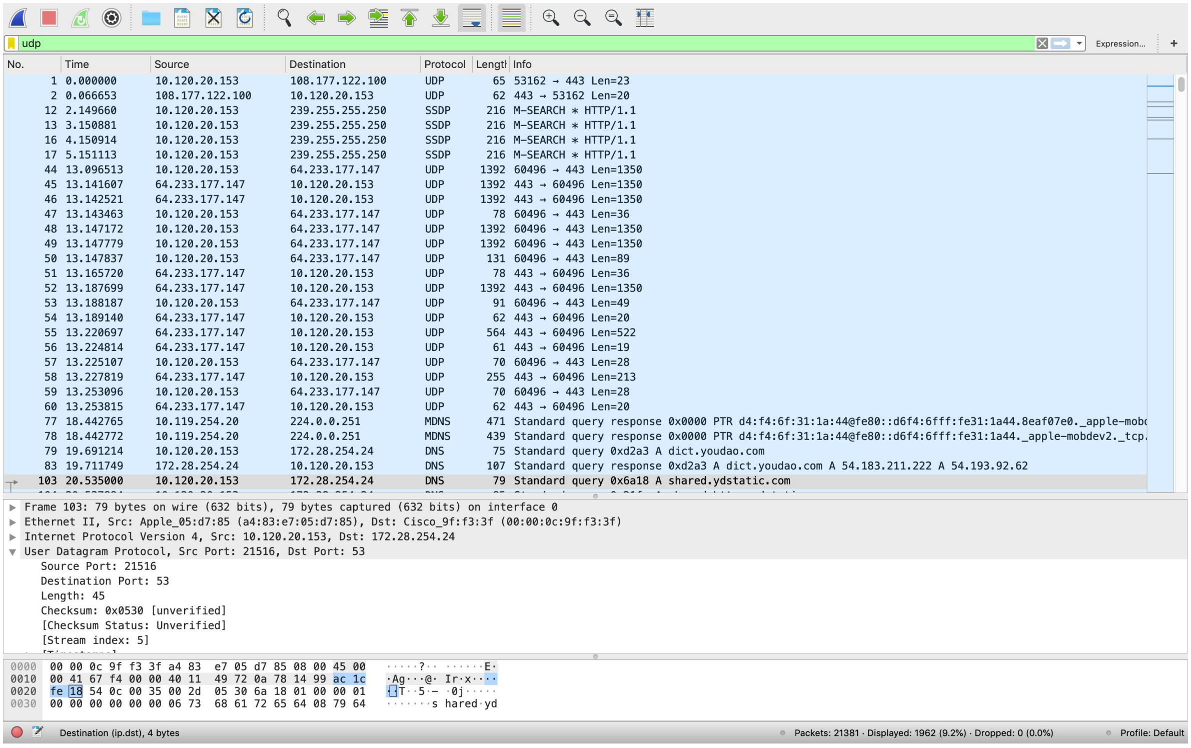
Lab3 – Yuanjie Yue 10/17/2019

Step 1. Capture a trace

1) Set up the filter to be udp, then start browsing some web sites that I have not visited for a long time.

