

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

Wireshark interface showing a filter applied: `dhcp`. The packet list displays four DHCP packets:

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
7785	126.275447	0.0.0.0	255.255.255.255	DHCP	344	68	67	DHCP Discover - Transaction ID 0x16d42866
7787	126.285479	10.60.0.1	10.60.16.227	DHCP	349	67	68	DHCP Offer - Transaction ID 0x16d42866
7788	126.286181	0.0.0.0	255.255.255.255	DHCP	370	68	67	DHCP Request - Transaction ID 0x16d42866
7789	126.294278	10.60.0.1	10.60.16.227	DHCP	354	67	68	DHCP ACK - Transaction ID 0x16d42866

The packet details pane shows the selected packet (7785) and its raw data in hexadecimal and ASCII:

```
> Frame 7785: 344 bytes on wire (2752 bits), 344 bytes captured (2752 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: 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
> Dynamic Host Configuration Protocol (Discover)

0000 ff ff ff ff ff ff ff ff 67 b7 4b 77 00 00 45 00 .....g.Kw..E-
0010 01 4a 3a ae 00 00 00 11 fe f5 00 00 00 00 ff ff ..J:.....
0020 ff ff 00 44 00 43 01 36 e9 d5 01 01 00 00 16 d4 ...D.C.6.....
0030 28 66 00 00 00 00 00 00 00 00 00 00 00 00 00 (f.....
0040 00 00 00 00 00 00 d8 9c 67 b7 4b 77 00 00 00 00 .....g.Kw.....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0110 00 00 00 00 00 00 63 82 53 63 35 01 01 3d 07 01 .....c.Sc5...=
0120 d8 9c 67 b7 4b 77 32 04 0a 3c 10 e3 0c 0f 44 45 ...g.Kw2.<...DE
0130 53 4b 54 4f 50 2d 48 31 39 36 50 41 31 3c 08 4d SKTOP-H1 96PA1c-M
0140 53 46 54 20 35 2e 30 37 0e 01 03 06 0f 1f 21 2b SFT 5.07 .....l+
0150 2c 2e 2f 77 79 f9 fc ff ,./wy...
```

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

i) DHCP Request

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcpc

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
7785	126.275447	0.0.0.0	255.255.255.255	DHCP	344	68	67	DHCP Discover - Transaction ID 0x16d42866
7787	126.285479	10.60.0.1	10.60.16.227	DHCP	349	67	68	DHCP Offer - Transaction ID 0x16d42866
7788	126.286181	0.0.0.0	255.255.255.255	DHCP	370	68	67	DHCP Request - Transaction ID 0x16d42866
7789	126.294278	10.60.0.1	10.60.16.227	DHCP	354	67	68	DHCP ACK - Transaction ID 0x16d42866

> Frame 7788: 370 bytes on wire (2960 bits), 370 bytes captured (2960 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: 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

> Dynamic Host Configuration Protocol (Request)

Message type: Boot Request (3)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0x16d42866

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: HonHaiPr_b7:4b:77 (d8:9c:67:b7:4b:77)

Client hardware address padding: 00000000000000000000

Server host name not given

Boot file name not given

Magic cookie: DHCP

> Option: (53) DHCP Message Type (Request)

> Option: (61) Client identifier

> Option: (50) Requested IP Address (10.60.16.227)

> Option: (54) DHCP Server Identifier (10.1.1.2)

> Option: (12) Host Name

> Option: (81) Client Fully Qualified Domain Name

> Option: (60) Vendor class identifier

> Option: (55) Parameter Request List

> Option: (255) End

0020 ff ff 00 44 00 43 01 50 55 94 01 06 00 16 d4 ...D.C.P.U.....

0030 28 66 00 00 00 00 00 00 00 00 00 00 00 00 (f.....<.....

0040 00 00 00 00 00 00 d8 9c 67 b7 4b 77 00 00 00g.Kw.....

0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00<.....

