Gamze AKYOL – 150140142 3.12.2017

BLG433E

COMPUTER COMMUNICATIONS

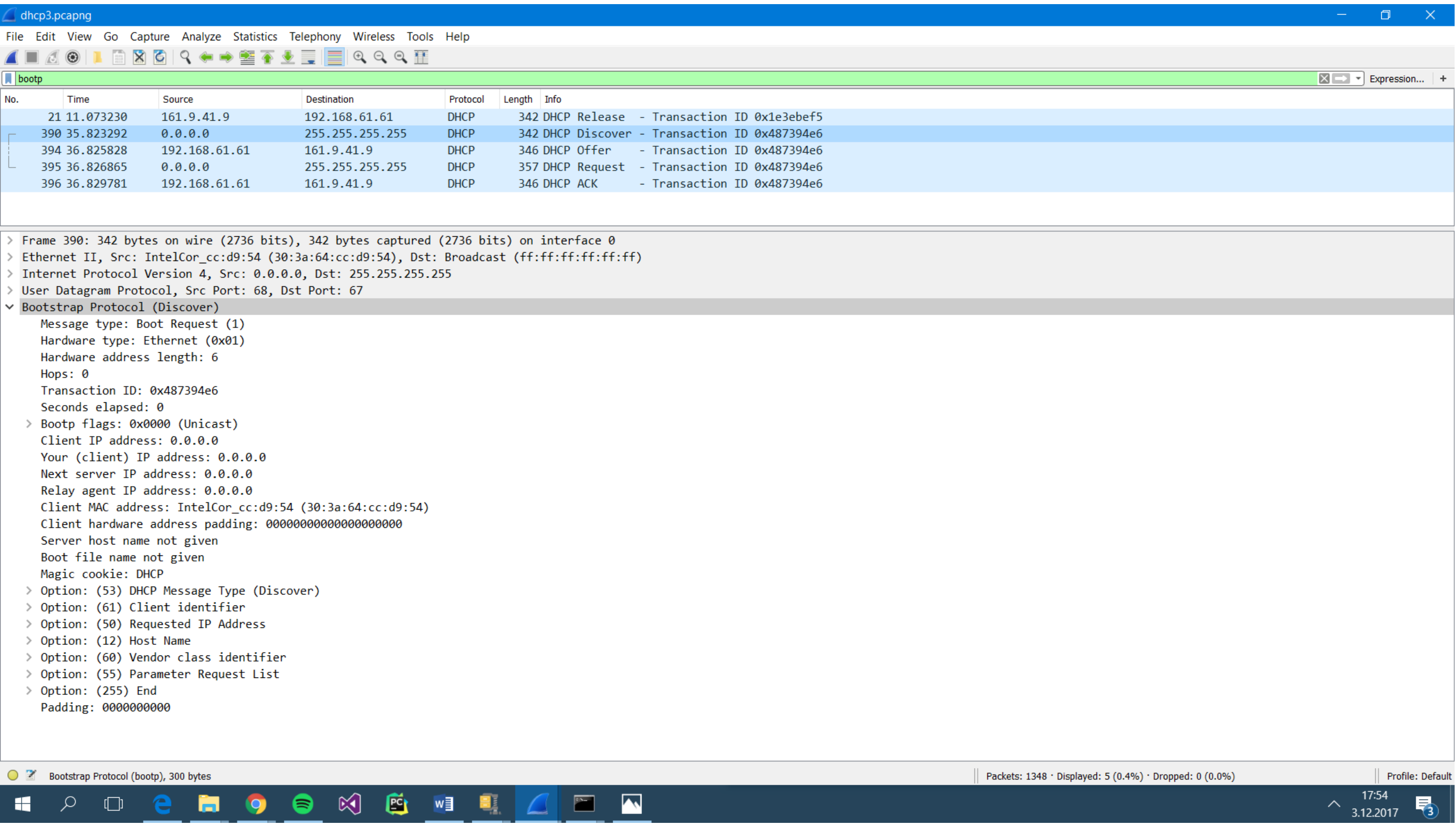
HOMEWORK 2

“Network Analyzing with Wireshark”

1. **Dynamic Host Configuration Protocol (DHCP)** is a protocol that assigns individual IP addresses to the hosts automatically from a block of addresses. It also gives information about subnet mask, address of a host’s first-hop router and address of a host’s local DNS server.
   DHCP contains four stages for a newly arriving host. The stages are described in below:
   a. **DHCP server discovery:** The newly arriving host’s task is to find DHCP server and this task is done using **DHCP discover message**. The DHCP discover message is in a UDP packet which is encapsulated with a IP datagram. The host sends the IP datagram but does not know the IP address of the server which will be connected to, so host does a broadcast with IP address 255.255.255.255 to all nodes in the subnet. Host’s assumed IP address is 0.0.0.0.
   b. **DHCP server offer:** The DHCP server which receives the discover message replies client with a **DHCP offer message** with a broadcast to all nodes on the subnet, with IP broadcast address 255.255.255.255. There may exist several DHCP servers, so the client may find the most appropriate server for itself. Each DHCP offer message contains the transaction ID of the discover message, the offered IP address for the DHCP client, the network mask and amount of time for which IP address will be valid.
   c. **DHCP request:** The client selects a DHCP server and sends a **DHCP request message** to selected server.
   d. **DHCP ACK:** The server responds request message of client with **DHCP ACK message** that indicates verifying requested parameters.

