# CS315: Lab Assignment 10

B Siddharth Prabhu
200010003@iitdh.ac.in

14 March 2023

## 1 Answers to Part 1: ICMP and Ping

Ping is a simple tool that allows anyone to verify if a host is live or not. Let us capture the packet trace for when ping is sent using ICMP (Internet Control Message Protocol) Echo, after which we shall answer some questions. Below are screenshots of the terminal and the Wireshark packet trace window, when the command `ping -c 10 www.iitdh.ac.in` is run.

```
siddharth@DESKTOP-5490SID-LINUX:~$ ping -c 10 www.iitdh.ac.in
PING www.iitdh.ac.in (10.250.200.15) 56(84) bytes of data.
64 bytes from www.iitdh.ac.in (10.250.200.15): icmp_seq=1 ttl=63 time=4.33 ms
64 bytes from www.iitdh.ac.in (10.250.200.15): icmp_seq=2 ttl=63 time=7.39 ms
64 bytes from www.iitdh.ac.in (10.250.200.15): icmp_seq=3 ttl=63 time=5.74 ms
64 bytes from www.iitdh.ac.in (10.250.200.15): icmp_seq=4 ttl=63 time=14.4 ms
64 bytes from www.iitdh.ac.in (10.250.200.15): icmp_seq=5 ttl=63 time=8.02 ms
64 bytes from www.iitdh.ac.in (10.250.200.15): icmp_seq=6 ttl=63 time=10.8 ms
64 bytes from www.iitdh.ac.in (10.250.200.15): icmp_seq=7 ttl=63 time=5.62 ms
64 bytes from www.iitdh.ac.in (10.250.200.15): icmp_seq=8 ttl=63 time=8.56 ms
64 bytes from www.iitdh.ac.in (10.250.200.15): icmp_seq=9 ttl=63 time=8.32 ms
64 bytes from www.iitdh.ac.in (10.250.200.15): icmp_seq=10 ttl=63 time=6.05 ms

--- www.iitdh.ac.in ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 4.329/7.923/14.407/2.787 ms
siddharth@DESKTOP-5490SID-LINUX:~$
```

