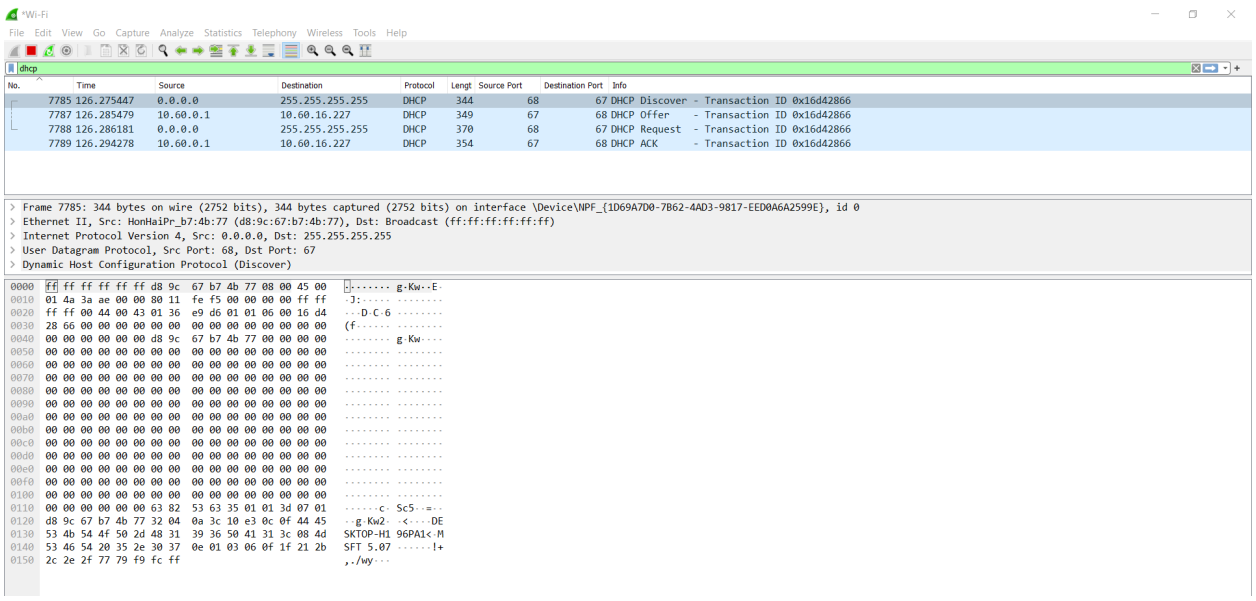
Lab 9: Wireshark --- ARP, DHCP, and ICMP

Kunal Ashish Kariwala - 2019A7PS0134G

The first and the second question were done on a windows machine due to the requirement of the ipconfig /renew and ipconfig /release commands for the first question and the arp -a, arp -d and ping commands for the second question. The third question was done on a mac machine because of the requirement of traceroute command with the --icmp (linux) -I (mac) which did not work in a windows machine. I tried doing it on a linux machine however my linux virtual env does not support wireshark.

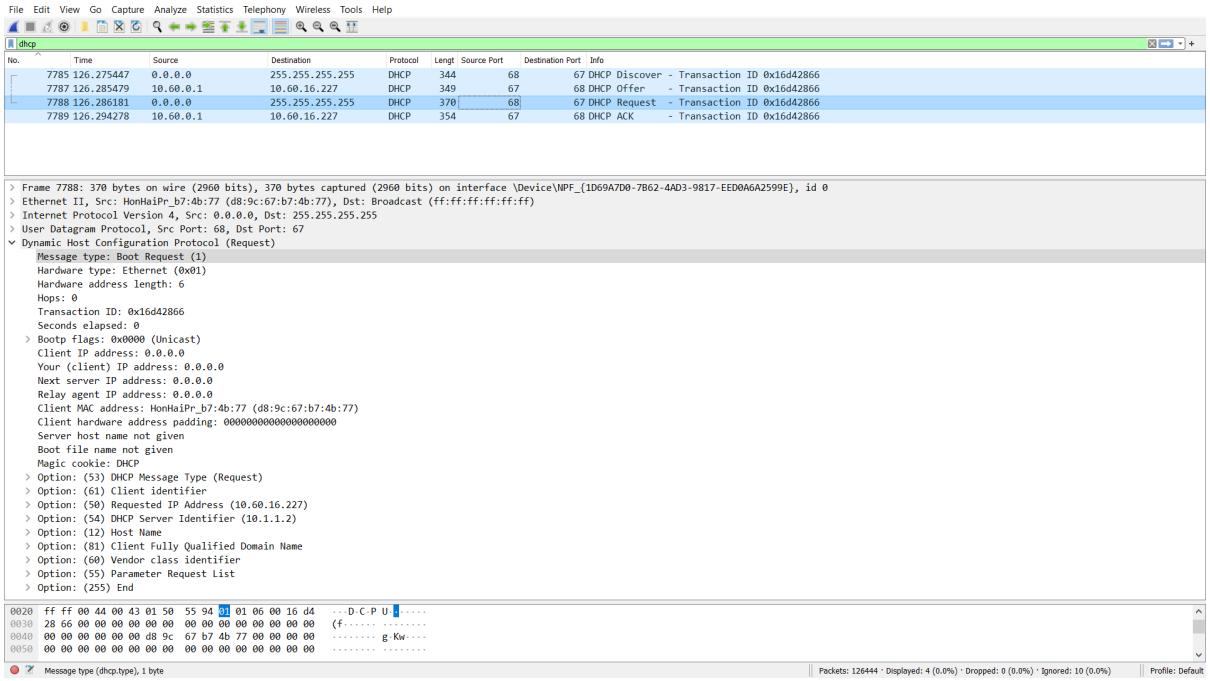
Question 1: Show a round of execution of the DHCP protocol. Write the filter and show the output in a screenshot.

