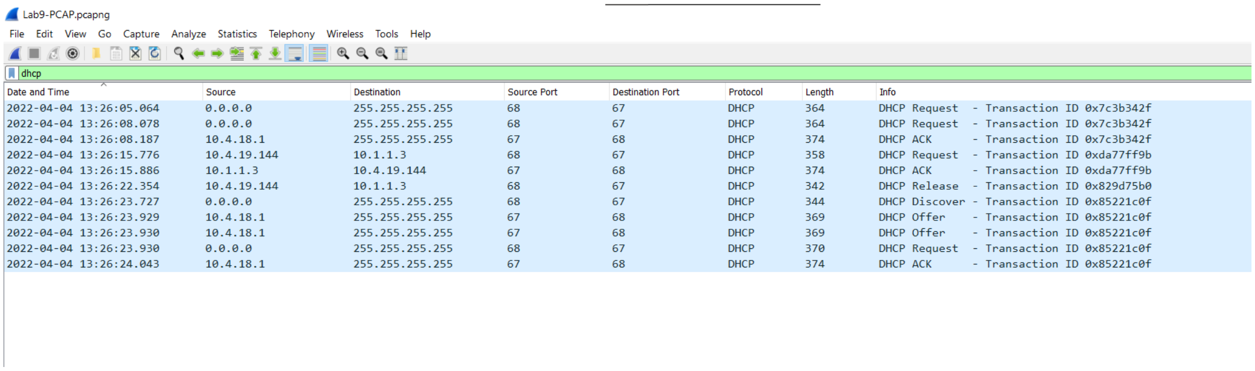
LAB 9 - Wireshark - ARP, DHCP, and ICMP

NAME - DEV GOEL
ID - 2019A7PS0236G

Q1. Show a round of execution of the DHCP protocol. Write the filter and show the output in a screenshot.

Filter - dhcp

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


Lab9-PCAP.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp

Date and Time	Source	Destination	Source Port	Destination Port	Protocol	Length	Info
2022-04-04 13:26:05.064	0.0.0.0	255.255.255.255	68	67	DHCP	364	DHCP Request - Transaction ID 0x7c3b342f
2022-04-04 13:26:08.078	0.0.0.0	255.255.255.255	68	67	DHCP	364	DHCP Request - Transaction ID 0x7c3b342f
2022-04-04 13:26:08.187	10.4.18.1	255.255.255.255	67	68	DHCP	374	DHCP ACK - Transaction ID 0x7c3b342f
2022-04-04 13:26:15.776	10.4.19.144	10.1.1.3	68	67	DHCP	358	DHCP Request - Transaction ID 0xda77ff9b
2022-04-04 13:26:15.886	10.1.1.3	10.4.19.144	67	68	DHCP	374	DHCP ACK - Transaction ID 0xda77ff9b
2022-04-04 13:26:22.354	10.4.19.144	10.1.1.3	68	67	DHCP	342	DHCP Release - Transaction ID 0x829d75b0
2022-04-04 13:26:23.727	0.0.0.0	255.255.255.255	68	67	DHCP	344	DHCP Discover - Transaction ID 0x85221c0f
2022-04-04 13:26:23.929	10.4.18.1	255.255.255.255	67	68	DHCP	369	DHCP Offer - Transaction ID 0x85221c0f
2022-04-04 13:26:23.930	10.4.18.1	255.255.255.255	67	68	DHCP	369	DHCP Offer - Transaction ID 0x85221c0f
2022-04-04 13:26:23.930	0.0.0.0	255.255.255.255	68	67	DHCP	370	DHCP Request - Transaction ID 0x85221c0f
2022-04-04 13:26:24.043	10.4.18.1	255.255.255.255	67	68	DHCP	374	DHCP ACK - Transaction ID 0x85221c0f

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

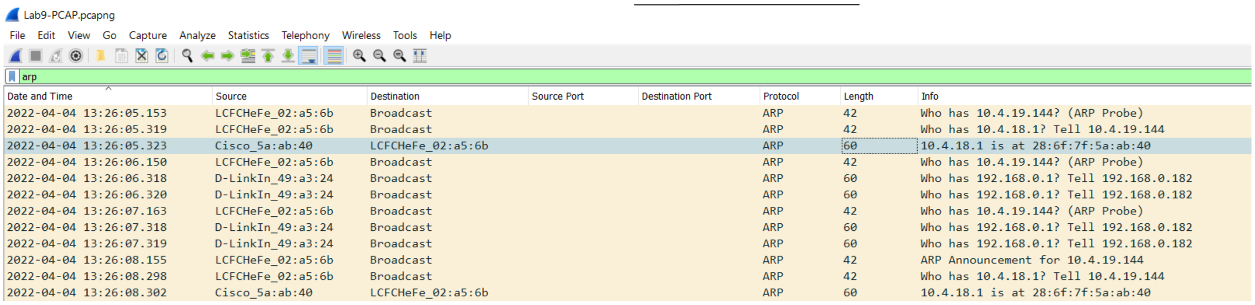
To find the IP address of the DHCP server and client, one of the multiple ways is to look at the ‘DHCP Release’ packet. The destination address in this is the DHCP server address, and the source address is the client address.
Therefore,

- ***DHCP server address*** - 10.1.1.3
- ***DHCP client address*** - 10.4.19.144

Q2. Show a round of execution of the ARP protocol. Write the filter and show the output in a screenshot.