Figure 1: Sending pings

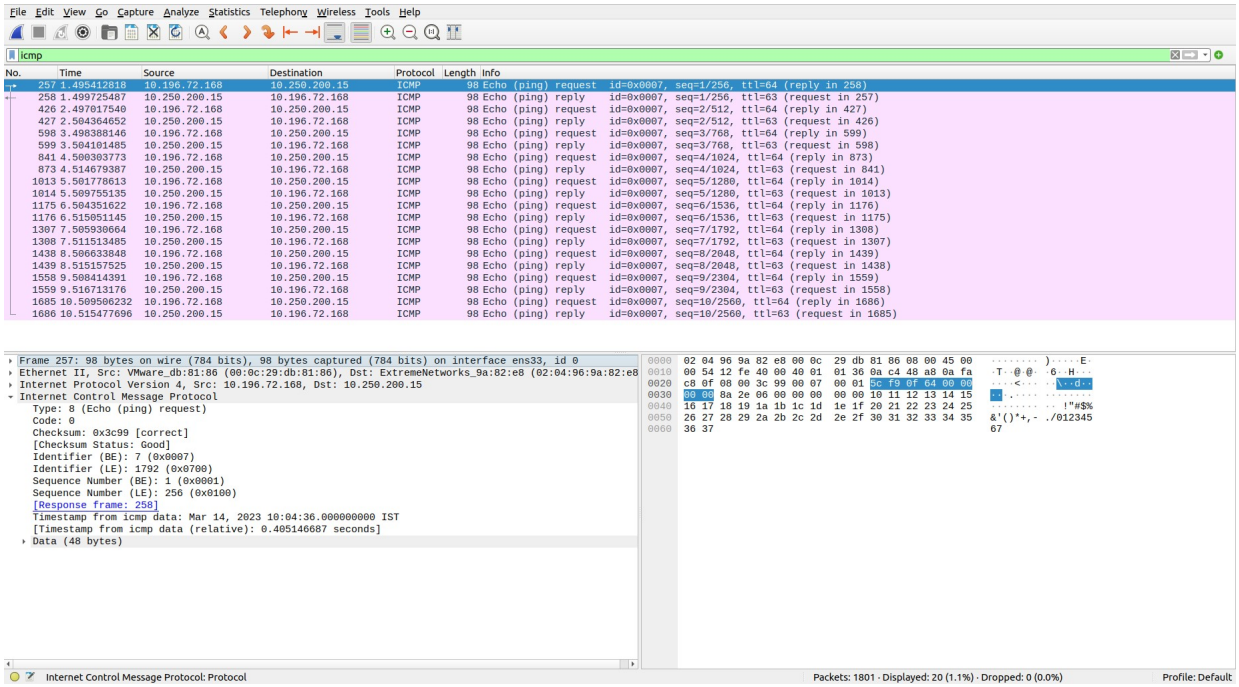


Figure 2: Packet Trace and details of ICMP Echo Request

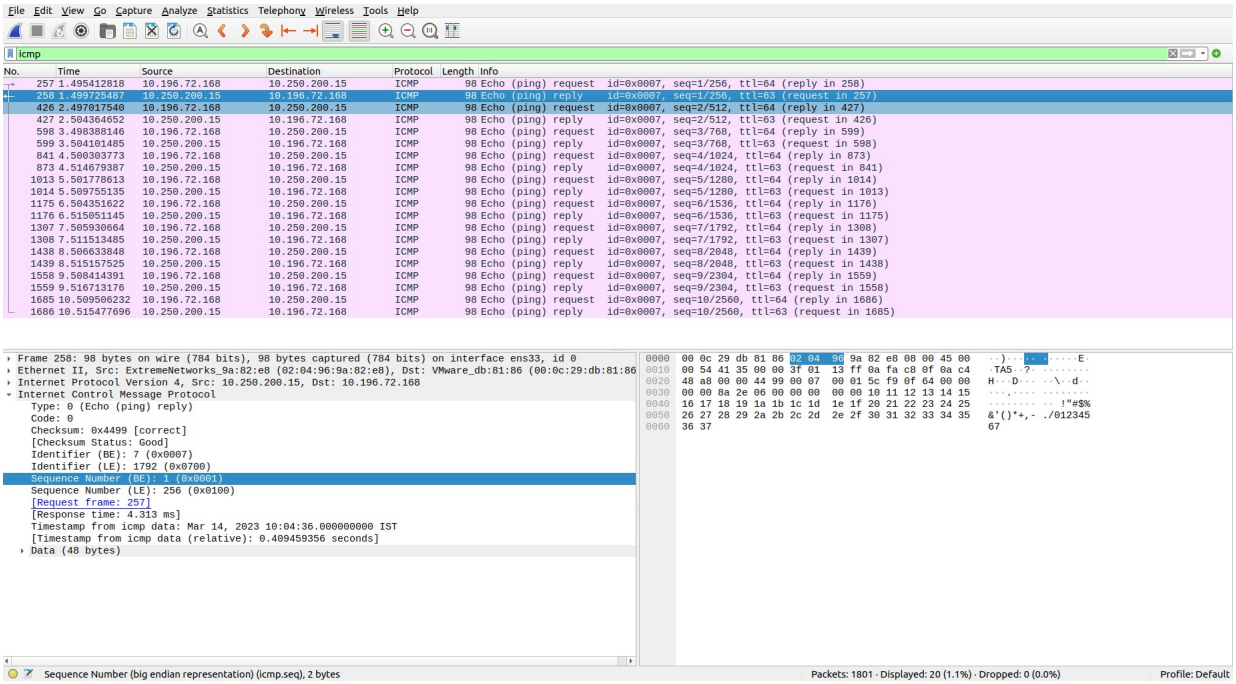


Figure 3: Packet Trace and details of ICMP Echo Response

## (1) What is the IP address of your host? Of the destination host?

- IP address of source host = `10.196.72.168`
- IP address of destination host = `10.250.200.15`

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

ICMP packet does not have source and destination port numbers since it is NOT a transport layer protocol; it is a network layer protocol used to communicate between hosts and routers, as opposed to between processes of applications. The pair (type, code) is enough to identify the message.

## (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?

As seen in Figure (2), the ICMP Request packet has the following details:

- ICMP type number = `8` (Echo request, i.e., ping request)
- ICMP code number = `0`
- Other fields in the ICMP packet include: Checksum, Identifier, Data (which contains timestamp), Sequence Number.
- Sizes of some fields are:
  Checksum (**2 Bytes**), Sequence Number (**2 Bytes**), Identifier (**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?**

Consider the ping reply packet pictured in Figure(3). Details that can be observed are as follows:

- ICMP type number = `0` (Echo reply, i.e., ping reply)
- ICMP code number = `0`
- Other fields in the ICMP packet include: Checksum, Identifier, Data (which contains timestamp), Sequence Number.
- Sizes of some fields are:
  Checksum (**2 Bytes**), Sequence Number (**2 Bytes**), Identifier (**2 Bytes**).

