

CS315 : Computer Networks Lab

Assignment 10

Sourabh Bhosale (200010004)

March 14, 2023

1 Part-1: ICMP and Ping

```
~ $ ping -c 10 www.iitdh.ac.in
PING www.iitdh.ac.in (10.250.200.15): 56 data bytes
64 bytes from 10.250.200.15: icmp_seq=0 ttl=63 time=5.719 ms
64 bytes from 10.250.200.15: icmp_seq=1 ttl=63 time=10.828 ms
64 bytes from 10.250.200.15: icmp_seq=2 ttl=63 time=6.937 ms
64 bytes from 10.250.200.15: icmp_seq=3 ttl=63 time=10.886 ms
64 bytes from 10.250.200.15: icmp_seq=4 ttl=63 time=11.866 ms
64 bytes from 10.250.200.15: icmp_seq=5 ttl=63 time=12.994 ms
64 bytes from 10.250.200.15: icmp_seq=6 ttl=63 time=6.911 ms
64 bytes from 10.250.200.15: icmp_seq=7 ttl=63 time=9.254 ms
64 bytes from 10.250.200.15: icmp_seq=8 ttl=63 time=11.873 ms
64 bytes from 10.250.200.15: icmp_seq=9 ttl=63 time=14.179 ms

--- www.iitdh.ac.in ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 5.719/10.145/14.179/2.692 ms
~ $
```

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

Source IP address: 10.196.77.134

Destination IP address: 10.250.200.15

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

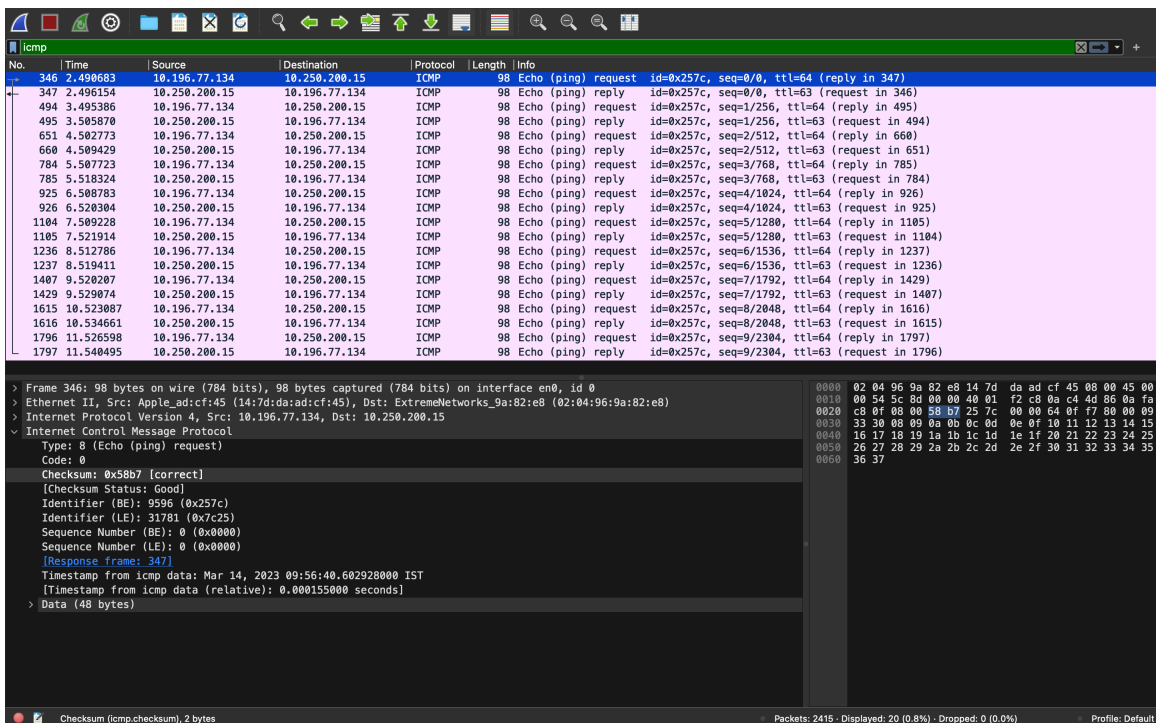
The ICMP packet does not have source and destination port numbers because it was designed to communicate network-layer information between hosts and routers, not between application layer processes.