   In Figure 1.1 and Figure 1.2, all 4 stages of DHCP can be observed which have same transaction IDs. In DHCP discover stage, the destination IP address can be observed as 255.255.255.255 because of broadcasting. The source IP address can be observed as 0.0.0.0 because the client does not have any IP address yet and its IP address is assumed as 0.0.0.0.

   To observe DHCP stages from Wireshark, firstly I released my current IP address with “ipconfig /release” command. Then, to take a new IP address, I wrote “ipconfig /renew” command to the terminal. I sniffed the packets synchronously with these commands.


dhcp3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
17:54
3.12.2017

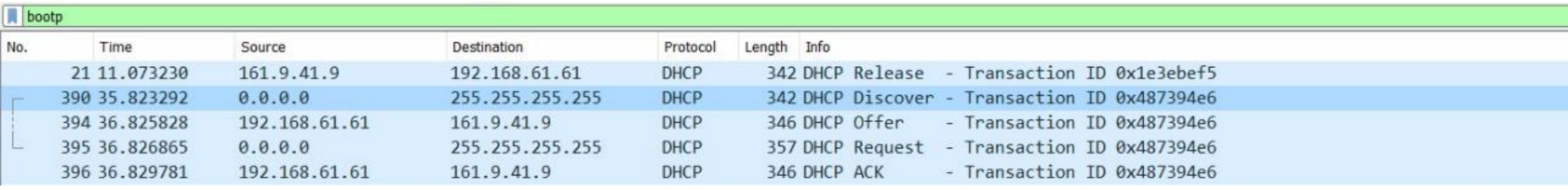
bootp

```
No.    Time        Source         Destination      Protocol  Length  Info
    21 11.073230   161.9.41.9     192.168.61.61    DHCP         342 DHCP Release  - Transaction ID 0x1e3ebef5
   390 35.823292   0.0.0.0        255.255.255.255  DHCP         342 DHCP Discover - Transaction ID 0x487394e6
   394 36.825828   192.168.61.61  161.9.41.9       DHCP         346 DHCP Offer    - Transaction ID 0x487394e6
   395 36.826865   0.0.0.0        255.255.255.255  DHCP         357 DHCP Request  - Transaction ID 0x487394e6
   396 36.829781   192.168.61.61  161.9.41.9       DHCP         346 DHCP ACK      - Transaction ID 0x487394e6
```

```
> Frame 390: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: IntelCor_cc:d9:54 (30:3a:64:cc:d9:54), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x487394e6
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCor_cc:d9:54 (30:3a:64:cc:d9:54)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
    Padding: 0000000000
```

Bootstrap Protocol (bootp), 300 bytes | Packets: 1348 · Displayed: 5 (0.4%) · Dropped: 0 (0.0%) | Profile: Default

