BLG 433E Computer Communications, Spring 2018
Homework #2
Due Dec 09, 2018

Kadir Emre Oto
(150140032)

1: DHCP (20 Points)

Use Wireshark to investigate DHCP protocol on your computer while getting an IP address from a DHCP server. Show the communication between your computer and the DHCP server with a sequence diagram and briefly describe each of the four messages seen in the diagram. (Hint: You can take on/off the airplane mode if you are not able to see discover and offer messages.)

```
154 18.832921    0.0.0.0          255.255.255.255    DHCP    342 DHCP Discover - Transaction ID 0x9b702295
162 19.849488    0.0.0.0          255.255.255.255    DHCP    342 DHCP Discover - Transaction ID 0x9b702295
163 19.855887    172.20.10.1      172.20.10.11       DHCP    342 DHCP Offer    - Transaction ID 0x9b702295
164 19.856274    0.0.0.0          255.255.255.255    DHCP    342 DHCP Request  - Transaction ID 0x9b702295
165 19.867343    172.20.10.1      172.20.10.11       DHCP    342 DHCP ACK      - Transaction ID 0x9b702295
```

Figure 1: DHCP Packet Diagram captured by Wireshark

As we can see in the Figure 1, there are four steps in Dynamic Host Configuration Protocol (DHCP) to lease for various DHCP options like IP addresses.

1. **DHCP Discover:** The client sends a DHCP server a request to lease an IP address.
2. **DHCP Offer:** The DPCP servers offer an IP address to the client.
3. **DHCP Request:** The client sends DHCP servers a request to lease one of IP adresses that are offered by DHCP servers.
4. **DHCP ACK:** The requested DHCP server sends the client an acknowledge for requsted IP address, and updates its DHCP database. After now, the client can start communications over the network.

2: Video and Voice Traffic (20 Points)

Try to capture a video traffic and a voice traffic over Wireshark on your computer. You can use one of the video/music sharing platforms. Please, state the protocols used by investigating packet headers. Is there any retransmission during the sessions using TCP or UDP protocols? Please, indicate and interpret the results.

In order to capture a video traffic, I used very popular video streaming website, netflix. This website broadcasts the videos by using Transmission Control Protocol (TCP). As we can see in Figure 2, some packets were retransmitted by the server (i.e. frame no 43767). The reason can be the latency in the acknowledge (ACK) packet from the client, and the server could think that the frame was not sent properly, and send the packet again.

In order to capture a voice traffic, I used an application, Discord. It allows the users to establish a voice chat by using User Datagram Protocol (UDP) (Figure 3). There is no retransmission during the session.

