Assignment 10

210010020

---

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

A]   Source: 10.200.181.153
             Destination: 10.195.250.62

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

A] ICMP packets communicate network level information and not between application layer processes.

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?

```
˅ Internet Control Message Protocol
        Type: 8 (Echo (ping) request)
        Code: 0
        Checksum: 0x4d52 [correct]
        [Checksum Status: Good]
        Identifier (BE): 1 (0x0001)
        Identifier (LE): 256 (0x0100)
        Sequence Number (BE): 9 (0x0009)
        Sequence Number (LE): 2304 (0x0900)
        [Response frame: 265]
   > Data (32 bytes)
```

Other fields in this ICMP packet:
Checksum, Checksum status ,Identifier ,Sequence number.
checksum, sequence number and identifier fields are of 2 bytes.

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?

A] Type 0 and code 0.

```
    Total Length: 60
    Identification: 0x0ac2 (2754)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 62
    Protocol: ICMP (1)
    Header Checksum: 0xac9c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.195.250.62
    Destination Address: 10.200.181.153
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x5552 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 9 (0x0009)
    Sequence Number (LE): 2304 (0x0900)
    [Request frame: 264]
    [Response time: 2.798 ms]
v Data (32 bytes)
     Data: 6162636465666768696a6b6c6d6e6f707172737475767761626364656667686869
     [Length: 32]
```

In addition to Request packet this has an extra field that is Response time.
Checksum, sequence number and identifier fields are of 2 bytes.

Part2:

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

A]   Source: 10.200.181.153
        Destination: 216.58.196.68

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

A] No, for UDP it would be 17.

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?

A] There is no response seen for this packet and Data field is of 64 bytes whereas in ping it was 32 bytes, field. Sequence number and checksum are different.

```
∨ Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0xf7eb [correct]
      [Checksum Status: Good]
      Identifier (BE): 1 (0x0001)
      Identifier (LE): 256 (0x0100)
      Sequence Number (BE): 19 (0x0013)
      Sequence Number (LE): 4864 (0x1300)
  ∨ [No response seen]
      > [Expert Info (Warning/Sequence): No response seen to ICMP request]
  ∨ Data (64 bytes)
        Data: 0000000000000000000000000000000000000000000000000000000000000000000000000000000
        [Length: 64]
```
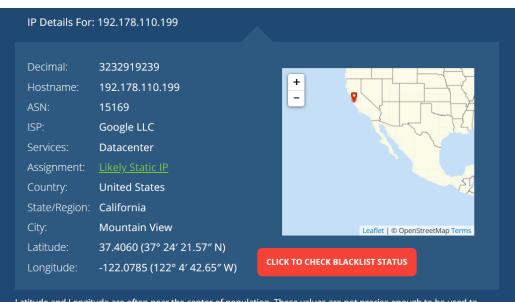
4. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

A] In the error message along with the IP and ICMP there is an extra 8 bytes that indicates error in the message sent. Unused is the extra field present here.

```
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
```

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?

A] The error packets have a TTL Expired error so error code = 11 and checksum unverified whereas the last three packets have error code 0 as the packets are sent before TTL expires. There is also data in these packets.

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

A] Link with significant delay: 12   202 ms   715 ms   204 ms 192.178.110.199.
This is originated from

IP Details For: 192.178.110.199

Decimal:	3232919239
Hostname:	192.178.110.199
ASN:	15169
ISP:	Google LLC
Services:	Datacenter
Assignment:	Likely Static IP
Country:	United States
State/Region:	California
City:	Mountain View
Latitude:	37.4060 (37° 24′ 21.57″ N)
Longitude:	-122.0785 (122° 4′ 42.65″ W)

Leaflet | © OpenStreetMap Terms

CLICK TO CHECK BLACKLIST STATUS

Latitude and Longitude are often near the center of population. These values are not precise enough to be used to identify a specific address, individual, or for legal purposes. IP data from IP2Location.