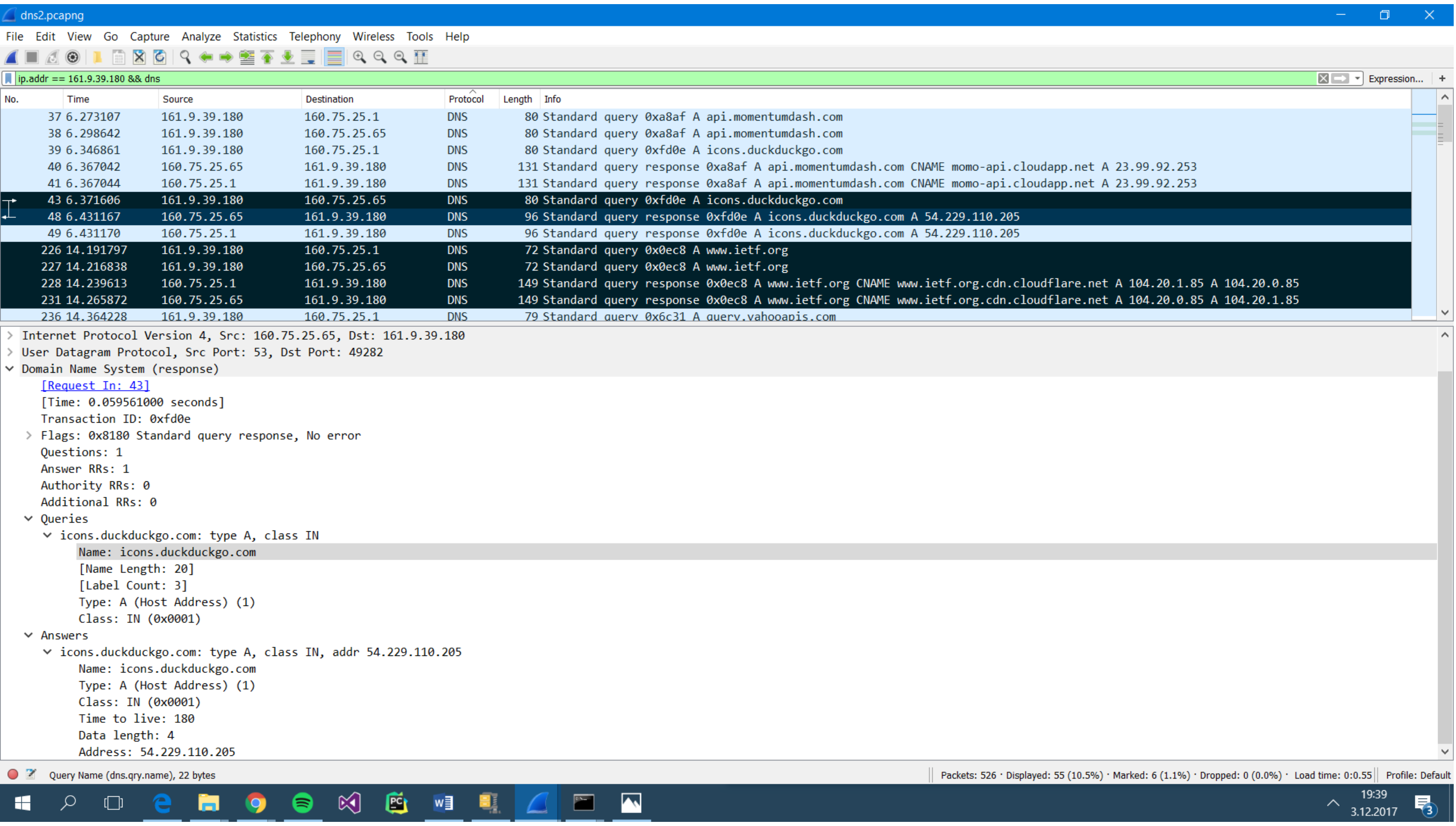
Figure 1.1: Wireshark screenshot shows DHCP stages


bootp

```
No.    Time        Source         Destination      Protocol  Length  Info
    21 11.073230   161.9.41.9     192.168.61.61    DHCP         342 DHCP Release  - Transaction ID 0x1e3ebef5
   390 35.823292   0.0.0.0        255.255.255.255  DHCP         342 DHCP Discover - Transaction ID 0x487394e6
   394 36.825828   192.168.61.61  161.9.41.9       DHCP         346 DHCP Offer    - Transaction ID 0x487394e6
   395 36.826865   0.0.0.0        255.255.255.255  DHCP         357 DHCP Request  - Transaction ID 0x487394e6
   396 36.829781   192.168.61.61  161.9.41.9       DHCP         346 DHCP ACK      - Transaction ID 0x487394e6
```

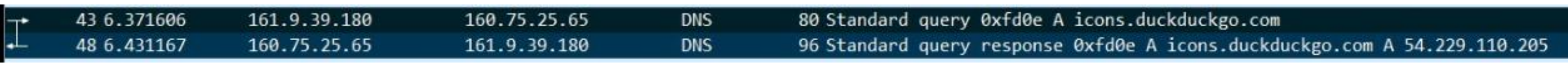
Figure 1.2: Expanded Wireshark screenshot of DHCP stages
(Stages with same Transaction IDs -last 4 rows- correspond one DHCP process.)

