet list on the left and a packet details pane on the right. The packet list shows several packets, with packet 61 selected. The packet details pane shows the structure of the selected packet, which is a User Datagram Protocol (UDP) segment. The 'Protocol' field is highlighted with a red circle and shows 'UDP (17)'. Below this, the 'User Datagram Protocol' section shows the source and destination ports: Source Port: 47697, Destination Port: 53. The packet bytes pane at the bottom shows the raw data of the packet, with the first few bytes highlighted in red.

No.	Time	Source	Destination	Protocol	Length	Info
1	22:45:05.483176	192.168.1.157	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
12	22:45:06.608422	192.168.1.157	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
13	22:45:06.610050	fe80::853:21fb:3d3...	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
36	22:45:09.067953	192.168.1.162	239.255.255.250	SSDP	318	NOTIFY * HTTP/1.1
61	22:45:12.973982	192.168.1.161	192.168.1.1	DNS	77	Standard query 0xa0a2 A as.eu.angsrvr.com
95	22:45:12.993444	192.168.1.1	192.168.1.161	DNS	270	Standard query response 0xa0a2 A as.eu.angsrvr.com CNAME lb-adselect-big-11
161	22:45:13.983277	192.168.1.162	239.255.255.250	SSDP	318	NOTIFY * HTTP/1.1

Identification: 0xcc7b (52347)

Flags: 0x00

Fragment offset: 0

Time to live: 64

**Protocol: UDP (17)**

Header checksum: 0x2a40 [validation disabled]  
[Header checksum status: Unverified]

Source: 192.168.1.161  
Destination: 192.168.1.1  
[Source GeoIP: Unknown]  
[Destination GeoIP: Unknown]

▼ User Datagram Protocol, Src Port: 47697, Dst Port: 53

Source Port: 47697  
Destination Port: 53  
Length: 43

0000 48 5d 36 f1 47 66 4c 32 75 9c a6 65 08 00 45 00 H]6.Gfl2 u..e..E.  
0010 00 3f cc 7b 00 00 40 11 2a 40 c0 a8 01 a1 c0 a8 .?.{..@.\*@.....  
0020 01 01 ba 51 00 35 00 2b 70 24 a0 a2 01 00 00 01 ...Q.5.+ p\$.....  
0030 00 00 00 00 00 02 61 73 02 65 75 07 61 6e 67 .....a s.eu.ang  
0040 73 72 76 72 03 63 6f 6d 00 00 01 00 01 srvr.com .....

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.

Ans) Host UDP packet source port = Reply packet UDP packet destination port  
and vice-versa Host UDP packet destination port = Reply packet UDP packet source port

Wireshark packet capture analysis showing a list of network packets and a detailed view of a User Datagram Protocol (UDP) packet.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
49	00:38:41.908107	192.168.1.161	52.71.156.78	TCP	66	54193 → 443 [FIN, ACK] Seq=1 Ack=1 Win=4096 Len=0 TSval=956518937 TSecr=136
50	00:38:41.908187	192.168.1.161	104.16.80.53	TCP	54	54202 → 80 [FIN, ACK] Seq=1 Ack=1 Win=8192 Len=0
51	00:38:41.908423	192.168.1.161	192.168.1.1	DNS	75	Standard query 0xcdb3 A apis.google.com
52	00:38:41.908595	192.168.1.161	192.168.1.1	DNS	79	Standard query 0x599f A clients5.google.com
53	00:38:41.908769	192.168.1.161	192.168.1.1	DNS	77	Standard query 0x6aa1 A fonts.gstatic.com
54	00:38:41.908906	192.168.1.161	192.168.1.1	DNS	73	Standard query 0x6085 A id.google.com
55	00:38:41.909176	192.168.1.161	192.168.1.1	DNS	85	Standard query 0x3ef0 A lh3.googleusercontent.com

**Packet Details:**

- Frame 51: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
- Ethernet II, Src: Apple\_9c:a6:65 (4c:32:75:9c:a6:65), Dst: Verizon\_f1:47:66 (48:5d:36:f1:47:66)
- Internet Protocol Version 4, Src: 192.168.1.161, Dst: 192.168.1.1
- User Datagram Protocol, Src Port: 50300, Dst Port: 53**
  - Source Port: 50300
  - Destination Port: 53
  - Length: 41
  - Checksum: 0x4865 [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 0]
  - Domain Name System (query)

**Packet Bytes:**

Offset	Hex	ASCII
0000	48 5d 36 f1 47 66 4c 32 75 9c a6 65 08 00 45 00	H]6.GfL2 u...E.
0010	00 3d 73 39 00 00 40 11 83 84 c0 a8 01 a1 c0 a8	..s9..@. ....
0020	01 01 c4 7c 00 35 00 29 48 65 cd b3 01 00 00 01	... .5.) He.....
0030	00 00 00 00 00 00 04 61 70 69 73 06 67 6f 6f 67	.....a pi\$goog
0040	6c 65 03 63 6f 6d 00 00 01 00 01	le.com.. ...