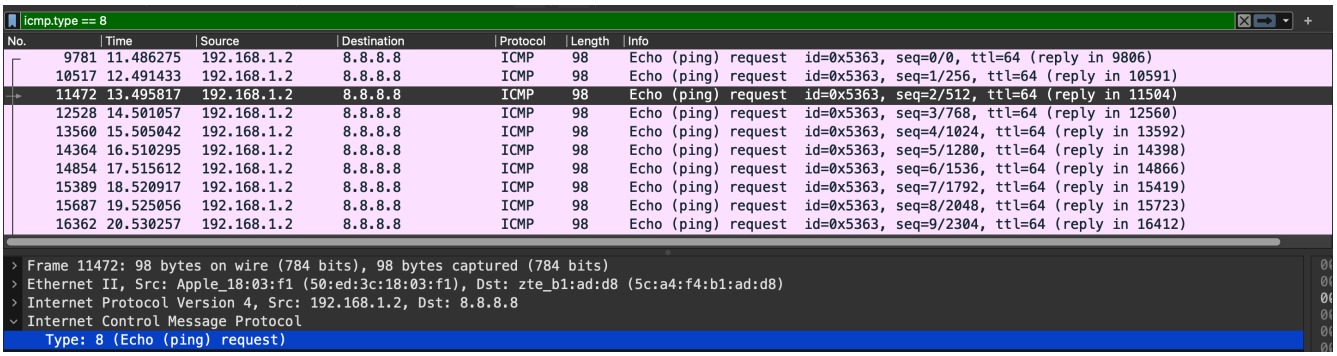
Student Information

Full Name : Mehmet Rüçhan Yavuzdemir
Id Number: 2522159

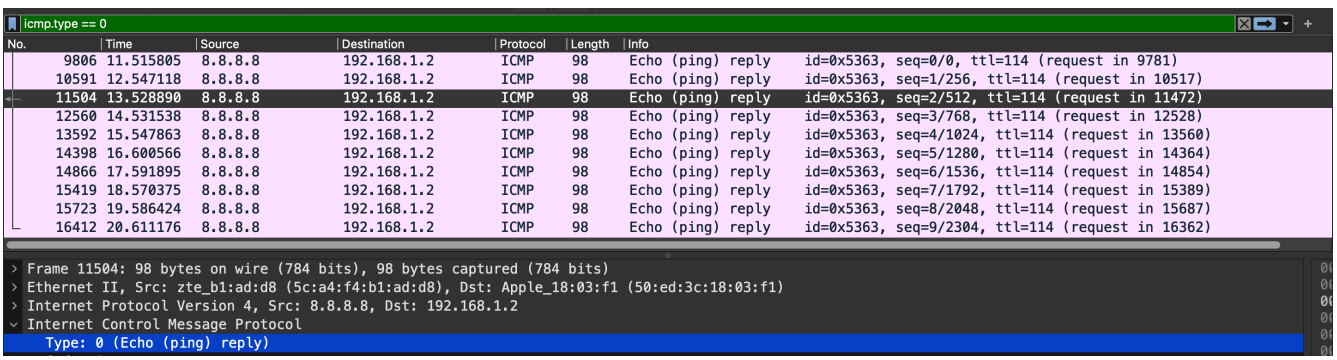


icmp.type == 8

No.	Time	Source	Destination	Protocol	Length	Info
9781	11.486275	192.168.1.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x5363, seq=0/0, ttl=64 (reply in 9806)
10517	12.491433	192.168.1.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x5363, seq=1/256, ttl=64 (reply in 10591)
11472	13.495817	192.168.1.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x5363, seq=2/512, ttl=64 (reply in 11504)
12528	14.501057	192.168.1.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x5363, seq=3/768, ttl=64 (reply in 12560)
13560	15.505042	192.168.1.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x5363, seq=4/1024, ttl=64 (reply in 13592)
14364	16.510295	192.168.1.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x5363, seq=5/1280, ttl=64 (reply in 14398)
14854	17.515612	192.168.1.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x5363, seq=6/1536, ttl=64 (reply in 14866)
15389	18.520917	192.168.1.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x5363, seq=7/1792, ttl=64 (reply in 15419)
15687	19.525056	192.168.1.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x5363, seq=8/2048, ttl=64 (reply in 15723)
16362	20.530257	192.168.1.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x5363, seq=9/2304, ttl=64 (reply in 16412)

```
> Frame 11472: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: Apple_18:03:f1 (50:ed:3c:18:03:f1), Dst: zte_b1:ad:d8 (5c:a4:f4:b1:ad:d8)
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 8.8.8.8
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
```