Message type (dhcp.type), 1 byte

Packets: 126444 · Displayed: 4 (0.0%) · Dropped: 0 (0.0%) · Ignored: 10 (0.0%) Profile: Default

ii) DHCP Reply

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcpc

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
7785	126.275447	0.0.0.0	255.255.255.255	DHCP	344	68	67	DHCP Discover - Transaction ID 0x16d42866
7787	126.285479	10.60.0.1	10.60.16.227	DHCP	349	67	68	DHCP Offer - Transaction ID 0x16d42866
7788	126.286181	0.0.0.0	255.255.255.255	DHCP	370	68	67	DHCP Request - Transaction ID 0x16d42866
7789	126.294278	10.60.0.1	10.60.16.227	DHCP	354	67	68	DHCP ACK - Transaction ID 0x16d42866

> Frame 7787: 349 bytes on wire (2792 bits), 349 bytes captured (2792 bits) on interface \Device\NPF_{1D69A7D0-7B62-4AD3-9817-EED0A6A2599E}, id 0

> Ethernet II, Src: Cisco_Sa:ab:40 (28:6f:7f:5a:ab:40), Dst: HonHaiPr_b7:4b:77 (d8:9c:67:b7:4b:77)

> Internet Protocol Version 4, Src: 10.60.0.1, Dst: 10.60.16.227

> User Datagram Protocol, Src Port: 67, Dst Port: 68

> Dynamic Host Configuration Protocol (Offer)

Message type: Boot Reply (2)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0x16d42866

Seconds elapsed: 0

> Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0

Your (client) IP address: 10.60.16.227

Next server IP address: 10.1.1.2

Relay agent IP address: 10.60.0.1

Client MAC address: HonHaiPr_b7:4b:77 (d8:9c:67:b7:4b:77)

Client hardware address padding: 00000000000000000000

Server host name not given

Boot file name not given

Magic cookie: DHCP

> Option: (53) DHCP Message Type (Offer)

> Option: (1) Subnet Mask (255.255.0.0)

> Option: (58) Renewal Time Value

> Option: (59) Rebinding Time Value

> Option: (51) IP Address Lease Time

> Option: (54) DHCP Server Identifier (10.1.1.2)

> Option: (3) Router

> Option: (6) Domain Name Server

> Option: (15) Domain Name

0020 10 e3 00 43 00 44 01 3b bd a9 02 01 06 00 16 d4 ...C.D.;.....

0030 28 66 00 00 00 00 00 00 00 00 0a 3c 10 e3 0a 01 (f.....<.....

0040 01 02 0a 3c 00 01 d8 9c 67 b7 4b 77 00 00 00g.Kw.....

0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00<.....

Message type (dhcp.type), 1 byte

Packets: 126645 · Displayed: 4 (0.0%) · Ignored: 7 (0.0%) Profile: Default

iii) DHCP ACK

The image shows a Wireshark packet capture of a DHCP ACK message. The packet list at the top shows four packets: 7785 (DHCP Discover), 7787 (DHCP Offer), 7788 (DHCP Request), and 7789 (DHCP ACK). The selected packet 7789 is expanded in the packet details pane, showing the following structure:

- Dynamic Host Configuration Protocol (ACK)
- Message type: Boot Reply (2)
- Hardware type: Ethernet (0x01)
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0x16d42866
- Seconds elapsed: 0
- Bootp flags: 0x0000 (Unicast)
- 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
- Client MAC address: HonHaiPr_b7:4b:77 (d8:9c:67:b7:4b:77)
- Client hardware address padding: 00000000000000000000
- Server host name not given
- Boot file name not given
- Magic cookie: DHCP
- Option: (53) DHCP Message Type (ACK)
- Option: (58) Renewal Time Value
- Option: (59) Rebinding Time Value
- Option: (51) IP Address Lease Time
- Option: (54) DHCP Server Identifier (10.1.1.2)
- Option: (1) Subnet Mask (255.255.0.0)
- Option: (81) Client Fully Qualified Domain Name
- Option: (3) Router
- Option: (6) Domain Name Server

The packet bytes pane at the bottom shows the raw data of the DHCP ACK packet, with the first 4 bytes highlighted as the message type (dhcp.type), 1 byte.