Filter - arp

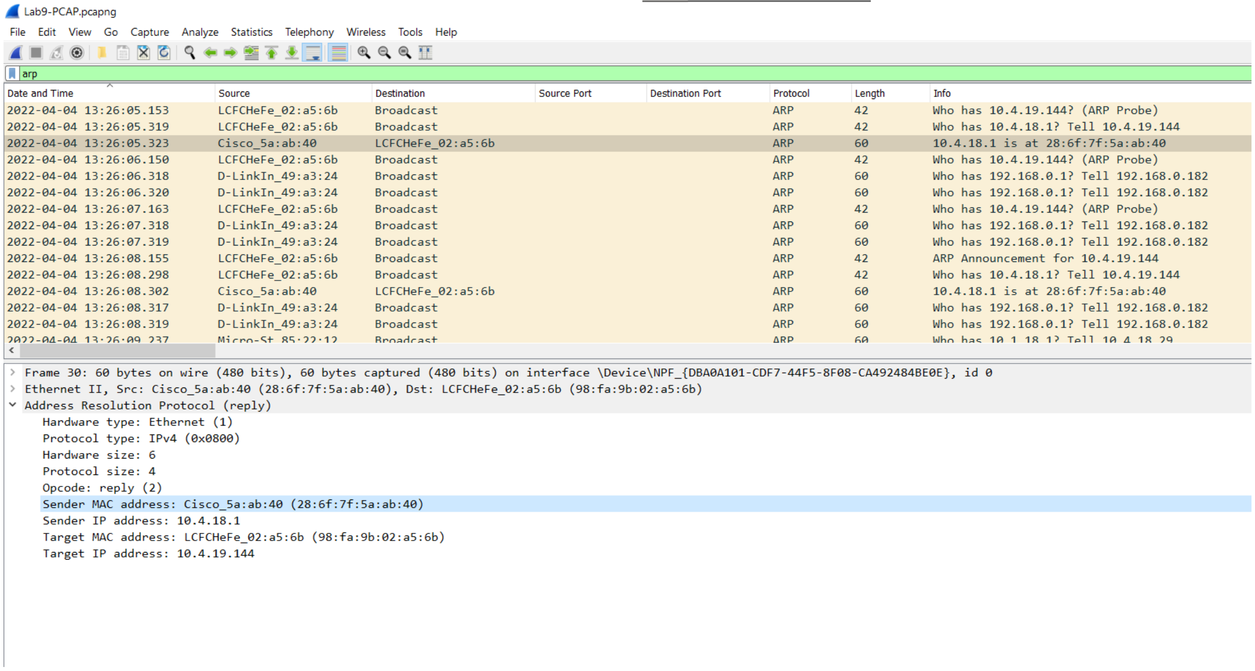
a. Show ARP Request (2 marks) and Reply (2 marks) messages in that round


Lab9-PCAP.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

Date and Time	Source	Destination	Source Port	Destination Port	Protocol	Length	Info
2022-04-04 13:26:05.153	LCFCHeFe_02:a5:6b	Broadcast			ARP	42	Who has 10.4.19.144? (ARP Probe)
2022-04-04 13:26:05.319	LCFCHeFe_02:a5:6b	Broadcast			ARP	42	Who has 10.4.18.1? Tell 10.4.19.144
2022-04-04 13:26:05.323	Cisco_5a:ab:40	LCFCHeFe_02:a5:6b			ARP	60	10.4.18.1 is at 28:6f:7f:5a:ab:40
2022-04-04 13:26:06.150	LCFCHeFe_02:a5:6b	Broadcast			ARP	42	Who has 10.4.19.144? (ARP Probe)
2022-04-04 13:26:06.318	D-LinkIn_49:a3:24	Broadcast			ARP	60	Who has 192.168.0.1? Tell 192.168.0.182
2022-04-04 13:26:06.320	D-LinkIn_49:a3:24	Broadcast			ARP	60	Who has 192.168.0.1? Tell 192.168.0.182
2022-04-04 13:26:07.163	LCFCHeFe_02:a5:6b	Broadcast			ARP	42	Who has 10.4.19.144? (ARP Probe)
2022-04-04 13:26:07.318	D-LinkIn_49:a3:24	Broadcast			ARP	60	Who has 192.168.0.1? Tell 192.168.0.182
2022-04-04 13:26:07.319	D-LinkIn_49:a3:24	Broadcast			ARP	60	Who has 192.168.0.1? Tell 192.168.0.182
2022-04-04 13:26:08.155	LCFCHeFe_02:a5:6b	Broadcast			ARP	42	ARP Announcement for 10.4.19.144
2022-04-04 13:26:08.298	LCFCHeFe_02:a5:6b	Broadcast			ARP	42	Who has 10.4.18.1? Tell 10.4.19.144
2022-04-04 13:26:08.302	Cisco_5a:ab:40	LCFCHeFe_02:a5:6b			ARP	60	10.4.18.1 is at 28:6f:7f:5a:ab:40