2. **Domain Name System (DNS)** ensures matching the IP addresses with hostnames for hosts. DNS contains the following steps:
   - **a.** Client runs the client side of the DNS application.
   - **b.** Browser extracts the hostname and passes to the client side.
   - **c.** DNS client sends a DNS query which includes hostname to the DNS server.
   - **d.** DNS client receives a response from the DNS server which includes the IP address of the host.
   - **e.** The browser takes the IP address of the host and provides a connection to the HTTP server.


dns2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
19:39
3.12.2017

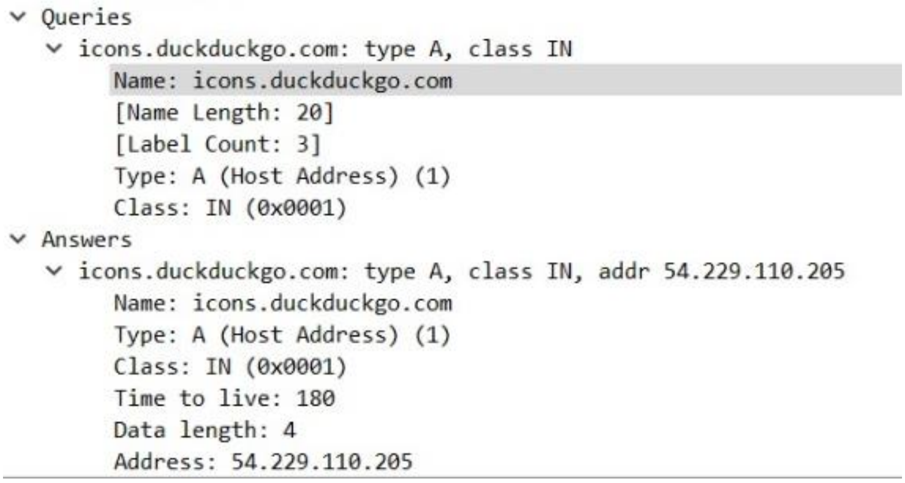
```
ip.addr == 161.9.39.180 && dns

No.   Time       Source         Destination    Protocol Length Info
   37 6.273107   161.9.39.180   160.75.25.1    DNS       80 Standard query 0xa8af A api.momentumdash.com
   38 6.298642   161.9.39.180   160.75.25.65   DNS       80 Standard query 0xa8af A api.momentumdash.com
   39 6.346861   161.9.39.180   160.75.25.1    DNS       80 Standard query 0xfd0e A icons.duckduckgo.com
   40 6.367042   160.75.25.65   161.9.39.180   DNS      131 Standard query response 0xa8af A api.momentumdash.com CNAME momo-api.cloudapp.net A 23.99.92.253
   41 6.367044   160.75.25.1    161.9.39.180   DNS      131 Standard query response 0xa8af A api.momentumdash.com CNAME momo-api.cloudapp.net A 23.99.92.253
   43 6.371606   161.9.39.180   160.75.25.65   DNS       80 Standard query 0xfd0e A icons.duckduckgo.com
   48 6.431167   160.75.25.65   161.9.39.180   DNS       96 Standard query response 0xfd0e A icons.duckduckgo.com A 54.229.110.205
   49 6.431170   160.75.25.1    161.9.39.180   DNS       96 Standard query response 0xfd0e A icons.duckduckgo.com A 54.229.110.205
  226 14.191797  161.9.39.180   160.75.25.1    DNS       72 Standard query 0x0ec8 A www.ietf.org
  227 14.216838  161.9.39.180   160.75.25.65   DNS       72 Standard query 0x0ec8 A www.ietf.org
  228 14.239613  160.75.25.1    161.9.39.180   DNS      149 Standard query response 0x0ec8 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85
  231 14.265872  160.75.25.65   161.9.39.180   DNS      149 Standard query response 0x0ec8 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104.20.1.85
  236 14.364228  161.9.39.180   160.75.25.1    DNS       79 Standard query 0x6c31 A query.yahooapis.com

> Internet Protocol Version 4, Src: 160.75.25.65, Dst: 161.9.39.180
> User Datagram Protocol, Src Port: 53, Dst Port: 49282
v Domain Name System (response)
    [Request In: 43]
    [Time: 0.059561000 seconds]
    Transaction ID: 0xfd0e
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v icons.duckduckgo.com: type A, class IN
          Name: icons.duckduckgo.com
          [Name Length: 20]
          [Label Count: 3]
          Type: A (Host Address) (1)
          Class: IN (0x0001)
  v Answers
    v icons.duckduckgo.com: type A, class IN, addr 54.229.110.205
          Name: icons.duckduckgo.com
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 180
          Data length: 4
          Address: 54.229.110.205

Query Name (dns.qry.name), 22 bytes    Packets: 526 · Displayed: 55 (10.5%) · Marked: 6 (1.1%) · Dropped: 0 (0.0%) · Load time: 0:0.55    Profile: Default
```

Figure 2.1: DNS queries and query responses for new web sites



```
   43 6.371606   161.9.39.180   160.75.25.65   DNS   80 Standard query 0xfd0e A icons.duckduckgo.com
   48 6.431167   160.75.25.65   161.9.39.180   DNS   96 Standard query response 0xfd0e A icons.duckduckgo.com A 54.229.110.205
```