2) Here is the scree shot, I have captured a bunch of packets under different protocols, like UDP, DNS.



```
No.  Time       Source          Destination      Protocol Lengtl Info
   1 0.000000   10.120.20.153   108.177.122.100  UDP        65 53162 → 443 Len=23
   2 0.066653   108.177.122.100 10.120.20.153    UDP        62 443 → 53162 Len=20
  12 2.149660   10.120.20.153   239.255.255.250  SSDP      216 M-SEARCH * HTTP/1.1
  13 3.150881   10.120.20.153   239.255.255.250  SSDP      216 M-SEARCH * HTTP/1.1
  16 4.150914   10.120.20.153   239.255.255.250  SSDP      216 M-SEARCH * HTTP/1.1
  17 5.151113   10.120.20.153   239.255.255.250  SSDP      216 M-SEARCH * HTTP/1.1
  44 13.096513  10.120.20.153   64.233.177.147   UDP      1392 60496 → 443 Len=1350
  45 13.141607  64.233.177.147  10.120.20.153    UDP      1392 443 → 60496 Len=1350
  46 13.142521  64.233.177.147  10.120.20.153    UDP      1392 443 → 60496 Len=1350
  47 13.143463  10.120.20.153   64.233.177.147   UDP        78 60496 → 443 Len=36
  48 13.147172  10.120.20.153   64.233.177.147   UDP      1392 60496 → 443 Len=1350
  49 13.147779  10.120.20.153   64.233.177.147   UDP      1392 60496 → 443 Len=1350
  50 13.147837  10.120.20.153   64.233.177.147   UDP       131 60496 → 443 Len=89
  51 13.165720  64.233.177.147  10.120.20.153    UDP        78 443 → 60496 Len=36
  52 13.187699  64.233.177.147  10.120.20.153    UDP      1392 443 → 60496 Len=1350
  53 13.188187  10.120.20.153   64.233.177.147   UDP        91 60496 → 443 Len=49
  54 13.189140  64.233.177.147  10.120.20.153    UDP        62 443 → 60496 Len=20
  55 13.220697  64.233.177.147  10.120.20.153    UDP       564 443 → 60496 Len=522
  56 13.224814  64.233.177.147  10.120.20.153    UDP        61 443 → 60496 Len=19
  57 13.225107  10.120.20.153   64.233.177.147   UDP        70 60496 → 443 Len=28
  58 13.227819  64.233.177.147  10.120.20.153    UDP       255 443 → 60496 Len=213
  59 13.253096  10.120.20.153   64.233.177.147   UDP        70 60496 → 443 Len=28
  60 13.253815  64.233.177.147  10.120.20.153    UDP        62 443 → 60496 Len=20
  77 18.442765  10.119.254.20   224.0.0.251      MDNS      471 Standard query response 0x0000 PTR d4:f4:6f:31:1a:44@fe80::d6f4:6fff:fe31:1a44.8eaf07e0._apple-mobd
  78 18.442772  10.119.254.20   224.0.0.251      MDNS      439 Standard query response 0x0000 PTR d4:f4:6f:31:1a:44@fe80::d6f4:6fff:fe31:1a44._apple-mobdev2._tcp.
  79 19.691214  10.120.20.153   172.28.254.24    DNS        75 Standard query 0xd2a3 A dict.youdao.com
  83 19.711749  172.28.254.24   10.120.20.153    DNS       107 Standard query response 0xd2a3 A dict.youdao.com A 54.183.211.222 A 54.193.92.62
 103 20.535000  10.120.20.153   172.28.254.24    DNS        79 Standard query 0x6a18 A shared.ydstatic.com
```

```
▶ Frame 103: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
▶ Ethernet II, Src: Apple_05:d7:85 (a4:83:e7:05:d7:85), Dst: Cisco_9f:f3:3f (00:00:0c:9f:f3:3f)
▶ Internet Protocol Version 4, Src: 10.120.20.153, Dst: 172.28.254.24
▼ User Datagram Protocol, Src Port: 21516, Dst Port: 53
    Source Port: 21516
    Destination Port: 53
    Length: 45
    Checksum: 0x0530 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
```

```
0000  00 00 0c 9f f3 3f a4 83  e7 05 d7 85 08 00 45 00   ·····?·· ······E·
0010  00 41 67 f4 00 00 40 11  49 72 0a 78 14 99 ac 1c   ·Ag···@· Ir·x····
0020  fe 18 54 0c 00 35 00 2d  05 30 6a 18 01 00 00 01   ··T··5·– ·0j·····
0030  00 00 00 00 00 00 06 73  68 61 72 65 64 08 79 64   ·······s hared·yd
```

Destination (ip.dst), 4 bytes   Packets: 21381 · Displayed: 1962 (9.2%) · Dropped: 0 (0.0%)   Profile: Default