# 2 Answers to Part 2: ICMP and Traceroute

Traceroute can be used to figure out the path a packet takes from source to destination. Let us capture a packet trace obtained during issuing of the traceroute command. Below are screenshots of the terminal, and of the corresponding Wireshark packet trace:

```
siddharth@DESKTOP-5490SID-LINUX:~$ traceroute -I www.google.com
traceroute to www.google.com (142.251.42.36), 30 hops max, 60 byte packets
 1  _gateway (10.196.3.250)  4.128 ms  3.872 ms  3.685 ms
 2  firewall.iitdh.ac.in (10.250.209.251)  3.510 ms  3.362 ms  3.218 ms
 3  14.139.150.65 (14.139.150.65)  3.358 ms  3.206 ms  3.056 ms
 4  * * *
 5  10.255.238.225 (10.255.238.225)  38.075 ms  37.936 ms  37.754 ms
 6  10.152.7.214 (10.152.7.214)  37.573 ms  40.908 ms  40.701 ms
 7  142.250.172.80 (142.250.172.80)  45.978 ms  45.792 ms  45.529 ms
 8  74.125.37.7 (74.125.37.7)  53.838 ms  50.068 ms  49.830 ms
 9  142.251.69.43 (142.251.69.43)  42.178 ms  41.971 ms  41.824 ms
10  bom12s20-in-f4.1e100.net (142.251.42.36)  43.884 ms  43.737 ms  43.600 ms
siddharth@DESKTOP-5490SID-LINUX:~$
```

Figure 4: Issuing Traceroute

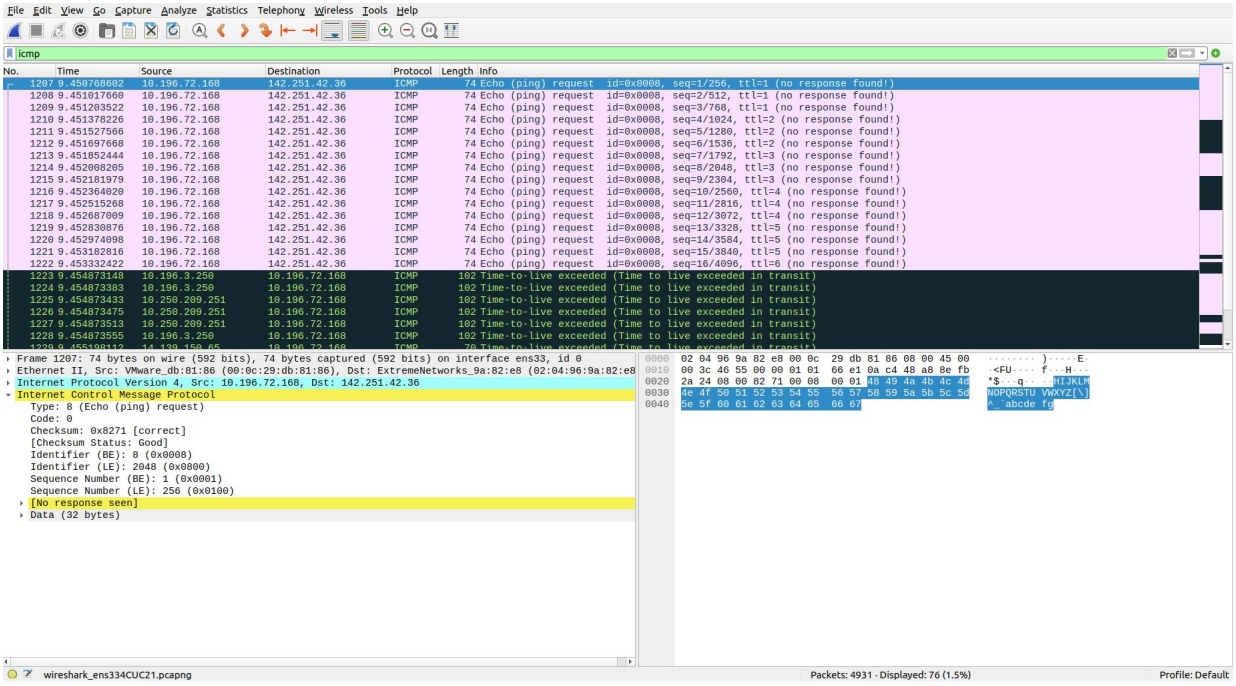


Figure 5: Packet Trace during Traceroute

## (1) What is the IP address of your host? What is the IP address of the target destination host?

- IP address of source host = `10.196.72.168`
- IP address of destination host = `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, then the IP protocol number would not still be 01. Instead, it would be `17` (i.e. 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?

In terms of what fields there are, the ICMP echo packet obtained here is the **same** as those of the first half of this lab. The timestamp seems to have not been extracted from the data, unlike the previous part.