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?

ICMP type : 8 (Echo (ping) request), Code number : 0

This ICMP packet has other fields like Checksum, Identifier (BE), Identifier (LE), Sequence Number (BE), Sequence Number (LE), Timestamp from icmp data and data field.

The checksum, sequence number and identifier fields are 2 bytes each.



No.	Time	Source	Destination	Protocol	Length	Info
346	2.490683	10.196.77.134	10.250.200.15	ICMP	98	Echo (ping) request id=0x257c, seq=0/0, ttl=64 (reply in 347)
347	2.496154	10.250.200.15	10.196.77.134	ICMP	98	Echo (ping) reply id=0x257c, seq=0/0, ttl=63 (request in 346)
494	3.495386	10.196.77.134	10.250.200.15	ICMP	98	Echo (ping) request id=0x257c, seq=1/256, ttl=64 (reply in 495)
495	3.505870	10.250.200.15	10.196.77.134	ICMP	98	Echo (ping) reply id=0x257c, seq=1/256, ttl=63 (request in 494)
651	4.502773	10.196.77.134	10.250.200.15	ICMP	98	Echo (ping) request id=0x257c, seq=2/512, ttl=64 (reply in 660)
660	4.509429	10.250.200.15	10.196.77.134	ICMP	98	Echo (ping) reply id=0x257c, seq=2/512, ttl=63 (request in 651)
784	5.507723	10.196.77.134	10.250.200.15	ICMP	98	Echo (ping) request id=0x257c, seq=3/768, ttl=64 (reply in 785)
785	5.518324	10.250.200.15	10.196.77.134	ICMP	98	Echo (ping) reply id=0x257c, seq=3/768, ttl=63 (request in 784)
925	6.508783	10.196.77.134	10.250.200.15	ICMP	98	Echo (ping) request id=0x257c, seq=4/1824, ttl=64 (reply in 926)
926	6.528384	10.250.200.15	10.196.77.134	ICMP	98	Echo (ping) reply id=0x257c, seq=4/1824, ttl=63 (request in 925)
1104	7.509228	10.196.77.134	10.250.200.15	ICMP	98	Echo (ping) request id=0x257c, seq=5/1280, ttl=64 (reply in 1105)
1105	7.521914	10.250.200.15	10.196.77.134	ICMP	98	Echo (ping) reply id=0x257c, seq=5/1280, ttl=63 (request in 1104)
1236	8.512786	10.196.77.134	10.250.200.15	ICMP	98	Echo (ping) request id=0x257c, seq=6/1536, ttl=64 (reply in 1237)
1237	8.519411	10.250.200.15	10.196.77.134	ICMP	98	Echo (ping) reply id=0x257c, seq=6/1536, ttl=63 (request in 1236)
1407	9.520207	10.196.77.134	10.250.200.15	ICMP	98	Echo (ping) request id=0x257c, seq=7/1792, ttl=64 (reply in 1429)
1429	9.529874	10.250.200.15	10.196.77.134	ICMP	98	Echo (ping) reply id=0x257c, seq=7/1792, ttl=63 (request in 1407)
1615	10.523087	10.196.77.134	10.250.200.15	ICMP	98	Echo (ping) request id=0x257c, seq=8/2048, ttl=64 (reply in 1616)
1616	10.534661	10.250.200.15	10.196.77.134	ICMP	98	Echo (ping) reply id=0x257c, seq=8/2048, ttl=63 (request in 1615)
1796	11.526598	10.196.77.134	10.250.200.15	ICMP	98	Echo (ping) request id=0x257c, seq=9/2304, ttl=64 (reply in 1797)
1797	11.548495	10.250.200.15	10.196.77.134	ICMP	98	Echo (ping) reply id=0x257c, seq=9/2304, ttl=63 (request in 1796)