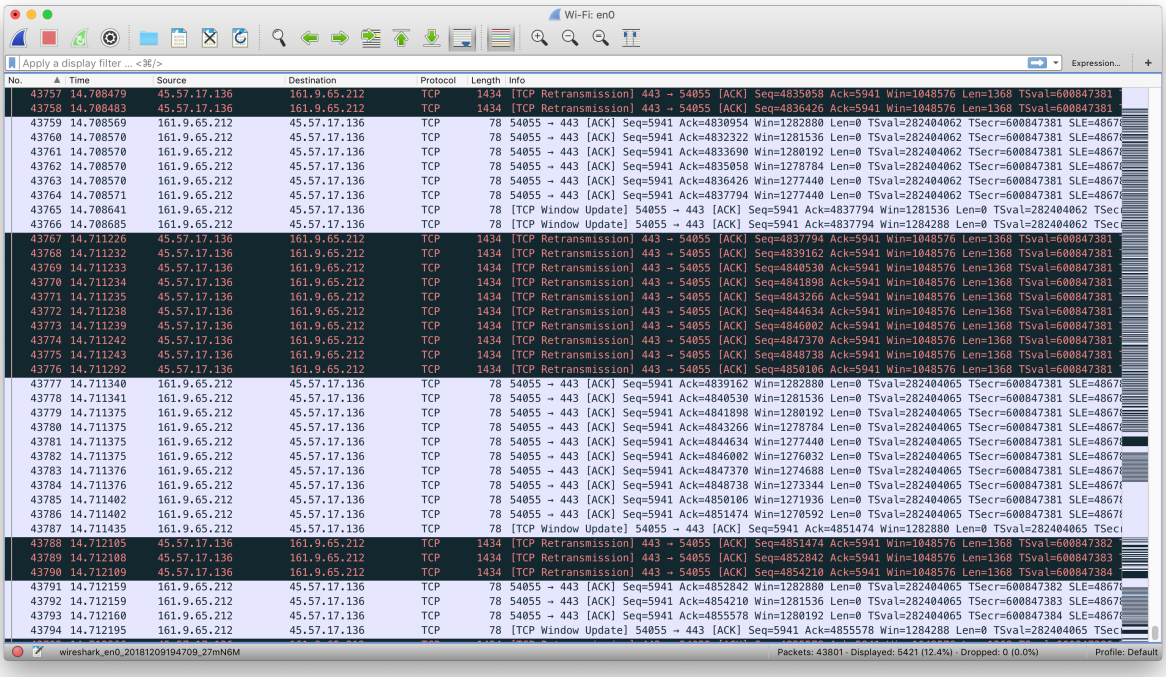

Figure 2: The Video Stream Frames captured by Wireshark

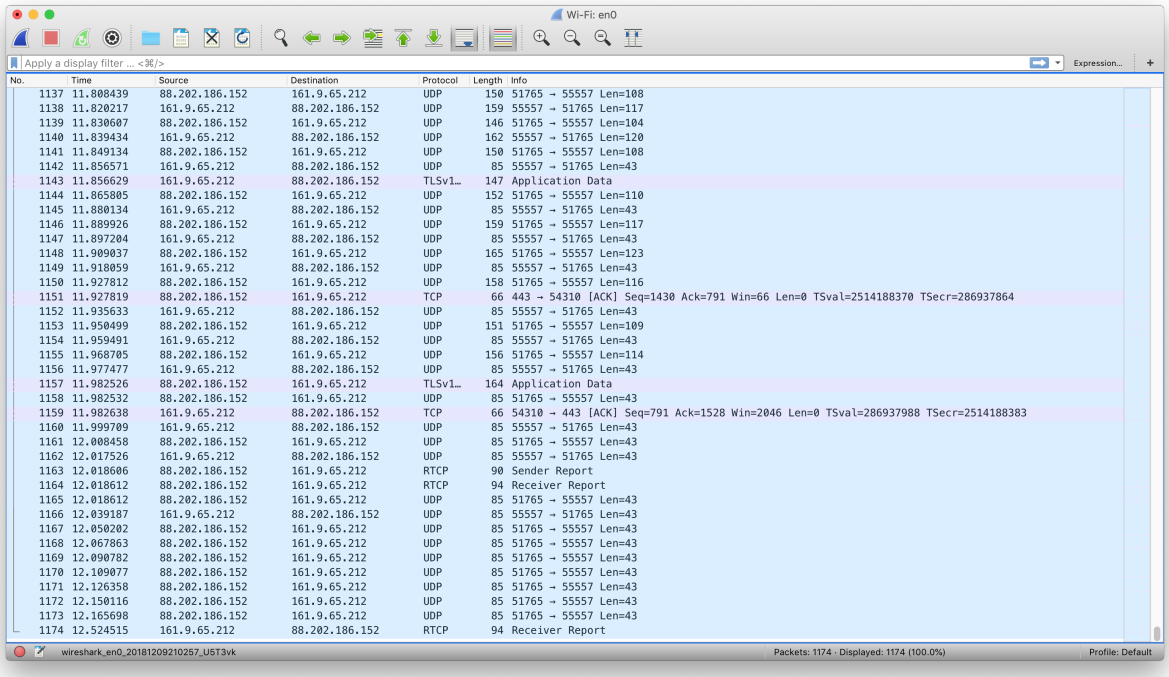

Figure 3: The Voice Stream Frames captured by Wireshark

3: Throughput, RTT, and Window Size (20 Points)

Try to capture a session that uses TCP protocol while listening to music or visiting a webpage. Using "Statistics" pane in Wireshark, Provide drawings for Throughput, RTT, and Window Size parameters over the session. Interpret the figures considering/referring TCP congestion control mechanism.

The drawings for Throughput, RTT, and Window Size parameters are provided in Figures 4, 5, 6, 7, 8, and 9.

