CENG 435 - Data Communications and Networking 2023-1 Wireshark Assignment 6

Anıl Eren Göçer
e2448397@ceng.metu.edu.tr

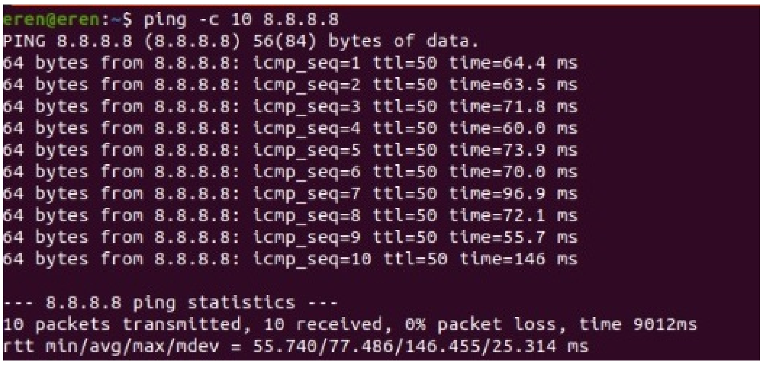
December 21, 2023

1 Introduction

2 ICMP Packet Analysis

2.1 Capture the Network Traffic

2.

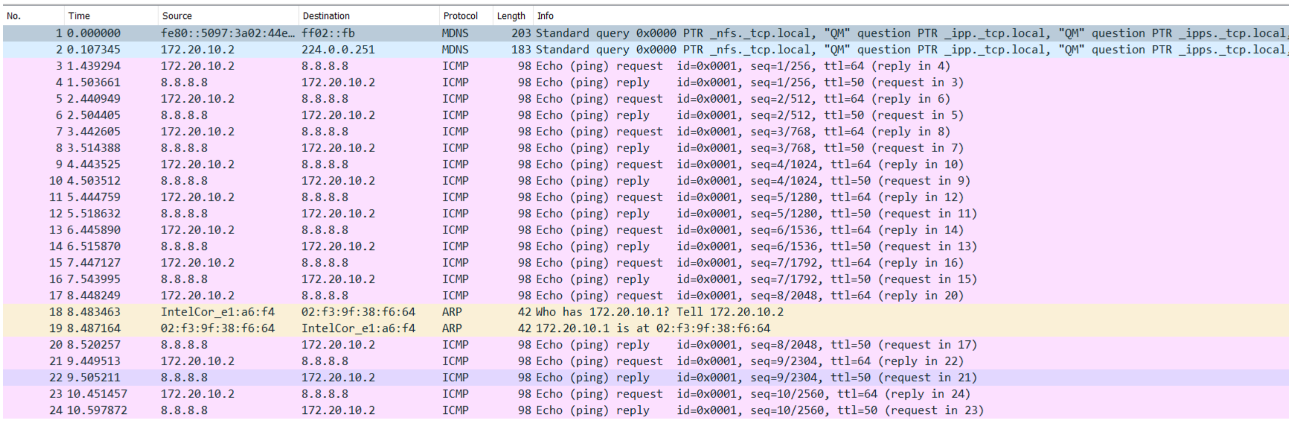


```
eren@eren:~$ ping -c 10 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=50 time=64.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=50 time=63.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=50 time=71.8 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=50 time=60.0 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=50 time=73.9 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=50 time=70.0 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=50 time=96.9 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=50 time=72.1 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=50 time=55.7 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=50 time=146 ms

--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9012ms
rtt min/avg/max/mdev = 55.740/77.486/146.455/25.314 ms
```

Figure 1: Output of ping on the terminal

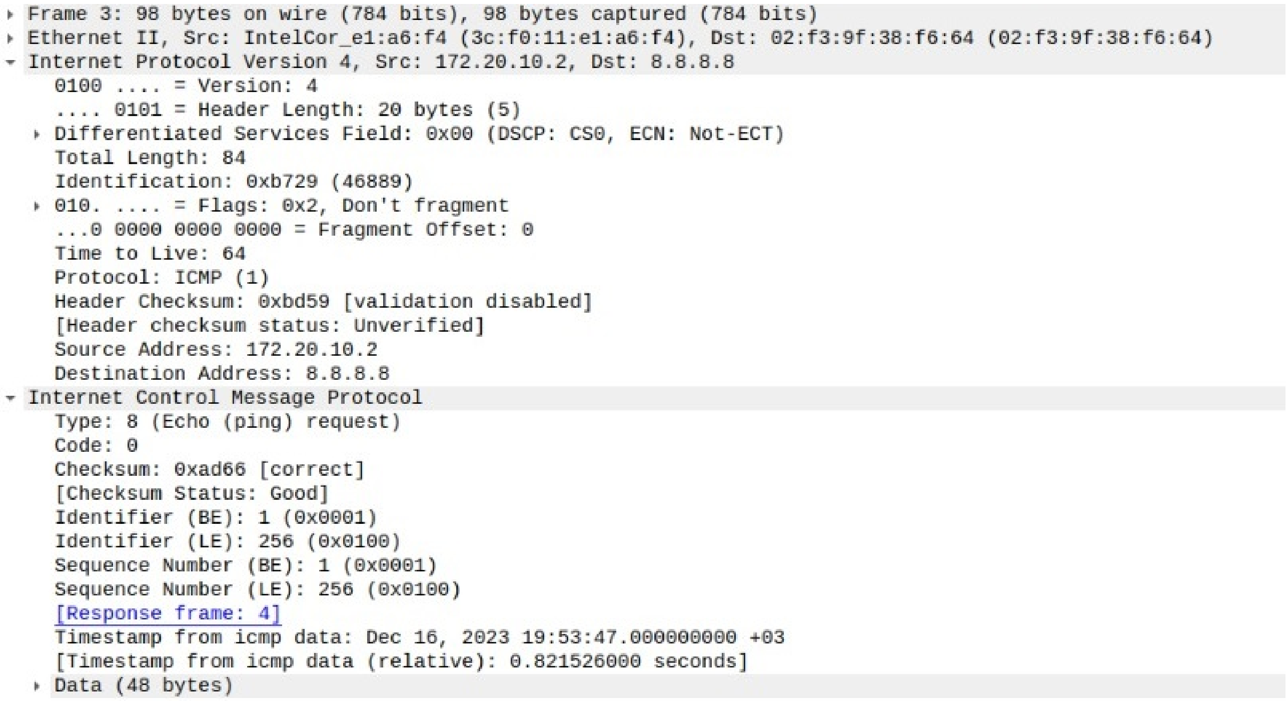
4.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::5097:3a02:44e…	ff02::fb	MDNS	203	Standard query 0x0000 PTR _nfs._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question PTR _ipps._tcp.local,
2	0.107345	172.20.10.2	224.0.0.251	MDNS	183	Standard query 0x0000 PTR _nfs._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question PTR _ipps._tcp.local,
3	1.439294	172.20.10.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 4)
4	1.503661	8.8.8.8	172.20.10.2	ICMP	98	Echo (ping) reply id=0x0001, seq=1/256, ttl=50 (request in 3)
5	2.440949	172.20.10.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=2/512, ttl=64 (reply in 6)
6	2.504405	8.8.8.8	172.20.10.2	ICMP	98	Echo (ping) reply id=0x0001, seq=2/512, ttl=50 (request in 5)
7	3.442605	172.20.10.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in 8)
8	3.514388	8.8.8.8	172.20.10.2	ICMP	98	Echo (ping) reply id=0x0001, seq=3/768, ttl=50 (request in 7)
9	4.443525	172.20.10.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=4/1024, ttl=64 (reply in 10)
10	4.503512	8.8.8.8	172.20.10.2	ICMP	98	Echo (ping) reply id=0x0001, seq=4/1024, ttl=50 (request in 9)
11	5.444759	172.20.10.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=5/1280, ttl=64 (reply in 12)
12	5.518632	8.8.8.8	172.20.10.2	ICMP	98	Echo (ping) reply id=0x0001, seq=5/1280, ttl=50 (request in 11)
13	6.445890	172.20.10.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=6/1536, ttl=64 (reply in 14)
14	6.515870	8.8.8.8	172.20.10.2	ICMP	98	Echo (ping) reply id=0x0001, seq=6/1536, ttl=50 (request in 13)
15	7.447127	172.20.10.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=7/1792, ttl=64 (reply in 16)
16	7.543995	8.8.8.8	172.20.10.2	ICMP	98	Echo (ping) reply id=0x0001, seq=7/1792, ttl=50 (request in 15)
17	8.448249	172.20.10.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=8/2048, ttl=64 (reply in 20)
18	8.483463	IntelCor_e1:a6:f4	02:f3:9f:38:f6:64	ARP	42	Who has 172.20.10.1? Tell 172.20.10.2
19	8.487164	02:f3:9f:38:f6:64	IntelCor_e1:a6:f4	ARP	42	172.20.10.1 is at 02:f3:9f:38:f6:64
20	8.520257	8.8.8.8	172.20.10.2	ICMP	98	Echo (ping) reply id=0x0001, seq=8/2048, ttl=50 (request in 17)
21	9.449513	172.20.10.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=9/2304, ttl=64 (reply in 22)
22	9.505211	8.8.8.8	172.20.10.2	ICMP	98	Echo (ping) reply id=0x0001, seq=9/2304, ttl=50 (request in 21)
23	10.451457	172.20.10.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=10/2560, ttl=64 (reply in 24)
24	10.597872	8.8.8.8	172.20.10.2	ICMP	98	Echo (ping) reply id=0x0001, seq=10/2560, ttl=50 (request in 23)