> Frame 346: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
> Ethernet II, Src: AppleAd:cf:45 (14:7d:da:ad:cf:45), Dst: ExtremeNetworks_9a:82:e8 (02:84:96:9a:82:e8)
> Internet Protocol Version 4, Src: 10.196.77.134, Dst: 10.250.200.15
v Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x58b7 [correct]
[Checksum Status: Good]
Identifier (BE): 9596 (0x257c)
Identifier (LE): 31781 (0x7c25)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[Response frame: 347]
Timestamp from icmp data: Mar 14, 2023 09:56:40.602928000 IST
[Timestamp from icmp data (relative): 0.000155000 seconds]
> Data (48 bytes)

0000 02 04 06 0a 02 e8 14 7d da ad cf 45 08 00 45 00
0010 00 54 5c 8d 00 00 40 01 f2 c8 0a c4 4d 86 0a fa
0020 c8 0f 08 00 58 b7 25 7c 00 00 64 0f f7 80 00 09
0030 33 30 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
0060 36 37

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: 0 (Echo (ping) reply), Code: 0

This ICMP packet has other fields like Checksum, Identifier (BE), Identifier (LE), Sequence

Number (BE), Sequence Number (LE), Response time, Timestamp from icmp data and data field.

The checksum, sequence number and identifier fields are 2 bytes each.

The image shows a Wireshark packet capture of ICMP Echo (ping) traffic. The top pane displays a list of 20 packets, all of which are Echo (ping) requests and replies. The source and destination IP addresses are 10.196.77.134 and 10.250.200.15, respectively. The protocol is ICMP, and the length is 98 bytes for all packets. The info column shows the sequence number and TTL for each packet.

No.	Time	Source	Destination	Protocol	Length	Info
346	2.490683	10.196.77.134	10.250.200.15	ICMP	98	Echo (ping) request id=0x257c, seq=0/0, ttl=64 (reply in 347)
347	2.491654	10.250.200.15	10.196.77.134	ICMP	98	Echo (ping) reply id=0x257c, seq=0/0, ttl=63 (request in 346)
494	3.495386	10.196.77.134	10.250.200.15	ICMP	98	Echo (ping) request id=0x257c, seq=1/256, ttl=64 (reply in 495)
495	3.505870	10.250.200.15	10.196.77.134	ICMP	98	Echo (ping) reply id=0x257c, seq=1/256, ttl=63 (request in 494)
651	4.502773	10.196.77.134	10.250.200.15	ICMP	98	Echo (ping) request id=0x257c, seq=2/512, ttl=64 (reply in 660)
660	4.509429	10.250.200.15	10.196.77.134	ICMP	98	Echo (ping) reply id=0x257c, seq=2/512, ttl=63 (request in 651)
784	5.507723	10.196.77.134	10.250.200.15	ICMP	98	Echo (ping) request id=0x257c, seq=3/768, ttl=64 (reply in 785)
785	5.518324	10.250.200.15	10.196.77.134	ICMP	98	Echo (ping) reply id=0x257c, seq=3/768, ttl=63 (request in 784)
925	6.508783	10.196.77.134	10.250.200.15	ICMP	98	Echo (ping) request id=0x257c, seq=4/1024, ttl=64 (reply in 926)
926	6.520384	10.250.200.15	10.196.77.134	ICMP	98	Echo (ping) reply id=0x257c, seq=4/1024, ttl=63 (request in 925)
1104	7.509228	10.196.77.134	10.250.200.15	ICMP	98	Echo (ping) request id=0x257c, seq=5/1280, ttl=64 (reply in 1105)
1105	7.521914	10.250.200.15	10.196.77.134	ICMP	98	Echo (ping) reply id=0x257c, seq=5/1280, ttl=63 (request in 1104)
1236	8.512786	10.196.77.134	10.250.200.15	ICMP	98	Echo (ping) request id=0x257c, seq=6/1536, ttl=64 (reply in 1237)
1237	8.519411	10.250.200.15	10.196.77.134	ICMP	98	Echo (ping) reply id=0x257c, seq=6/1536, ttl=63 (request in 1236)
1407	9.520207	10.196.77.134	10.250.200.15	ICMP	98	Echo (ping) request id=0x257c, seq=7/1792, ttl=64 (reply in 1429)
1429	9.529074	10.250.200.15	10.196.77.134	ICMP	98	Echo (ping) reply id=0x257c, seq=7/1792, ttl=63 (request in 1407)
1615	10.523087	10.196.77.134	10.250.200.15	ICMP	98	Echo (ping) request id=0x257c, seq=8/2048, ttl=64 (reply in 1616)
1616	10.534661	10.250.200.15	10.196.77.134	ICMP	98	Echo (ping) reply id=0x257c, seq=8/2048, ttl=63 (request in 1615)
1796	11.526598	10.196.77.134	10.250.200.15	ICMP	98	Echo (ping) request id=0x257c, seq=9/2304, ttl=64 (reply in 1797)
1797	11.540495	10.250.200.15	10.196.77.134	ICMP	98	Echo (ping) reply id=0x257c, seq=9/2304, ttl=63 (request in 1796)