Filter applied = dhcp

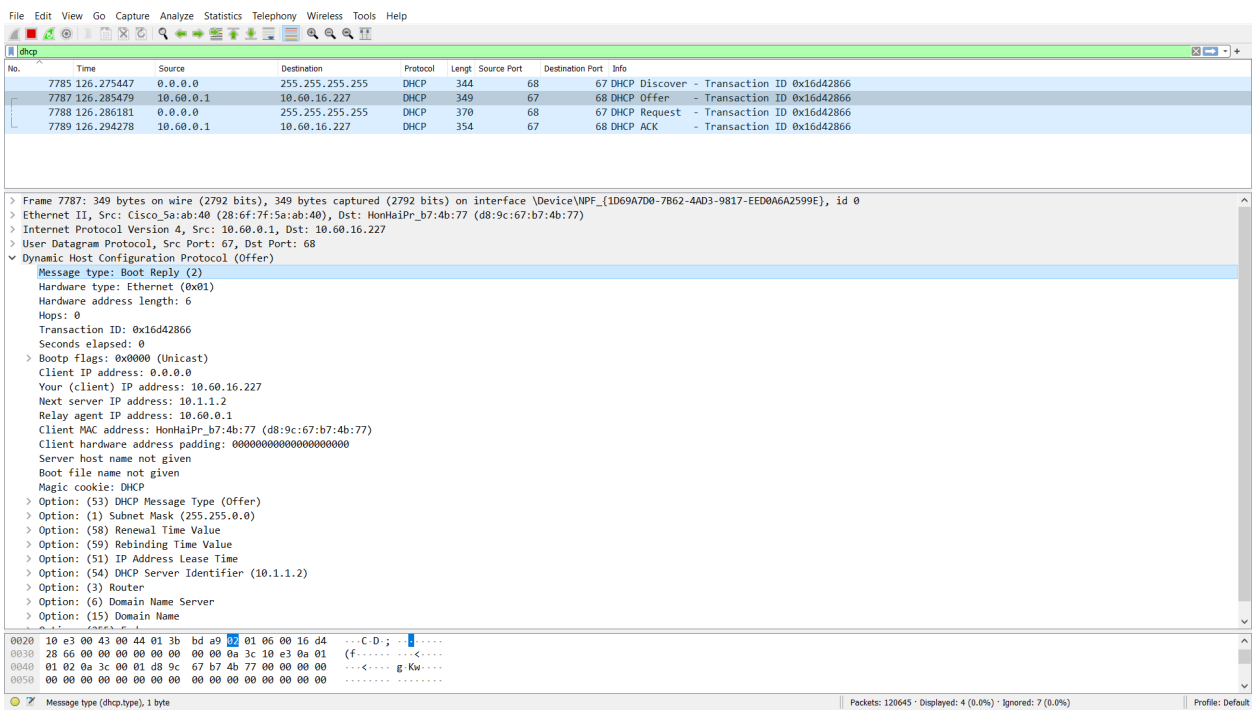


Show DHCP Request (2 marks), Reply (2 marks), and ACK messages (2 marks) in that Round.