Figure 2.2: DNS query and query response for the hostname “www.duckduckgo.com”



```
v Queries
  v icons.duckduckgo.com: type A, class IN
        Name: icons.duckduckgo.com
        [Name Length: 20]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
v Answers
  v icons.duckduckgo.com: type A, class IN, addr 54.229.110.205
        Name: icons.duckduckgo.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 180
        Data length: 4
        Address: 54.229.110.205
```

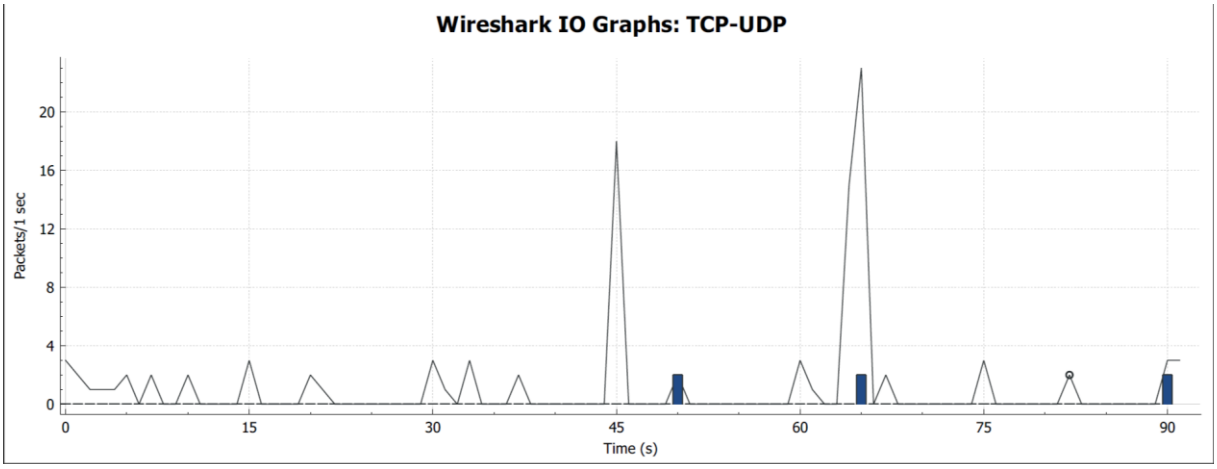
Figure 2.3: IP address of the www.duckduckgo.com is 54.229.110.205.

IP address of the DNS server is 160.75.25.65 from the Figure 2.2, because destination address of the standard query is DNS server's IP address and source of the standard query is DNS client. After DNS query, DNS query response comes from the DNS server and its destination address is DNS client.

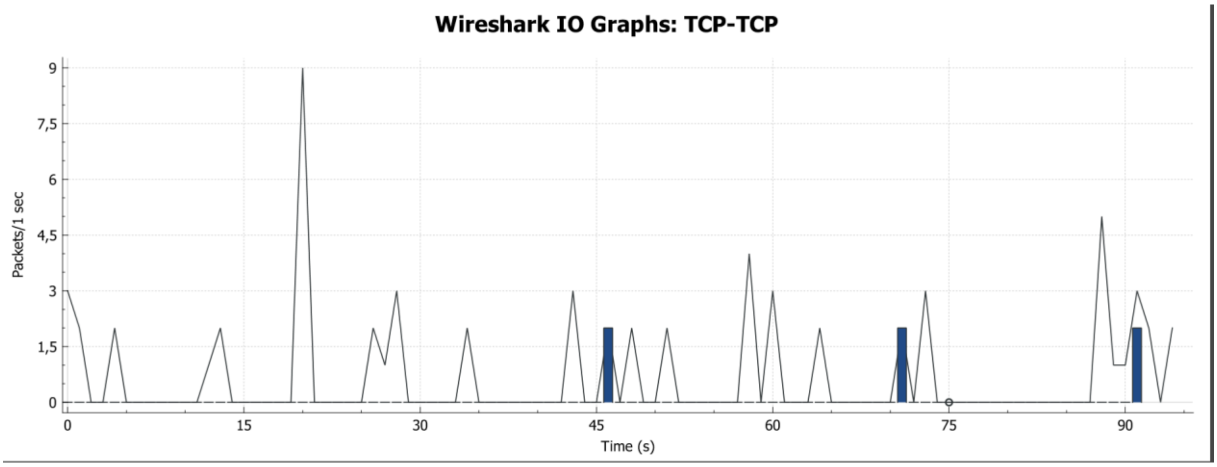
IP address of the website (which has the hostname "www.duckduckgo.com") is 54.229.110.205 from Figure 2.3. Host's IP address is indicated at "Answers" part of the Figure 2.3.

3. Bandwidth is determined as 100Mbit and in each sequence, bandwidth is increased with 100 Mbit up to 500 Mbit.
Packet length: 500B
Number of generated packets per flow: 100M
For each analysis, 2 servers and 2 clients are generated with iperf3 and I/O graphs are observed with Wireshark.

