

Name: Serena Anthony
Roll : B210031CS

Assignment 2

Part I: ICMP using ping

ping -c 10 www.google.com

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

Src host IP addr: 2401:4900:614d:68a2:446c:2052:ef64:6880

Destination host IP addr: 2404:6800:4007:811::2004

Source IP address → address of our host

Destination IP address → address of destination host

```
[Coloring Rule String: icmp || icmpv6]
- Ethernet II, Src: IntelCor_6b:e7:c5 (2c:6d:c1:6b:e7:c5), Dst: da:71:9a:cb:f2:b9 (da:71:9a:cb:f2:b9)
  > Destination: da:71:9a:cb:f2:b9 (da:71:9a:cb:f2:b9)
  > Source: IntelCor_6b:e7:c5 (2c:6d:c1:6b:e7:c5)
  Type: IPv6 (0x86dd)
- Internet Protocol Version 6, Src: 2401:4900:614d:68a2:446c:2052:ef64:6880, Dst: 2404:6800:4007:811::2004
  0110 .... = Version: 6
```

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

ICMP (Internet Control Message Protocol) is the protocol which operates at the network layer whereas port numbers are associated with transport layer protocols such as TCP & UDP.

Since ICMP operates at lower layer therefore it doesn't have source and destination port numbers.

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?

ICMP Type: Echo (ping) request (128)

ICMP Code: 0

Other fields in the ICMP packet include:

- Identifier (usually a unique number to match requests with replies)
- Sequence number (incremented for each request)
- Checksum (used for error-checking)

Length of Checksum: 2 bytes

Length of Sequence number: 2 bytes

Length of Identifier: 2 bytes

```
2401:4900:614d:68a2::... 2404:6800:4007:811::... ICMPv6 118 Echo (ping) request id=0xb39e, seq=10, hop li
2404:6800:4007:811::... 2401:4900:614d:68a2::... ICMPv6 118 Echo (ping) reply id=0xb39e, seq=10, hop li

Type: IPv6 (0x86dd)
- Internet Protocol Version 6, Src: 2401:4900:614d:68a2:446c:2052:ef64:6880, Dst: 2404:6800:4007:811:
  0110 .... = Version: 6
  > .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 1010 1000 0011 0011 0010 = Flow Label: 0xa8332
  Payload Length: 64
  Next Header: ICMPv6 (58)
  Hop Limit: 64
  Source Address: 2401:4900:614d:68a2:446c:2052:ef64:6880
  Destination Address: 2404:6800:4007:811::2004
- Internet Control Message Protocol v6
  Type: Echo (ping) request (128)
  Code: 0
  Checksum: 0x78ee [correct]
  [Checksum Status: Good]
  Identifier: 0xb39e
  Sequence: 10
  [Response In: 96]
- Data (56 bytes)
  Data: f7220c660000000009bdc0d0000000000101112131415161718191a1b1c1d1e1f20212223...
  [Length: 56]
```

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?

ICMP Type: Echo (ping) reply (129)

ICMP Code: 0

Other fields in the ICMP packet include:

- Identifier (usually a unique number to match requests with replies)
- Sequence number (incremented for each request)
- Checksum (used for error-checking)

Checksum: 2 bytes

Sequence number: 2 bytes

Identifier: 2 bytes

```
2404:6800:4007:811:... 2401:4900:614d:68a2:... ICMPv6 118 Echo (ping) reply id=0xb39e, seq=10, hop li
Internet Protocol Version 6, Src: 2404:6800:4007:811::2004, Dst: 2401:4900:614d:68a2:446c:2052:ef64
  0110 .... = Version: 6
  ▸ .... 1011 1000 .... .... = Traffic Class: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    .... 1010 1000 0011 0011 0010 = Flow Label: 0xa8332
    Payload Length: 64
    Next Header: ICMPv6 (58)
    Hop Limit: 58
    Source Address: 2404:6800:4007:811::2004
    Destination Address: 2401:4900:614d:68a2:446c:2052:ef64:6880
  ▾ Internet Control Message Protocol v6
    Type: Echo (ping) reply (129)
    Code: 0
    Checksum: 0x77ee [correct]
    [Checksum Status: Good]
    Identifier: 0xb39e
    Sequence: 10
    [Response To: 95]
    [Response Time: 105.931 ms]
  ▾ Data (56 bytes)
    Data: f7220c660000000009bdc0d0000000000101112131415161718191a1b1c1d1e1f20212223...
    [Length: 56]
```

