

### Step3:

Wi-Fi: en0 (udp)

Apply a display filter ... <=>

No.	Time	Source	Destination	Protocol	Length	Info
6	1.401444	172.217.5.110	192.168.0.10	UDP	303	https(443) → 52307 Len=261
7	1.401875	172.217.5.110	192.168.0.10	UDP	83	https(443) → 52307 Len=41
8	1.409225	192.168.0.10	172.217.5.110	UDP	71	52307 → https(443) Len=29
9	5.213059	192.168.0.10	75.75.75.75	DNS	123	Standard query 0xbbf2 A science-edge-external-prod-73889260.us-west-2.elb
10	5.227699	75.75.75.75	192.168.0.10	DNS	251	Standard query response 0xbbf2 A science-edge-external-prod-73889260.us-w
11	5.419902	192.168.0.10	75.75.75.75	DNS	74	Standard query 0x3273 A api.placed.com
12	5.432608	75.75.75.75	192.168.0.10	DNS	244	Standard query response 0x3273 A api.placed.com CNAME server-api-prod-placed-2-

▶ Frame 9: 123 bytes on wire (984 bits), 123 bytes captured (984 bits)

▶ Ethernet II, Src: Apple\_9a:80:a3 (f4:5c:89:9a:80:a3), Dst: Motorola\_ff:d7:40 (88:b4:a6:ff:d7:40)

▶ Internet Protocol Version 4, Src: 192.168.0.10, Dst: 75.75.75.75

▼ User Datagram Protocol, Src Port: 57367 (57367), Dst Port: domain (53)

Source Port: 57367 (57367)

Destination Port: domain (53)

Length: 89

Checksum: 0xe327 [unverified]

[Checksum Status: Unverified]

[Stream index: 1]

▶ [Timestamps]

▶ Domain Name System (query)

0000 88 b4 a6 ff d7 40 f4 5c 89 9a 80 a3 08 00 45 00 .....@.....E.  
0010 00 6d 5a 77 00 00 ff 11 09 c0 c0 a8 00 0a 4b 4b ..mZW.....-KK  
0020 4b 4b e0 17 00 35 00 59 e3 27 bb f2 01 00 00 01 KK...S-Y.....  
0030 00 00 00 00 00 00 23 73 63 69 65 6e 63 65 2d 65 .....#s cience-e  
0040 64 67 65 2d 65 78 74 65 72 6e 61 6c 2d 70 72 6f dge--exte rnal-pro  
0050 64 2d 37 33 38 38 39 32 36 30 09 75 73 2d 77 65 d-738892 60 us-we  
0060 73 74 2d 32 03 65 6c 62 09 61 6d 61 7a 6f 6e 61 st-2-elb .amazona  
0070 77 73 03 63 6f 6d 00 00 01 00 01 ws.com...

Length (udp.length), 2 bytes

Packets: 38 · Displayed: 38 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

1. What does the Length field include? The UDP payload, UDP payload and UDP header, or UDP payload, UDP header, and lower layer headers?

UDP payload and UDP header

2. How long in bits is the UDP checksum?

16bits

3. How long in bytes is the entire UDP header?

8bytes

### Step4:

1. Give the value of the IP Protocol field that identifies the upper layer protocol as UDP.

No.	Time	Source	Destination	Protocol	Length	Info
8	1.409225	192.168.0.10	172.217.5.110	UDP	71	5230/ → https(443) Len=29
9	5.213059	192.168.0.10	75.75.75.75	DNS	123	Standard query 0xbbf2 A science-edge-external-prod-73889260.us-west-2.e
10	5.227699	75.75.75.75	192.168.0.10	DNS	251	Standard query response 0xbbf2 A science-edge-external-prod-73889260.us
11	5.419902	192.168.0.10	75.75.75.75	DNS	74	Standard query 0x3273 A api.placed.com
12	5.432608	75.75.75.75	192.168.0.10	DNS	244	Standard query response 0x3273 A api.placed.com CNAME server-api-prod-p
13	5.574065	192.168.0.10	75.75.75.75	DNS	72	Standard query 0xc8d7 A p.placed.com
14	5.587011	75.75.75.75	192.168.0.10	DNS	230	Standard query response 0xc8d7 A p.placed.com CNAME pixel-prod-2-162693
15	5.953637	192.168.0.10	75.75.75.75	DNS	78	Standard query 0xaf80 A tanestry.tanad.com