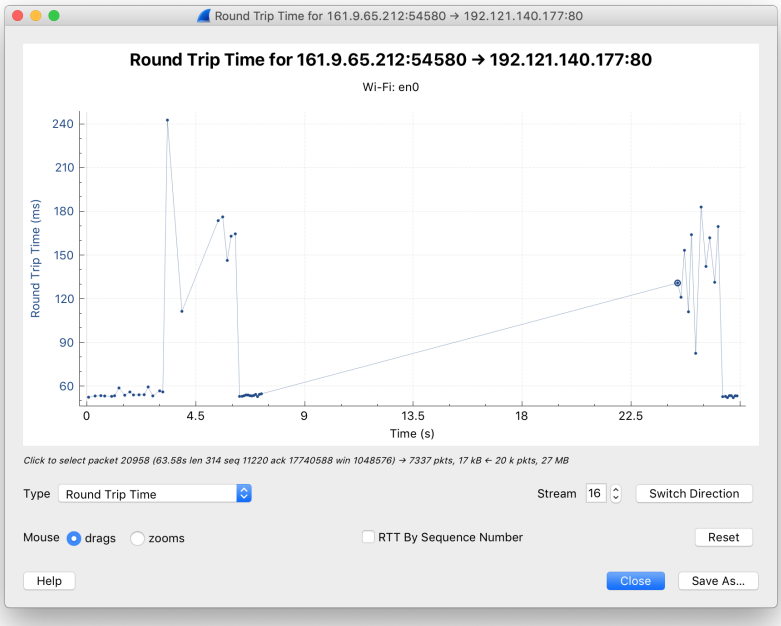

Figure 4: Round Trip Time for client to server

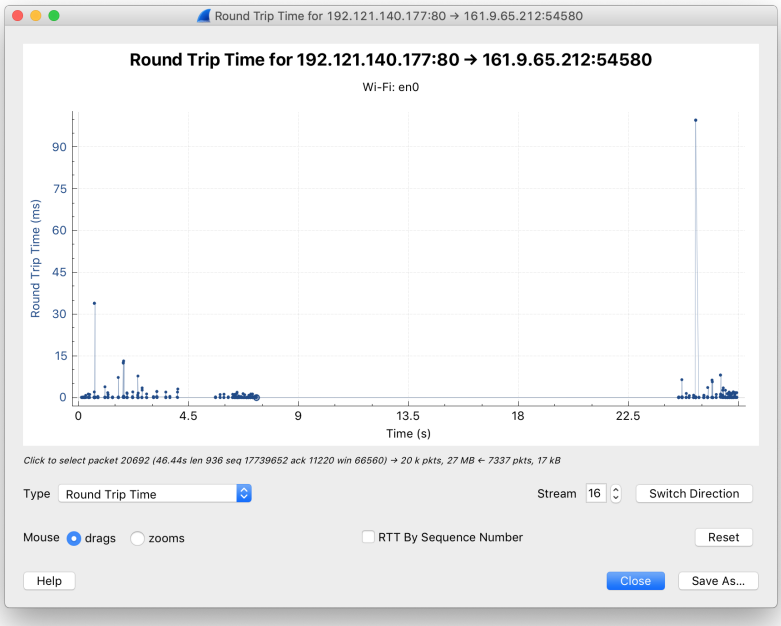

Figure 5: Round Trip Time for server to client

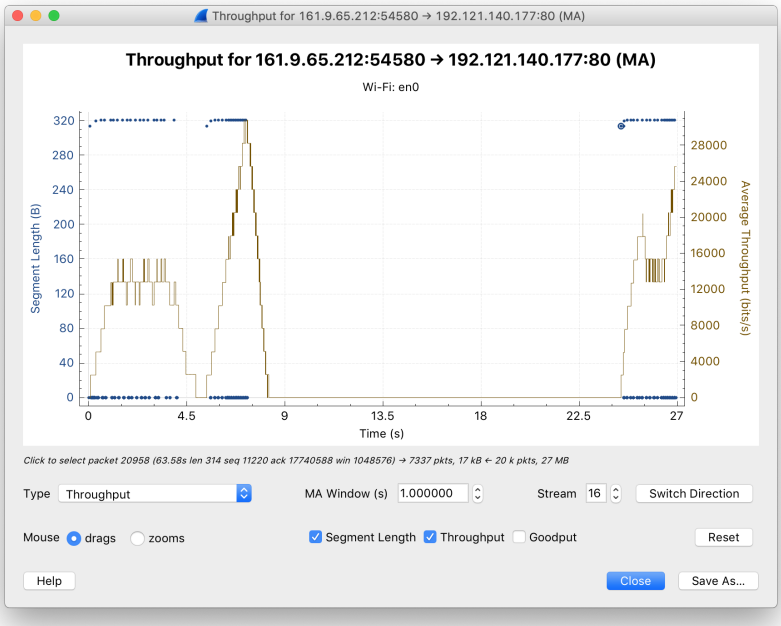

Figure 6: Throuhput for client to server

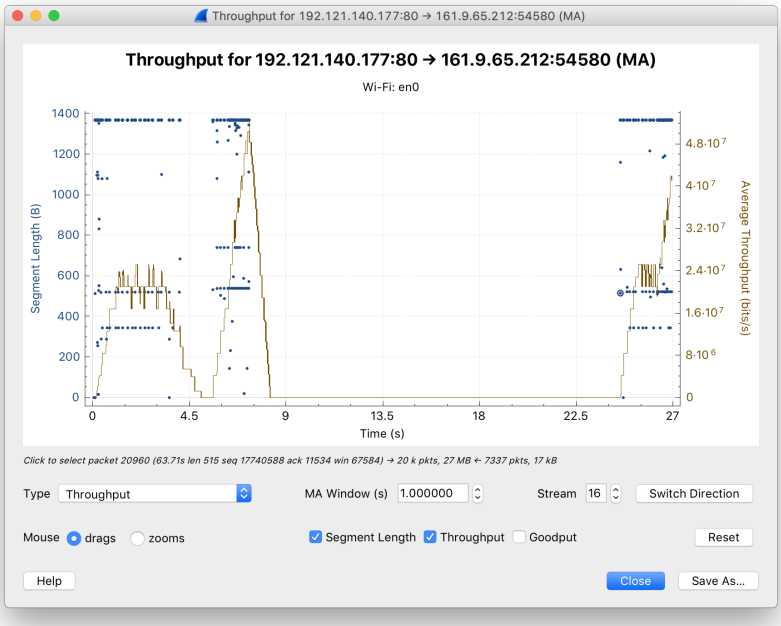