The bottom pane shows the details of the selected packet (Frame 347). It indicates that the packet is 98 bytes long and was captured on interface en0. The Ethernet II header shows the source MAC address as 02:04:96:9a:82:e8 and the destination MAC address as 08:00:27:00:00:00. The Internet Protocol Version 4 header shows the source IP as 10.250.200.15 and the destination IP as 10.196.77.134. The Internet Control Message Protocol header shows the type as Echo (ping) reply, code as 0, and checksum as 0x60b7. The data field shows the ICMP Echo (ping) data, including the sequence number (0x0000) and the timestamp (0.005626000 seconds).

Checksum (icmp.checksum), 2 bytes

Packets: 2415 - Displayed: 20 (0.8%) - Dropped: 0 (0.0%)

Profile: Default

2 Part-2: ICMP and Traceroute

```
~ $ traceroute -I www.google.com
traceroute to www.google.com (142.251.42.36), 64 hops max, 72 byte packets
 1  10.196.3.250 (10.196.3.250)  4.926 ms  6.505 ms  6.282 ms
 2  firewall.iitdh.ac.in (10.250.209.251)  17.380 ms  5.955 ms  6.241 ms
 3  14.139.150.65 (14.139.150.65)  8.046 ms  5.084 ms  5.234 ms
 4  * * *
 5  10.255.238.225 (10.255.238.225)  42.341 ms  47.803 ms  40.101 ms
 6  10.152.7.214 (10.152.7.214)  38.586 ms  40.038 ms  38.643 ms
 7  142.250.172.80 (142.250.172.80)  51.304 ms  53.725 ms  50.435 ms
 8  74.125.37.7 (74.125.37.7)  52.984 ms  49.824 ms  49.035 ms
 9  142.251.69.43 (142.251.69.43)  39.440 ms  39.043 ms  38.729 ms
10  bom12s20-in-f4.1e100.net (142.251.42.36)  47.908 ms  40.478 ms  40.771 ms
~ $
```

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

Source IP address: 10.196.77.134

Destination IP address: 142.251.42.36

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

No. If ICMP sent UDP packets instead, the IP protocol number should be 0x11.

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?

The ICMP echo packet has the same fields as the ping query packets. Only the 'Timestamp from icmp data' field is not there.