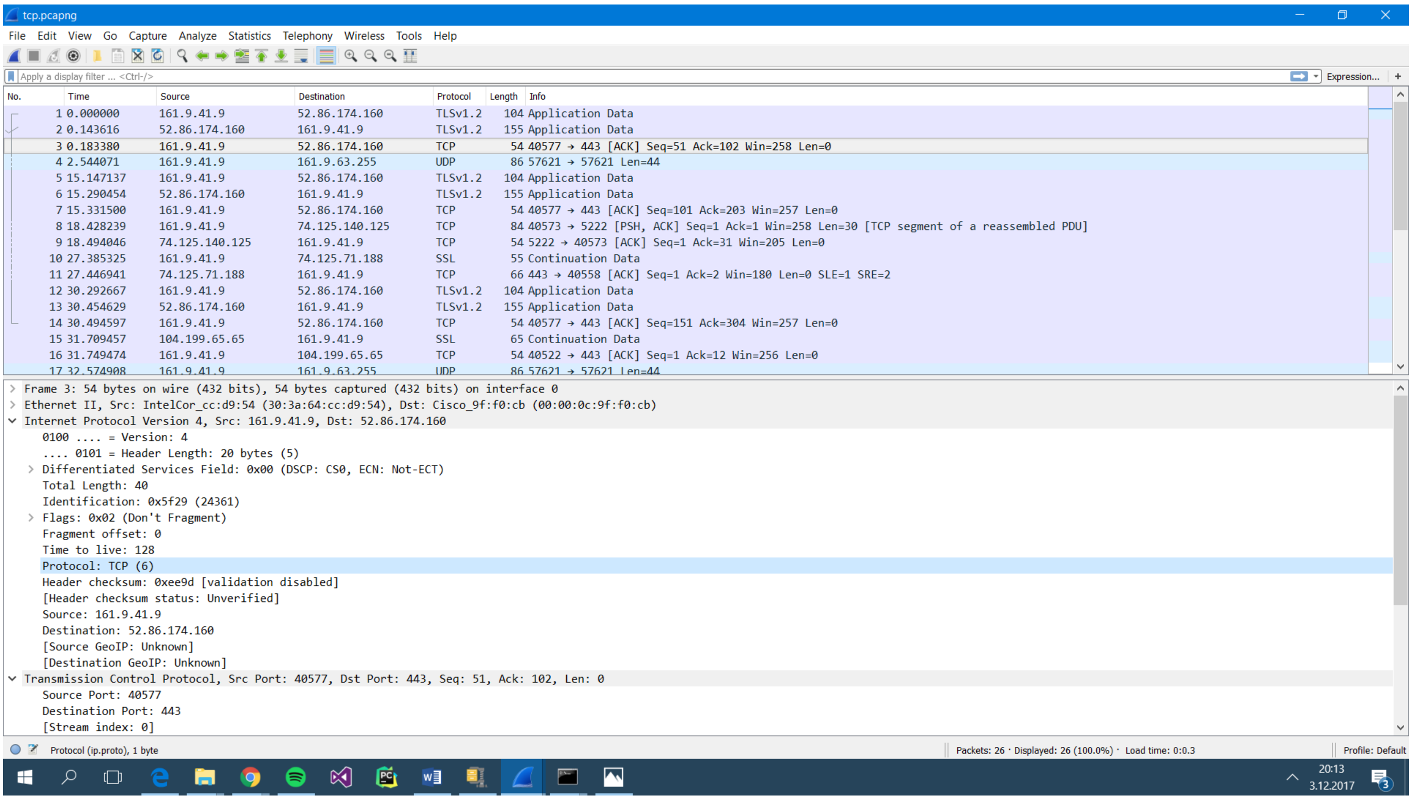
Analysis 1:



Analysis 2:



- Packet header is larger in TCP (192 bit) than in UDP (64 bit). Because of that, in Analysis 1, the generated packets are less.