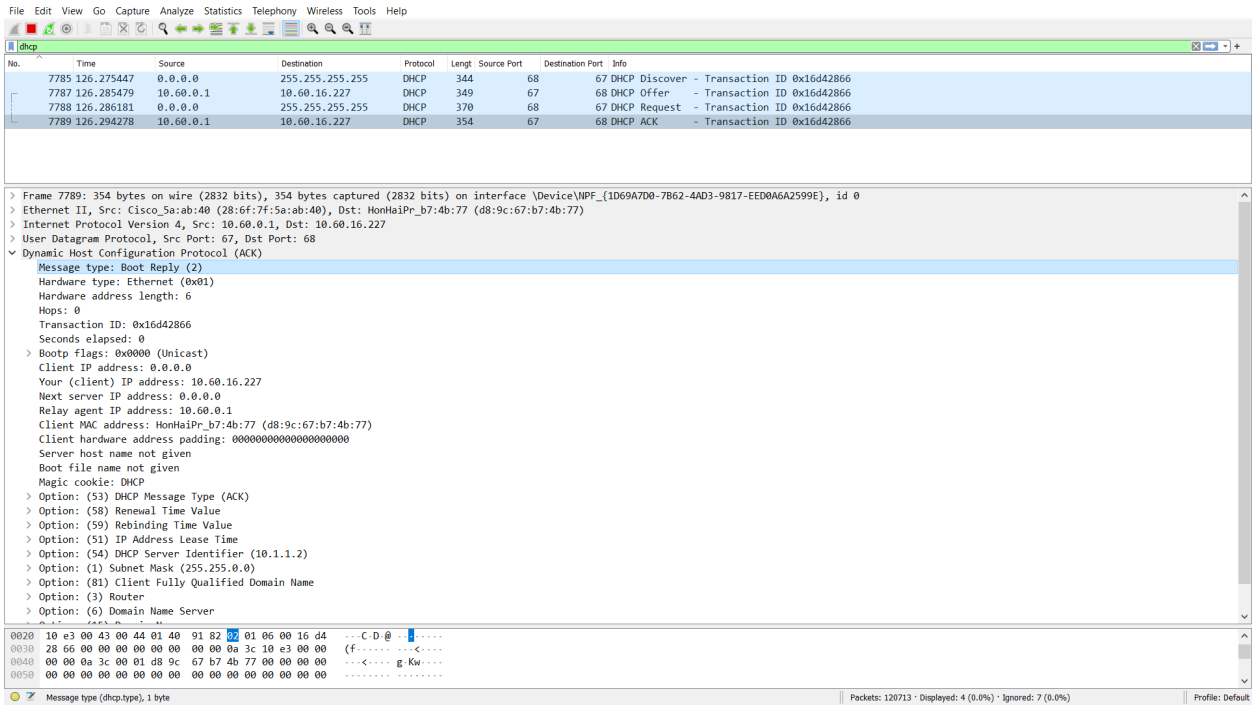
i)DHCP Request



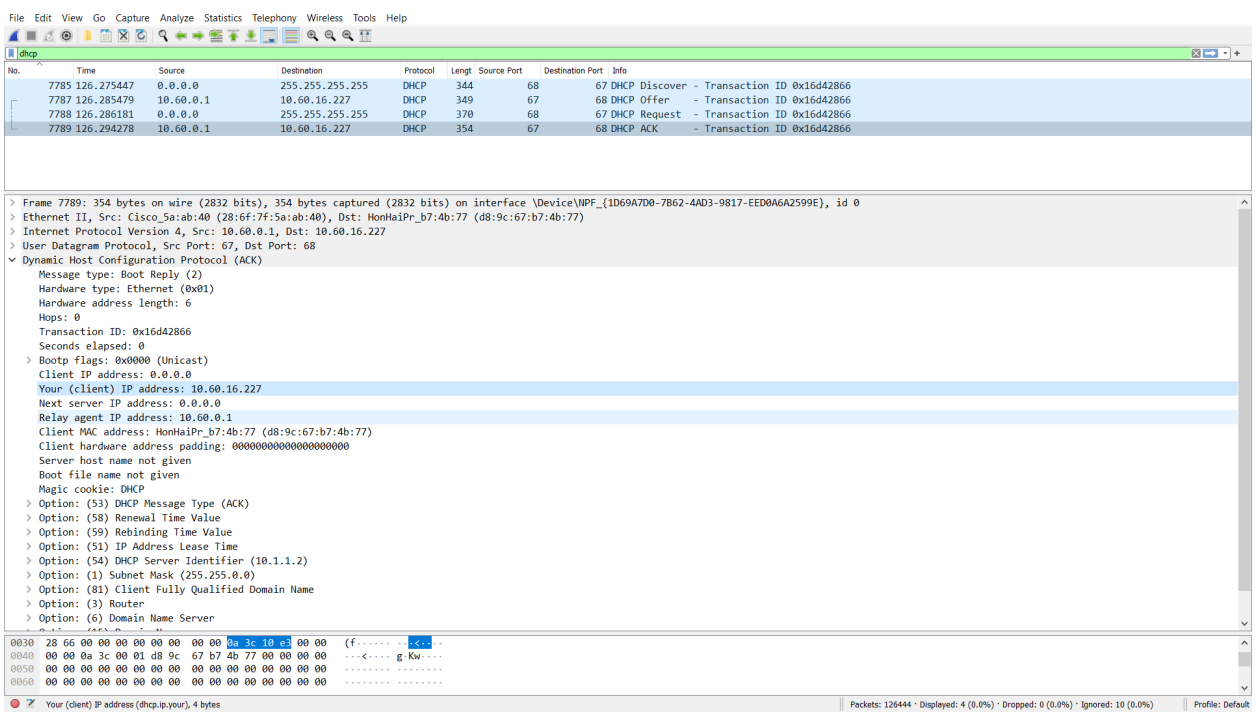
ii) DHCP Reply



iii) DHCP ACK



A) Find out IP addresses of the DHCP server (2 marks) and client (2 marks).