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


Lab9-PCAP.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

Date and Time	Source	Destination	Source Port	Destination Port	Protocol	Length	Info
2022-04-04 13:26:05.153	LCFCHeFe_02:a5:6b	Broadcast			ARP	42	Who has 10.4.19.144? (ARP Probe)
2022-04-04 13:26:05.319	LCFCHeFe_02:a5:6b	Broadcast			ARP	42	Who has 10.4.18.1? Tell 10.4.19.144
2022-04-04 13:26:05.323	Cisco_5a:ab:40	LCFCHeFe_02:a5:6b			ARP	60	10.4.18.1 is at 28:6f:7f:5a:ab:40
2022-04-04 13:26:06.150	LCFCHeFe_02:a5:6b	Broadcast			ARP	42	Who has 10.4.19.144? (ARP Probe)
2022-04-04 13:26:06.318	D-LinkIn_49:a3:24	Broadcast			ARP	60	Who has 192.168.0.1? Tell 192.168.0.182
2022-04-04 13:26:06.320	D-LinkIn_49:a3:24	Broadcast			ARP	60	Who has 192.168.0.1? Tell 192.168.0.182
2022-04-04 13:26:07.163	LCFCHeFe_02:a5:6b	Broadcast			ARP	42	Who has 10.4.19.144? (ARP Probe)
2022-04-04 13:26:07.318	D-LinkIn_49:a3:24	Broadcast			ARP	60	Who has 192.168.0.1? Tell 192.168.0.182
2022-04-04 13:26:07.319	D-LinkIn_49:a3:24	Broadcast			ARP	60	Who has 192.168.0.1? Tell 192.168.0.182
2022-04-04 13:26:08.155	LCFCHeFe_02:a5:6b	Broadcast			ARP	42	ARP Announcement for 10.4.19.144
2022-04-04 13:26:08.298	LCFCHeFe_02:a5:6b	Broadcast			ARP	42	Who has 10.4.18.1? Tell 10.4.19.144
2022-04-04 13:26:08.302	Cisco_5a:ab:40	LCFCHeFe_02:a5:6b			ARP	60	10.4.18.1 is at 28:6f:7f:5a:ab:40
2022-04-04 13:26:08.317	D-LinkIn_49:a3:24	Broadcast			ARP	60	Who has 192.168.0.1? Tell 192.168.0.182
2022-04-04 13:26:08.319	D-LinkIn_49:a3:24	Broadcast			ARP	60	Who has 192.168.0.1? Tell 192.168.0.182
2022-04-04 13:26:09.237	Micro-St_85:22:12	Broadcast			ARP	60	Who has 10.4.18.1? Tell 10.4.18.29

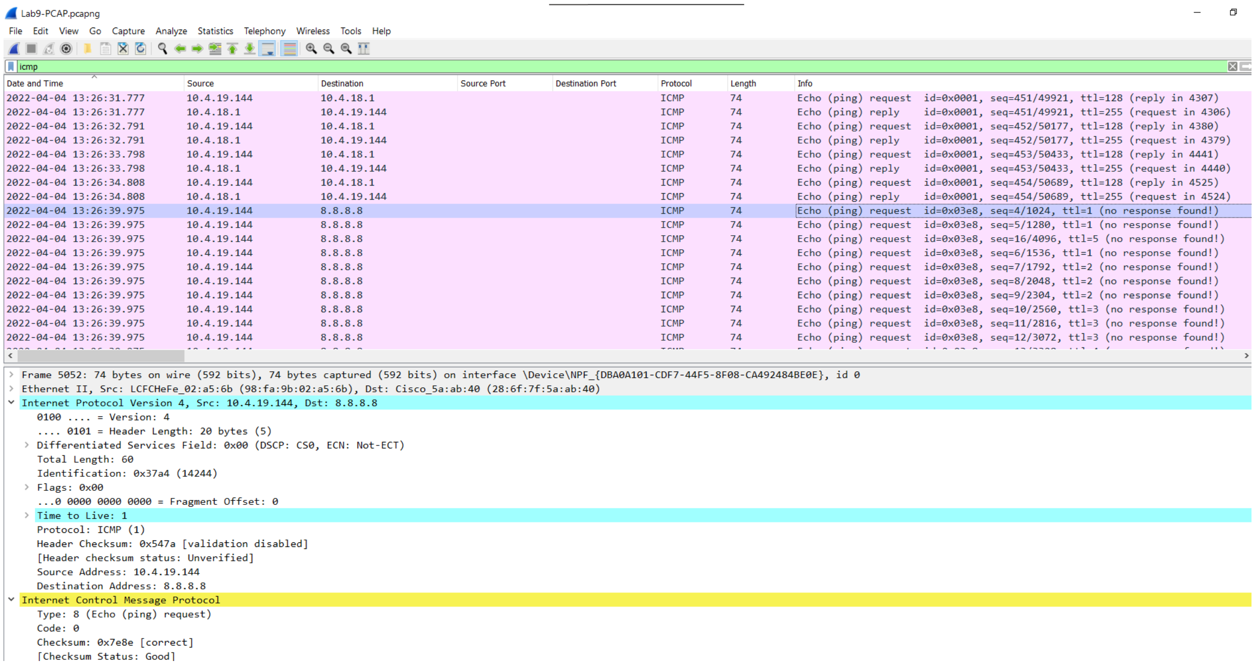
```
> Frame 30: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{DBA0A101-CDF7-44F5-8F08-CA492484BE0E}, id 0
> Ethernet II, Src: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40), Dst: LCFCHeFe_02:a5:6b (98:fa:9b:02:a5:6b)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40)
    Sender IP address: 10.4.18.1
    Target MAC address: LCFCHeFe_02:a5:6b (98:fa:9b:02:a5:6b)
    Target IP address: 10.4.19.144
```

We can see the sender MAC address in the ARP reply packet.

The MAC address is - 28:6f:7f:5a:ab:40

Q3. Show a round of execution of the `traceroute’ command for dns.google.