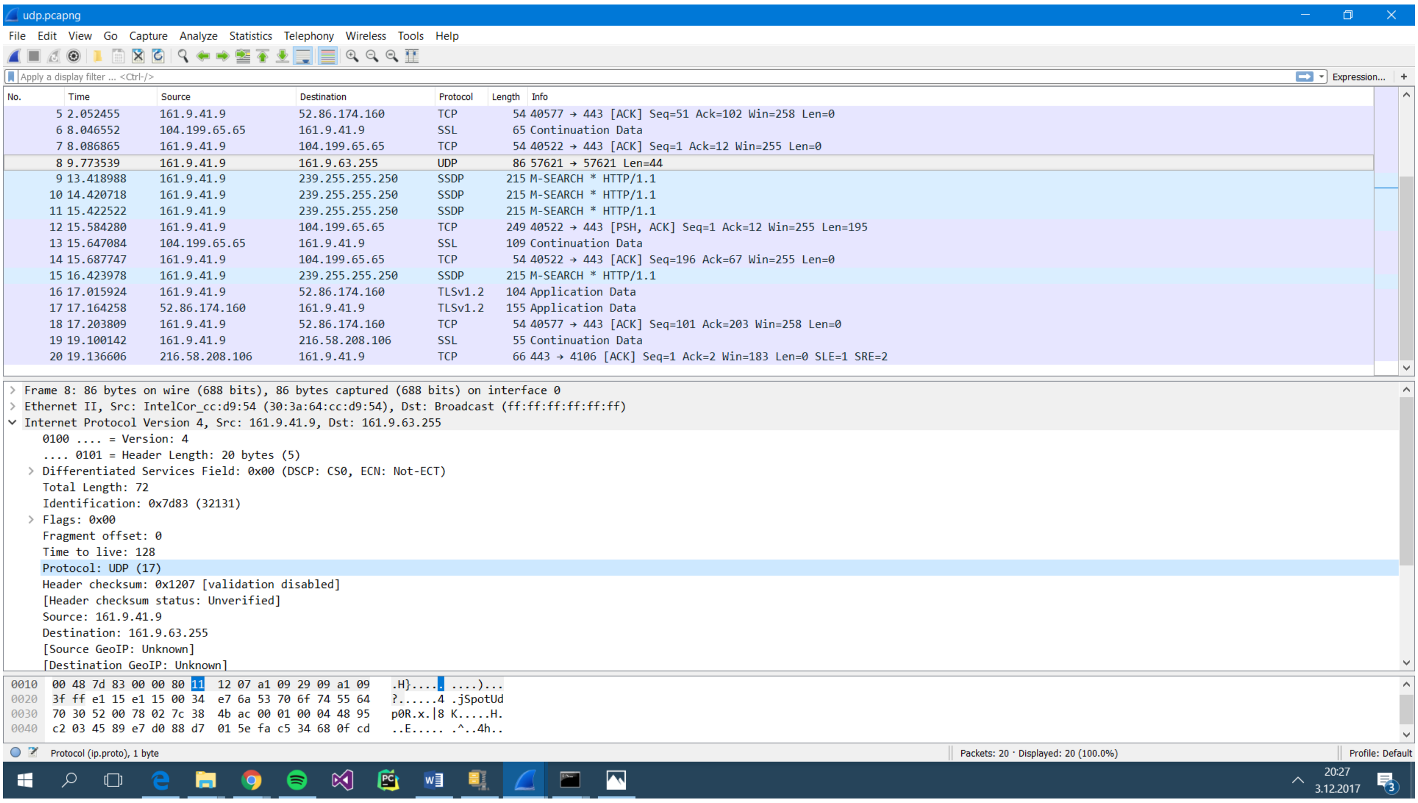
tcp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.  Time        Source          Destination     Protocol  Length Info
   1 0.000000    161.9.41.9      52.86.174.160   TLSv1.2   104 Application Data
   2 0.143616    52.86.174.160   161.9.41.9      TLSv1.2   155 Application Data
   3 0.183380    161.9.41.9      52.86.174.160   TCP        54 40577 → 443 [ACK] Seq=51 Ack=102 Win=258 Len=0
   4 2.544071    161.9.41.9      161.9.63.255    UDP        86 57621 → 57621 Len=44
   5 15.147137   161.9.41.9      52.86.174.160   TLSv1.2   104 Application Data
   6 15.290454   52.86.174.160   161.9.41.9      TLSv1.2   155 Application Data
   7 15.331500   161.9.41.9      52.86.174.160   TCP        54 40577 → 443 [ACK] Seq=101 Ack=203 Win=257 Len=0
   8 18.428239   161.9.41.9      74.125.140.125  TCP        84 40573 → 5222 [PSH, ACK] Seq=1 Ack=1 Win=258 Len=30 [TCP segment of a reassembled PDU]
   9 18.494046   74.125.140.125  161.9.41.9      TCP        54 5222 → 40573 [ACK] Seq=1 Ack=31 Win=205 Len=0
  10 27.385325   161.9.41.9      74.125.71.188   SSL        55 Continuation Data
  11 27.446941   74.125.71.188   161.9.41.9      TCP        66 443 → 40558 [ACK] Seq=1 Ack=2 Win=180 Len=0 SLE=1 SRE=2
  12 30.292667   161.9.41.9      52.86.174.160   TLSv1.2   104 Application Data
  13 30.454629   52.86.174.160   161.9.41.9      TLSv1.2   155 Application Data
  14 30.494597   161.9.41.9      52.86.174.160   TCP        54 40577 → 443 [ACK] Seq=151 Ack=304 Win=257 Len=0
  15 31.709457   104.199.65.65   161.9.41.9      SSL        65 Continuation Data
  16 31.749474   161.9.41.9      104.199.65.65   TCP        54 40522 → 443 [ACK] Seq=1 Ack=12 Win=256 Len=0
  17 32.574908   161.9.41.9      161.9.63.255    UDP        86 57621 → 57621 Len=44
```