No.	Time	Source	Destination	Protocol	Length	Info
2887	21.024119	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=21/5376, ttl=7 (no response found!)
2888	21.074154	142.250.172.80	10.196.77.134	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
2889	21.074594	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=22/5632, ttl=8 (no response found!)
2903	21.1212237	74.125.37.7	10.196.77.134	ICMP	114	Time-to-live exceeded (Time to live exceeded in transit)
2905	21.133314	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=23/5888, ttl=8 (no response found!)
2907	21.182857	74.125.37.7	10.196.77.134	ICMP	114	Time-to-live exceeded (Time to live exceeded in transit)
2908	21.183232	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=24/6144, ttl=8 (no response found!)
2920	21.231943	74.125.37.7	10.196.77.134	ICMP	114	Time-to-live exceeded (Time to live exceeded in transit)
2921	21.232300	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=25/6400, ttl=9 (no response found!)
2922	21.271433	142.251.69.43	10.196.77.134	ICMP	114	Time-to-live exceeded (Time to live exceeded in transit)
2925	21.278087	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=26/6656, ttl=9 (no response found!)
2937	21.316821	142.251.69.43	10.196.77.134	ICMP	114	Time-to-live exceeded (Time to live exceeded in transit)
2938	21.317172	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=27/6912, ttl=9 (no response found!)
2939	21.353599	142.251.69.43	10.196.77.134	ICMP	114	Time-to-live exceeded (Time to live exceeded in transit)
2940	21.355949	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=28/7168, ttl=10 (reply in 2954)
2954	21.403636	142.251.42.36	10.196.77.134	ICMP	86	Echo (ping) reply id=0xfc82, seq=28/7168, ttl=55 (request in 2940)
2957	21.408630	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=29/7424, ttl=10 (reply in 2958)
2958	21.448807	142.251.42.36	10.196.77.134	ICMP	86	Echo (ping) reply id=0xfc82, seq=29/7424, ttl=55 (request in 2957)
2959	21.449208	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=30/7680, ttl=10 (reply in 2960)
2960	21.489645	142.251.42.36	10.196.77.134	ICMP	86	Echo (ping) reply id=0xfc82, seq=30/7680, ttl=55 (request in 2959)
3032	22.017498	10.196.77.134	10.250.200.3	ICMP	70	Destination unreachable (Port unreachable)

> Frame 2940: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface en0, id 0
 > Ethernet II, Src: Apple_ad:cf:45 (14:7d:da:ad:cf:45), Dst: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)
 > Internet Protocol Version 4, Src: 10.196.77.134, Dst: 142.251.42.36
 > Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0xfb50 [correct]
 [Checksum Status: Good]
 Identifier (BE): 64642 (0xfc82)
 Identifier (LE): 33532 (0x82fc)
 Sequence Number (BE): 28 (0x001c)
 Sequence Number (LE): 7168 (0x1c00)
 [Response frame: 2954]
 > Data (44 bytes)

0000 02 04 96 9a 82 e8 14 7d da ad cf 45 08 00 45 00
 0010 00 48 fc 9e 00 00 0a 01 a2 ad 0a c4 4d 86 be fb
 0020 2a 24 08 00 fb 60 fc 82 00 1c 00 00 00 00 00
 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0050 00 00 00 00 00 00

Data (data), 44 bytes
 Packets: 3303 - Displayed: 59 (1.8%) - Dropped: 0 (0.0%)
 Profile: Default

4. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

The ICMP error packet has more fields than ICMP echo packet. It contains both the IP header and the first 8 bytes of the original ICMP packet that the error is for.

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?

The last three ICMP packets are message type 0 (echo reply) rather than 11 (TTL expired). They are different because the datagrams have made it all the way to the destination host before the TTL exceeded/expired.