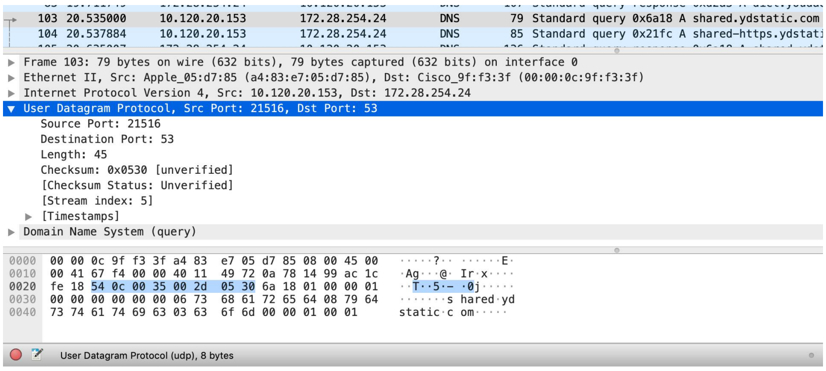
Step 2 & 3. Inspect the Trace and UDP Message Structure

By looking at the details of the UDP messages in your trace, answer these questions:

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

It includes UDP payload and UDP header.

As we could see, in this case, Length is 45, it equals the header length (8bytes) plus payload length (37bytes).

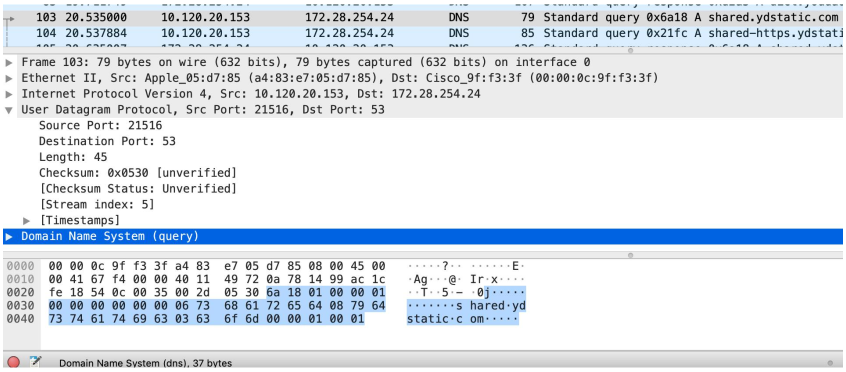


```
 103 20.535000  10.120.20.153   172.28.254.24    DNS        79 Standard query 0x6a18 A shared.ydstatic.com
 104 20.537884  10.120.20.153   172.28.254.24    DNS        85 Standard query 0x21fc A shared-https.ydstati
```

```
▶ Frame 103: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
▶ Ethernet II, Src: Apple_05:d7:85 (a4:83:e7:05:d7:85), Dst: Cisco_9f:f3:3f (00:00:0c:9f:f3:3f)
▶ Internet Protocol Version 4, Src: 10.120.20.153, Dst: 172.28.254.24
▼ User Datagram Protocol, Src Port: 21516, Dst Port: 53
    Source Port: 21516
    Destination Port: 53
    Length: 45
    Checksum: 0x0530 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
  ▶ [Timestamps]
▶ Domain Name System (query)
```

```
0000  00 00 0c 9f f3 3f a4 83  e7 05 d7 85 08 00 45 00   ·····?·· ······E·
0010  00 41 67 f4 00 00 40 11  49 72 0a 78 14 99 ac 1c   ·Ag···@· Ir·x····
0020  fe 18 54 0c 00 35 00 2d  05 30 6a 18 01 00 00 01   ··T··5·– ·0j·····
0030  00 00 00 00 00 00 06 73  68 61 72 65 64 08 79 64   ·······s hared·yd
0040  73 74 61 74 69 63 03 63  6f 6d 00 00 01 00 01      static·c om·····
```

User Datagram Protocol (udp), 8 bytes



```
 103 20.535000  10.120.20.153   172.28.254.24    DNS        79 Standard query 0x6a18 A shared.ydstatic.com
 104 20.537884  10.120.20.153   172.28.254.24    DNS        85 Standard query 0x21fc A shared-https.ydstati
```

