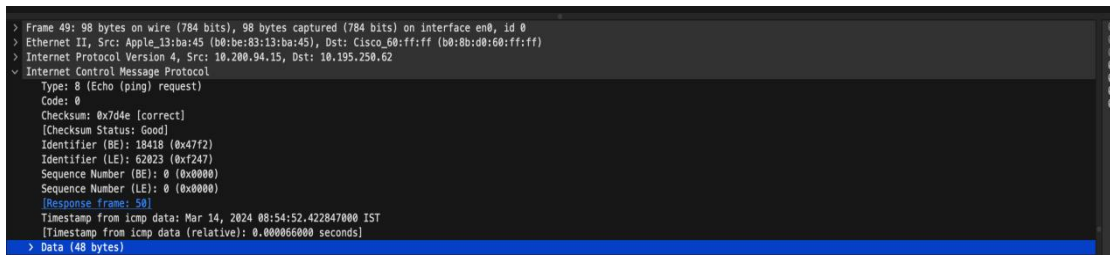


# Assignment 10

## 210010033

### Part 1:

1. Source IP: 10.200.94.15  
Destination IP: 10.195.250.62
2. ICMP is a network layer protocol, hence it does not contain source, destination port number which are usually required in application and transport layer protocols.
- 3.



```
> Frame 49: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
> Ethernet II, Src: Apple_13:ba:45 (b0:be:83:13:ba:45), Dst: Cisco_60:ff:ff (b0:8b:d0:60:ff:ff)
> Internet Protocol Version 4, Src: 10.200.94.15, Dst: 10.195.250.62
< Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x7d4e [correct]
  [Checksum Status: Good]
  Identifier (BE): 18418 (0x47f2)
  Identifier (LE): 62023 (0xf247)
  Sequence Number (BE): 0 (0x0000)
  Sequence Number (LE): 0 (0x0000)
  [Response frame: 50]
  Timestamp from icmp data: Mar 14, 2024 08:54:52.422847000 IST
  [Timestamp from icmp data (relative): 0.000066000 seconds]
> Data (48 bytes)
```

Type: 8 (Echo (ping) request)  
Code: 0

Other fields include Checksum, Identifiers,  
Sequence Numbers, Timestamps, Data

Checksum is 2 bytes. Sequence number is 2 bytes  
and Identifier is 2 bytes

4.

```
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x854e [correct]
[Checksum Status: Good]
Identifier (BE): 18418 (0x47f2)
Identifier (LE): 62023 (0xf247)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[Request frame: 49]
[Response time: 4.095 ms]
Timestamp from icmp data: Mar 14, 2024 08:54:52.422847000 IST
[Timestamp from icmp data (relative): 0.004161000 seconds]
> Data (48 bytes)
```

Type: 0 (Echo (ping) reply)

Code: 0

Other fields include Checksum, Identifiers, Sequence Numbers, Timestamps, Response Time and Data

Checksum, Sequence number and identifier are 2 bytes each.

Part 2:

1. Source IP:10.200.94.15  
Destination IP: 142.250.183.132

2. If we use the UDP stream, the protocol number would be 17.

```
> Frame 6: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface en0, id 0
> Ethernet II, Src: Apple_13:ba:45 (b0:be:83:13:ba:45), Dst: Cisco_60:ff:ff (b0:8b:d0:60:ff:ff)
> Internet Protocol Version 4, Src: 10.200.94.15, Dst: 142.250.183.132
> Internet Control Message Protocol
Type: 0 (Echo (ping) request)
Code: 0
Checksum: 0x055f [correct]
[Checksum Status: Good]
Identifier (BE): 02111 (0xf29f)
Identifier (LE): 40946 (0x9ff2)
Sequence Number (BE): 1 (0x0001)
Sequence Number (LE): 256 (0x0100)
> [No response seen]
> Data (44 bytes)
```

3. No Response Seen field was extra field compared to from the ICMP ping query packets in the first half of this lab. Also, values of identifiers, checksum were completely different.

4.

```
> Frame 1188: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface en0, id 0
> Ethernet II, Src: Cisco_12:2a:c2 (f8:7a:41:12:2a:c2), Dst: Apple_13:ba:45 (08:0e:83:13:ba:45)
> Internet Protocol Version 4, Src: 142.250.214.113, Dst: 10.200.94.15
> 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: 10.200.94.15, Dst: 142.250.183.132
> Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x053c [unverified] [in ICMP error packet]
  [Checksum Status: Unverified]
  Identifier (BE): 62111 (0xf29f)
  Identifier (LE): 48946 (0xaf22)
  Sequence Number (BE): 36 (0x0024)
  Sequence Number (LE): 9216 (0x2400)
  Data (44 bytes)
```

The error packet itself contains IP and ICMP information. Also it has an Unused field.

5.

```
> Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x0d39 [correct]
  [Checksum Status: Good]
  Identifier (BE): 62111 (0xf29f)
  Identifier (LE): 48946 (0xaf22)
  Sequence Number (BE): 36 (0x0024)
  Sequence Number (LE): 9984 (0x2700)
  [Request frame: 1195]
  [Response time: 41.663 ms]
  Data (44 bytes)
```

The error packets sent were type 11, compared to the last three packets which are of type 0. They are different because they have all arrived before the TTL expires whereas the error packet exceeded its TTL.

6.

1	10.200.92.2 (10.200.92.2)	6.093 ms	4.084 ms	4.745 ms
2	10.240.0.1 (10.240.0.1)	16.129 ms	52.814 ms	55.042 ms
3	10.240.240.1 (10.240.240.1)	4.255 ms	4.053 ms	4.079 ms
4	117.205.73.161 (117.205.73.161)	5.437 ms	13.845 ms	5.616 ms
5	***			
6	***			
7	142.250.160.26 (142.250.160.26)	18.904 ms	18.518 ms	18.054 ms
8	216.239.43.135 (216.239.43.135)	21.611 ms	21.265 ms	23.161 ms
9	142.251.50.58 (142.251.50.58)	22.496 ms	24.567 ms	21.480 ms
10	142.250.56.38 (142.250.56.38)	49.771 ms	47.485 ms	48.271 ms
11	142.250.226.135 (142.250.226.135)	45.478 ms	44.522 ms	44.742 ms
12	142.250.214.113 (142.250.214.113)	40.599 ms	40.605 ms	42.003 ms
13	bm07s31-in-f4.1e100.net (142.250.183.132)	43.636 ms	43.810 ms	44.517 ms

A larger time gap is seen between the 9<sup>th</sup> and 10<sup>th</sup> traceroute packets.