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


Lab9-PCAP.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

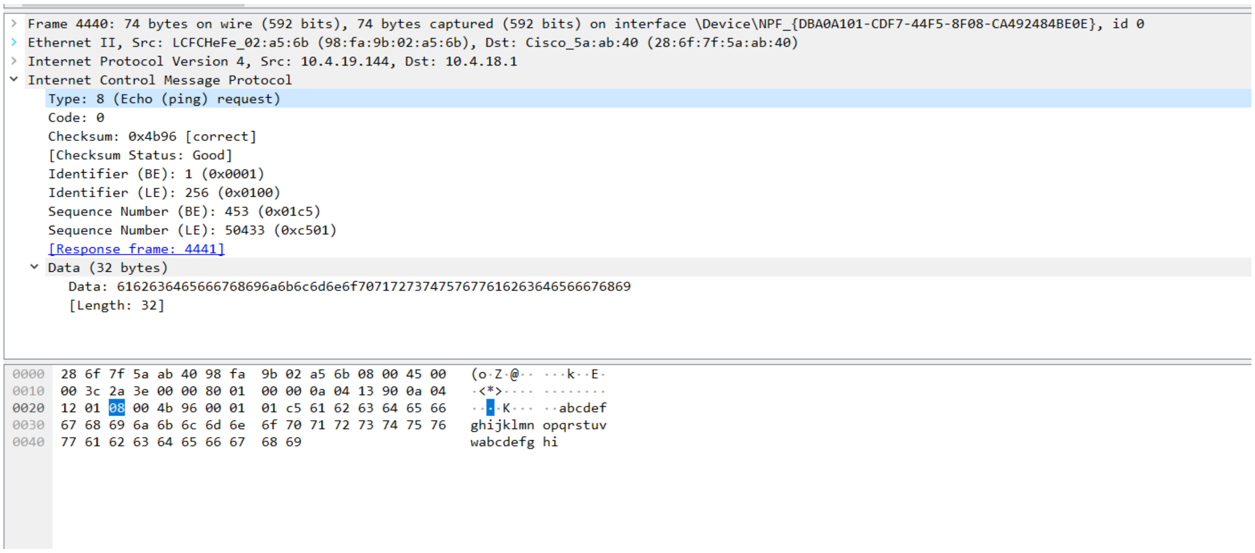
icmp

Date and Time	Source	Destination	Source Port	Destination Port	Protocol	Length	Info
2022-04-04 13:26:31.777	10.4.19.144	10.4.18.1			ICMP	74	Echo (ping) request id=0x0001, seq=451/49921, ttl=128 (reply in 4307)
2022-04-04 13:26:31.777	10.4.18.1	10.4.19.144			ICMP	74	Echo (ping) reply id=0x0001, seq=451/49921, ttl=255 (request in 4306)
2022-04-04 13:26:32.791	10.4.19.144	10.4.18.1			ICMP	74	Echo (ping) request id=0x0001, seq=452/50177, ttl=128 (reply in 4380)
2022-04-04 13:26:32.791	10.4.18.1	10.4.19.144			ICMP	74	Echo (ping) reply id=0x0001, seq=452/50177, ttl=255 (request in 4379)
2022-04-04 13:26:33.798	10.4.19.144	10.4.18.1			ICMP	74	Echo (ping) request id=0x0001, seq=453/50433, ttl=128 (reply in 4441)
2022-04-04 13:26:33.798	10.4.18.1	10.4.19.144			ICMP	74	Echo (ping) reply id=0x0001, seq=453/50433, ttl=255 (request in 4440)
2022-04-04 13:26:34.808	10.4.19.144	10.4.18.1			ICMP	74	Echo (ping) request id=0x0001, seq=454/50689, ttl=128 (reply in 4525)
2022-04-04 13:26:34.808	10.4.18.1	10.4.19.144			ICMP	74	Echo (ping) reply id=0x0001, seq=454/50689, ttl=255 (request in 4524)
2022-04-04 13:26:39.975	10.4.19.144	8.8.8.8			ICMP	74	Echo (ping) request id=0x03e8, seq=4/1024, ttl=1 (no response found!)
2022-04-04 13:26:39.975	10.4.19.144	8.8.8.8			ICMP	74	Echo (ping) request id=0x03e8, seq=5/1280, ttl=1 (no response found!)
2022-04-04 13:26:39.975	10.4.19.144	8.8.8.8			ICMP	74	Echo (ping) request id=0x03e8, seq=16/4096, ttl=5 (no response found!)
2022-04-04 13:26:39.975	10.4.19.144	8.8.8.8			ICMP	74	Echo (ping) request id=0x03e8, seq=6/1536, ttl=1 (no response found!)
2022-04-04 13:26:39.975	10.4.19.144	8.8.8.8			ICMP	74	Echo (ping) request id=0x03e8, seq=7/1792, ttl=2 (no response found!)
2022-04-04 13:26:39.975	10.4.19.144	8.8.8.8			ICMP	74	Echo (ping) request id=0x03e8, seq=8/2048, ttl=2 (no response found!)
2022-04-04 13:26:39.975	10.4.19.144	8.8.8.8			ICMP	74	Echo (ping) request id=0x03e8, seq=9/2304, ttl=2 (no response found!)
2022-04-04 13:26:39.975	10.4.19.144	8.8.8.8			ICMP	74	Echo (ping) request id=0x03e8, seq=10/2560, ttl=3 (no response found!)
2022-04-04 13:26:39.975	10.4.19.144	8.8.8.8			ICMP	74	Echo (ping) request id=0x03e8, seq=11/2816, ttl=3 (no response found!)
2022-04-04 13:26:39.975	10.4.19.144	8.8.8.8			ICMP	74	Echo (ping) request id=0x03e8, seq=12/3072, ttl=3 (no response found!)