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

The image shows a Wireshark packet capture of a DHCP ACK message, similar to the one above. The packet list at the top shows four packets: 7785 (DHCP Discover), 7787 (DHCP Offer), 7788 (DHCP Request), and 7789 (DHCP ACK). The selected packet 7789 is expanded in the packet details pane, showing the following structure:

- Dynamic Host Configuration Protocol (ACK)
- Message type: Boot Reply (2)
- Hardware type: Ethernet (0x01)
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0x16d42866
- Seconds elapsed: 0
- Bootp flags: 0x0000 (Unicast)
- 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
- Client MAC address: HonHaiPr_b7:4b:77 (d8:9c:67:b7:4b:77)
- Client hardware address padding: 00000000000000000000
- Server host name not given
- Boot file name not given
- Magic cookie: DHCP
- Option: (53) DHCP Message Type (ACK)
- Option: (58) Renewal Time Value
- Option: (59) Rebinding Time Value
- Option: (51) IP Address Lease Time
- Option: (54) DHCP Server Identifier (10.1.1.2)
- Option: (1) Subnet Mask (255.255.0.0)
- Option: (81) Client Fully Qualified Domain Name
- Option: (3) Router
- Option: (6) Domain Name Server

The packet bytes pane at the bottom shows the raw data of the DHCP ACK packet, with the first 4 bytes highlighted as the message type (dhcp.type), 1 byte.

Client IP address: 0.0.0.0

Your (client) IP address: 10.60.16.227

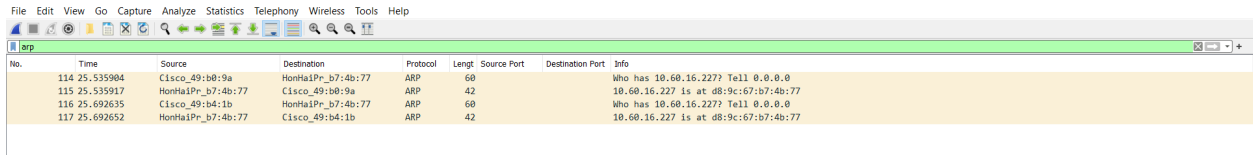
Next server IP address: 0.0.0.0

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.

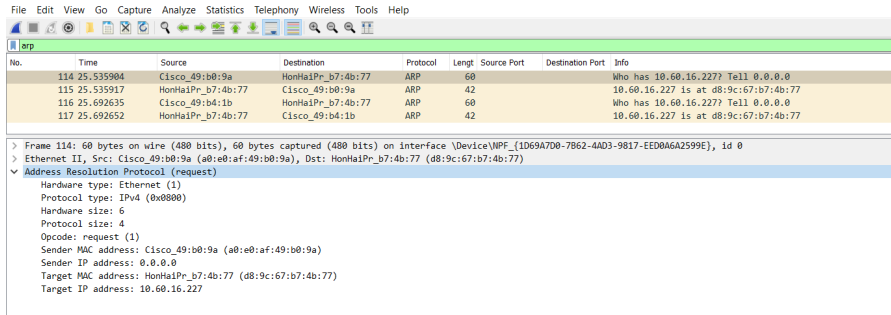


Wireshark interface showing the ARP table. The table has columns: No., Time, Source, Destination, Protocol, Length, Source Port, Destination Port, and Info.

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
114	25.535984	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.