Figure 7: Throuhput for server to client

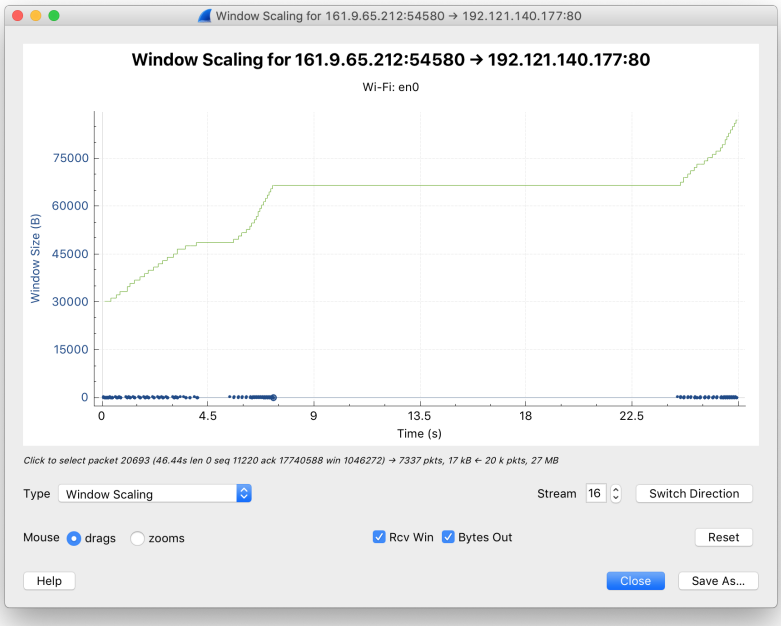

Figure 8: Window Scaling for client to server

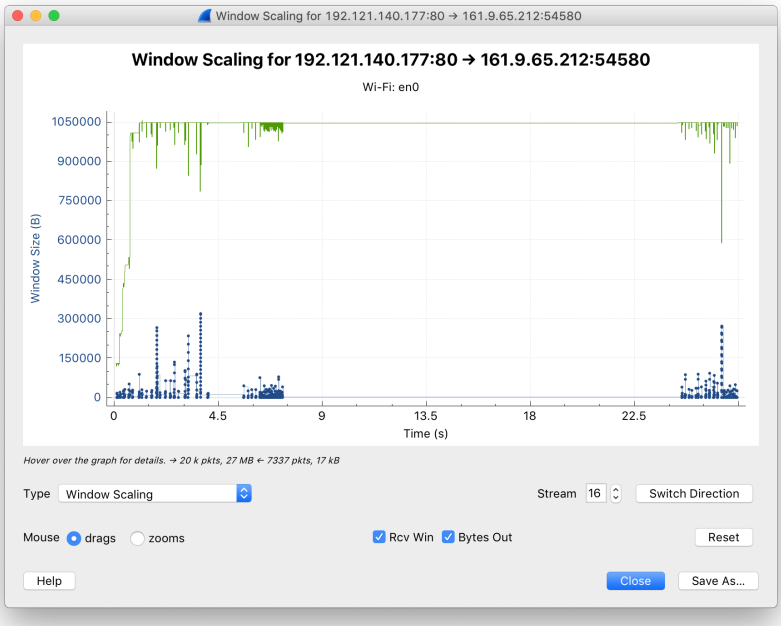

Figure 9: Window Scaling for server to client

4: File Transfer (20 Points)

Download a file on your browser and try to capture ftp packets over Wireshark. If you can't capture any, what may be the reason for that? Try the process with the link given, "ftp://speedtest.tele2.net/", and take a screenshot of an ftp packet. Interpret the steps you covered during the file transfer process.