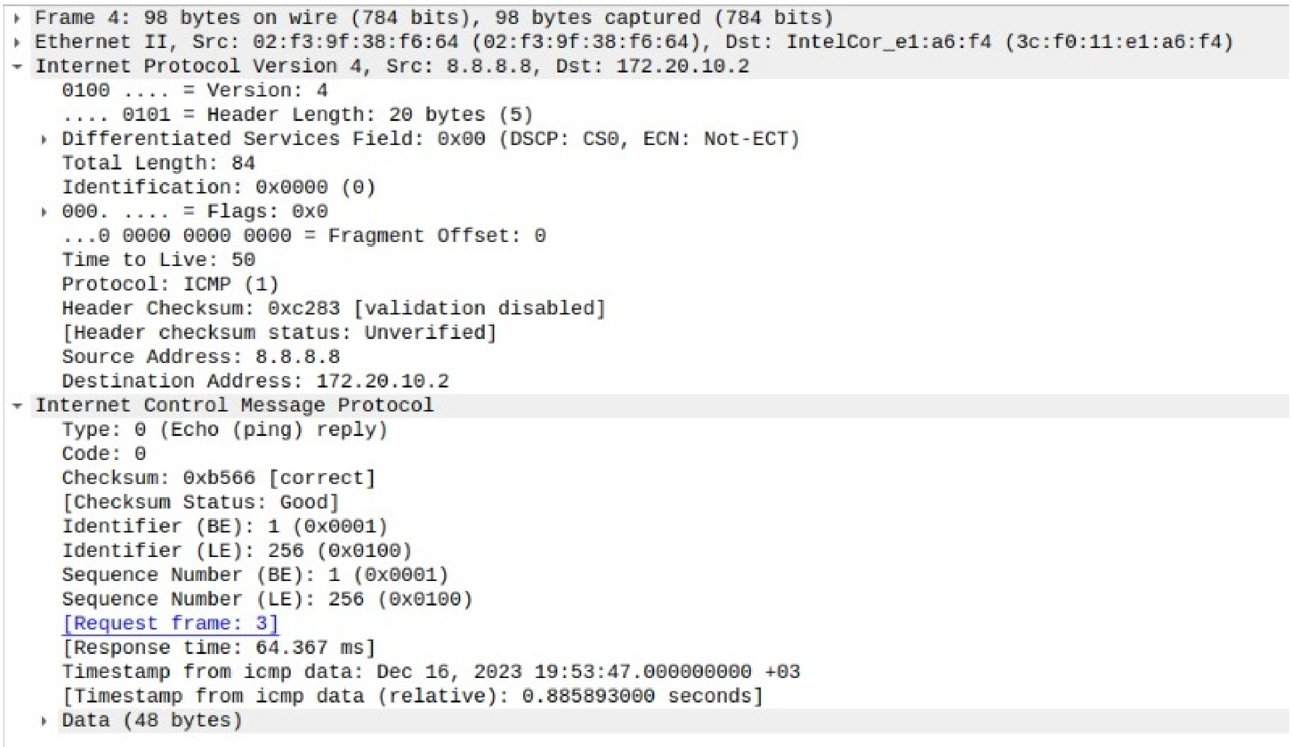
Figure 2: Existence of 10 ICMP requests and 10 ICMP responses

5.



```
▸ Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▸ Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64)
▾ Internet Protocol Version 4, Src: 172.20.10.2, 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: 84
    Identification: 0xb729 (46889)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0xbd59 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.20.10.2
    Destination Address: 8.8.8.8
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xad66 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 4]
    Timestamp from icmp data: Dec 16, 2023 19:53:47.000000000 +03
    [Timestamp from icmp data (relative): 0.821526000 seconds]
  ▸ Data (48 bytes)
```