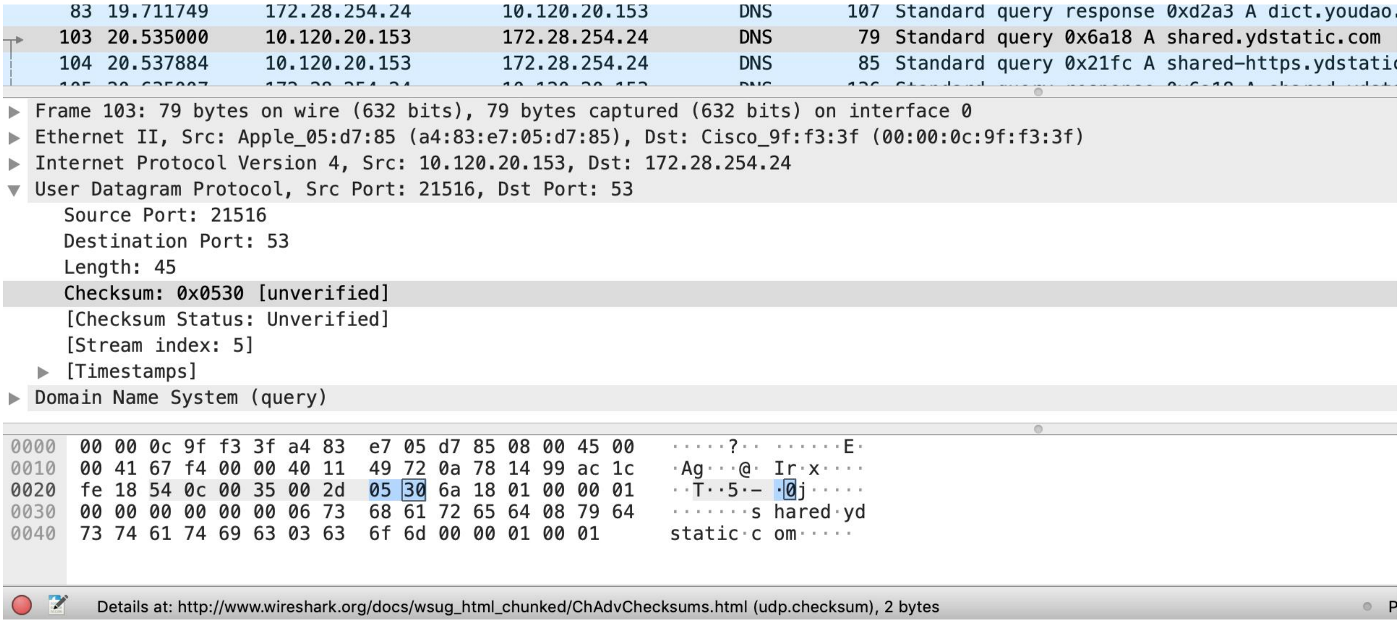
```
▶ Frame 103: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
▶ Ethernet II, Src: Apple_05:d7:85 (a4:83:e7:05:d7:85), Dst: Cisco_9f:f3:3f (00:00:0c:9f:f3:3f)
▶ Internet Protocol Version 4, Src: 10.120.20.153, Dst: 172.28.254.24
▼ User Datagram Protocol, Src Port: 21516, Dst Port: 53
    Source Port: 21516
    Destination Port: 53
    Length: 45
    Checksum: 0x0530 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
  ▶ [Timestamps]
▶ Domain Name System (query)
```

```
0000  00 00 0c 9f f3 3f a4 83  e7 05 d7 85 08 00 45 00   ·····?·· ······E·
0010  00 41 67 f4 00 00 40 11  49 72 0a 78 14 99 ac 1c   ·Ag···@· Ir·x····
0020  fe 18 54 0c 00 35 00 2d  05 30 6a 18 01 00 00 01   ··T··5·– ·0j·····
0030  00 00 00 00 00 00 06 73  68 61 72 65 64 08 79 64   ·······s hared·yd
0040  73 74 61 74 69 63 03 63  6f 6d 00 00 01 00 01      static·c om·····
```