Figure 1: Request Packet IP addresses



icmp.type == 0

No.	Time	Source	Destination	Protocol	Length	Info
9806	11.515805	8.8.8.8	192.168.1.2	ICMP	98	Echo (ping) reply id=0x5363, seq=0/0, ttl=114 (request in 9781)
10591	12.547118	8.8.8.8	192.168.1.2	ICMP	98	Echo (ping) reply id=0x5363, seq=1/256, ttl=114 (request in 10517)
11504	13.528890	8.8.8.8	192.168.1.2	ICMP	98	Echo (ping) reply id=0x5363, seq=2/512, ttl=114 (request in 11472)
12560	14.531538	8.8.8.8	192.168.1.2	ICMP	98	Echo (ping) reply id=0x5363, seq=3/768, ttl=114 (request in 12528)
13592	15.547863	8.8.8.8	192.168.1.2	ICMP	98	Echo (ping) reply id=0x5363, seq=4/1024, ttl=114 (request in 13560)
14398	16.600566	8.8.8.8	192.168.1.2	ICMP	98	Echo (ping) reply id=0x5363, seq=5/1280, ttl=114 (request in 14364)
14866	17.591895	8.8.8.8	192.168.1.2	ICMP	98	Echo (ping) reply id=0x5363, seq=6/1536, ttl=114 (request in 14854)
15419	18.570375	8.8.8.8	192.168.1.2	ICMP	98	Echo (ping) reply id=0x5363, seq=7/1792, ttl=114 (request in 15389)
15723	19.586424	8.8.8.8	192.168.1.2	ICMP	98	Echo (ping) reply id=0x5363, seq=8/2048, ttl=114 (request in 15687)
16412	20.611176	8.8.8.8	192.168.1.2	ICMP	98	Echo (ping) reply id=0x5363, seq=9/2304, ttl=114 (request in 16362)

```
> Frame 11504: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: zte_b1:ad:d8 (5c:a4:f4:b1:ad:d8), Dst: Apple_18:03:f1 (50:ed:3c:18:03:f1)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.2
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
```

Figure 2: Response Packet IP addresses

Answer 1

By looking at Figure 1, for the request packets, the source IP address is `192.168.1.2` and the destination IP address is `8.8.8.8`. Again, by looking at Figure 2, for the response (reply) packets, the source IP address is `8.8.8.8` and the destination IP address is `192.168.1.2`.

Answer 2

No, there is no port information because `ICMP` was designed to communicate network layer information between hosts and routers. No upper-layer protocol is built at the top of `ICMP`.

Answer 3

a)

According to the `ICMP RFC 792` on page 20, there are **11** types of `ICMP` packets. Hence, its purpose is to identify what type of `ICMP` packet is being transferred.

0 Echo Reply

3 Destination Unreachable

4 Source Quench

5 Redirect

8 Echo

11 Time Exceeded

12 Parameter Problem

13 Timestamp

14 Timestamp Reply

15 Information Request

16 Information Reply

b)

In my opinion, the `Code` field is like an option or flag extending information provided by the `Type` field. According to the `ICMP RFC 792` on page 4, Destination Unreachable Message has the `Type` value 3, and 6 distinct `Code` values. Therefore, its purpose is to provide extra information besides `Type`.

0 = net unreachable

1 = host unreachable

2 = protocol unreachable

3 = port unreachable

4 = fragmentation needed and DF set

5 = source route failed

c)

`Type` and `Code` values together specify the `ICMP` packet and provide enough information regarding what happened in the network layer. Both have 8-bit lengths, but we can see from parts a and b that their values are not even close to the limit, they are very small.