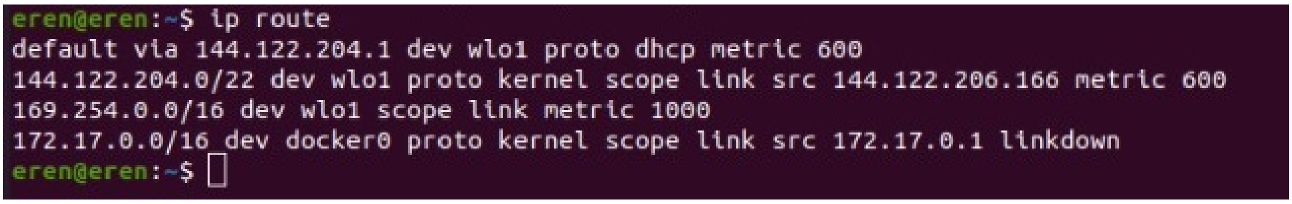
Figure 3: Packet Details of an ICMP request



```
▸ Frame 4: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▸ Ethernet II, Src: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64), Dst: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
▾ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 172.20.10.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x0000 (0)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 50
    Protocol: ICMP (1)
    Header Checksum: 0xc283 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 8.8.8.8
    Destination Address: 172.20.10.2
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xb566 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Request frame: 3]
    [Response time: 64.367 ms]
    Timestamp from icmp data: Dec 16, 2023 19:53:47.000000000 +03
    [Timestamp from icmp data (relative): 0.885893000 seconds]
  ▸ Data (48 bytes)
```

Figure 4: Packet Details of an ICMP response

6.



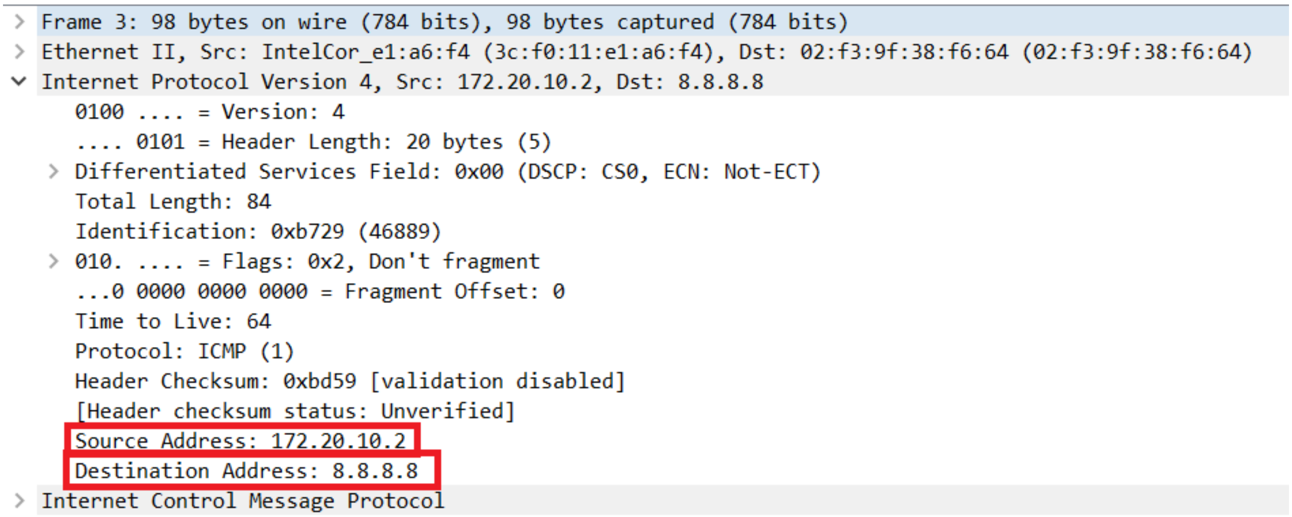
```
eren@eren:~$ ip route
default via 144.122.204.1 dev wlo1 proto dhcp metric 600
144.122.204.0/22 dev wlo1 proto kernel scope link src 144.122.206.166 metric 600
169.254.0.0/16 dev wlo1 scope link metric 1000
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
eren@eren:~$ 
```

Figure 5: Routing Table Information

3 Questions

1.

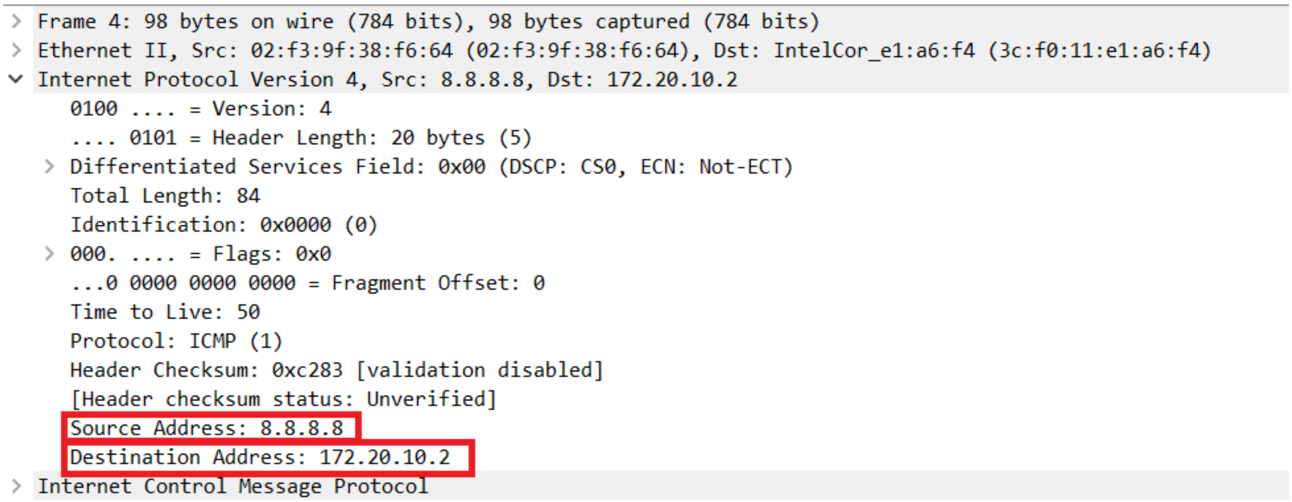
IP address of the source host of the request: 172.20.10.2
IP address of the destination host of the request: 8.8.8.8



```
> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64)
v Internet Protocol Version 4, Src: 172.20.10.2, 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: 84
     Identification: 0xb729 (46889)
   > 010. .... = Flags: 0x2, Don't fragment
     ...0 0000 0000 0000 = Fragment Offset: 0
     Time to Live: 64
     Protocol: ICMP (1)
     Header Checksum: 0xbd59 [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 172.20.10.2
     Destination Address: 8.8.8.8
> Internet Control Message Protocol
```

Figure 6: IP addresses of the source host and the destination host of the request

IP address of the source host of the reply: 8.8.8.8
IP address of the destination host of the reply: 172.20.10.2



```
> Frame 4: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64), Dst: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
v Internet Protocol Version 4, Src: 8.8.8.8, Dst: 172.20.10.2
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 84
     Identification: 0x0000 (0)
   > 000. .... = Flags: 0x0
     ...0 0000 0000 0000 = Fragment Offset: 0
     Time to Live: 50
     Protocol: ICMP (1)
     Header Checksum: 0xc283 [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 8.8.8.8
     Destination Address: 172.20.10.2
> Internet Control Message Protocol
```

Figure 7: IP addresses of the source host and the destination host of the reply

2. There is **NOT** any port number of information in neither request nor reply packets. The reason is that network layer and below layers (namely link and physical) used to transfer ICMP packets. Since ports remains between transport layer and application layer, which are the layers above network layer, there is no need to include port number information in this communication.