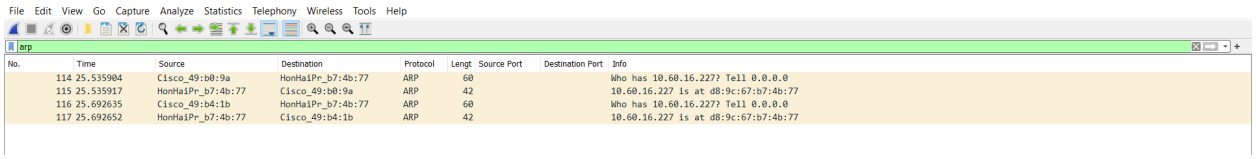


```
Client IP address: 0.0.0.0
Your (client) IP address: 10.60.16.227
Next server IP address: 0.0.0.0
Relay agent IP address: 10.60.0.1
```

Server IP Address:-10.60.0.1

Client IP Address:-10.60.16.227

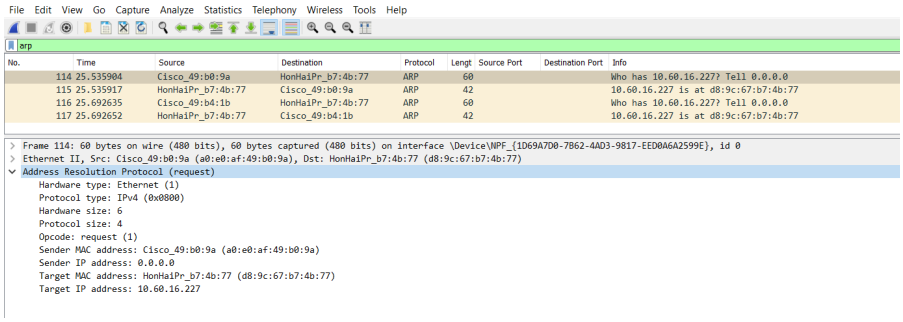
Question 2: Show a round of execution of the ARP protocol. Write the filter and show the output in a screenshot.



No.	Time	Source	Destination	Protocol	Lengt	Source Port	Destination Port	Info
114	25.535904	Cisco_49:b0:9a	HonHaiPr_b7:4b:77	ARP	60			Who has 10.60.16.227? Tell 0.0.0.0
115	25.535917	HonHaiPr_b7:4b:77	Cisco_49:b0:9a	ARP	42			10.60.16.227 is at d8:9c:67:b7:4b:77
116	25.692635	Cisco_49:b4:1b	HonHaiPr_b7:4b:77	ARP	60			Who has 10.60.16.227? Tell 0.0.0.0
117	25.692652	HonHaiPr_b7:4b:77	Cisco_49:b4:1b	ARP	42			10.60.16.227 is at d8:9c:67:b7:4b:77

A) Show ARP Request (2 marks) and Reply (2 marks) messages in that round.