Domain Name System (dns), 37 bytes

2. How long in bits is the UDP checksum?

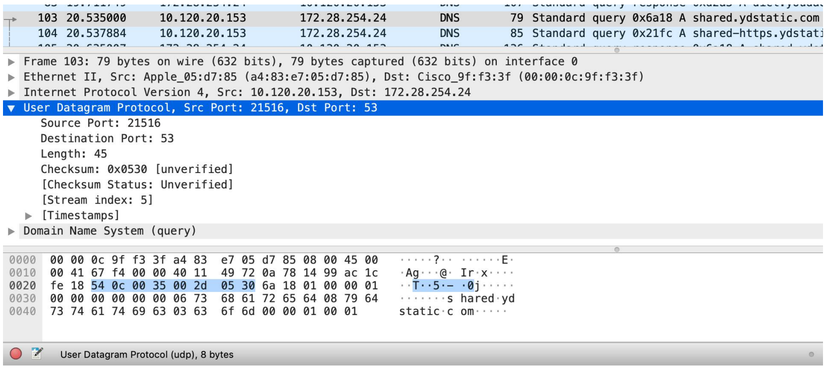
The checksum is 2 bytes, which is 16 bits long.



```
  83 19.711749    172.28.254.24     10.120.20.153     DNS     107 Standard query response 0xd2a3 A dict.youdao.
 103 20.535000    10.120.20.153     172.28.254.24     DNS      79 Standard query 0x6a18 A shared.ydstatic.com
 104 20.537884    10.120.20.153     172.28.254.24     DNS      85 Standard query 0x21fc A shared-https.ydstatic

▶ Frame 103: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
▶ Ethernet II, Src: Apple_05:d7:85 (a4:83:e7:05:d7:85), Dst: Cisco_9f:f3:3f (00:00:0c:9f:f3:3f)
▶ Internet Protocol Version 4, Src: 10.120.20.153, Dst: 172.28.254.24
▼ User Datagram Protocol, Src Port: 21516, Dst Port: 53
     Source Port: 21516
     Destination Port: 53
     Length: 45
     Checksum: 0x0530 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 5]
   ▶ [Timestamps]
▶ Domain Name System (query)

0000  00 00 0c 9f f3 3f a4 83  e7 05 d7 85 08 00 45 00   ·····?·· ······E·
0010  00 41 67 f4 00 00 40 11  49 72 0a 78 14 99 ac 1c   ·Ag···@· Ir·x····
0020  fe 18 54 0c 00 35 00 2d  05 30 6a 18 01 00 00 01   ··T··5·- ·0j·····
0030  00 00 00 00 00 00 06 73  68 61 72 65 64 08 79 64   ·······s hared·yd
0040  73 74 61 74 69 63 03 63  6f 6d 00 00 01 00 01      static·c om·····

Details at: http://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html (udp.checksum), 2 bytes
```

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

UDP header is 8 bytes.



```
 103 20.535000    10.120.20.153     172.28.254.24     DNS      79 Standard query 0x6a18 A shared.ydstatic.com
 104 20.537884    10.120.20.153     172.28.254.24     DNS      85 Standard query 0x21fc A shared-https.ydstati

▶ Frame 103: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
▶ Ethernet II, Src: Apple_05:d7:85 (a4:83:e7:05:d7:85), Dst: Cisco_9f:f3:3f (00:00:0c:9f:f3:3f)
▶ Internet Protocol Version 4, Src: 10.120.20.153, Dst: 172.28.254.24
▼ User Datagram Protocol, Src Port: 21516, Dst Port: 53
     Source Port: 21516
     Destination Port: 53
     Length: 45
     Checksum: 0x0530 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 5]
   ▶ [Timestamps]
▶ Domain Name System (query)

0000  00 00 0c 9f f3 3f a4 83  e7 05 d7 85 08 00 45 00   ·····?·· ······E·
0010  00 41 67 f4 00 00 40 11  49 72 0a 78 14 99 ac 1c   ·Ag···@· Ir·x····
0020  fe 18 54 0c 00 35 00 2d  05 30 6a 18 01 00 00 01   ··T··5·- ·0j·····
0030  00 00 00 00 00 00 06 73  68 61 72 65 64 08 79 64   ·······s hared·yd
0040  73 74 61 74 69 63 03 63  6f 6d 00 00 01 00 01      static·c om·····

User Datagram Protocol (udp), 8 bytes
```

Thus, we could see that the UDP Message Structure looks like this:

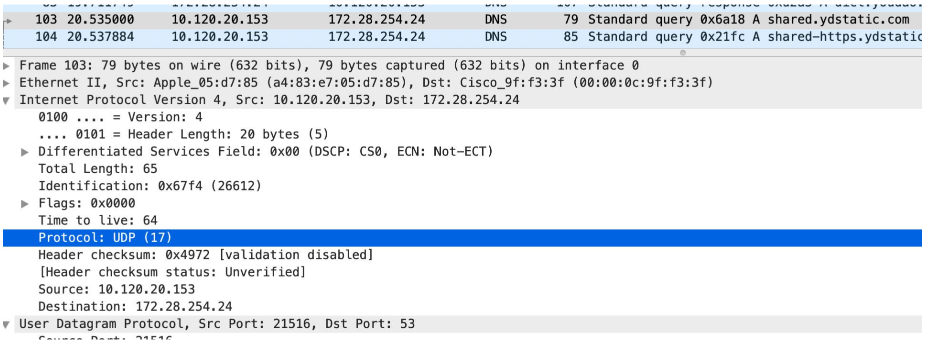
Source Port + Destination Port + Length + Checksum

2 bytes 2 bytes 2 bytes 2 bytes

Step 4. Usage of UDP

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

The value of the IP header field ‘Protocol’ is 17, it identifies its upper layer protocol is UDP.



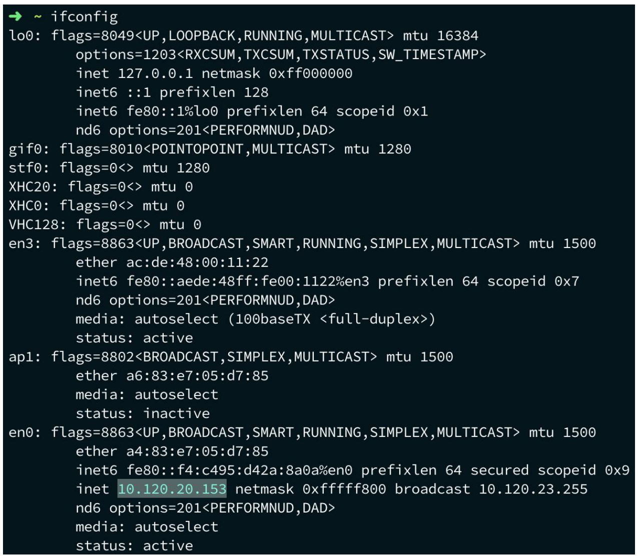
```
 103 20.535000    10.120.20.153     172.28.254.24     DNS      79 Standard query 0x6a18 A shared.ydstatic.com
 104 20.537884    10.120.20.153     172.28.254.24     DNS      85 Standard query 0x21fc A shared-https.ydstatic

▶ Frame 103: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
▶ Ethernet II, Src: Apple_05:d7:85 (a4:83:e7:05:d7:85), Dst: Cisco_9f:f3:3f (00:00:0c:9f:f3:3f)
▼ Internet Protocol Version 4, Src: 10.120.20.153, Dst: 172.28.254.24
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 65
     Identification: 0x67f4 (26612)
   ▶ Flags: 0x0000
     Time to live: 64
     Protocol: UDP (17)
     Header checksum: 0x4972 [validation disabled]
     [Header checksum status: Unverified]
     Source: 10.120.20.153
     Destination: 172.28.254.24
▼ User Datagram Protocol, Src Port: 21516, Dst Port: 53
```

2. Examine the UDP messages and give the destination IP addresses that are used when your computer is

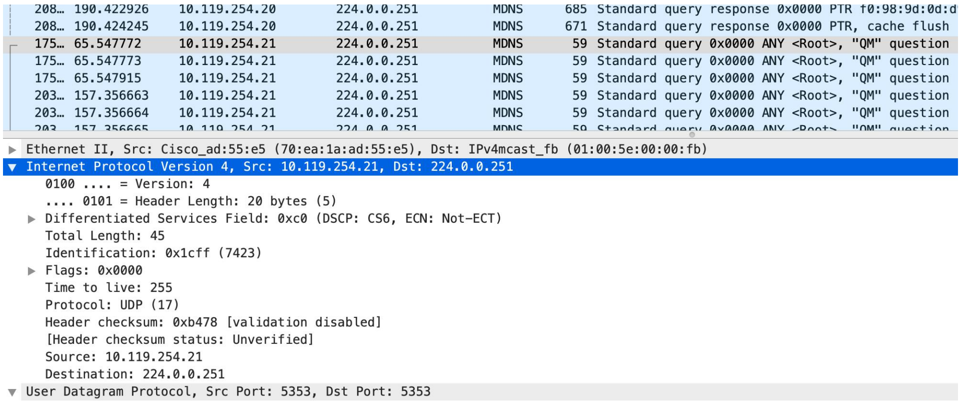
neither the source IP address nor the destination IP address. (If you have only your computer as the source or destination IP address then you may use the supplied trace.)

