# Student Information

Full Name: Deniz Polat
Id Number: 2237790

# Screenshots

Put **ICMP request**, **ICMP reply** and **route table** screenshots in this section.

```
▶ Frame 2: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▶ Ethernet II, Src: IntelCor_33:98:e3 (f8:59:71:33:98:e3), Dst: Zte_94:62:91 (dc:f8:b9:94:62:91)
▶ Internet Protocol Version 4, Src: 192.168.1.37, Dst: 1.1.1.1
▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x81ac [correct]
    [Checksum Status: Good]
    Identifier (BE): 4349 (0x10fd)
    Identifier (LE): 64784 (0xfd10)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Response frame: 3]
    Timestamp from icmp data: Jan 14, 2021 19:24:40.000000000 +03
    [Timestamp from icmp data (relative): 0.701033723 seconds]
  ▼ Data (48 bytes)
```

Figure 1: ICMP request

```
▶ Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▶ Ethernet II, Src: Zte_94:62:91 (dc:f8:b9:94:62:91), Dst: IntelCor_33:98:e3 (f8:59:71:33:98:e3)
▶ Internet Protocol Version 4, Src: 1.1.1.1, Dst: 192.168.1.37
▼ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x89ac [correct]
    [Checksum Status: Good]
    Identifier (BE): 4349 (0x10fd)
    Identifier (LE): 64784 (0xfd10)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Request frame: 2]
    [Response time: 26,144 ms]
    Timestamp from icmp data: Jan 14, 2021 19:24:40.000000000 +03
    [Timestamp from icmp data (relative): 0.727177523 seconds]
```

Figure 2: ICMP reply

```
deniz@deniz:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    600    0        0 wlp3s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 wlp3s0
192.168.1.0     0.0.0.0         255.255.255.0   U     600    0        0 wlp3s0
deniz@deniz:~$
```

Figure 3: Route Table

# Answers

## 1. (10 Points)

**Request**
**Source host:** 192.168.1.37
**Destination host:** 1.1.1.1

**Reply**
**Source host:** 1.1.1.1
**Destination host:** 192.168.1.37

## 2. (20 Points)

Since the network software is able to translate the ICMP message by itself, (without directing the ICMP message to a process inside application layer) it does not have network-layer information communication between application layer processes. Instead, it makes network-layer information communication between hosts and routers. Therefore, it does not have any source and destination port numbers.

## 3a. (15 Points)

Type and Code together tells us the message itself being received. Type identifies the message where Code gives extra information according to given Type.

## 3b. (15 Points)

Request Type is 8 and Request Code is 0, as seen in Figure 1. Type 8 means *Echo* and Code 0 for Type 8 means *No Code*
Reply Type is 0 and Reply Code is also 0, as seen in Figure 2. Type 0 means *Echo Reply* and Code 0 for Type 0 means *No Code*

(For this Type/Code to message (meaning) translation, I have used registries from Internet Assigned Numbers Authority webpage (https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml))

## 4. (20 Points)

As seen in 1st line of Figure 1, we can see that 98 bytes are transferred in total.
Ethernet protocol header : 14 bytes
IPv4 protocol header : 20 bytes
ICMP : 64 bytes (Type: 1 byte + Code: 1 byte + Checksum: 2 bytes + Identifier: 2 bytes + Sequence number: 2 bytes + Timestamp : 8 bytes + Data : 48 bytes)
Summing up all of them, we get $14 + 20 + 64 = 98$ bytes in total.

## 5. (20 Points)

First rule, which has destination 0.0.0.0 (default destination) is the one that my computer connects to network and sends ping requests. Therefore, if we delete this rule, there won't be any way to route the ping request and therefore no ping requests will be sent.