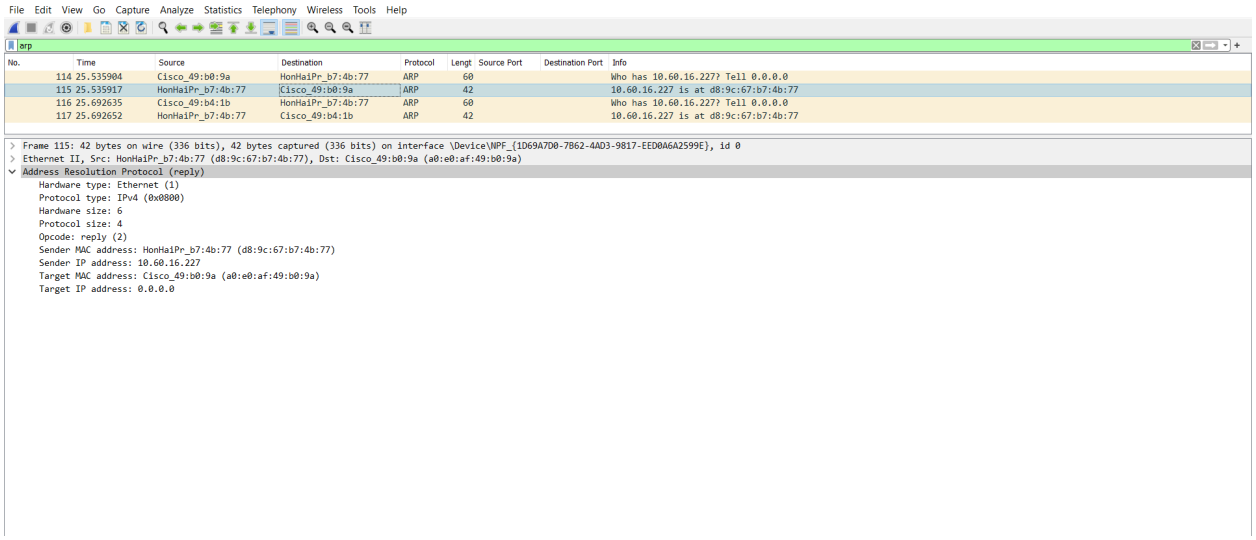
ARP Request



No.	Time	Source	Destination	Protocol	Lengt	Source Port	Destination Port	Info
114	25.535904	Cisco_49:b0:9a	HonHaiPr_b7:4b:77	ARP	60			Who has 10.60.16.227? Tell 0.0.0.0
115	25.535917	HonHaiPr_b7:4b:77	Cisco_49:b0:9a	ARP	42			10.60.16.227 is at d8:9c:67:b7:4b:77
116	25.692635	Cisco_49:b4:1b	HonHaiPr_b7:4b:77	ARP	60			Who has 10.60.16.227? Tell 0.0.0.0
117	25.692652	HonHaiPr_b7:4b:77	Cisco_49:b4:1b	ARP	42			10.60.16.227 is at d8:9c:67:b7:4b:77

```
> Frame 114: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{1D69A7D0-7B62-4AD3-9817-EED0A6A2599E}, id 0
> Ethernet II, Src: Cisco_49:b0:9a (a0:e0:af:49:b0:9a), Dst: HonHaiPr_b7:4b:77 (d8:9c:67:b7:4b:77)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Cisco_49:b0:9a (a0:e0:af:49:b0:9a)
    Sender IP address: 0.0.0.0
    Target MAC address: HonHaiPr_b7:4b:77 (d8:9c:67:b7:4b:77)
    Target IP address: 10.60.16.227
```

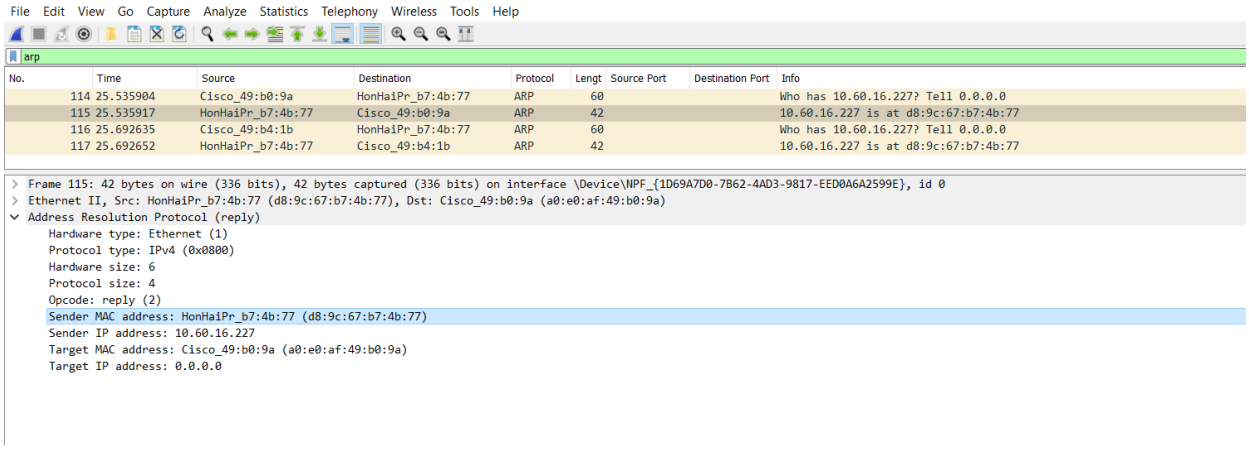
ARP Reply



No.	Time	Source	Destination	Protocol	Lengt	Source Port	Destination Port	Info
114	25.535904	Cisco_49:b0:9a	HonHaiPr_b7:4b:77	ARP	60			Who has 10.60.16.227? Tell 0.0.0.0
115	25.535917	HonHaiPr_b7:4b:77	Cisco_49:b0:9a	ARP	42			10.60.16.227 is at d8:9c:67:b7:4b:77
116	25.692635	Cisco_49:b4:1b	HonHaiPr_b7:4b:77	ARP	60			Who has 10.60.16.227? Tell 0.0.0.0
117	25.692652	HonHaiPr_b7:4b:77	Cisco_49:b4:1b	ARP	42			10.60.16.227 is at d8:9c:67:b7:4b:77

```
> Frame 115: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{1D69A7D0-7B62-4AD3-9817-EED0A6A2599E}, id 0
> Ethernet II, Src: HonHaiPr_b7:4b:77 (d8:9c:67:b7:4b:77), Dst: Cisco_49:b0:9a (a0:e0:af:49:b0:9a)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: HonHaiPr_b7:4b:77 (d8:9c:67:b7:4b:77)
    Sender IP address: 10.60.16.227
    Target MAC address: Cisco_49:b0:9a (a0:e0:af:49:b0:9a)
    Target IP address: 0.0.0.0
```