Use ifconfig command to find out my current ip, which is 10.120.20.153.

Sort the source ip in the wireshark console, one of the destination IP that is used is 224.0.0.251, which is for multicast DNS.



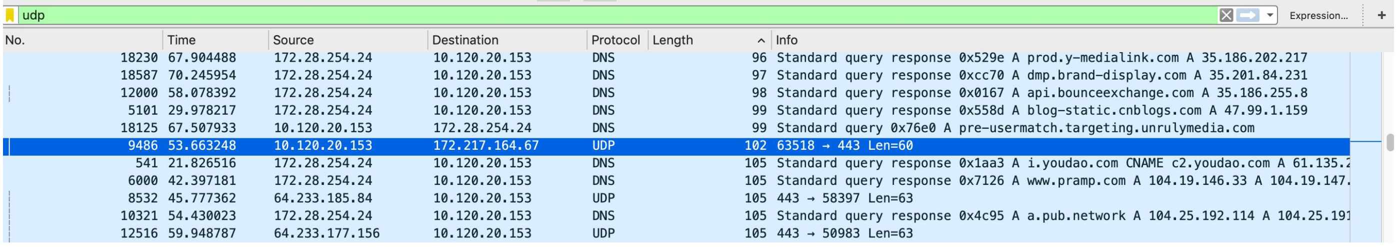
```
➜ ~ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
XHC20: flags=0<> mtu 0
XHC0: flags=0<> mtu 0
VHC128: flags=0<> mtu 0
en3: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether ac:de:48:00:11:22
        inet6 fe80::aede:48ff:fe00:1122%en3 prefixlen 64 scopeid 0x7
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (100baseTX <full-duplex>)
        status: active
ap1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> mtu 1500
        ether a6:83:e7:05:d7:85
        media: autoselect
        status: inactive
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether a4:83:e7:05:d7:85
        inet6 fe80::f4:c495:d42a:8a0a%en0 prefixlen 64 secured scopeid 0x9
        inet 10.120.20.153 netmask 0xfffff800 broadcast 10.120.23.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
```



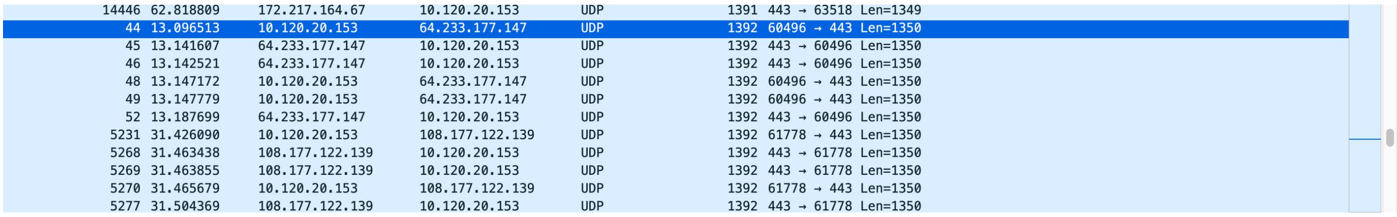
```
  208… 190.422926   10.119.254.20     224.0.0.251      MDNS    685 Standard query response 0x0000 PTR f0:98:9d:0d:d
  208… 190.424245   10.119.254.20     224.0.0.251      MDNS    671 Standard query response 0x0000 PTR, cache flush
  175… 65.547772    10.119.254.21     224.0.0.251      MDNS     59 Standard query 0x0000 ANY <Root>, "QM" question
  175… 65.547773    10.119.254.21     224.0.0.251      MDNS     59 Standard query 0x0000 ANY <Root>, "QM" question
  175… 65.547915    10.119.254.21     224.0.0.251      MDNS     59 Standard query 0x0000 ANY <Root>, "QM" question
  203… 157.356663   10.119.254.21     224.0.0.251      MDNS     59 Standard query 0x0000 ANY <Root>, "QM" question
  203… 157.356664   10.119.254.21     224.0.0.251      MDNS     59 Standard query 0x0000 ANY <Root>, "QM" question
  203… 157.356665   10.119.254.21     224.0.0.251      MDNS     59 Standard query 0x0000 ANY <Root>, "QM" question

▶ Ethernet II, Src: Cisco_ad:55:e5 (70:ea:1a:ad:55:e5), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
▼ Internet Protocol Version 4, Src: 10.119.254.21, Dst: 224.0.0.251
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 45
    Identification: 0x1cff (7423)
  ▶ Flags: 0x0000
    Time to live: 255
    Protocol: UDP (17)
    Header checksum: 0xb478 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.119.254.21
    Destination: 224.0.0.251
▼ User Datagram Protocol, Src Port: 5353, Dst Port: 5353
```