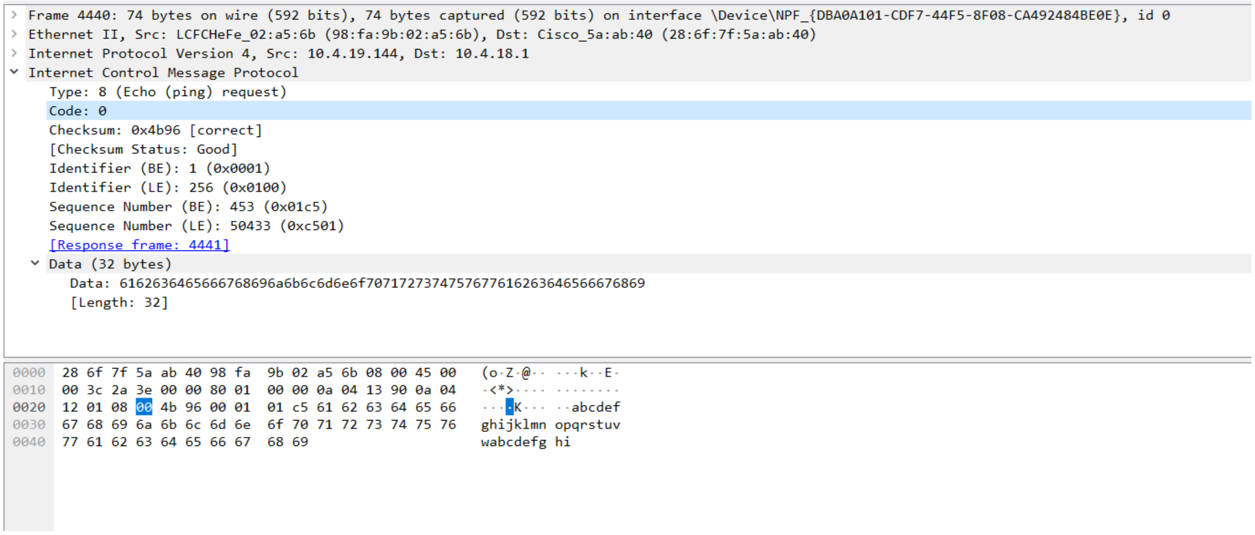
```
> Frame 5052: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{DBA0A101-CDF7-44F5-8F08-CA492484BE0E}, id 0
> Ethernet II, Src: LCFCHeFe_02:a5:6b (98:fa:9b:02:a5:6b), Dst: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40)
v Internet Protocol Version 4, Src: 10.4.19.144, Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x37a4 (14244)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x547a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.4.19.144
    Destination Address: 8.8.8.8
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x7e8e [correct]
    [Checksum Status: Good]
```

The IP address of the host - 10.4.19.144
The IP address of the destination (dns.google) - 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)



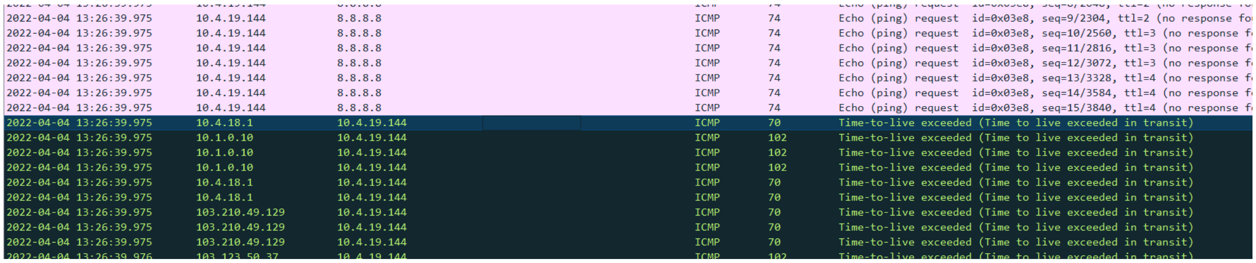
```
> Frame 4440: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{DBA0A101-CDF7-44F5-8F08-CA492484BE0E}, id 0
> Ethernet II, Src: LCFCHeFe_02:a5:6b (98:fa:9b:02:a5:6b), Dst: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40)
> Internet Protocol Version 4, Src: 10.4.19.144, Dst: 10.4.18.1
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4b96 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 453 (0x01c5)
    Sequence Number (LE): 50433 (0xc501)
    [Response frame: 4441]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]

0000  28 6f 7f 5a ab 40 98 fa  9b 02 a5 6b 08 00 45 00   (o·Z·@··  ···k··E·
0010  00 3c 2a 3e 00 00 80 01  00 00 0a 04 13 90 0a 04   ·<*>····  ········
0020  12 01 08 00 4b 96 00 01  01 c5 61 62 63 64 65 66   ····K···  ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```



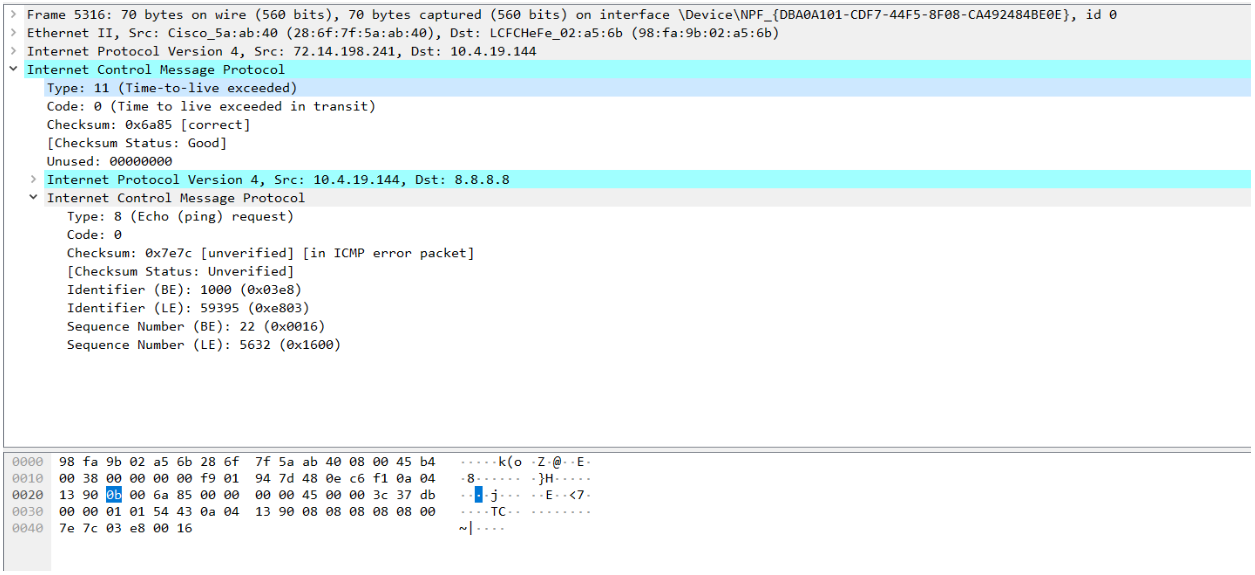
```
> Frame 4440: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{DBA0A101-CDF7-44F5-8F08-CA492484BE0E}, id 0
> Ethernet II, Src: LCFCHeFe_02:a5:6b (98:fa:9b:02:a5:6b), Dst: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40)
> Internet Protocol Version 4, Src: 10.4.19.144, Dst: 10.4.18.1
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4b96 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 453 (0x01c5)
    Sequence Number (LE): 50433 (0xc501)
    [Response frame: 4441]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]