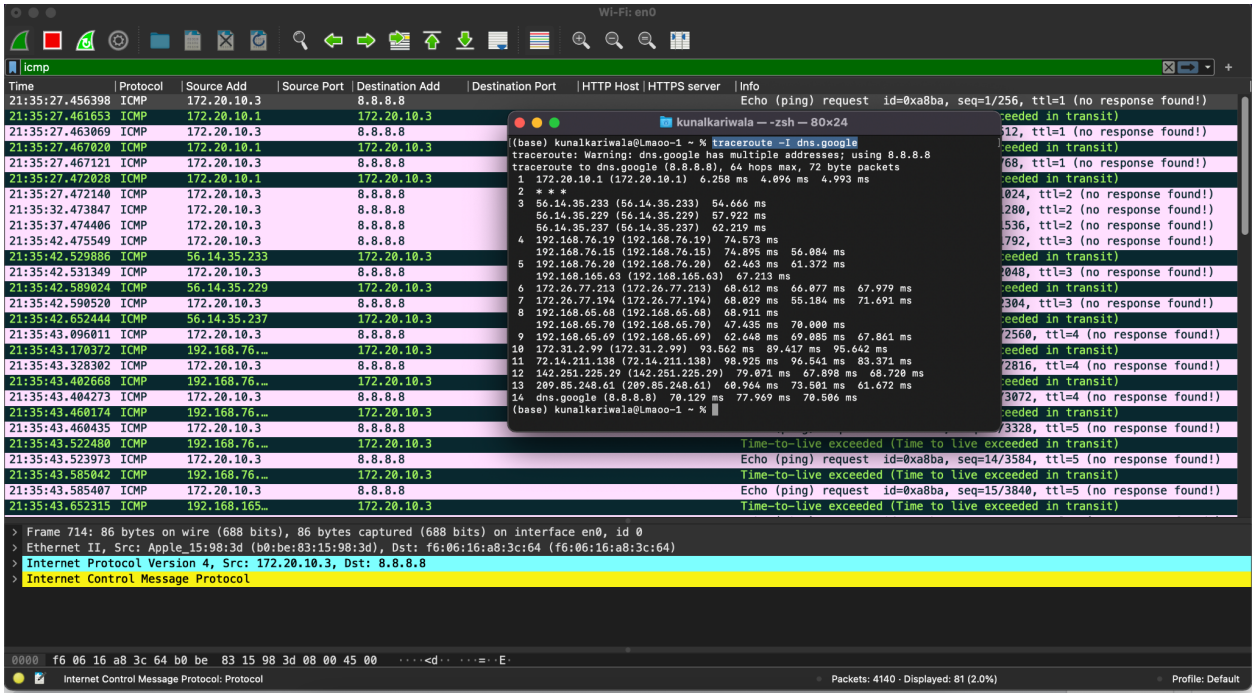
B) Find the MAC address of the replier (2 marks).



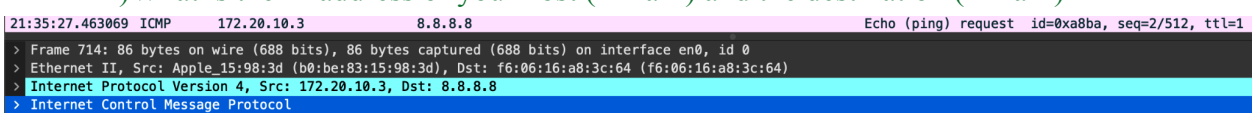
MAC address - d8:9c:67:b7:4b:77

Question 3: Show a round of execution of the `traceroute' command for dns.google.

Command used : traceroute -I dns.google (for macOS)



A)What is the IP address of your host (1 mark) and the destination (1 mark)