3.

Link to RFC 792: `https://datatracker.ietf.org/doc/html/rfc792`

(a) According to the RFC 792 ICMP Protocol Specification, "type" field can take the values with their meanings as: 0 Echo Reply, 8 Echo Request, 15 Information Request, 16 Information Reply and so on. Therefore, the purpose of this field is to specify what kind of message it is. This helps to receiving side of that message to reply in a correct way. You can think this "type" field like HTTP message types GET, POST, DELETE and so on. In short, type field's purpose is to differentiate between different ICMP messages with different purposes.

(b) According to the RFC 792 ICMP Protocol Specification, "code" field can take the values with their meanings as: 0 net reachable, 1 host unreachable, 5 source route failed and so on. Therefore, the purpose of this field is to give information about the communication environment which includes source host, destination host, underlying network etc. It helps communication participants to understand the status of the network and other participants. You can think this "code" field like HTTP status codes 200 OK, 404 Not Found, 301 Moved Permanently and so on.

Also, note that these two fields ("type" and "code") are interpreted together to give more specific information.

(c) In all my ICMP requests "type" field value is 8 and it means this package belongs to a ICMP Echo request message. In all my ICMP replies "type" field value is 0 and it means this package belongs to a ICMP Echo reply message. In all of my ICMP requests and replies, "code" field is 0. According to RCF 792 ICMP Protocol Specification, it is the default code field value for ICMP Echo request and reply messages, which have "type" field value 8 and 0 respectively. Therefore, it does not have any specific meaning.

4.

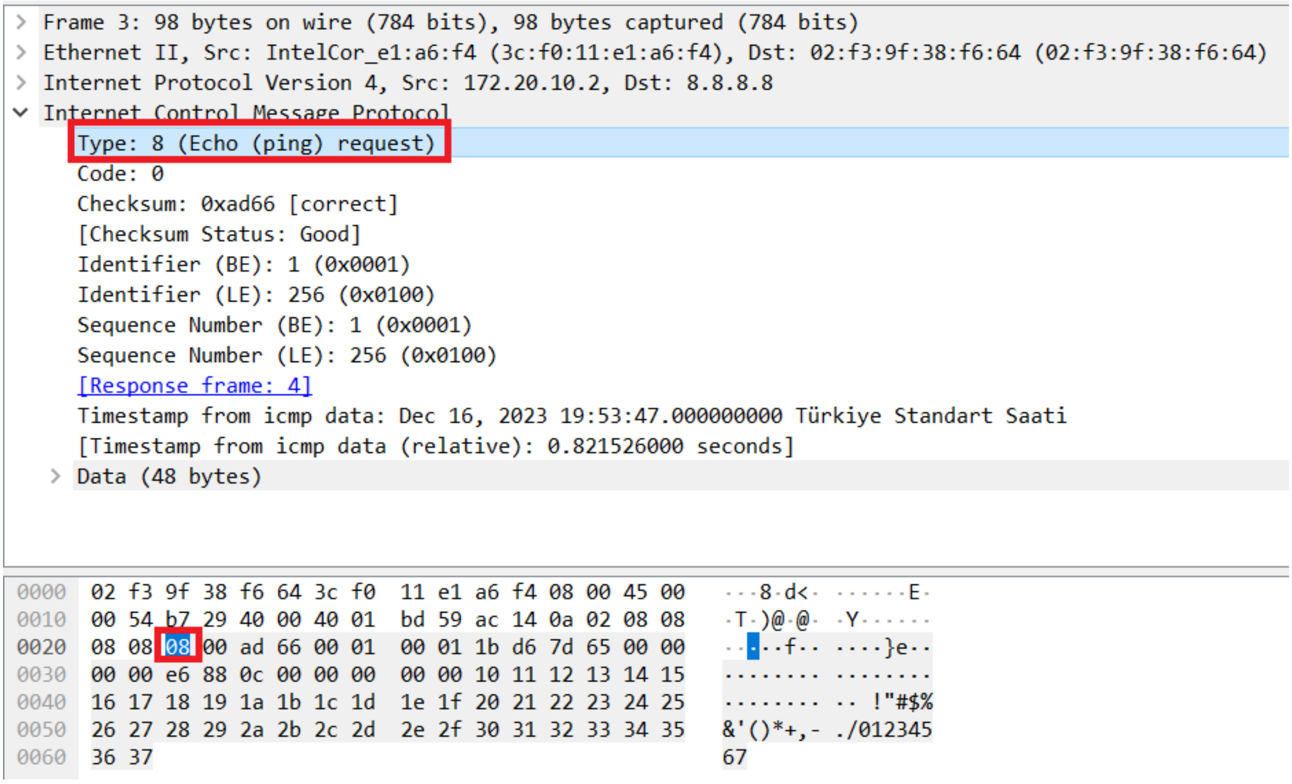
1 byte for "Type" field
1 byte for "Code" filed
2 bytes for "Checksum" field
2 bytes for "Identifier" field
2 bytes for "Sequence Number" field
8 bytes for "Timestamp" field
48 bytes for Data (Payload)

In total: 64 bytes

Type: It determines the type of ICMP message. For an ICMP Echo request, it is set to 8.
Code: It gives additional information (can be considered as status) regarding an ICMP message. For an ICMP Echo Request, it is set to 0.
Checksum: It is used for error-checking of the ICMP message to ensure the integrity of the packet during transmission.

Identifier: It is used to match ICMP Echo requests and corresponding ICMP Echo replies. Its value is 1 for all requests and replies in my pcap file.
Sequence Number: It is used to identify ICMP Echo requests and ICMP Echo replies. As I can observe in my pcap file, corresponding ICMP Echo requests and ICMP Echo replies have the same "Sequence Number" field value and they are incremented by 1 for each request and reply pair. Also, it is used together with Identifier to match requests and replies.
Timestamp: It includes timestamp information associated with the Echo Request. It is used to measure round-trip-rime (RTT).
Data (Payload): It includes the actual data being sent. In the context of a ping (Echo Request), this data may include arbitrary information or zeros, depending on the implementation. In my case it looks like an arbitrary data. This is returned back in corresponding ping (Echo reply).

