Assignment 10

Part-1

1. IP address of host: 10.240.203.43

The IP address of the destination host is: 10.195.250.62

icmp									
No.	Time	Source	Destination	Protocol	Length	Info			
→ 30	3.396610	10.240.203.43	10.195.250.62	ICMP	74	Echo	(ping)	request	

2. 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. For Echo (ping) request

ICMP Type: 8

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

	icmp									
No		Time	Source	Destination	Protocol I	Length	Info			
	30	3.396610	10.240.203.43	10.195.250.62	ICMP	74	Echo	(ping)	req	uest
4	31	3.402941	10.195.250.62	10.240.203.43	ICMP	74	Echo	(ping)	rep	ly
>	Frame	30: 74 bytes on wire	(592 bits). 74 bytes	captured (592 bits) o	n interfa	ice \D	evice	0000	f8	7a 4:
			•					0010		3c d
>	Internet Protocol Version 4, Src: 10.240.203.43, Dst: 10.195.250.62							0020		3e 08
~	∨ Internet Control Message Protocol							0040		68 69 61 62
Type: 8 (Echo (ping) request)										
Code: 0										
Checksum: 0x4d5a [correct]										
[Checksum Status: Good]										
Identifier (BE): 1 (0x0001)										
Identifier (LE): 256 (0x0100)										
Sequence Number (BE): 1 (0x0001)										
Sequence Number (LE): 256 (0x0100)										
[Response frame: 31]										
	> Dat	a (32 bytes)								

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

4. For Echo (ping) reply

ICMP Type: 0

Code: 0

Other fields present in the ICMP packet are:

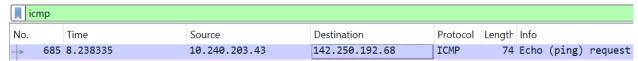
- Checksum
- Identifier (BE)
- Identifier (LE)
- Sequence Number (BE)
- Sequence Number (LE)
- Timestamp from ICMP data

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

```
10.195.250.62
                                                  10.240.203.43
                                                                        ICMP
     31 3.402941
                                                                                   74 Echo (ping) reply
> Frame 31: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device
                                                                                                  14 13
                                                                                                  00 3c |
> Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: AzureWaveTec_c7:3e:39 (14:13
                                                                                            0020
                                                                                                  cb 2b
> Internet Protocol Version 4, Src: 10.195.250.62, Dst: 10.240.203.43
                                                                                            0030
                                                                                                  67 68
Internet Control Message Protocol
                                                                                            0040
     Type: 0 (Echo (ping) reply)
     Code: 0
     Checksum: 0x555a [correct]
     [Checksum Status: Good]
     Identifier (BE): 1 (0x0001)
     Identifier (LE): 256 (0x0100)
     Sequence Number (BE): 1 (0x0001)
     Sequence Number (LE): 256 (0x0100)
     [Request frame: 30]
     [Response time: 6.331 ms]
  > Data (32 bytes)
```

Part-2

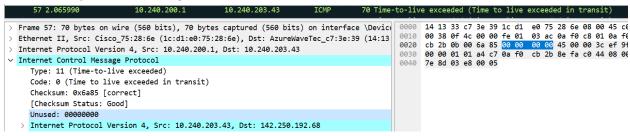
Source IP address: 10.240.203.43
 Destination IP address: 142.250.192.68



- 2. It would be different if ICMP sent UDP packets. Instead of 01, it would be switched to 0 X 11 (= 17).
- **3.** The ICMP echo packet has the **same fields** as the ping query packets.

```
685 8.238335
                              10.240.203.43
                                                   142.250.192.68
                                                                        ICMP
                                                                                   74 Echo (ping) request
    686 8.238347
                             10.240.203.43
                                                   142.250.192.68
                                                                        ICMP
                                                                                   74 Echo (ping) request
                                                                                                  f8 7a 4
> Frame 685: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Devi
                                                                                            0000
                                                                                            0010
                                                                                                  00 3c e
> Ethernet II, Src: AzureWaveTec c7:3e:39 (14:13:33:c7:3e:39), Dst: Cisco 13:2a:c2 (f8:7a
                                                                                            9929 cg 44 9
> Internet Protocol Version 4, Src: 10.240.203.43, Dst: 142.250.192.68
                                                                                            0030 4e 4f 5
Internet Control Message Protocol
                                                                                            0040 5e 5f 6
     Type: 8 (Echo (ping) request)
     Code: 0
     Checksum: 0x7e6a [correct]
     [Checksum Status: Good]
     Identifier (BE): 1000 (0x03e8)
     Identifier (LE): 59395 (0xe803)
     Sequence Number (BE): 40 (0x0028)
     Sequence Number (LE): 10240 (0x2800)
     [Response frame: 695]
  > Data (32 bytes)
```

4. 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.** The last three ICMP packets received by the source host are messages of **Type 0 (echo reply)**, **not Type 11 (TTL expired)**. They differ because the datagrams reached the target host before the TTL expired.
- 6. The connection between points 3 and 4 or 9 and 10 has a much greater latency

```
paru04@LAPTOP-NVGR5VB8:~$ traceroute -I www.google.com
traceroute to www.google.com (142.250.192.68), 30 hops max, 60 byte packets
   LAPTOP-NVGR5VB8.mshome.net (172.23.208.1) 0.465 ms 0.449 ms 0.448 ms
   10.240.200.1 (10.240.200.1) 2.044 ms 2.565 ms 2.564 ms
   10.240.240.1 (10.240.240.1) 2.781 ms 2.781 ms
   117.205.73.161 (117.205.73.161) 28.601 ms 28.600 ms
 5
   * * *
 6
   * * *
 7
   142.250.160.26 (142.250.160.26) 18.553 ms 24.637 ms 19.690 ms
   142.251.227.217 (142.251.227.217)
                                      20.545 ms 20.541 ms
                                                           20.539 ms
9
   142.251.229.250 (142.251.229.250) 20.536 ms
                                               20.534 ms
                                                           20.532 ms
10
   64.233.174.3 (64.233.174.3)
                                23.752 ms 23.749 ms 23.747 ms
11
   142.251.49.232 (142.251.49.232) 52.257 ms 52.255 ms 52.253 ms
12
   192.178.110.207 (192.178.110.207)
                                     52.096 ms 52.094 ms 52.071 ms
13
   108.170.226.131 (108.170.226.131) 51.047 ms * *
   bom12s16-in-f4.1e100.net (142.250.192.68)
                                            57.473 ms 57.471 ms 57.469 ms
```