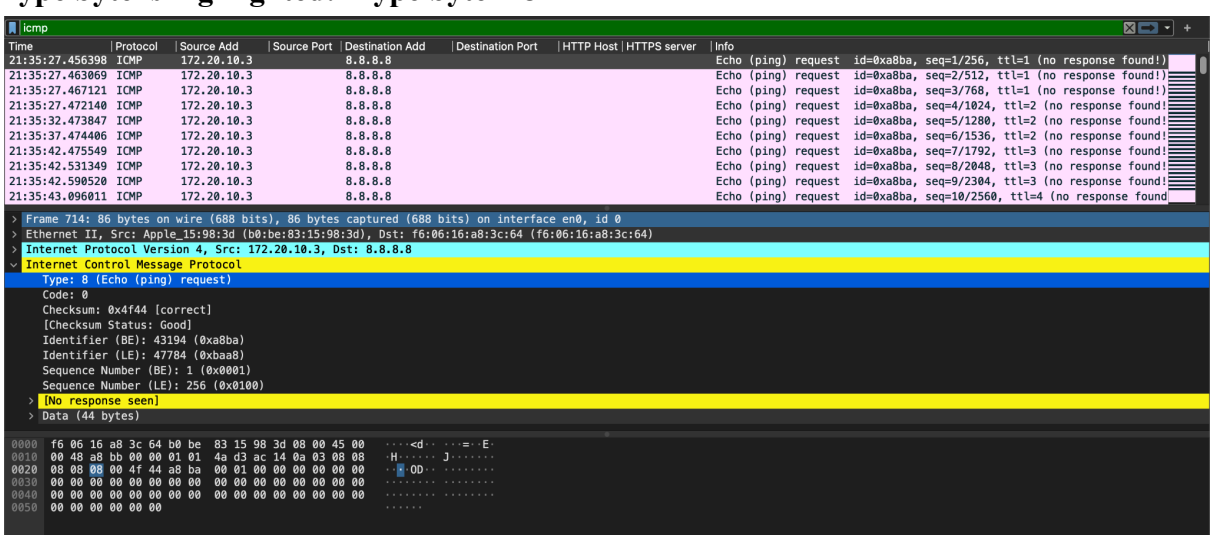


IP address of host : 172.20.10.1

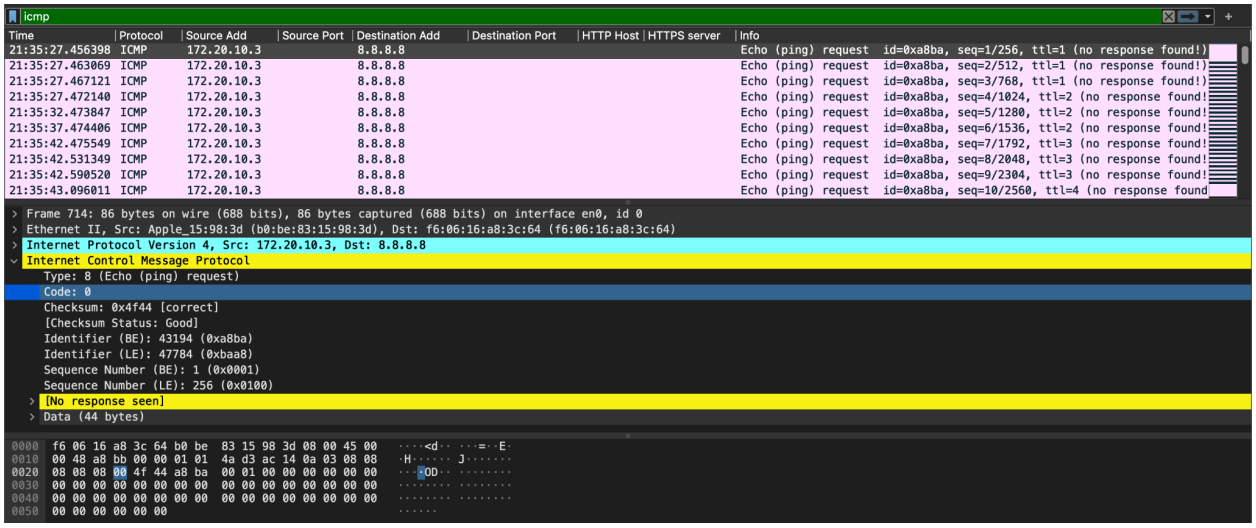
IP Address of destination : 8.8.8.8

B) Examine the raw bytes of the ICMP echo packet. Capture a screenshot of the raw bytes and identify the bytes that represent the type and code. (3 marks)