0000  28 6f 7f 5a ab 40 98 fa  9b 02 a5 6b 08 00 45 00   (o·Z·@··  ···k··E·
0010  00 3c 2a 3e 00 00 80 01  00 00 0a 04 13 90 0a 04   ·<*>····  ········
0020  12 01 08 00 4b 96 00 01  01 c5 61 62 63 64 65 66   ····K···  ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

The raw bytes representing the type and code can be seen in the screenshots.
The type is **8 (echo (ping) request)**, and code is **0**.

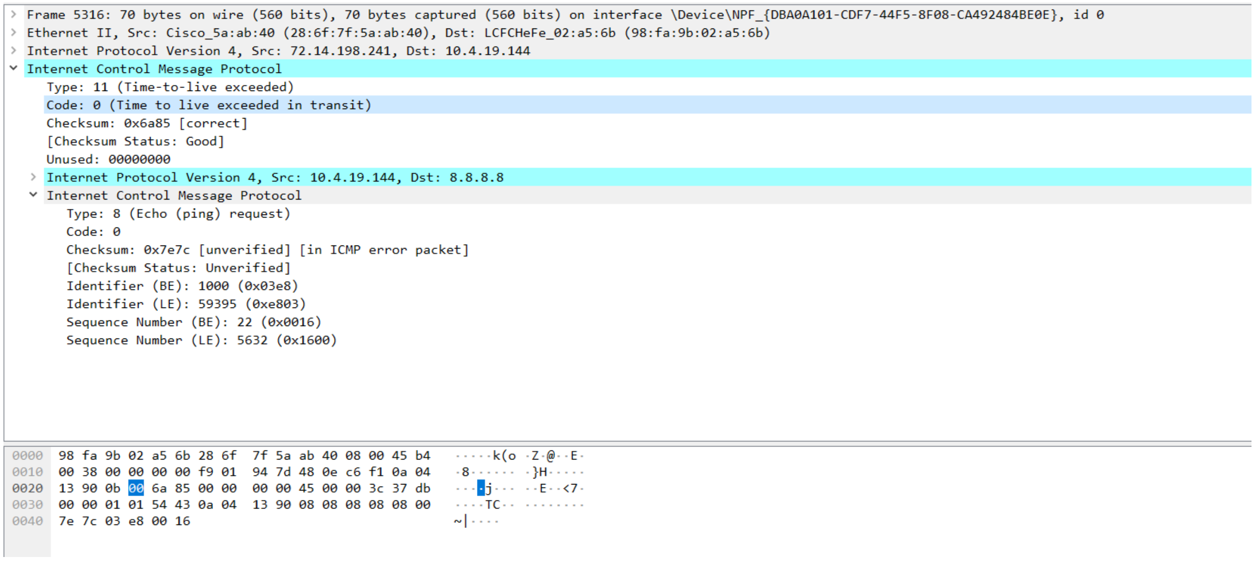
c. Examine the raw bytes of the ICMP error packet. Capture a screenshot of the raw bytes and identify the bytes that represent the type and code. (3 marks)



```
2022-04-04 13:26:39.975   10.4.19.144       8.8.8.8        ICMP   74    Echo (ping) request  id=0x03e8, seq=9/2304, ttl=2 (no response fo
2022-04-04 13:26:39.975   10.4.19.144       8.8.8.8        ICMP   74    Echo (ping) request  id=0x03e8, seq=10/2560, ttl=3 (no response f
2022-04-04 13:26:39.975   10.4.19.144       8.8.8.8        ICMP   74    Echo (ping) request  id=0x03e8, seq=11/2816, ttl=3 (no response f
2022-04-04 13:26:39.975   10.4.19.144       8.8.8.8        ICMP   74    Echo (ping) request  id=0x03e8, seq=12/3072, ttl=3 (no response f
2022-04-04 13:26:39.975   10.4.19.144       8.8.8.8        ICMP   74    Echo (ping) request  id=0x03e8, seq=13/3328, ttl=4 (no response f
2022-04-04 13:26:39.975   10.4.19.144       8.8.8.8        ICMP   74    Echo (ping) request  id=0x03e8, seq=14/3584, ttl=4 (no response f
2022-04-04 13:26:39.975   10.4.19.144       8.8.8.8        ICMP   74    Echo (ping) request  id=0x03e8, seq=15/3840, ttl=4 (no response f
2022-04-04 13:26:39.975   10.4.18.1         10.4.19.144    ICMP   70    Time-to-live exceeded (Time to live exceeded in transit)
2022-04-04 13:26:39.975   10.1.0.10         10.4.19.144    ICMP   102   Time-to-live exceeded (Time to live exceeded in transit)
2022-04-04 13:26:39.975   10.1.0.10         10.4.19.144    ICMP   102   Time-to-live exceeded (Time to live exceeded in transit)
2022-04-04 13:26:39.975   10.1.0.10         10.4.19.144    ICMP   102   Time-to-live exceeded (Time to live exceeded in transit)
2022-04-04 13:26:39.975   10.4.18.1         10.4.19.144    ICMP   70    Time-to-live exceeded (Time to live exceeded in transit)
2022-04-04 13:26:39.975   10.4.18.1         10.4.19.144    ICMP   70    Time-to-live exceeded (Time to live exceeded in transit)
2022-04-04 13:26:39.975   103.210.49.129    10.4.19.144    ICMP   70    Time-to-live exceeded (Time to live exceeded in transit)
2022-04-04 13:26:39.975   103.210.49.129    10.4.19.144    ICMP   70    Time-to-live exceeded (Time to live exceeded in transit)
2022-04-04 13:26:39.975   103.210.49.129    10.4.19.144    ICMP   70    Time-to-live exceeded (Time to live exceeded in transit)
2022-04-04 13:26:39.976   103.123.50.37     10.4.19.144    ICMP   102   Time-to-live exceeded (Time to live exceeded in transit)
```