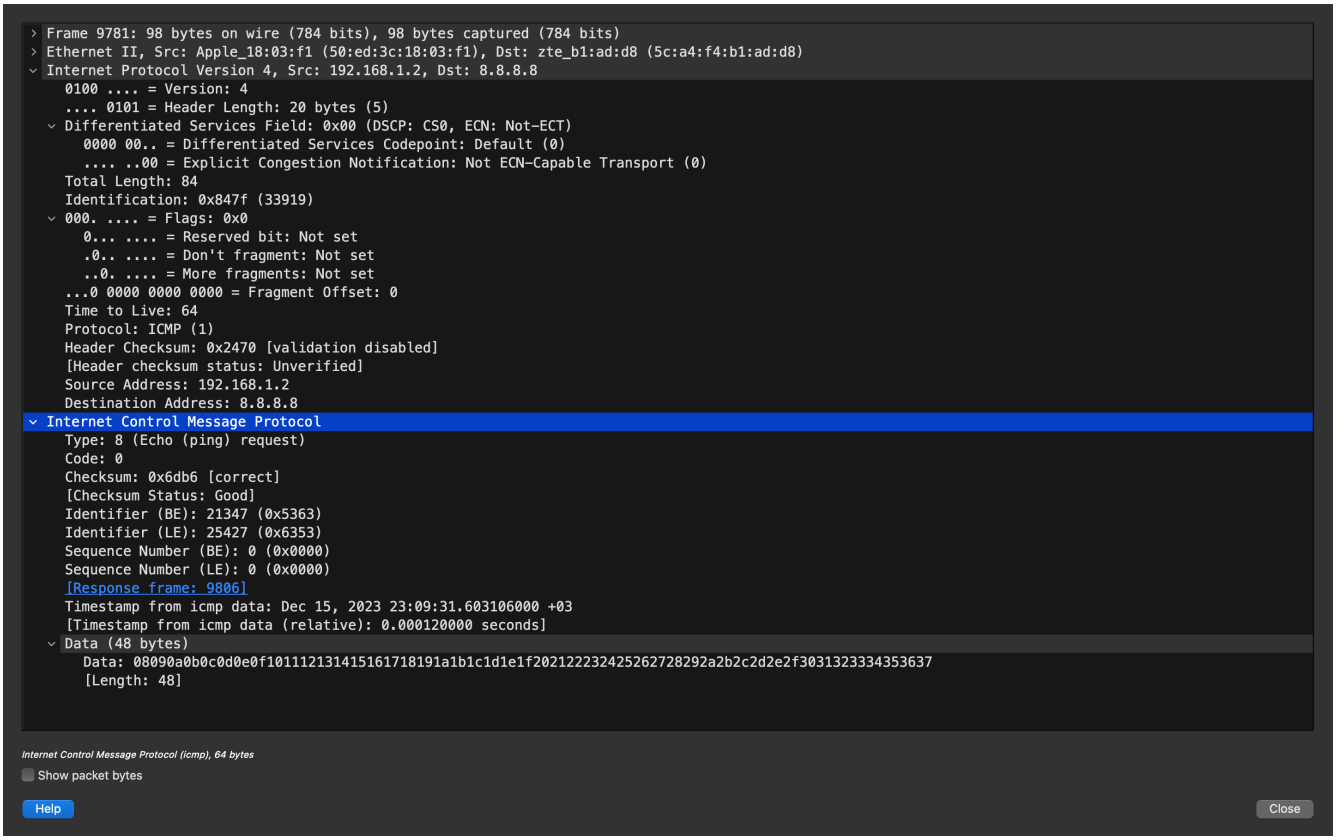


Figure 3: Packet Details - Request

Answer 4

The `ICMP` payload is `48` bytes. To be able to find how many bytes are transferred inside this `ICMP` packet, we have to find the `ICMP` header length as well. To do that, we can trace the packet bytes and match them with the header information parsed by the Wireshark, or we can do the math and see that the IP payload is `Total Length - Header Length = 84 - 20 = 64` bytes, and the `ICMP` payload is 48 bytes, so its `16` bytes, both work. Hence, the `ICMP` header length is `16` bytes. In total, `48 + 16 = 64` bytes transferred inside the `ICMP` packet. There are `Type` and `Code` fields that we have discussed in the previous questions in-depth. They together specify the `ICMP` packet and provide enough information regarding what happened in the network layer. `Checksum` field is responsible for detecting bit flips. The `Identifier` field uniquely identifies the `ICMP` packet, with Low Endian, and Back Endian fields. The `Sequence Number` is used for in-order and reliable delivery, with Low Endian, and Back Endian fields. The `Timestamp` indicates the packet transmission time. Finally, the `Data` field contains the `ICMP` payload.