Part II: ICMP using traceroute

i. *traceroute -l www.youtube.com 64*

ii. *traceroute -l www.youtube.com 3000*

1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window.

No.	Time	Source	Destination	Protocol	Length	Info
5	0.184249943	192.168.83.113	142.250.196.14	ICMP	78	Echo (ping) request id=0x575d, s
<ul style="list-style-type: none"> Frame 5: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface wlp0s20f3, id 0 Ethernet II, Src: IntelCor_6b:e7:c5 (2c:6d:c1:6b:e7:c5), Dst: da:71:9a:cb:f2:b9 (da:71:9a:cb:f2:b9) Internet Protocol Version 4, Src: 192.168.83.113, Dst: 142.250.196.14 <ul style="list-style-type: none"> 0100 = Version: 4 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 64 Identification: 0x4108 (16648) 000. = Flags: 0x0 ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 1 Protocol: ICMP (1) Header Checksum: 0x1193 [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.83.113 Destination Address: 142.250.196.14 Internet Control Message Protocol 						

2. Which of the IP datagrams are fragmented?

Ans:

IP datagrams are fragmented when the size of the packet exceeds the Maximum Transmission Unit of the network path. The More fragments (MF) bit is set indicating that there is fragmentation.

The Fragment offset is set to 1480 in the second image which further confirms that the packet is a part of a fragmented IP datagram.

IP datagrams of the second traceroute command, with size of 3000 bytes are fragmented.

No.	Time	Source	Destination	Protocol	Length	Info
147	13.742180668	2401:4900:614d:68a2...	2401:4900:614d:68a2...	DNS	244	Standard query response 0xb0b0 AAAA www.youtube.com
148	13.743473135	192.168.83.113	142.250.196.46	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0144)
Frame 148: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface wlp0s20f3, id 0 Ethernet II, Src: IntelCor_6b:e7:c5 (2c:6d:c1:6b:e7:c5), Dst: da:71:9a:cb:f2:b9 (da:71:9a:cb:f2:b9) Destination: da:71:9a:cb:f2:b9 (da:71:9a:cb:f2:b9) Source: IntelCor_6b:e7:c5 (2c:6d:c1:6b:e7:c5) Type: IPv4 (0x0800) Internet Protocol Version 4, Src: 192.168.83.113, Dst: 142.250.196.46 0100 = Version: 4 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 1500 Identification: 0x0144 (324) 001. = Flags: 0x1, More fragments 0... = Reserved bit: Not set .0.. = Don't fragment: Not set ..1. = More fragments: Set ...0 0000 0000 0000 = Fragment Offset: 0						
149	13.743491482	192.168.83.113	142.250.196.46	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=0144)
150	13.743494764	192.168.83.113	142.250.196.46	ICMP	54	Echo (ping) request id=0x577f, seq=1/256, ttl=1 (no response)
Frame 149: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface wlp0s20f3, id 0 Ethernet II, Src: IntelCor_6b:e7:c5 (2c:6d:c1:6b:e7:c5), Dst: da:71:9a:cb:f2:b9 (da:71:9a:cb:f2:b9) Destination: da:71:9a:cb:f2:b9 (da:71:9a:cb:f2:b9) Source: IntelCor_6b:e7:c5 (2c:6d:c1:6b:e7:c5) Type: IPv4 (0x0800) Internet Protocol Version 4, Src: 192.168.83.113, Dst: 142.250.196.46 0100 = Version: 4 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 1500 Identification: 0x0144 (324) 001. = Flags: 0x1, More fragments 0... = Reserved bit: Not set .0.. = Don't fragment: Not set ..1. = More fragments: Set ...0 0000 1011 1001 = Fragment Offset: 1480						

3. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?