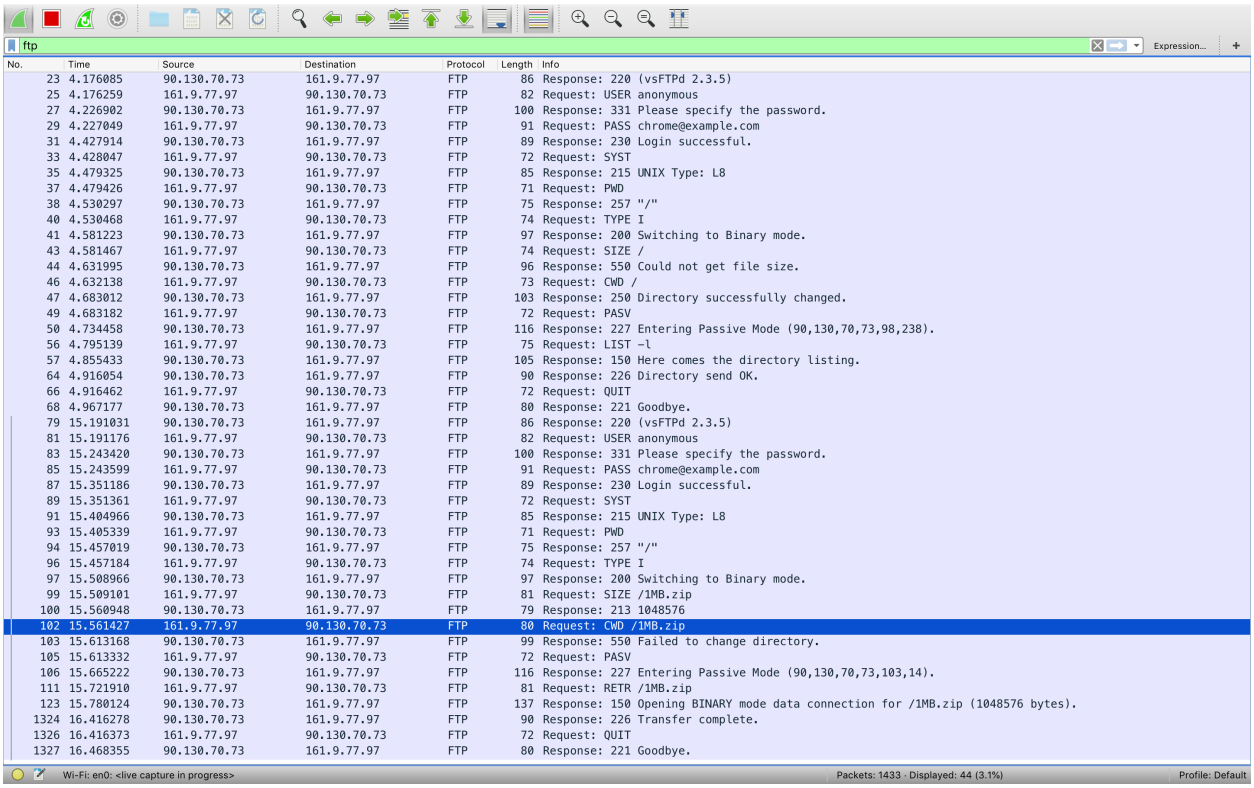

Figure 10: FTP Packet Diagram captured by Wireshark

There are two ftp sessions stated in Figure 10. At every session user should send its username using the command "USER username" (i.e. frames no: 25, and 81 in Figure 10). Then the server wants the client to specify the password. Because the client is anonymous, browsers sends a sample password automatically. After a successfull login, the client requests the system type with the command "SYST", and the server responds the relevant information. PWD command is used to get the current directory, and CWD is used to change the working directory. To download a file from the server, the client sends the command "RETR filepath" to the server (frame no: 111), after that server broadcasts the file. At the end, the client send "QUIT" command in order to close connection, the server responds that request with "221 Goodbye" command.

5: Protocol Analysis (20 Points)

(a) How many different traffic protocols do you capture in Wireshark? Please give them in a list.

1. Transmission Control Protocol (TCP)
2. User Datagram Protocol (UDP)
3. Transport Layer Security (TLSv1.2)
4. Dynamic Host Configuration Protocol (DHCP)
5. Extensible Authentication Protocol (EAP)
6. Extensible Authentication Protocol over LAN (EAPOL)
7. Address Resolution Protocol (ARP)
8. Domain Name System (DNS)
9. Internet Control Message Protocol (ICMPv6)
10. Internet Group Management Protocol (IGMPv3, and IGMPv6)
11. Multicast DNS (MDNS)
12. NetBIOS Name Service (NBNS)
13. Simple Service Discovery Protocol (SSDP)
14. File Transfer Protocol (FTP)

(b) What are the specific protocol numbers of transport layer protocols (TCP, UDP, and ICMP)? Please provide screenshots from Wireshark to show them in packet headers.