No.	Time	Source	Destination	Protocol	Length	Info
433	2.421988	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=1/256, ttl=1 (no response found!)
434	2.425775	10.196.77.134	10.196.77.134	ICMP	114	Time-to-live exceeded (Time to live exceeded in transit)
437	2.431985	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=2/512, ttl=1 (no response found!)
439	2.438474	10.196.77.134	10.196.77.134	ICMP	114	Time-to-live exceeded (Time to live exceeded in transit)
439	2.438496	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=3/768, ttl=1 (no response found!)
440	2.444573	10.196.77.134	10.196.77.134	ICMP	114	Time-to-live exceeded (Time to live exceeded in transit)
441	2.444811	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=4/1024, ttl=2 (no response found!)
450	2.461832	10.250.209.251	10.196.77.134	ICMP	114	Time-to-live exceeded (Time to live exceeded in transit)
454	2.469594	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=5/1280, ttl=2 (no response found!)
455	2.475282	10.250.209.251	10.196.77.134	ICMP	114	Time-to-live exceeded (Time to live exceeded in transit)
456	2.475603	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=6/1536, ttl=2 (no response found!)
457	2.481581	10.250.209.251	10.196.77.134	ICMP	114	Time-to-live exceeded (Time to live exceeded in transit)
458	2.481833	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=7/1792, ttl=3 (no response found!)
459	2.489850	10.196.77.134	10.196.77.134	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
462	2.497617	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=8/2048, ttl=3 (no response found!)
463	2.502480	14.139.150.65	10.196.77.134	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
464	2.502723	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=9/2304, ttl=3 (no response found!)
465	2.507728	14.139.150.65	10.196.77.134	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
466	2.508020	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=10/2560, ttl=4 (no response found!)
1114	7.509386	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=11/2816, ttl=4 (no response found!)
1713	12.514293	10.196.77.134	142.251.42.36	ICMP	86	Echo (ping) request id=0xfc82, seq=12/3072, ttl=4 (no response found!)

> Frame 465: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface en0, id 0
 > Ethernet II, Src: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8), Dst: Apple_ad:cf:45 (14:7d:da:ad:cf:45)
 > Internet Protocol Version 4, Src: 14.139.150.65, Dst: 10.196.77.134
 > 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: 10.196.77.134, Dst: 142.251.42.36
 > Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0xfb73 [unverified] [in ICMP error packet]
 [Checksum Status: Unverified]
 Identifier (BE): 64642 (0xfc82)
 Identifier (LE): 33532 (0x82fc)
 Sequence Number (BE): 9 (0x0009)
 Sequence Number (LE): 2384 (0x0900)

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

There is a link between steps 3 and 5 that has a significantly longer delay. This maybe a transoceanic link.

3 Part-3: UDP Pinger

3.1 Screenshots

```
○ CS315 CN lab/Submissions/Assignment-10 $ python3 UDPPingerServer.py
*** Server started ***
Started UDP server on port 12000
█
```

```
● CS315 CN lab/Submissions/Assignment-10 $ python3 UDPPingerClient.py
*** Client started ***
Sent Ping #1 Tue Mar 14 11:41:24 2023
Received b'PING #1 TUE MAR 14 11:41:24 2023'
RTT: 0.0021278858184814453 seconds

Sent Ping #2 Tue Mar 14 11:41:24 2023
Received b'PING #2 TUE MAR 14 11:41:24 2023'
RTT: 0.00041103363037109375 seconds

Sent Ping #3 Tue Mar 14 11:41:24 2023
Received b'PING #3 TUE MAR 14 11:41:24 2023'
RTT: 0.00045680999755859375 seconds

Sent Ping #4 Tue Mar 14 11:41:24 2023
Received b'PING #4 TUE MAR 14 11:41:24 2023'
RTT: 0.0004019737243652344 seconds

Sent Ping #5 Tue Mar 14 11:41:24 2023
#5 Requested Time out

Sent Ping #6 Tue Mar 14 11:41:25 2023
Received b'PING #6 TUE MAR 14 11:41:25 2023'
RTT: 0.0005698204040527344 seconds

Sent Ping #7 Tue Mar 14 11:41:25 2023
Received b'PING #7 TUE MAR 14 11:41:25 2023'
RTT: 0.0006730556488037109 seconds

Sent Ping #8 Tue Mar 14 11:41:25 2023
Received b'PING #8 TUE MAR 14 11:41:25 2023'
RTT: 0.0005738735198974609 seconds

Sent Ping #9 Tue Mar 14 11:41:25 2023
Received b'PING #9 TUE MAR 14 11:41:25 2023'
RTT: 0.0008988380432128906 seconds

Sent Ping #10 Tue Mar 14 11:41:25 2023
Received b'PING #10 TUE MAR 14 11:41:25 2023'
RTT: 0.0007731914520263672 seconds

** closing socket **
○ CS315 CN lab/Submissions/Assignment-10 $ █
```