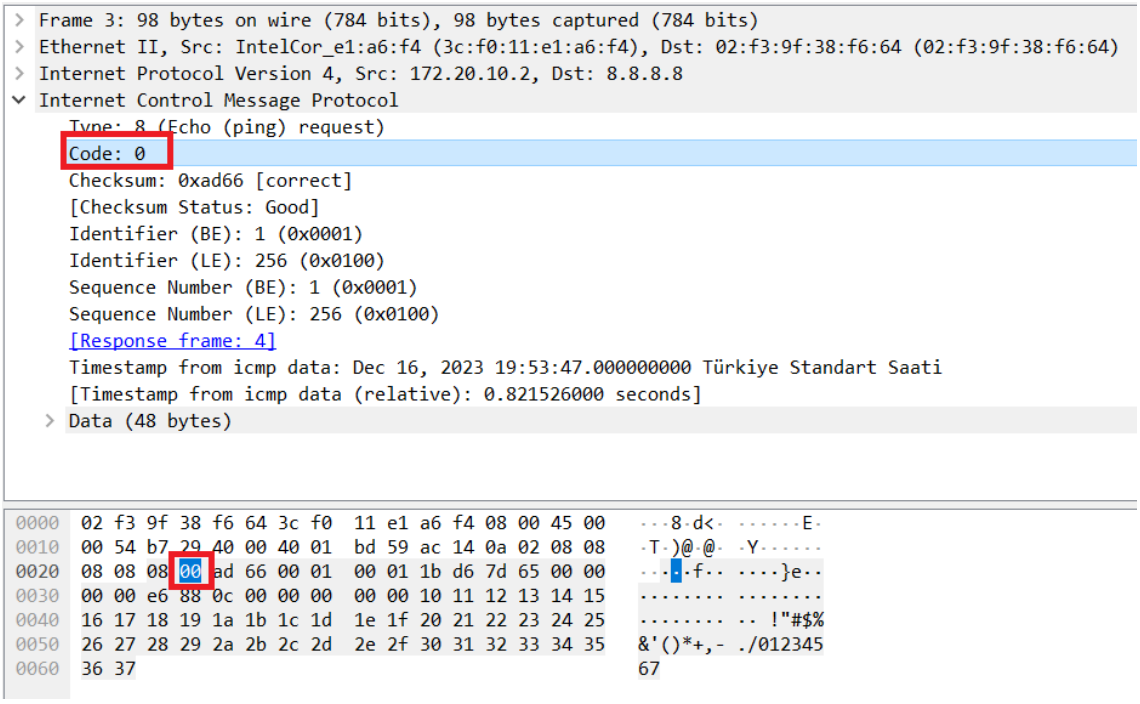
If you want how I reach numerical results, here are the screenshots.



```
> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 8.8.8.8
v Internet Control Message Protocol
     Type: 8 (Echo (ping) request)
     Code: 0
     Checksum: 0xad66 [correct]
     [Checksum Status: Good]
     Identifier (BE): 1 (0x0001)
     Identifier (LE): 256 (0x0100)
     Sequence Number (BE): 1 (0x0001)
     Sequence Number (LE): 256 (0x0100)
     [Response frame: 4]
     Timestamp from icmp data: Dec 16, 2023 19:53:47.000000000 Türkiye Standart Saati
     [Timestamp from icmp data (relative): 0.821526000 seconds]
   > Data (48 bytes)

0000  02 f3 9f 38 f6 64 3c f0  11 e1 a6 f4 08 00 45 00   ···8·d<· ······E·
0010  00 54 b7 29 40 00 40 01  bd 59 ac 14 0a 02 08 08   ·T·)@·@· ·Y······
0020  08 08 08 00 ad 66 00 01  00 01 1b d6 7d 65 00 00   ······f·· ····}e··
0030  00 00 e6 88 0c 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

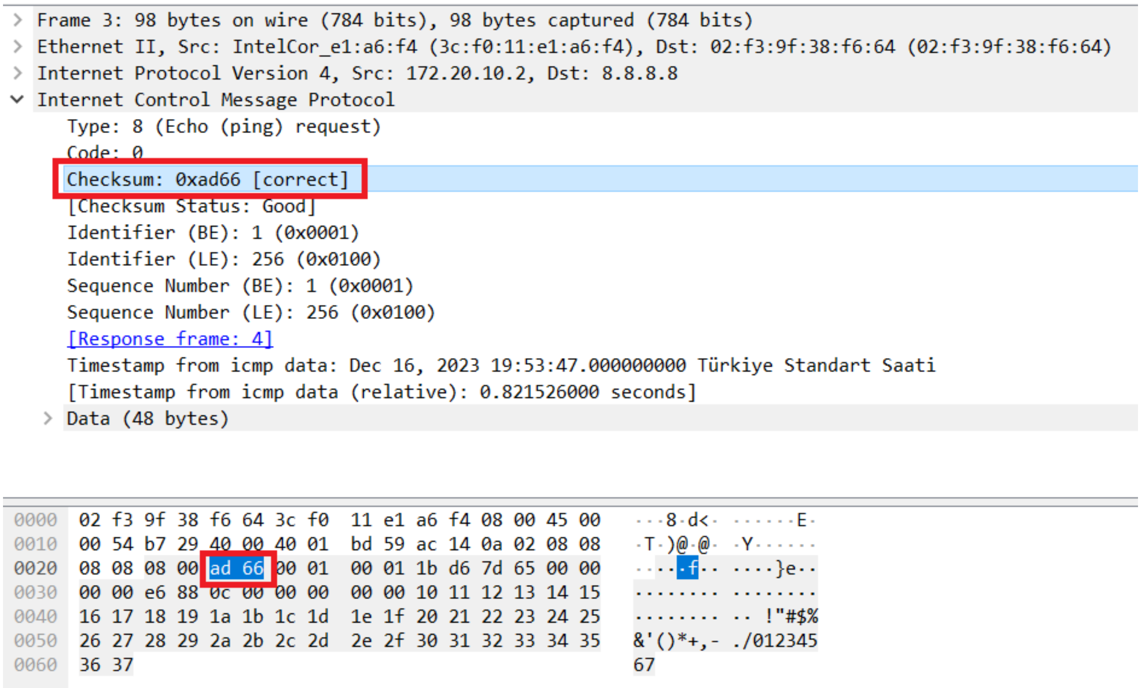
Figure 8: "Type" field



```
> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 8.8.8.8
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xad66 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 4]
    Timestamp from icmp data: Dec 16, 2023 19:53:47.000000000 Türkiye Standart Saati
    [Timestamp from icmp data (relative): 0.821526000 seconds]
  > Data (48 bytes)

0000  02 f3 9f 38 f6 64 3c f0  11 e1 a6 f4 08 00 45 00   ···8·d<· ······E·
0010  00 54 b7 29 40 00 40 01  bd 59 ac 14 0a 02 08 08   ·T·)@·@· ·Y······
0020  08 08 08 00 ad 66 00 01  00 01 1b d6 7d 65 00 00   ·····f·· ····}e··
0030  00 00 e6 88 0c 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

