CS315: Assignment-10

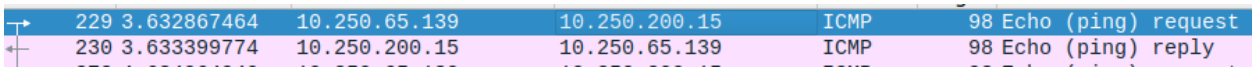
Name: Shahil Patel
Roll No.: 200010039

Part-1: ICMP and Ping

1. What is the IP address of your host? What is the IP address of the destination host?

Ans: IP address of host: **10.250.65.139**

The IP address of the destination host is: **0.250.200.15**



229	3.632867464	10.250.65.139	10.250.200.15	ICMP	98	Echo (ping) request
230	3.633399774	10.250.200.15	10.250.65.139	ICMP	98	Echo (ping) reply

2. Why is it that an ICMP packet does not have source and destination port numbers?

Ans: The ICMP packet does not contain source or destination port numbers because it was created to send network-layer information between hosts and routers rather than between application-layer processes. There is a "**Type**" and a "**Code**" in every ICMP packet. The particular message being received is identified by the Type/Code combination. No port numbers are required to direct an ICMP message to an application layer process because ***the network program understands all ICMP messages***.

3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number, and identifier fields?

Ans: ICMP type: **8 (Echo (ping) request)**

Code: **0**

Other fields present in the ICMP packet are:

- ***Checksum***
- ***Identifier (BE)***

- ***Identifier (LE)***
- ***Sequence Number (BE)***
- ***Sequence Number (LE)***
- ***Timestamp from ICMP data***

The size of the checksum, sequence number, and identifier fields is **2 bytes** each.

```
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xac02 [correct]
[Checksum Status: Good]
Identifier (BE): 3 (0x0003)
Identifier (LE): 768 (0x0300)
Sequence number (BE): 1 (0x0001)
Sequence number (LE): 256 (0x0100)
[Response frame: 141]
Timestamp from icmp data: Mar 14, 2023 10:21:23.000000000 IST
```

4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number, and identifier fields?

Ans: ICMP type: **0 (Echo (ping) reply)**

Code: **0**

Other fields present in this ICMP packet are:

- ***Checksum***
- ***Identifier (BE)***
- ***Identifier (LE)***
- ***Sequence Number (BE)***
- ***Sequence Number (LE)***
- ***Timestamp from ICMP data***

The size of the checksum, sequence number, and identifier fields is **2 bytes** each.

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xb402 [correct]
    [Checksum Status: Good]
    Identifier (BE): 3 (0x0003)
    Identifier (LE): 768 (0x0300)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Request frame: 140]
    [Response time: 0.540 ms]
    Timestamp from icmp data: Mar 14, 2023 10:21:23.000000000 IST
```

Part-2: ICMP and Traceroute

1. What is the IP address of your host? What is the IP address of the target destination host?

Ans: Source IP address: **10.250.65.139**

Destination IP address: **142.251.42.36**

```
169 7.430912593   10.250.65.139      142.251.42.36      ICMP      74 Echo (ping) request
```

2. If ICMP sent UDP packets, would the IP protocol number still be 01 for the probe packets? If not, what would it be?

Ans: It would be different if ICMP sent UDP packets. Instead of **01,** it would be switched to **0 X 11**.

3. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?

Ans: The ICMP echo packet has the **same fields** as the ping query packets.

4. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

Ans: The ICMP ***error packet is different from the ping query packets***. It contains the **IP header** and the **first 8 bytes** of the original ICMP packet for which the error is.

5. 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?

Ans: The following three ICMP packets are message type 0 (echo reply), not 11. (TTL expired). They differ because the datagrams reached the target host before the TTL expired.

6. Within the traceroute measurements, is there a link whose delay is significantly longer than others?

Ans: The connection between points 3 and 4 or 4 and 5 has a much greater latency.

```
traceroute to www.google.com (172.217.174.228), 64 hops max, 72 byte packets
 1  10.196.3.250 (10.196.3.250)  9.209 ms  5.915 ms  7.268 ms
 2  firewall.iitdh.ac.in (10.250.209.251)  5.079 ms  4.612 ms  5.426 ms
 3  14.139.150.65 (14.139.150.65)  6.170 ms  6.984 ms  6.605 ms
 4  * * *
 5  10.255.238.225 (10.255.238.225)  48.528 ms  41.230 ms  43.402 ms
 6  10.152.7.214 (10.152.7.214)  53.125 ms  39.942 ms  41.185 ms
 7  142.250.172.80 (142.250.172.80)  48.158 ms  47.430 ms  45.586 ms
 8  72.14.238.215 (72.14.238.215)  47.643 ms  45.844 ms  46.402 ms
 9  216.239.50.167 (216.239.50.167)  47.384 ms  48.191 ms  49.200 ms
10  bom12s03-in-f4.1e100.net (172.217.174.228)  42.008 ms  42.255 ms  43.209 ms
```