Type byte is highlighted:- Type byte = 8

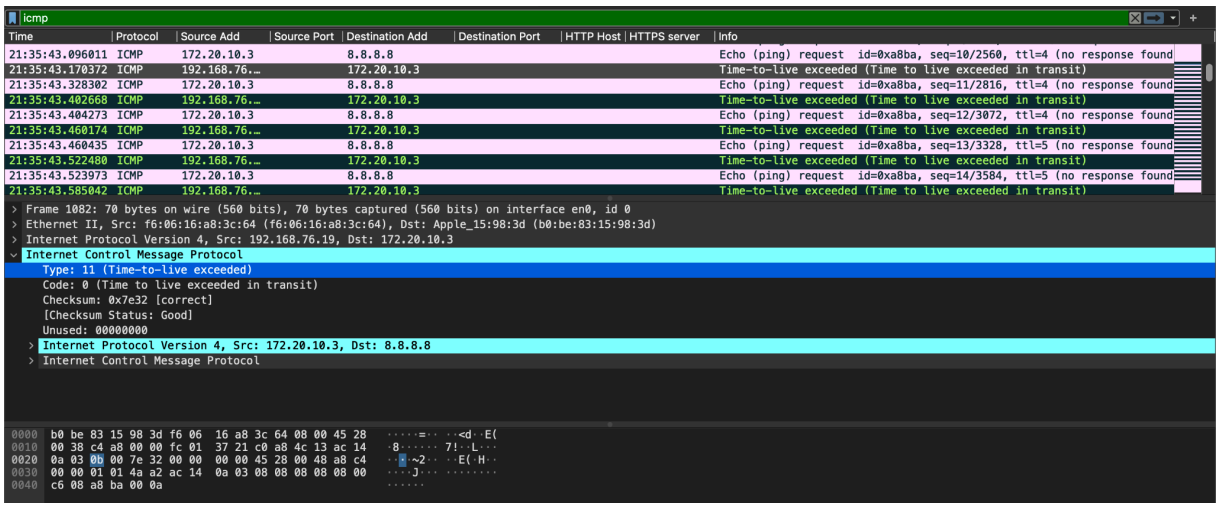


Code byte is highlighted :- Code byte = 0

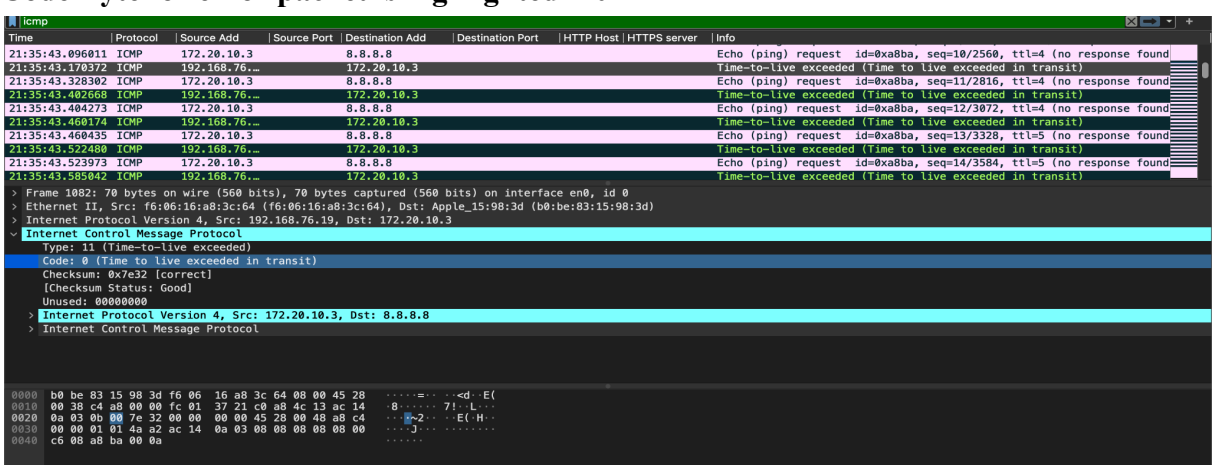


C) Examine the raw bytes of the ICMP error packet. Capture a screenshot of the raw bytes and identify the bytes that represent the type and code. (3 marks)

Type byte for error packet : 11



Code Byte for error packet is highlighted = 0



D) Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different? (4 marks)

```
21:35:47.894187 ICMP    8.8.8.8          172.20.10.3      Echo (ping) reply    id=0xa8ba, seq=40/10240, ttl=112 (request in 1270)
21:35:47.895570 ICMP    172.20.10.3      8.8.8.8          Echo (ping) request  id=0xa8ba, seq=41/10496, ttl=14 (reply in 1279)
21:35:47.973244 ICMP    8.8.8.8          172.20.10.3      Echo (ping) reply    id=0xa8ba, seq=41/10496, ttl=112 (request in 1278)
21:35:47.973598 ICMP    172.20.10.3      8.8.8.8          Echo (ping) request  id=0xa8ba, seq=42/10752, ttl=14 (reply in 1282)
21:35:48.043851 ICMP    8.8.8.8          172.20.10.3      Echo (ping) reply    id=0xa8ba, seq=42/10752, ttl=112 (request in 1280)

> Frame 1282: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface en0, id 0
> Ethernet II, Src: f6:06:16:a8:3c:64 (f6:06:16:a8:3c:64), Dst: Apple_15:98:3d (b0:be:83:15:98:3d)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 172.20.10.3
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x571b [correct]
    [Checksum Status: Good]
    Identifier (BE): 43194 (0xa8ba)
    Identifier (LE): 47784 (0xbaa8)

0000  b0 be 83 15 98 3d f6 06  16 a8 3c 64 08 00 45 60   ·····=·· ··<d··E`
0010  00 48 00 00 00 00 70 01  84 2e 08 08 08 08 ac 14   ·H····p· ······· 
0020  0a 03 00 00 57 1b a8 ba  00 2a 00 00 00 00 00 00   ····W··· ·*····· 
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ····· ····· 
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ····· ····· 
0050  00 00 00 00 00 00                                  ····· 
```

Last 3 packets:-

```
> Frame 1277: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface en0, id 0
> Ethernet II, Src: f6:06:16:a8:3c:64 (f6:06:16:a8:3c:64), Dst: Apple_15:98:3d (b0:be:83:15:98:3d)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 172.20.10.3
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x571d [correct]
    [Checksum Status: Good]
    Identifier (BE): 43194 (0xa8ba)
    Identifier (LE): 47784 (0xbaa8)
    Sequence Number (BE): 40 (0x0028)
    Sequence Number (LE): 10240 (0x2800)
    [Request frame: 1270]
    [Response time: 69.855 ms]
  > Data (44 bytes)
```

Error packet:-

```
> Frame 1168: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface en0, id 0
> Ethernet II, Src: f6:06:16:a8:3c:64 (f6:06:16:a8:3c:64), Dst: Apple_15:98:3d (b0:be:83:15:98:3d)
> Internet Protocol Version 4, Src: 72.14.211.138, Dst: 172.20.10.3
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0x7e21 [correct]
    [Checksum Status: Good]
    Unused: 00
    Length: 17
    [Length of original datagram: 68]
    Unused: 0000
  > Internet Protocol Version 4, Src: 172.20.10.3, Dst: 8.8.8.8
  > Internet Control Message Protocol
```

<u>How are they different?</u>

1) Type for the last 3 ICMP packets is 0 whereas it is 11 for the error packet
2) We can see a response time in the Last 3 packets
3) The source IP for the last 3 ICMP packets is 8.8.8.8(The IP add of the website we traceroute to) where as for the error packet its 72.14.211.138

<u>Why are they different?</u>

The last 3 packets are actually replies from the destination server(google) whereas the error packets could be sent by intermediate hops/routers and signify an error.