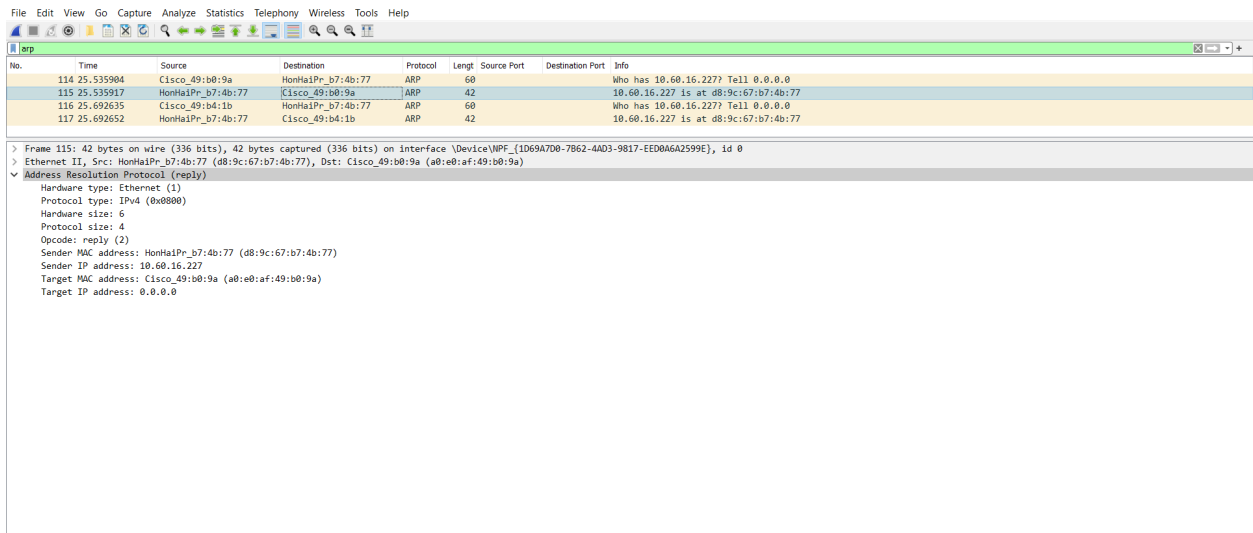
ARP Request



Wireshark interface showing the details of the ARP request (Frame 114). The details pane shows the following information:

- Frame 114: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{1D69A7D0-7B62-4A03-9817-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)
- 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



Wireshark interface showing the details of the ARP reply (Frame 115). The details pane shows the following information:

- Frame 115: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{1D69A7D0-7B62-4A03-9817-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)
- 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).

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

No.	Time	Source	Destination	Protocol	Length	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)

✓ Address Resolution Protocol (reply)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x8800)

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

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)

```
Time      | Protocol | Source Add | Source Port | Destination Add | Destination Port | HTTP Host | HTTPS server | Info
21:35:27.456398 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=1/256, ttl=1 (no response found!)
21:35:27.461653 | ICMP | 172.20.10.1 | 172.20.10.3 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=2/512, ttl=1 (no response found!)
21:35:27.463069 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=3/768, ttl=1 (no response found!)
21:35:27.467020 | ICMP | 172.20.10.1 | 172.20.10.3 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=4/1024, ttl=2 (no response found!)
21:35:27.467121 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=5/1280, ttl=2 (no response found!)
21:35:27.472028 | ICMP | 172.20.10.1 | 172.20.10.3 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=6/1536, ttl=2 (no response found!)
21:35:27.472140 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=7/1792, ttl=3 (no response found!)
21:35:32.473847 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=8/2048, ttl=3 (no response found!)
21:35:37.474406 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=9/2304, ttl=3 (no response found!)
21:35:42.475549 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=10/2560, ttl=4 (no response found!)
21:35:42.529886 | ICMP | 56.14.35.233 | 172.20.10.3 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=11/2816, ttl=4 (no response found!)
21:35:42.531349 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=12/3072, ttl=4 (no response found!)
21:35:42.589024 | ICMP | 56.14.35.229 | 172.20.10.3 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=13/3328, ttl=4 (no response found!)
21:35:42.590520 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=14/3584, ttl=5 (no response found!)
21:35:42.652444 | ICMP | 56.14.35.237 | 172.20.10.3 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=15/3840, ttl=5 (no response found!)
21:35:43.096011 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=16/4096, ttl=5 (no response found!)
21:35:43.170372 | ICMP | 192.168.76... | 172.20.10.3 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=17/4352, ttl=5 (no response found!)
21:35:43.320302 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=18/4608, ttl=5 (no response found!)
21:35:43.402669 | ICMP | 192.168.76... | 172.20.10.3 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=19/4864, ttl=5 (no response found!)
21:35:43.404273 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=20/5120, ttl=5 (no response found!)
21:35:43.460174 | ICMP | 192.168.76... | 172.20.10.3 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=21/5376, ttl=5 (no response found!)
21:35:43.460435 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=22/5632, ttl=5 (no response found!)
21:35:43.522480 | ICMP | 192.168.76... | 172.20.10.3 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=23/5888, ttl=5 (no response found!)
21:35:43.523973 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=24/6144, ttl=5 (no response found!)
21:35:43.585042 | ICMP | 192.168.76... | 172.20.10.3 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=25/6400, ttl=5 (no response found!)
21:35:43.585407 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=26/6656, ttl=5 (no response found!)
21:35:43.652315 | ICMP | 192.168.165... | 172.20.10.3 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=27/6912, ttl=5 (no response found!)

> Frame 714: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface en0, id 0
> Ethernet II, Src: Apple_15:98:3d (b0:be:83:15:98:3d), Dst: f6:06:16:a8:3c:64 (f6:06:16:a8:3c:64)
> Internet Protocol Version 4, Src: 172.20.10.3, Dst: 8.8.8.8
> Internet Control Message Protocol

0000  f6 06 16 a8 3c 64 b0 be 83 15 98 3d 08 00 45 00  ....<d...-E
0010  00 48 a8 bb 00 00 01 01 4a d3 ac 14 0a 03 08 08  H.....J.....
0020  08 08 08 00 4f 44 a8 ba 00 01 00 00 00 00 00 00  OD.....
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 00 00 00 00 00 00 00 00 00 00
```

