Lab - 10

Shashank P
200010048

- **Setup**

On running the **ping** command, the following outputs are displayed in the terminal.

```
C:\Users\Shashank>ping www.iitdh.ac.in

Pinging www.iitdh.ac.in [10.250.200.15] with 32 bytes of data:
Reply from 10.250.200.15: bytes=32 time=4ms TTL=63
Reply from 10.250.200.15: bytes=32 time=3ms TTL=63
Reply from 10.250.200.15: bytes=32 time=3ms TTL=63
Reply from 10.250.200.15: bytes=32 time=9ms TTL=63

Ping statistics for 10.250.200.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 9ms, Average = 4ms
```

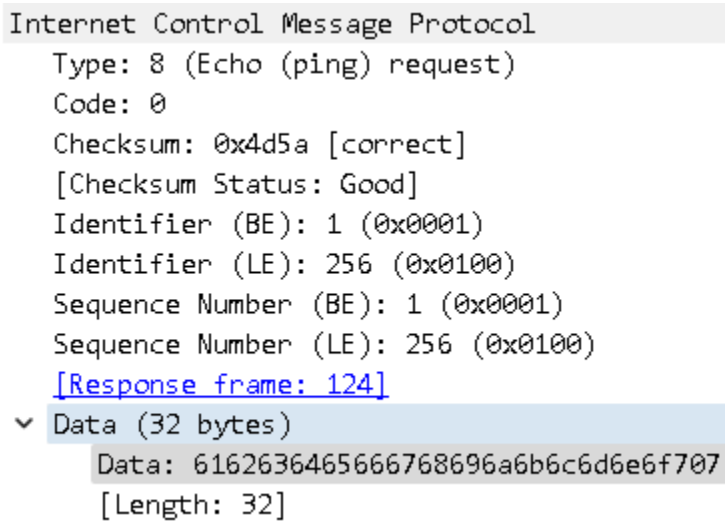
- **Part 1**

1. The IP address of my host is **10.196.9.219, and** the IP address of the destination host is **10.250.200.15**

	Time	Source	Destination	Protocol
122	0.959078	10.196.9.219	10.250.200.15	ICMP

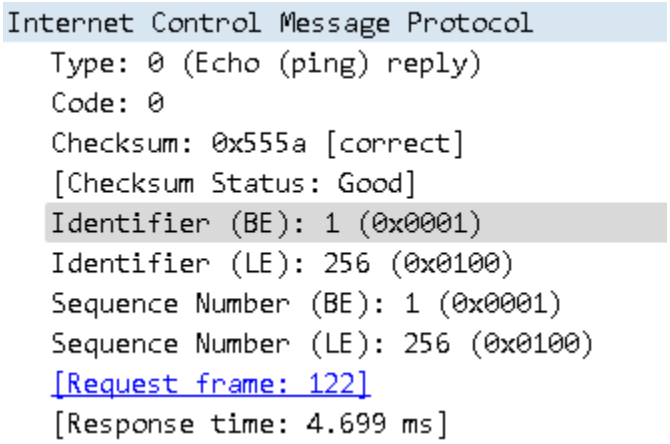
2. Since **ICMP** is a network layer protocol, it only requires the source and destination address as port numbers are present in the **transport layer.**

3. The **ICMP** type is **8 (Echo (ping) request),** and the code is **0.** The ICMP packet has fields such as **Checksum, Identifier, Sequence Number and Data.**



Checksum is size **2 bytes**; Identifier is size **2 bytes; sequence** number is size **2 bytes.**

4. The **ICMP** type is **0 (Echo (ping) reply),** and the code is **0.** The ICMP packet has fields such as **Checksum, Identifier, Sequence Number and Data.** Checksum is size **2 bytes**; Identifier is size **2 bytes; sequence** number is size **2 bytes.**



- **Part 2**

On running **tracert** the following output is obtained.

```
C:\Users\Shashank>tracert www.google.com

Tracing route to www.google.com [142.250.182.132]
over a maximum of 30 hops:

  1     4 ms    11 ms     5 ms  10.196.3.250
  2     3 ms     3 ms     3 ms  firewall.iitdh.ac.in [10.250.209.251]
  3     6 ms     5 ms     4 ms  14.139.150.65
  4     *        *        *     Request timed out.
  5    40 ms    38 ms    41 ms  10.255.238.225
  6    36 ms    37 ms    38 ms  10.152.7.214
  7    41 ms    41 ms    43 ms  72.14.204.62
  8    41 ms    43 ms    41 ms  142.251.76.33
  9    46 ms    45 ms    44 ms  108.170.248.194
 10    45 ms    44 ms    48 ms  72.14.232.51
 11    45 ms    55 ms    56 ms  74.125.242.129
 12    48 ms    49 ms    51 ms  216.239.56.65
 13    44 ms    43 ms    43 ms  maa05s22-in-f4.1e100.net [142.250.182.132]

Trace complete.
```

1. The IP address of my host is **10.196.9.219,** and the IP address of the destination port is **142.250.182.132**

```
Internet Protocol Version 4, Src: 10.196.9.219, Dst: 142.250.182.132
```

2. If ICMP sends UDP packets, The IP protocol number is **17,** while the IP protocol number for **ICMP** is **1.**

3. The ICMP echo packets have the same **type** and **code** as **part 1.**

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7f9 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 5 (0x0005)
    Sequence Number (LE): 1280 (0x0500)
```

4. The extra fields included are **Unused, IP** layer of echo request **and ICMP** of the echo request. The Type is also changed to **11 (Time-to-live exceeded).**

```
Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
    [Checksum Status: Good]
    Unused: 00000000
  > Internet Protocol Version 4, Src: 10.196.9.219, Dst: 142.250.182.132
  > Internet Control Message Protocol
```

5. The last three packets do not contain an error message. They also do not contain the requested **IP and ICMP** packets. Also, the type number is **0 (Echo (ping) reply).** This is because, in the end, the **TTL** value is large enough that the **ICMP** packet successfully reaches the destination before getting dropped. This allows the destination to send a successful reply.

```
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xffd3 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 43 (0x002b)
    Sequence Number (LE): 11008 (0x2b00)
    [Request frame: 12557]
    [Response time: 43.239 ms]
  > Data (64 bytes)
```

6. From the output of **tracert,** we can observe that the delay around link numbers **3-4-5** is significantly longer than others.

```
1     4 ms    11 ms     5 ms  10.196.3.250
2     3 ms     3 ms     3 ms  firewall.iitdh.ac.in [10.250.209.251]
3     6 ms     5 ms     4 ms  14.139.150.65
4     *        *        *     Request timed out.
5    40 ms    38 ms    41 ms  10.255.238.225
6    36 ms    37 ms    38 ms  10.152.7.214
7    41 ms    41 ms    43 ms  72.14.204.62
```

- **Part 3**

On running the UDP client pinger, the following output is obtained.