

UDP

No.	Source	Destination	Protocol	Length	Info
38	10.1.40.31	10.4.20.204	DNS	76	Standard query 0xacbd A proxy.iiit.ac.in
39	10.1.40.31	10.4.20.204	DNS	76	Standard query 0xdcef AAAA proxy.iiit.ac.in
40	10.4.20.204	10.1.40.31	DNS	160	Standard query response 0xacbd A proxy.iiit.ac.in A 10.4.2
41	10.4.20.204	10.1.40.31	DNS	132	Standard query response 0xdcef AAAA proxy.iiit.ac.in SOA n
83	10.1.40.31	10.4.20.204	DNS	76	Standard query 0x90ab A proxy.iiit.ac.in
84	10.1.40.31	10.4.20.204	DNS	76	Standard query 0x3675 AAAA proxy.iiit.ac.in
▶ Frame 38: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0					
▶ Ethernet II, Src: HewlettP_17:85:a8 (70:5a:0f:17:85:a8), Dst: Cisco_76:47:49 (64:00:f1:76:47:49)					
▶ Internet Protocol Version 4, Src: 10.1.40.31, Dst: 10.4.20.204					
▼ User Datagram Protocol, Src Port: 42374, Dst Port: 53					
Source Port: 42374					
Destination Port: 53					
Length: 42					
▶ checksum: 0xb733 [correct]					
[checksum Status: Good]					
[Stream index: 9]					
▶ Domain Name System (query)					

Figure 1: UDP Header Fields

1. Select one packet. From this packet, determine how many fields are there in the UDP header. Name these fields.

Answer : UDP header contains 4 fields:

- Source port
- Destination port
- Length
- Checksum

2. The value in the length field is the length of what? Verify your claim with the captured UDP packet.

Answer : The value in the length field is the sum of the 8 header bytes, plus the 34 encapsulated data bytes.

3. Observe the source address. Verify that the source address is your IP address.

Answer : The source address is 10.1.40.31 which is same as my IP address.

```
kunal@hp:~/Documents/Networks/Wireshark-Lab$ ifconfig
eno1      Link encap:Ethernet  HWaddr 70:5a:0f:17:85:a8
          inet addr:10.1.40.31  Bcast:10.1.40.255  Mask:255.255.255.0
          inet6 addr: fe80::2b8c:57e:ab6f:b8ac/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:70935 errors:0 dropped:0 overruns:0 frame:0
          TX packets:41543 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:50214534 (50.2 MB)  TX bytes:16826495 (16.8 MB)
```

Figure 2: My IP address using ifconfig

4. Observe the destination address.

Answer : The destination address is 10.4.20.204

5. What is the maximum number of bytes that can be included in a UDP payload?

Answer : The maximum number of bytes that can be included in a UDP payload is $2^{16} - 1$ less the header bytes. This gives $65535 - 8 = 65527$ bytes..

6. What is the largest possible port number?

Answer : The largest possible source port number is $2^{16} - 1 = 65535$.

7. What is the protocol number for UDP?

Answer : The IP protocol number for UDP is 0x11 hex, which is 17 in decimal value.

No.	Source	Destination	Protocol	Length	Info
38	10.1.40.31	10.4.20.204	DNS	76	Standard query 0xacbd A proxy.iiit.ac.in
39	10.1.40.31	10.4.20.204	DNS	76	Standard query 0xdcef AAAA proxy.iiit.ac.in
40	10.4.20.204	10.1.40.31	DNS	160	Standard query response 0xacbd A proxy.iiit.ac
41	10.4.20.204	10.1.40.31	DNS	132	Standard query response 0xdcef AAAA proxy.iiit
▶ Frame 38: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0					
▶ Ethernet II, Src: HewlettP_17:85:a8 (70:5a:0f:17:85:a8), Dst: Cisco_76:47:49 (64:00:f1:76:47:49)					
▼ Internet Protocol Version 4, Src: 10.1.40.31, Dst: 10.4.20.204					
0100 = Version: 4					
.... 0101 = Header Length: 20 bytes (5)					
▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)					
Total Length: 62					
Identification: 0xa199 (41369)					
▶ Flags: 0x02 (Don't Fragment)					
Fragment offset: 0					
Time to live: 64					
Protocol: UDP (17)					
Header checksum: 0x4826 [validation disabled]					
[Header checksum status: Unverified]					
Source: 10.1.40.31					
Destination: 10.4.20.204					
[Source GeoIP: Unknown]					
[Destination GeoIP: Unknown]					
▶ User Datagram Protocol, Src Port: 42374, Dst Port: 53					

Figure 3: Protocol number of UDP

8. Search “UDP” on google and determine the fields on which the UDP checksum is calculated.

Answer : The UDP checksum is calculated as the 16-bit one's complement of the one's complement sum of a pseudo header of information from the IP header, the UDP header, and the data. This is padded as needed with zero bytes at the end to make a multiple of two bytes. If the checksum is computed to be 0, it must be set to 0xFFFF.