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

```
21:35:27.463069 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=2/512, ttl=1
> Frame 714: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface en0, id 0
> Ethernet II, Src: Apple_15:98:3d (b0:be:83:15:98:3d), Dst: f6:06:16:a8:3c:64 (f6:06:16:a8:3c:64)
> Internet Protocol Version 4, Src: 172.20.10.3, Dst: 8.8.8.8
> Internet Control Message Protocol
```

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)

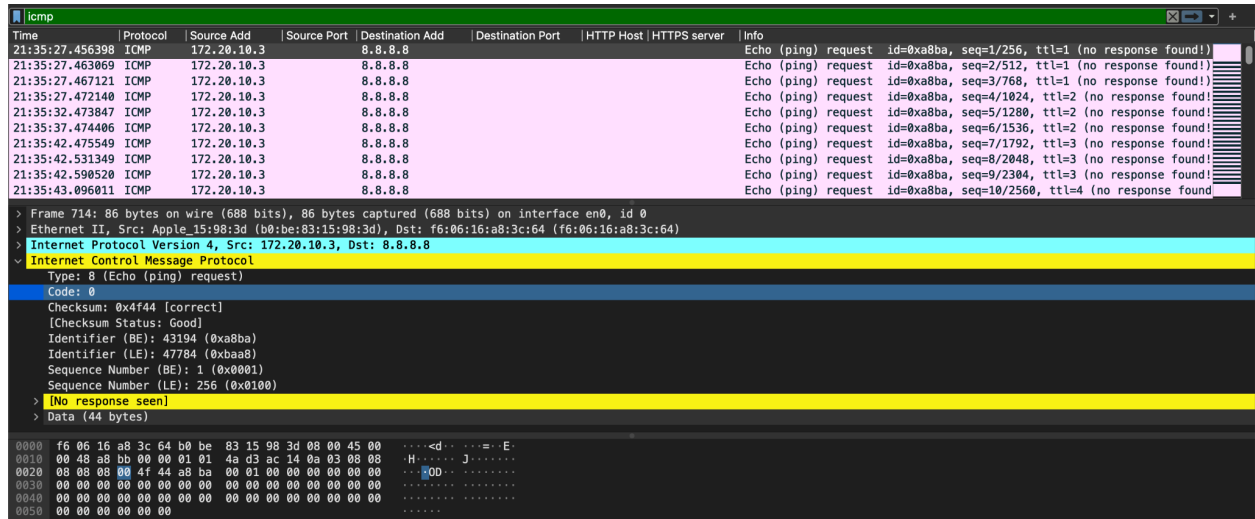
Type byte is highlighted:- Type byte = 8

```
Time      | Protocol | Source Add | Source Port | Destination Add | Destination Port | HTTP Host | HTTPS server | Info
21:35:27.456398 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=1/256, ttl=1 (no response found!)
21:35:27.463069 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=2/512, ttl=1 (no response found!)
21:35:27.467121 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=3/768, ttl=1 (no response found!)
21:35:27.472140 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=4/1024, ttl=2 (no response found!)
21:35:32.473847 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=5/1280, ttl=2 (no response found!)
21:35:37.474406 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=6/1536, ttl=2 (no response found!)
21:35:42.475549 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=7/1792, ttl=3 (no response found!)
21:35:42.531349 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=8/2048, ttl=3 (no response found!)
21:35:42.590520 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=9/2304, ttl=3 (no response found!)
21:35:43.096011 | ICMP | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | 172.20.10.3 | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=10/2560, ttl=4 (no response found!)

> Frame 714: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface en0, id 0
> Ethernet II, Src: Apple_15:98:3d (b0:be:83:15:98:3d), Dst: f6:06:16:a8:3c:64 (f6:06:16:a8:3c:64)
> Internet Protocol Version 4, Src: 172.20.10.3, Dst: 8.8.8.8
> Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4f44 [correct]
  [Checksum Status: Good]
  Identifier (BE): 43194 (0xa8ba)
  Identifier (LE): 47784 (0xbaa8)
  Sequence Number (BE): 1 (0x0001)
  Sequence Number (LE): 256 (0x0100)
> [No response seen]
> Data (44 bytes)

0000  f6 06 16 a8 3c 64 b0 be 83 15 98 3d 08 00 45 00  ....<d...-E
0010  00 48 a8 bb 00 00 01 01 4a d3 ac 14 0a 03 08 08  H.....J.....
0020  08 08 08 00 4f 44 a8 ba 00 01 00 00 00 00 00 00  OD.....
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 00 00 00 00 00 00 00 00 00 00
```