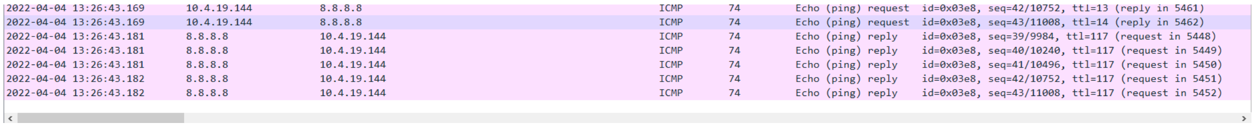
```
> Frame 5316: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{DBA0A101-CDF7-44F5-8F08-CA492484BE0E}, id 0
> Ethernet II, Src: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40), Dst: LCFCHeFe_02:a5:6b (98:fa:9b:02:a5:6b)
> Internet Protocol Version 4, Src: 72.14.198.241, Dst: 10.4.19.144
v Internet Control Message Protocol
     Type: 11 (Time-to-live exceeded)
     Code: 0 (Time to live exceeded in transit)
     Checksum: 0x6a85 [correct]
     [Checksum Status: Good]
     Unused: 00000000
   > Internet Protocol Version 4, Src: 10.4.19.144, Dst: 8.8.8.8
   v Internet Control Message Protocol
        Type: 8 (Echo (ping) request)
        Code: 0
        Checksum: 0x7e7c [unverified] [in ICMP error packet]
        [Checksum Status: Unverified]
        Identifier (BE): 1000 (0x03e8)
        Identifier (LE): 59395 (0xe803)
        Sequence Number (BE): 22 (0x0016)
        Sequence Number (LE): 5632 (0x1600)

0000  98 fa 9b 02 a5 6b 28 6f  7f 5a ab 40 08 00 45 b4   ·····k(o ·Z·@··E·
0010  00 38 00 00 00 00 f9 01  94 7d 48 0e c6 f1 0a 04   ·8······ ·}H·····
0020  13 90 0b 00 6a 85 00 00  00 00 45 00 00 3c 37 db   ····j··· ··E··<7·
0030  00 00 01 01 54 43 0a 04  13 90 08 08 08 08 08 00   ····TC·· ········
0040  7e 7c 03 e8 00 16                                  ~|····
```



```
> Frame 5316: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{DBA0A101-CDF7-44F5-8F08-CA492484BE0E}, id 0
> Ethernet II, Src: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40), Dst: LCFCHeFe_02:a5:6b (98:fa:9b:02:a5:6b)
> Internet Protocol Version 4, Src: 72.14.198.241, Dst: 10.4.19.144
v Internet Control Message Protocol
     Type: 11 (Time-to-live exceeded)
     Code: 0 (Time to live exceeded in transit)
     Checksum: 0x6a85 [correct]
     [Checksum Status: Good]
     Unused: 00000000
   > Internet Protocol Version 4, Src: 10.4.19.144, Dst: 8.8.8.8
   v Internet Control Message Protocol
        Type: 8 (Echo (ping) request)
        Code: 0
        Checksum: 0x7e7c [unverified] [in ICMP error packet]
        [Checksum Status: Unverified]
        Identifier (BE): 1000 (0x03e8)
        Identifier (LE): 59395 (0xe803)
        Sequence Number (BE): 22 (0x0016)
        Sequence Number (LE): 5632 (0x1600)

0000  98 fa 9b 02 a5 6b 28 6f  7f 5a ab 40 08 00 45 b4   ·····k(o ·Z·@··E·
0010  00 38 00 00 00 00 f9 01  94 7d 48 0e c6 f1 0a 04   ·8······ ·}H·····
0020  13 90 0b 00 6a 85 00 00  00 00 45 00 00 3c 37 db   ····j··· ··E··<7·
0030  00 00 01 01 54 43 0a 04  13 90 08 08 08 08 08 00   ····TC·· ········
0040  7e 7c 03 e8 00 16                                  ~|····
```