9. Examine a pair of UDP packets in which the first packet is sent by your host and the second packet is a reply to the first packet. Describe the relationship between the port numbers in the two packets.

No.	Source	Destination	Protocol	Length	Info
38	10.1.40.31	10.4.20.204	DNS	76	Standard query 0xacbd A proxy.iiit.ac.in
39	10.1.40.31	10.4.20.204	DNS	76	Standard query 0xdcef AAAA proxy.iiit.ac.in
40	10.4.20.204	10.1.40.31	DNS	160	Standard query response 0xacbd A proxy.iiit.ac.in A 10.4.20.10
41	10.4.20.204	10.1.40.31	DNS	132	Standard query response 0xdcef AAAA proxy.iiit.ac.in SOA ns3.i
▶ Frame 38: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0					
▶ Ethernet II, Src: HewlettP_17:85:a8 (70:5a:0f:17:85:a8), Dst: Cisco_76:47:49 (64:00:f1:76:47:49)					
▶ Internet Protocol Version 4, Src: 10.1.40.31, Dst: 10.4.20.204					
▼ User Datagram Protocol, Src Port: 42374, Dst Port: 53					
Source Port: 42374					
Destination Port: 53					
Length: 42					
▶ Checksum: 0xb733 [correct]					
[Checksum status: good]					
0000	64 00 f1 76 47 49 70 5a 0f 17 85 a8 08 00 45 00	d..vGIpZE.			
0010	00 3e a1 99 40 00 40 11 48 26 0a 01 28 1f 0a 04	.>...@.@. H&..(...			
0020	14 cc a5 80 00 35 00 2a b7 33 ac bd 01 00 00 01	...5.*.3.....			
0030	00 00 00 00 00 00 05 70 72 6f 78 79 04 69 69 69p roxy.iii			
0040	74 02 61 63 02 69 6e 00 00 01 00 01	t.ac.in.			

Figure 4: UDP sent by my host

No.	Source	Destination	Protocol	Length	Info
38	10.1.40.31	10.4.20.204	DNS	76	Standard query 0xacbd A proxy.iiit.ac.in
39	10.1.40.31	10.4.20.204	DNS	76	Standard query 0xdcef AAAA proxy.iiit.ac.in
40	10.4.20.204	10.1.40.31	DNS	160	Standard query response 0xacbd A proxy.iiit.ac.in A 10.4.
41	10.4.20.204	10.1.40.31	DNS	132	Standard query response 0xdcef AAAA proxy.iiit.ac.in SOA
▶ Frame 40: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface 0 ▶ Ethernet II, Src: Cisco_76:47:49 (64:00:f1:76:47:49), Dst: HewlettP_17:85:a8 (70:5a:0f:17:85:a8) ▶ Internet Protocol Version 4, Src: 10.4.20.204, Dst: 10.1.40.31 ▼ User Datagram Protocol, Src Port: 53, Dst Port: 42374 Source Port: 53 Destination Port: 42374 Length: 126 ▶ Checksum: 0x1013 [correct] [checksum status: Good]					
0000	70 5a 0f 17 85 a8 64 00	f1 76 47 49 08 00 45 00	pZ...d. .vGI..E.		
0010	00 92 e2 c2 00 00 3e 11	48 a9 0a 04 14 cc 0a 01>. H.....		
0020	28 1f 00 35 a5 86 00 7e	10 13 ac bd 85 80 00 01	(..5..~		
0030	00 01 00 02 00 02 05 70	72 6f 78 79 04 69 69 69p roxy.iii		
0040	74 a2 61 63 a2 6a 6a 00	00 01 00 01 c0 ac 00 01	t ac in		

Figure 5: UDP reply to my host

Answer : 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.