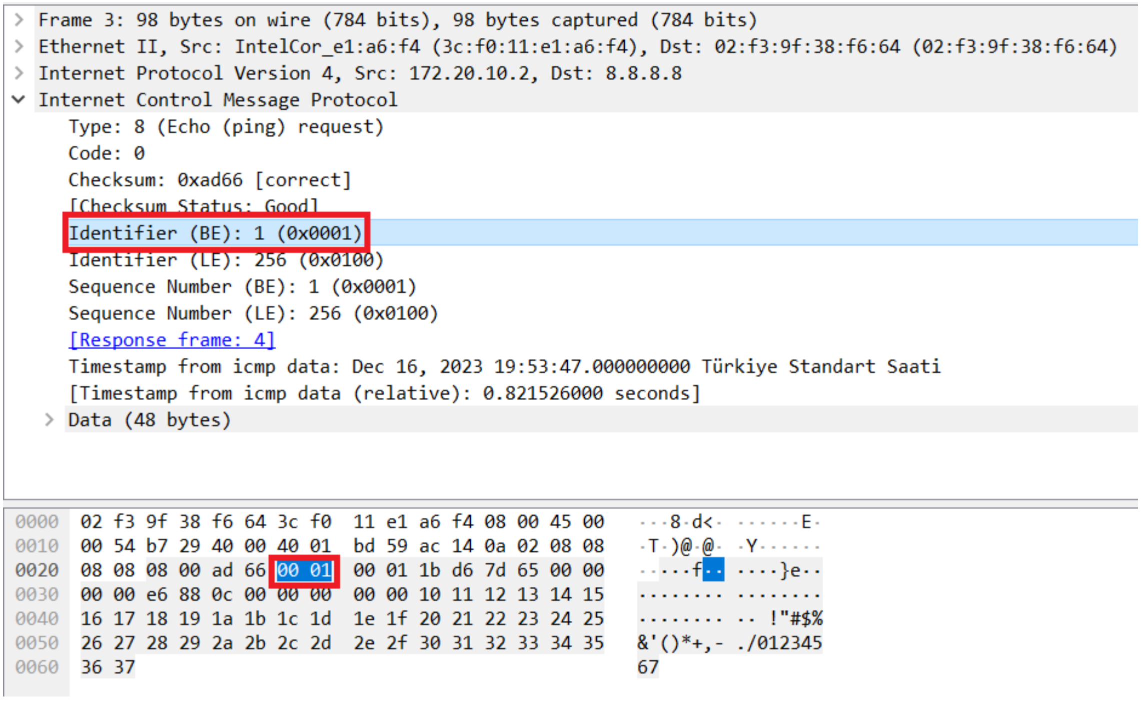
Figure 9: “Code” field



```
> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 8.8.8.8
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xad66 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 4]
    Timestamp from icmp data: Dec 16, 2023 19:53:47.000000000 Türkiye Standart Saati
    [Timestamp from icmp data (relative): 0.821526000 seconds]
  > Data (48 bytes)

0000  02 f3 9f 38 f6 64 3c f0  11 e1 a6 f4 08 00 45 00   ···8·d<· ······E·
0010  00 54 b7 29 40 00 40 01  bd 59 ac 14 0a 02 08 08   ·T·)@·@· ·Y······
0020  08 08 08 00 ad 66 00 01  00 01 1b d6 7d 65 00 00   ·····f·· ····}e··
0030  00 00 e6 88 0c 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

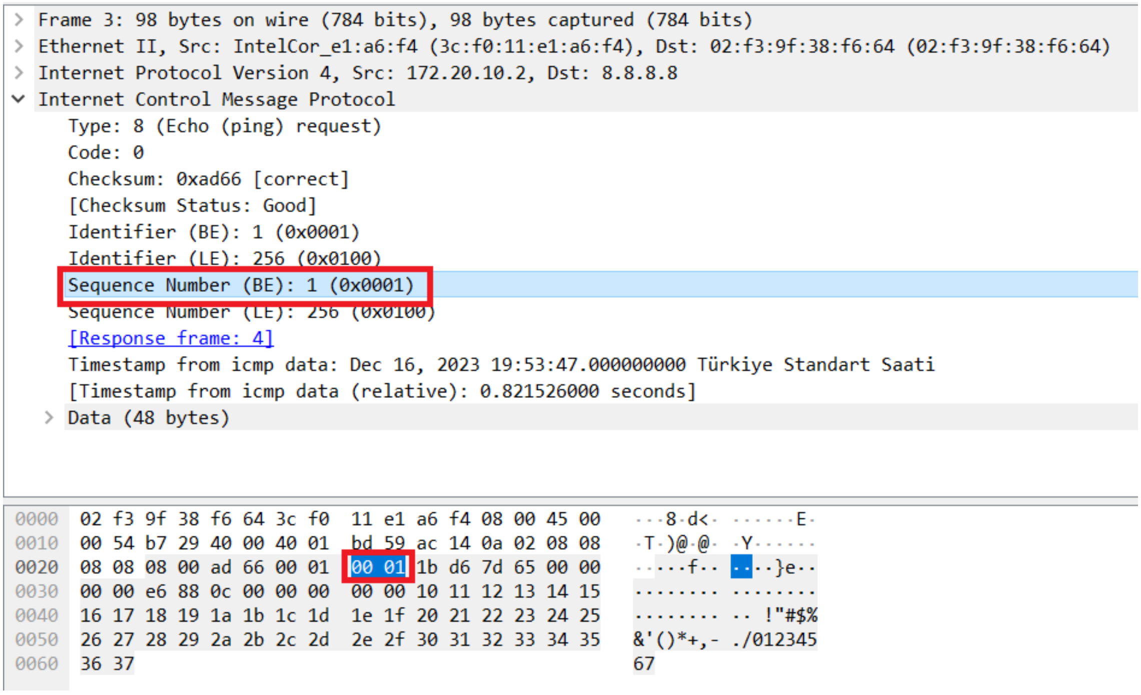
Figure 10: “Checksum” field



```
> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 8.8.8.8
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xad66 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 4]
    Timestamp from icmp data: Dec 16, 2023 19:53:47.000000000 Türkiye Standart Saati
    [Timestamp from icmp data (relative): 0.821526000 seconds]
  > Data (48 bytes)
```

```
0000  02 f3 9f 38 f6 64 3c f0  11 e1 a6 f4 08 00 45 00   ···8·d<· ······E·
0010  00 54 b7 29 40 00 40 01  bd 59 ac 14 0a 02 08 08   ·T·)@·@· ·Y······
0020  08 08 08 00 ad 66 00 01  00 01 1b d6 7d 65 00 00   ·····f·· ····}e··
0030  00 00 e6 88 0c 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