Code byte is highlighted :- Code byte = 0

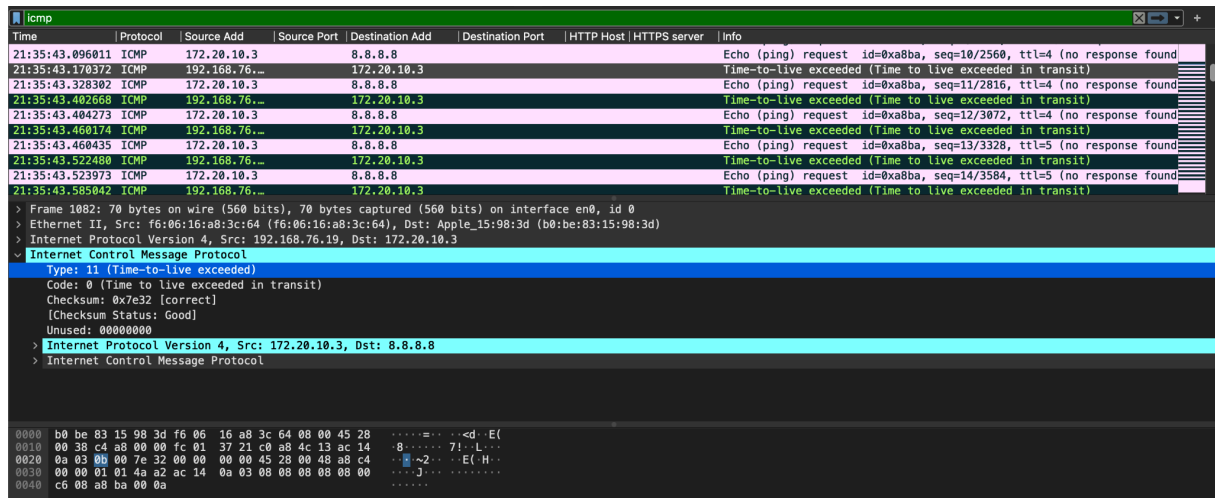


```
Time | Protocol | Source Add | Source Port | Destination Add | Destination Port | HTTP Host | HTTPS server | Info
21:35:27.456398 ICMP | 172.20.10.3 | | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=1/256, ttl=1 (no response found!)
21:35:27.463869 ICMP | 172.20.10.3 | | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=2/512, ttl=1 (no response found!)
21:35:27.467121 ICMP | 172.20.10.3 | | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=3/768, ttl=1 (no response found!)
21:35:27.472140 ICMP | 172.20.10.3 | | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=4/1024, ttl=2 (no response found!)
21:35:32.473847 ICMP | 172.20.10.3 | | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=5/1280, ttl=2 (no response found!)
21:35:37.474406 ICMP | 172.20.10.3 | | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=6/1536, ttl=2 (no response found!)
21:35:42.475549 ICMP | 172.20.10.3 | | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=7/1792, ttl=3 (no response found!)
21:35:42.531349 ICMP | 172.20.10.3 | | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=8/2048, ttl=3 (no response found!)
21:35:42.590525 ICMP | 172.20.10.3 | | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=9/2304, ttl=3 (no response found!)
21:35:43.096011 ICMP | 172.20.10.3 | | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=10/2560, ttl=4 (no response found!)

> Frame 714: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface en0, id 0
> Ethernet II, Src: Apple_15:98:3d (b0:be:83:15:98:3d), Dst: f6:06:16:a8:3c:64 (f6:06:16:a8:3c:64)
> Internet Protocol Version 4, Src: 172.20.10.3, Dst: 8.8.8.8
> Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4f44 [correct]
  [Checksum Status: Good]
  Identifier (BE): 43194 (0xa8ba)
  Identifier (LE): 47784 (0xbaa8)
  Sequence Number (BE): 1 (0x0001)
  Sequence Number (LE): 256 (0x0100)
  [No response seen]
  Data (44 bytes)
  0000 f6 06 16 a8 3c 64 b0 be 83 15 98 3d 08 00 45 00 .....<d.....E
  0010 00 48 a8 bb 00 00 01 01 4a d3 ac 14 0a 03 08 08 .....H.....
  0020 08 08 08 00 4f 4a a8 ba 00 01 00 00 00 00 00 00 .....00.....
  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 00 00 00 00 00 00 00 00 00 00 .....
```