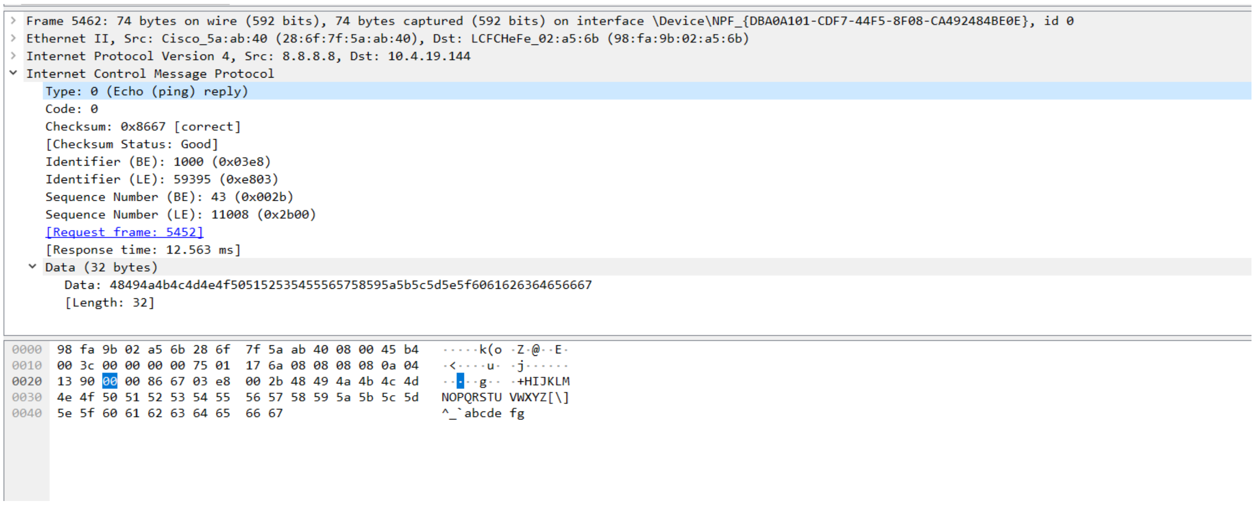
The raw bytes representing the type and code can be seen in the screenshots.
The type is **11 (Time-to-live exceeded)**, and code is **0 (Time to live exceeded in transit)**.

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)



```
2022-04-04 13:26:43.169   10.4.19.144   8.8.8.8       ICMP   74   Echo (ping) request  id=0x03e8, seq=42/10752, ttl=13 (reply in 5461)
2022-04-04 13:26:43.169   10.4.19.144   8.8.8.8       ICMP   74   Echo (ping) request  id=0x03e8, seq=43/11008, ttl=14 (reply in 5462)
2022-04-04 13:26:43.181   8.8.8.8       10.4.19.144   ICMP   74   Echo (ping) reply    id=0x03e8, seq=39/9984, ttl=117 (request in 5448)
2022-04-04 13:26:43.181   8.8.8.8       10.4.19.144   ICMP   74   Echo (ping) reply    id=0x03e8, seq=40/10240, ttl=117 (request in 5449)
2022-04-04 13:26:43.181   8.8.8.8       10.4.19.144   ICMP   74   Echo (ping) reply    id=0x03e8, seq=41/10496, ttl=117 (request in 5450)
2022-04-04 13:26:43.182   8.8.8.8       10.4.19.144   ICMP   74   Echo (ping) reply    id=0x03e8, seq=42/10752, ttl=117 (request in 5451)
2022-04-04 13:26:43.182   8.8.8.8       10.4.19.144   ICMP   74   Echo (ping) reply    id=0x03e8, seq=43/11008, ttl=117 (request in 5452)
```

The last 3 packets can be seen in the screenshot above.



```
> Frame 5462: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{DBA0A101-CDF7-44F5-8F08-CA492484BE0E}, id 0
> Ethernet II, Src: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40), Dst: LCFCHeFe_02:a5:6b (98:fa:9b:02:a5:6b)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 10.4.19.144
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x8667 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1000 (0x03e8)
    Identifier (LE): 59395 (0xe803)
    Sequence Number (BE): 43 (0x002b)
    Sequence Number (LE): 11008 (0x2b00)
    [Request frame: 5452]
    [Response time: 12.563 ms]
  v Data (32 bytes)
      Data: 48494a4b4c4d4e4f505152535455565758595a5b5c5d5e5f6061626364656667
      [Length: 32]

0000  98 fa 9b 02 a5 6b 28 6f  7f 5a ab 40 08 00 45 b4   ·····k(o ·Z·@··E·
0010  00 3c 00 00 00 00 75 01  17 6a 08 08 08 08 0a 04   ·<····u· ·j······
0020  13 90 00 00 86 67 03 e8  00 2b 48 49 4a 4b 4c 4d   ·····g·· ·+HIJKLM
0030  4e 4f 50 51 52 53 54 55  56 57 58 59 5a 5b 5c 5d   NOPQRSTU VWXYZ[\]
0040  5e 5f 60 61 62 63 64 65  66 67                     ^_`abcde fg
```

The contents of one of the last 3 packets are shown in the screenshot above.

The last three ICMP packets are **message type 0** (echo reply). The ICMP error packets had **type 11** (TTL expired).

The ICMP error packets contain both the IP header and the first 8 bytes of the original ICMP packet that the error is actually for.

The reason for this difference can be explained by the datagrams. The datagrams made it all the way to the destination host before the TTL expired. Thus, they received the status of 0 which indicates successful reply.