Ans:

The fields that typically change from one datagram to the next within a series of ICMP messages include:

- Header Checksum
- Identification field

Time-to-live (TTL) field decreases by one each time the packet passes through a router.

7	0.184291389	192.168.83.113	142.250.196.14	ICMP	78 Echo (ping) request	id=0x575d, seq=3/768, ttl=1
8	0.184304185	192.168.83.113	142.250.196.14	ICMP	78 Echo (ping) request	id=0x575d, seq=4/1024, ttl=2

▶ Frame 7: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface wlp0s20f3, id 0
 ▼ Ethernet II, Src: IntelCor_6b:e7:c5 (2c:6d:c1:6b:e7:c5), Dst: da:71:9a:cb:f2:b9 (da:71:9a:cb:f2:b9)
 ▶ Destination: da:71:9a:cb:f2:b9 (da:71:9a:cb:f2:b9)
 ▶ Source: IntelCor_6b:e7:c5 (2c:6d:c1:6b:e7:c5)
 Type: IPv4 (0x0800)
 ▼ Internet Protocol Version 4, Src: 192.168.83.113, Dst: 142.250.196.14
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 64
 Identification: 0x410a (16650)
 ▼ 000. = Flags: 0x0
 0... = Reserved bit: Not set
 .0.. = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment Offset: 0
 ▶ Time to Live: 1
 Protocol: ICMP (1)
 Header Checksum: 0x1191 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 192.168.83.113
 Destination Address: 142.250.196.14
 ▶ Internet Control Message Protocol

6	0.184289191	192.168.83.113	142.250.196.14	ICMP	78 Echo (ping) request	id=0x575d, seq=2/512, ttl=1
7	0.184291389	192.168.83.113	142.250.196.14	ICMP	78 Echo (ping) request	id=0x575d, seq=3/768, ttl=1
8	0.184304185	192.168.83.113	142.250.196.14	ICMP	78 Echo (ping) request	id=0x575d, seq=4/1024, ttl=2

▶ Frame 8: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface wlp0s20f3, id 0
 ▼ Ethernet II, Src: IntelCor_6b:e7:c5 (2c:6d:c1:6b:e7:c5), Dst: da:71:9a:cb:f2:b9 (da:71:9a:cb:f2:b9)
 ▶ Destination: da:71:9a:cb:f2:b9 (da:71:9a:cb:f2:b9)
 ▶ Source: IntelCor_6b:e7:c5 (2c:6d:c1:6b:e7:c5)
 Type: IPv4 (0x0800)
 ▼ Internet Protocol Version 4, Src: 192.168.83.113, Dst: 142.250.196.14
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 64
 Identification: 0x410b (16651)
 ▼ 000. = Flags: 0x0
 0... = Reserved bit: Not set
 .0.. = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment Offset: 0
 ▶ Time to Live: 2
 Protocol: ICMP (1)
 Header Checksum: 0x1090 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 192.168.83.113
 Destination Address: 142.250.196.14
 ▶ Internet Control Message Protocol

4. Which fields stay constant? Why?

The **source IP** address remains constant in a series of ICMP packets sent during a traceroute operation because it identifies the sender of the packets. In traceroute, the packets are all being sent from the same host (my computer) to the same destination (www.youtube.com in this case).

The **destination IP** address remains constant throughout the traceroute operation. Traceroute sends a series of ICMP Echo Request packets towards a specific destination, typically to discover the route taken by packets from the source to the destination.

Protocol field is constant as it indicated that it is ICMP (Internet Control Message Protocol).