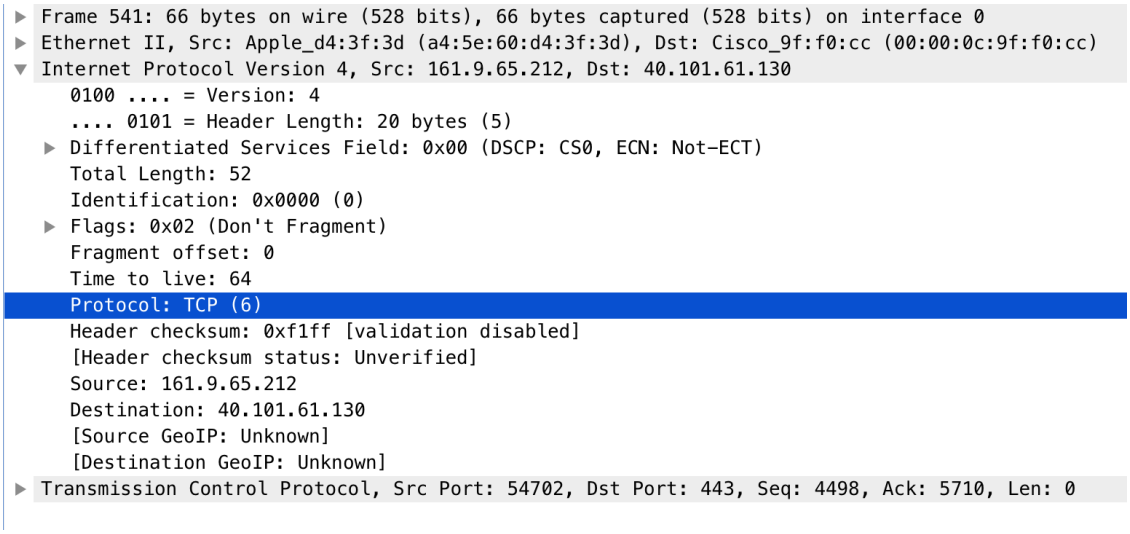

Figure 11: TCP Number

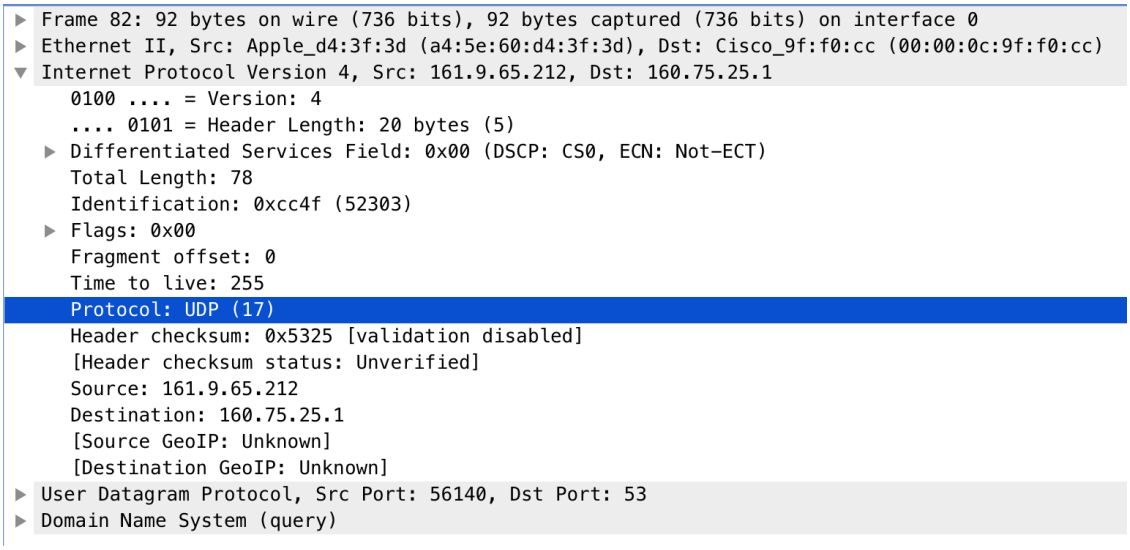

Figure 12: UDP Number

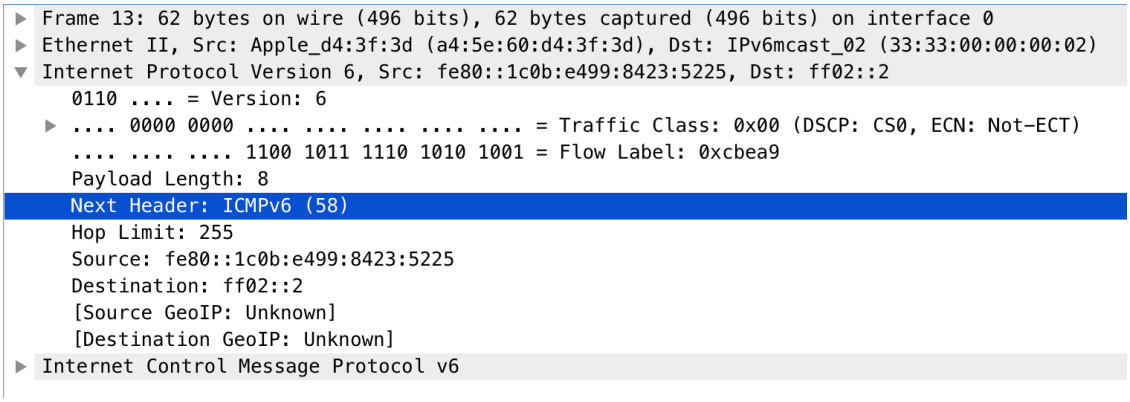

Figure 13: ICMP Number