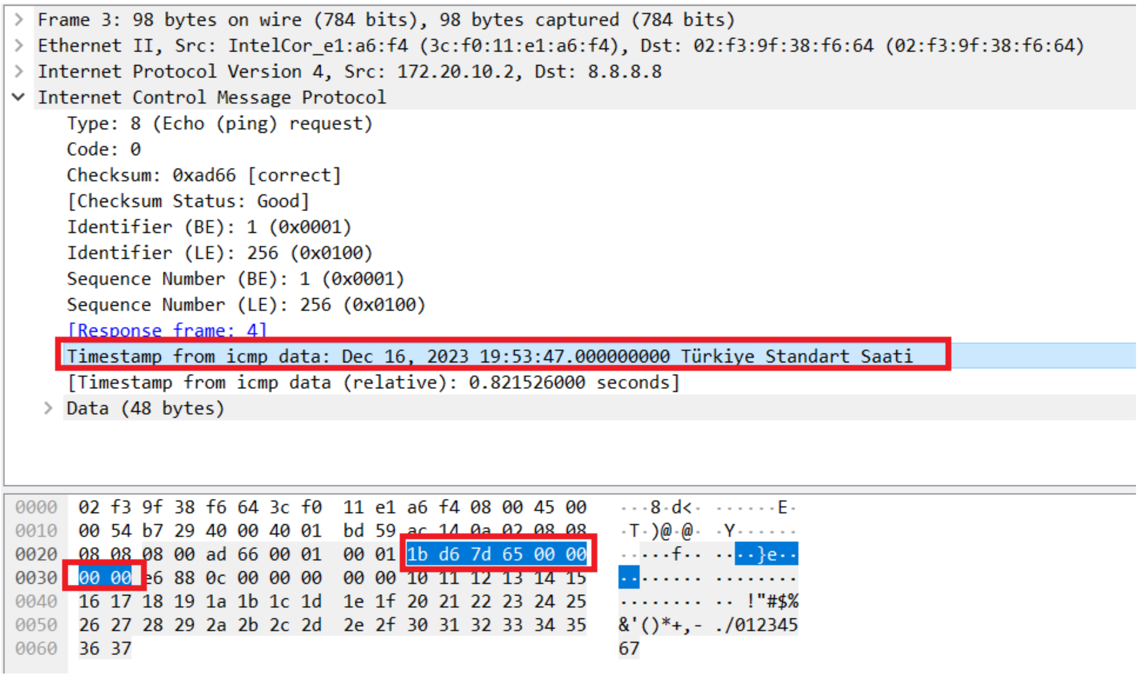
Figure 11: “Identifier” field



```
> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 8.8.8.8
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xad66 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 4]
    Timestamp from icmp data: Dec 16, 2023 19:53:47.000000000 Türkiye Standart Saati
    [Timestamp from icmp data (relative): 0.821526000 seconds]
  > Data (48 bytes)
```

```
0000  02 f3 9f 38 f6 64 3c f0  11 e1 a6 f4 08 00 45 00   ···8·d<· ······E·
0010  00 54 b7 29 40 00 40 01  bd 59 ac 14 0a 02 08 08   ·T·)@·@· ·Y······
0020  08 08 08 00 ad 66 00 01  00 01 1b d6 7d 65 00 00   ·····f·· ····}e··
0030  00 00 e6 88 0c 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

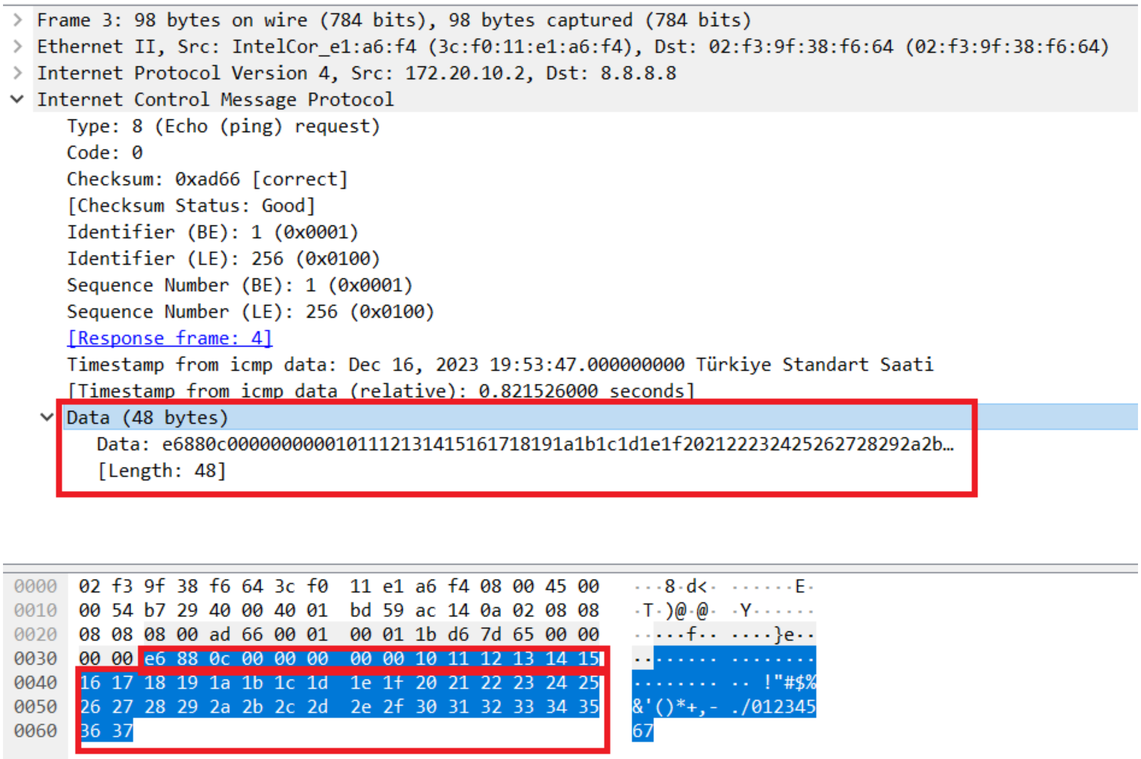
Figure 12: “Sequence Number” field



```
> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 8.8.8.8
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xad66 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 4]
    Timestamp from icmp data: Dec 16, 2023 19:53:47.000000000 Türkiye Standart Saati
    [Timestamp from icmp data (relative): 0.821526000 seconds]
  > Data (48 bytes)

0000  02 f3 9f 38 f6 64 3c f0  11 e1 a6 f4 08 00 45 00   ···8·d<· ······E·
0010  00 54 b7 29 40 00 40 01  bd 59 ac 14 0a 02 08 08   ·T·)@·@· ·Y······
0020  08 08 08 00 ad 66 00 01  00 01 1b d6 7d 65 00 00   ·····f·· ····}e··
0030  00 00 e6 88 0c 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