```
> Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: IntelCor_cc:d9:54 (30:3a:64:cc:d9:54), Dst: Cisco_9f:f0:cb (00:00:0c:9f:f0:cb)
v Internet Protocol Version 4, Src: 161.9.41.9, Dst: 52.86.174.160
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x5f29 (24361)
  > Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xee9d [validation disabled]
    [Header checksum status: Unverified]
    Source: 161.9.41.9
    Destination: 52.86.174.160
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
v Transmission Control Protocol, Src Port: 40577, Dst Port: 443, Seq: 51, Ack: 102, Len: 0
    Source Port: 40577
    Destination Port: 443
    [Stream index: 0]
```

```
Protocol (ip.proto), 1 byte          Packets: 26 · Displayed: 26 (100.0%) · Load time: 0:0.3          Profile: Default
```

Figure 3.1: Protocol number of TCP is 6 as shown in Wireshark capture.



udp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.  Time        Source          Destination      Protocol  Length Info
   5 2.052455    161.9.41.9      52.86.174.160    TCP        54 40577 → 443 [ACK] Seq=51 Ack=102 Win=258 Len=0
   6 8.046552    104.199.65.65   161.9.41.9       SSL        65 Continuation Data
   7 8.086865    161.9.41.9      104.199.65.65    TCP        54 40522 → 443 [ACK] Seq=1 Ack=12 Win=255 Len=0
   8 9.773539    161.9.41.9      161.9.63.255     UDP        86 57621 → 57621 Len=44
   9 13.418988   161.9.41.9      239.255.255.250  SSDP      215 M-SEARCH * HTTP/1.1
  10 14.420718   161.9.41.9      239.255.255.250  SSDP      215 M-SEARCH * HTTP/1.1
  11 15.422522   161.9.41.9      239.255.255.250  SSDP      215 M-SEARCH * HTTP/1.1
  12 15.584280   161.9.41.9      104.199.65.65    TCP       249 40522 → 443 [PSH, ACK] Seq=1 Ack=12 Win=255 Len=195
  13 15.647084   104.199.65.65   161.9.41.9       SSL       109 Continuation Data
  14 15.687747   161.9.41.9      104.199.65.65    TCP        54 40522 → 443 [ACK] Seq=196 Ack=67 Win=255 Len=0
  15 16.423978   161.9.41.9      239.255.255.250  SSDP      215 M-SEARCH * HTTP/1.1
  16 17.015924   161.9.41.9      52.86.174.160    TLSv1.2   104 Application Data
  17 17.164258   52.86.174.160   161.9.41.9       TLSv1.2   155 Application Data
  18 17.203809   161.9.41.9      52.86.174.160    TCP        54 40577 → 443 [ACK] Seq=101 Ack=203 Win=258 Len=0
  19 19.100142   161.9.41.9      216.58.208.106   SSL        55 Continuation Data
  20 19.136606   216.58.208.106  161.9.41.9       TCP        66 443 → 4106 [ACK] Seq=1 Ack=2 Win=183 Len=0 SLE=1 SRE=2
```

```
> Frame 8: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
> Ethernet II, Src: IntelCor_cc:d9:54 (30:3a:64:cc:d9:54), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Internet Protocol Version 4, Src: 161.9.41.9, Dst: 161.9.63.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 72
    Identification: 0x7d83 (32131)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x1207 [validation disabled]
    [Header checksum status: Unverified]
    Source: 161.9.41.9
    Destination: 161.9.63.255
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

```
0010  00 48 7d 83 00 00 80 11  12 07 a1 09 29 09 a1 09   .H}..... ....)...
0020  3f ff e1 15 e1 15 00 34  e7 6a 53 70 6f 74 55 64   ?......4 .jSpotUd
0030  70 30 52 00 78 02 7c 38  4b ac 00 01 00 04 48 95   p0R.x.|8 K.....H.
0040  c2 03 45 89 e7 d0 88 d7  01 5e fa c5 34 68 0f cd   ..E..... .^..4h..
```

```
Protocol (ip.proto), 1 byte          Packets: 20 · Displayed: 20 (100.0%)          Profile: Default
```

Figure 3.2: Protocol number of UDP is 17 as shown in Wireshark capture.