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

Sort the length of the packets in ascending order, we could easily see that, around half of all my 20 thousand packets have a length less 100. Besides, the other one third have a length equal to or more than 1392.



```
No.           Time        Source           Destination      Protocol Length  Info
        18230 67.904488   172.28.254.24    10.120.20.153    DNS          96  Standard query response 0x529e A prod.y-medialink.com A 35.186.202.217
        18587 70.245954   172.28.254.24    10.120.20.153    DNS          97  Standard query response 0xcc70 A dmp.brand-display.com A 35.201.84.231
        12000 58.078392   172.28.254.24    10.120.20.153    DNS          98  Standard query response 0x0167 A api.bounceexchange.com A 35.186.255.8
         5101 29.978217   172.28.254.24    10.120.20.153    DNS          99  Standard query response 0x558d A blog-static.cnblogs.com A 47.99.1.159
        18125 67.507933   10.120.20.153    172.28.254.24    DNS          99  Standard query 0x76e0 A pre-usermatch.targeting.unrulymedia.com
         9486 53.663248   10.120.20.153    172.217.164.67   UDP         102  63518 → 443 Len=60
          541 21.826516   172.28.254.24    10.120.20.153    DNS         105  Standard query response 0x1aa3 A i.youdao.com CNAME c2.youdao.com A 61.135.2
         6000 42.397181   172.28.254.24    10.120.20.153    DNS         105  Standard query response 0x7126 A www.pramp.com A 104.19.146.33 A 104.19.147.
         8532 45.777362   64.233.185.84    10.120.20.153    UDP         105  443 → 58397 Len=63
        10321 54.430023   172.28.254.24    10.120.20.153    DNS         105  Standard query response 0x4c95 A a.pub.network A 104.25.192.114 A 104.25.191
        12516 59.948787   64.233.177.156   10.120.20.153    UDP         105  443 → 50983 Len=63
```



```
        14446 62.818809   172.217.164.67   10.120.20.153    UDP        1391  443 → 63518 Len=1349
           44 13.096513   10.120.20.153    64.233.177.147   UDP        1392  60496 → 443 Len=1350
           45 13.141607   64.233.177.147   10.120.20.153    UDP        1392  443 → 60496 Len=1350
           46 13.142521   64.233.177.147   10.120.20.153    UDP        1392  443 → 60496 Len=1350
           48 13.147172   10.120.20.153    64.233.177.147   UDP        1392  60496 → 443 Len=1350
           49 13.147779   10.120.20.153    64.233.177.147   UDP        1392  60496 → 443 Len=1350
           52 13.187699   64.233.177.147   10.120.20.153    UDP        1392  443 → 60496 Len=1350
         5231 31.426090   10.120.20.153    108.177.122.139  UDP        1392  61778 → 443 Len=1350
         5268 31.463438   108.177.122.139  10.120.20.153    UDP        1392  443 → 61778 Len=1350
         5269 31.463855   108.177.122.139  10.120.20.153    UDP        1392  443 → 61778 Len=1350
         5270 31.465679   10.120.20.153    108.177.122.139  UDP        1392  61778 → 443 Len=1350
         5277 31.504369   108.177.122.139  10.120.20.153    UDP        1392  443 → 61778 Len=1350
```