Figure 13: “Timestamp” field



```
> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 8.8.8.8
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xad66 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 4]
    Timestamp from icmp data: Dec 16, 2023 19:53:47.000000000 Türkiye Standart Saati
    [Timestamp from icmp data (relative): 0.821526000 seconds]
  v Data (48 bytes)
      Data: e6880c000000000010111213141516171819 1a1b1c1d1e1f202122232425262728292a2b…
      [Length: 48]

0000  02 f3 9f 38 f6 64 3c f0  11 e1 a6 f4 08 00 45 00   ···8·d<· ······E·
0010  00 54 b7 29 40 00 40 01  bd 59 ac 14 0a 02 08 08   ·T·)@·@· ·Y······
0020  08 08 08 00 ad 66 00 01  00 01 1b d6 7d 65 00 00   ·····f·· ····}e··
0030  00 00 e6 88 0c 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

Figure 14: Data (Payload)

5. The first line in my routing table is:

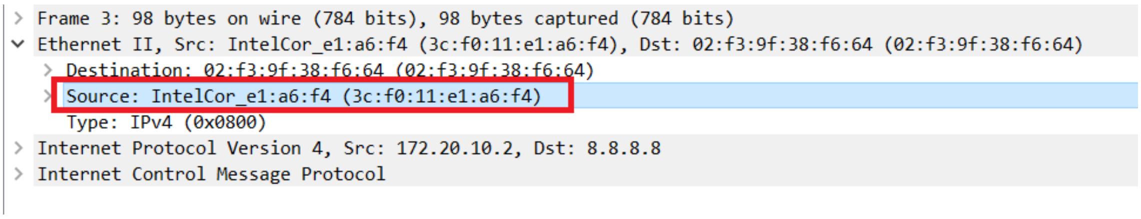
default via 144.122.204.1 dev wlo proto dhcp metric 600

This is the default gateway for my machine. That is, any packet with a destination outside of my subnet 144.122.204.0/22 is sent through the gateway 144.122.204.1.

Therefore, I should remove this rule so that the outgoing packets will be dropped, and my machine cannot send any ping requests.

6.

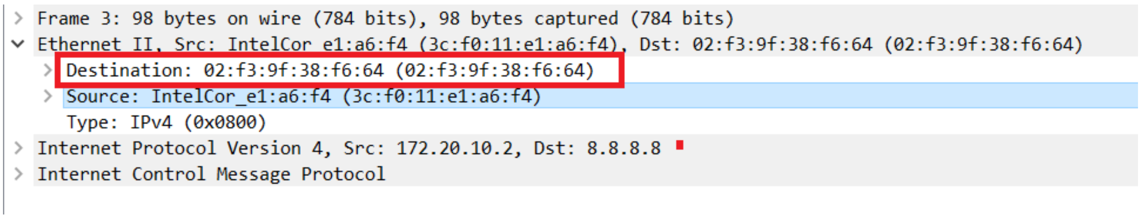
(a) My computer's Ethernet address: 3c:f0:11:e1:a6:f4



```
> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
v Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64)
  > Destination: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64)
  > Source: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 8.8.8.8
> Internet Control Message Protocol
```

Figure 15: My computer's Ethernet address

(b) Destination's Ethernet address: 02:f3:9f:38:f6:64 and this address belongs to the network interface of the destination machine.



```
> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
v Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64)
  > Destination: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64)
  > Source: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 8.8.8.8
> Internet Control Message Protocol
```

Figure 16: Destination's Ethernet address

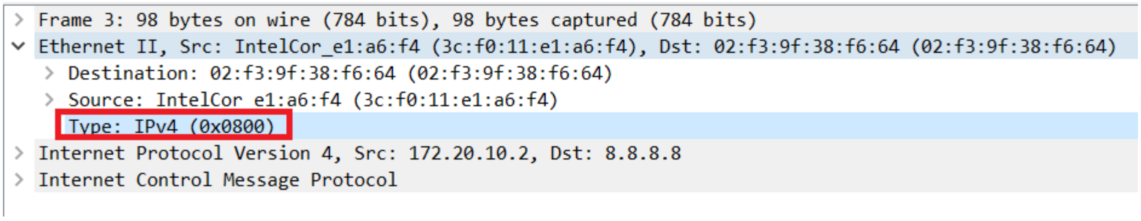
(c) I encountered 3 different values:

IPv4: This value indicates that the payload of the Ethernet frame is an IPv4 packet. IPv4 is the most widely used version of the Internet Protocol and is the foundation of the current Internet.

IPv6: This value indicates that the payload of the Ethernet frame is an IPv6 packet. IPv6 is the next-generation Internet Protocol designed to replace IPv4, providing a larger address space among other improvements.

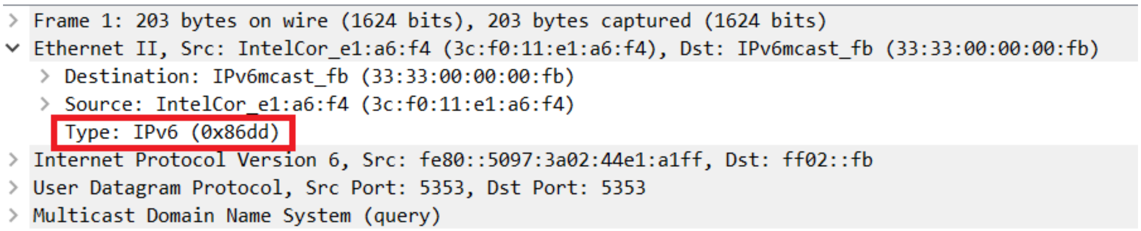
ARP: This value indicates that the payload of the Ethernet frame is an ARP (Address Resolution Protocol) packet. ARP is used for mapping an IP address to a MAC address within a local network.

If you want, here are the screenshots.



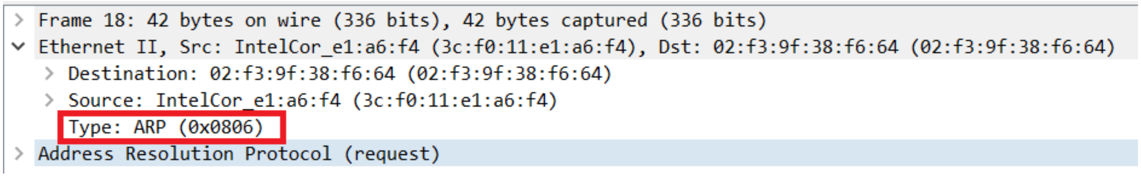
```
> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
v Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64)
    > Destination: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64)
    > Source: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
      Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 8.8.8.8
> Internet Control Message Protocol
```

Figure 17: IPv4



```
> Frame 1: 203 bytes on wire (1624 bits), 203 bytes captured (1624 bits)
v Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: IPv6mcast_fb (33:33:00:00:00:fb)
    > Destination: IPv6mcast_fb (33:33:00:00:00:fb)
    > Source: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
      Type: IPv6 (0x86dd)
> Internet Protocol Version 6, Src: fe80::5097:3a02:44e1:a1ff, Dst: ff02::fb
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (query)
```

Figure 18: IPv6



```
> Frame 18: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
v Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64)
    > Destination: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64)
    > Source: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
      Type: ARP (0x0806)
> Address Resolution Protocol (request)
```

Figure 19: ARP