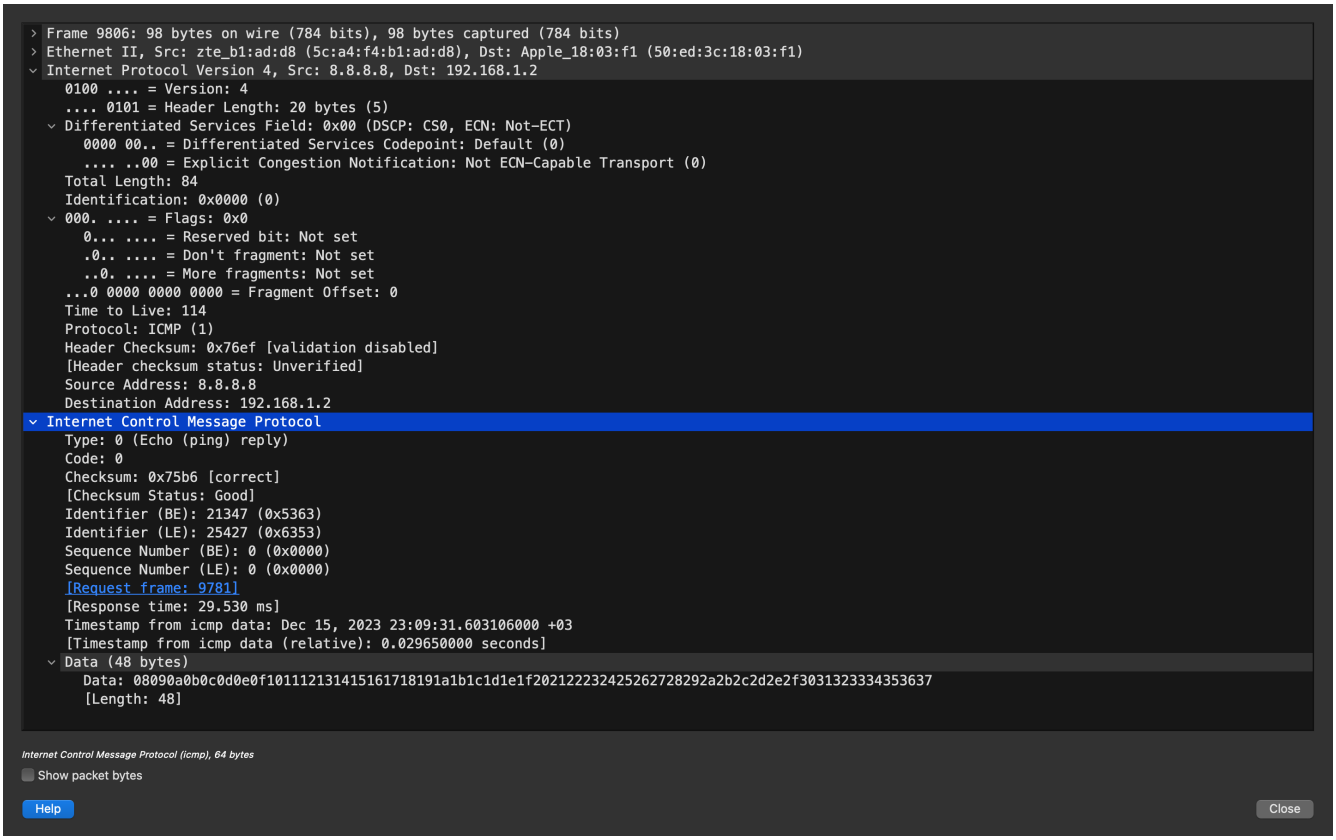


Figure 4: Packet Details - Response

Figure 5: Routing Table

Answer 5

We can remove `default via 192.168.1.1 dev en0` default gateway line to prevent outgoing packets and block ping requests as we are trying to reach an IP address, `8.8.8.8`, that is outside of my subnet.

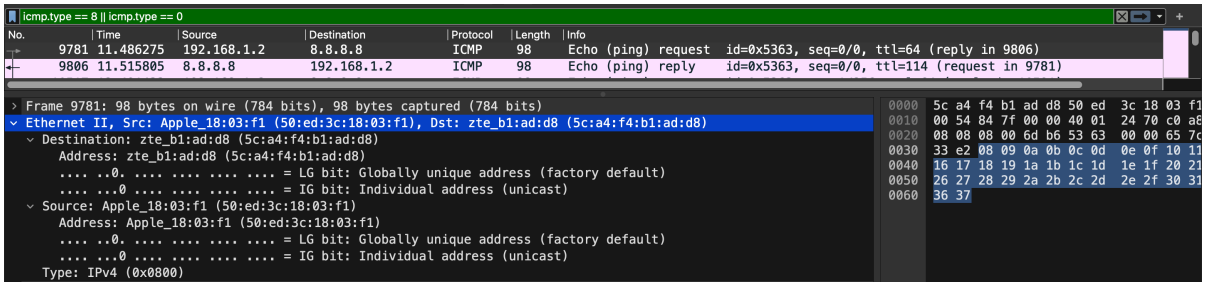


Figure 6: Link Layer

Answer 6

a)

My computer's 48-bit `MAC` address is `50:ed:3c:18:03:f1`, which can be seen under `Source Address`.

b)

The 48-bit destination `MAC` address is `5c:a4:f4:b1:ad:d8`, which can be seen under `Destination Address`. According to the line `zte_b1:ad:d8 (5c:a4:f4:b1:ad:d8)`, we can identify that this address belongs to a ZTE brand device.

c)

Among all `Type` values under the link layer, I have only observed one value, `IPv4 (0x0800)`. Hence, this link layer technology employs the upper layer protocol IP of version 4.