▶ Frame 9: 123 bytes on wire (984 bits), 123 bytes captured (984 bits)  
 ▶ Ethernet II, Src: Apple\_9a:80:a3 (f4:5c:89:9a:80:a3), Dst: Motorola\_ff:d7:40 (88:b4:a6:ff:d7:40)  
 ▼ Internet Protocol Version 4, Src: 192.168.0.10, Dst: 75.75.75.75  
     0100 .... = Version: 4  
     .... 0101 = Header Length: 20 bytes (5)  
     ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
         Total Length: 109  
         Identification: 0x5a77 (23159)  
     ▶ Flags: 0x0000  
         Time to live: 255  
     Protocol: UDP (17)  
     Header checksum: 0x09c0 [validation disabled]  
     [Header checksum status: Unverified]  
     Source: 192.168.0.10  
     Destination: 75.75.75.75  
 ▼ User Datagram Protocol, Src Port: 57367 (57367), Dst Port: domain (53)  
     Source Port: 57367 (57367)  
     Destination Port: domain (53)  
     Length: 89  
     Checksum: 0xe377 [unverified]

0000	88 b4 a6 ff d7 40 f4 5c	89 9a 80 a3 08 00 45 00	.....@.\.....E.
0010	00 6d 5a 77 00 00 ff 11	09 c0 c0 a8 00 0a 4b 4b	..mZw.....KK
0020	4b 4b e0 17 00 35 00 59	e3 27 bb f2 01 00 00 01	KK.....5.Y.....
0030	00 00 00 00 00 00 23 73	63 69 65 6e 63 65 2d 65	.....#s cience-e
0040	64 67 65 2d 65 78 74 65	72 6e 61 6c 2d 70 72 6f	dge-exte rnal-pro
0050	64 2d 37 33 38 38 39 32	36 30 09 75 73 2d 77 65	d-738892 60.us-we
0060	73 74 2d 32 03 65 6c 62	09 61 6d 61 7a 6f 6e 61	st-2.elb .amazona
0070	77 73 03 63 6f 6d 00 00	01 00 01	ws.com... ..

2. Examine the UDP messages and give the destination IP addresses that are used when your computer is neither the source IP address nor the destination IP address. (If you have only your computer as the source or destination IP address then you may use the supplied trace.)

```

more command is one of: name, getifaddr, ifconfig, ifdown, ifup, getoption, getpacket, getvpacket, ...
~$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
    inet 127.0.0.1 netmask 0xff000000
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
    nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
XHC20: flags=0<> mtu 0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether f4:5c:89:9a:80:a3
    inet 192.168.0.10 netmask 0xfffff00 broadcast 192.168.0.255
    media: autoselect
    status: active
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
    options=400<CHANNEL_IO>
    ether 06:5c:89:9a:80:a3
    media: autoselect
    status: inactive
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1484
    options=400<CHANNEL_IO>
    ether 06:ea:87:75:33:21
    inet6 fe80::4ea:87ff:fe75:3321%awdl0 prefixlen 64 scopeid 0x7
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active
llw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 06:ea:87:75:33:21
    inet6 fe80::4ea:87ff:fe75:3321%llw0 prefixlen 64 scopeid 0x8
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    options=460<TS04,TS06,CHANNEL_IO>
    ether 82:13:12:68:f3:80
    media: autoselect <full-duplex>
    status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    options=460<TS04,TS06,CHANNEL_IO>
    ether 82:13:12:68:f3:81
    media: autoselect <full-duplex>

```

3. What is the typical size of UDP messages in your trace?

Below 200bytes