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)

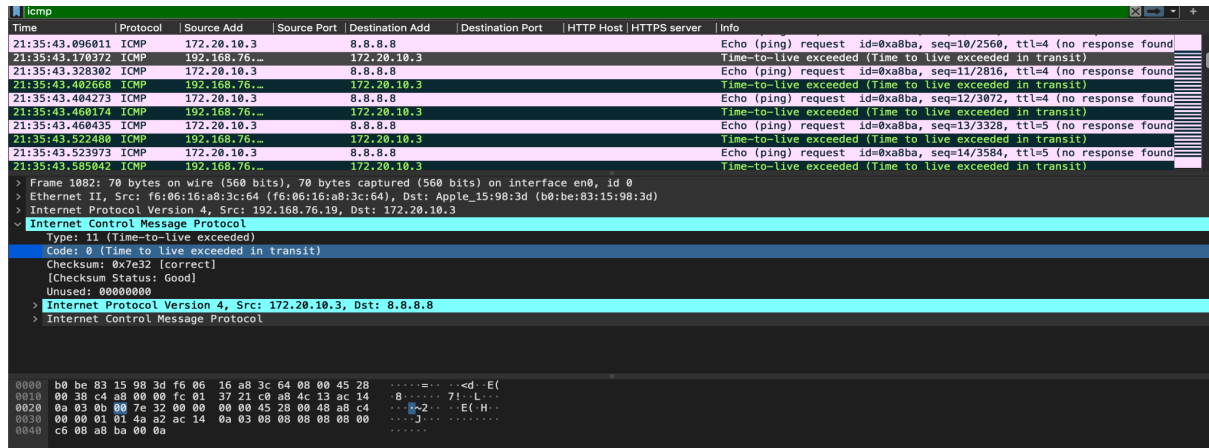
Type byte for error packet : 11



```
Time | Protocol | Source Add | Source Port | Destination Add | Destination Port | HTTP Host | HTTPS server | Info
21:35:43.096011 ICMP | 172.20.10.3 | | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=10/2560, ttl=4 (no response found)
21:35:43.170372 ICMP | 192.168.76.19 | 172.20.10.3 | Time-to-live exceeded (Time to live exceeded in transit)
21:35:43.328302 ICMP | 172.20.10.3 | | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=11/2816, ttl=4 (no response found)
21:35:43.402668 ICMP | 192.168.76.19 | 172.20.10.3 | Time-to-live exceeded (Time to live exceeded in transit)
21:35:43.404273 ICMP | 172.20.10.3 | | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=12/3072, ttl=4 (no response found)
21:35:43.460174 ICMP | 192.168.76.19 | 172.20.10.3 | Time-to-live exceeded (Time to live exceeded in transit)
21:35:43.460435 ICMP | 172.20.10.3 | | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=13/3328, ttl=5 (no response found)
21:35:43.522480 ICMP | 192.168.76.19 | 172.20.10.3 | Time-to-live exceeded (Time to live exceeded in transit)
21:35:43.523973 ICMP | 172.20.10.3 | | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=14/3584, ttl=5 (no response found)
21:35:43.585042 ICMP | 192.168.76.19 | 172.20.10.3 | Time-to-live exceeded (Time to live exceeded in transit)

> Frame 1082: 70 bytes on wire (560 bits), 70 bytes captured (560 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: 192.168.76.19, Dst: 172.20.10.3
> Internet Control Message Protocol
  Type: 11 (Time-to-live exceeded)
  Code: 0 (Time to live exceeded in transit)
  Checksum: 0x7e32 [correct]
  [Checksum Status: Good]
  Unused: 00000000
  > Internet Protocol Version 4, Src: 172.20.10.3, Dst: 8.8.8.8
  > Internet Control Message Protocol
  0000 b0 be 83 15 98 3d f6 06 16 a8 3c 64 08 00 45 28 .....<d.....E
  0010 00 38 c4 a8 00 00 fc 01 37 21 c0 a8 4c 13 ac 14 .....8.....7!.....
  0020 0a 03 00 00 7e 32 00 00 00 00 45 28 00 48 a8 c4 .....~2.....E(H..
  0030 00 00 01 01 4a a2 ac 14 0a 03 08 08 08 08 08 00 .....J.....
  0040 c6 08 a8 ba 00 0a .....
```

Code Byte for error packet is highlighted = 0



```
Time | Protocol | Source Add | Source Port | Destination Add | Destination Port | HTTP Host | HTTPS server | Info
21:35:43.096011 ICMP | 172.20.10.3 | | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=10/2560, ttl=4 (no response found)
21:35:43.170372 ICMP | 192.168.76.19 | 172.20.10.3 | Time-to-live exceeded (Time to live exceeded in transit)
21:35:43.328302 ICMP | 172.20.10.3 | | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=11/2816, ttl=4 (no response found)
21:35:43.402668 ICMP | 192.168.76.19 | 172.20.10.3 | Time-to-live exceeded (Time to live exceeded in transit)
21:35:43.404273 ICMP | 172.20.10.3 | | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=12/3072, ttl=4 (no response found)
21:35:43.460174 ICMP | 192.168.76.19 | 172.20.10.3 | Time-to-live exceeded (Time to live exceeded in transit)
21:35:43.460435 ICMP | 172.20.10.3 | | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=13/3328, ttl=5 (no response found)
21:35:43.522480 ICMP | 192.168.76.19 | 172.20.10.3 | Time-to-live exceeded (Time to live exceeded in transit)
21:35:43.523973 ICMP | 172.20.10.3 | | 8.8.8.8 | Echo (ping) request id=0xa8ba, seq=14/3584, ttl=5 (no response found)
21:35:43.585042 ICMP | 192.168.76.19 | 172.20.10.3 | Time-to-live exceeded (Time to live exceeded in transit)

> Frame 1082: 70 bytes on wire (560 bits), 70 bytes captured (560 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: 192.168.76.19, Dst: 172.20.10.3
> Internet Control Message Protocol
  Type: 11 (Time-to-live exceeded)
  Code: 0 (Time to live exceeded in transit)
  Checksum: 0x7e32 [correct]
  [Checksum Status: Good]
  Unused: 00000000
  > Internet Protocol Version 4, Src: 172.20.10.3, Dst: 8.8.8.8
  > Internet Control Message Protocol
  0000 b0 be 83 15 98 3d f6 06 16 a8 3c 64 08 00 45 28 .....<d.....E
  0010 00 38 c4 a8 00 00 fc 01 37 21 c0 a8 4c 13 ac 14 .....8.....7!.....
  0020 0a 03 00 00 7e 32 00 00 00 00 45 28 00 48 a8 c4 .....~2.....E(H..
  0030 00 00 01 01 4a a2 ac 14 0a 03 08 08 08 08 08 00 .....J.....
  0040 c6 08 a8 ba 00 0a .....
```


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
> 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  ....p.....
  0020  0a 03 00 00 57 1b a8 ba 00 2a 00 00 00 00 00 00  ..M.....
  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 00 00 00 00 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
> 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
> 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

```

How are they different?

- 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

Why are they different?

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.