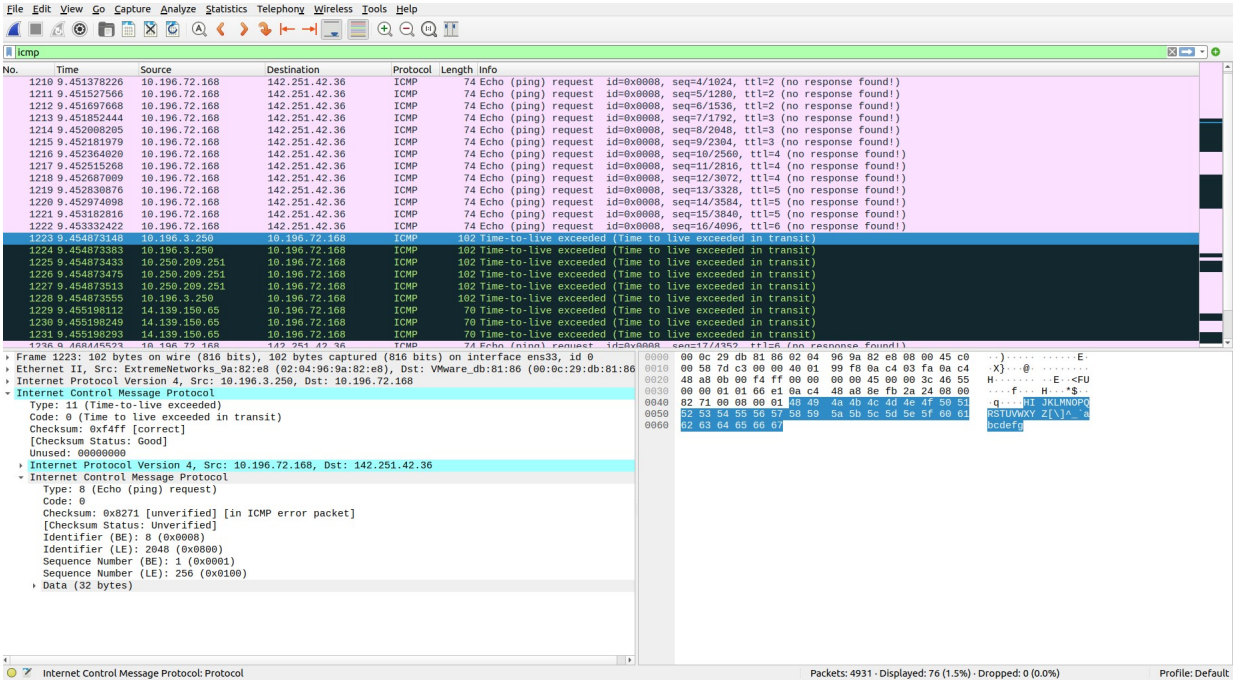


Figure 6: ICMP Error packet

## (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 additional fields are:

- IP Header details
- Original ICMP Packet that the Error is for.
- Some unused bits are also present.

### (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 received by the source host are ICMP Echo reply packets, and are not ICMP error packets. This difference is because the datagrams have reached the destination without expiring due to TTL (Time To Live).

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

Between the 3rd and 5th hops, there is a router that did not reply to the ICMP Echo request. This happens to also be where the delay is significantly longer than others. This could be due to the link potentially being trans-oceanic.

## 3 Socket Programming: UDP Pinger

Refer to `UDPPingerServer.py` and `200010003_client.py` . Screenshots of working client are below:

```
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop/CS315 CN_Lab/Submissions/Assignment 10$ python3 200010003_client.py

Sent Ping 1 Wed Mar 15 09:45:57 2023
Received PING 1 WED MAR 15 09:45:57 2023
RTT: 0.06742715835571289 seconds

Sent Ping 2 Wed Mar 15 09:45:57 2023
Ping 2 Request Timed out

Sent Ping 3 Wed Mar 15 09:45:58 2023
Ping 3 Request Timed out

Sent Ping 4 Wed Mar 15 09:46:00 2023
Received PING 4 WED MAR 15 09:46:00 2023
RTT: 0.0009837150573730469 seconds

Sent Ping 5 Wed Mar 15 09:46:00 2023
Received PING 5 WED MAR 15 09:46:00 2023
RTT: 0.0007140636444091797 seconds

Sent Ping 6 Wed Mar 15 09:46:00 2023
Received PING 6 WED MAR 15 09:46:00 2023
RTT: 0.0010030269622802734 seconds

Sent Ping 7 Wed Mar 15 09:46:00 2023
Received PING 7 WED MAR 15 09:46:00 2023
RTT: 0.0025298595428466797 seconds
```

Figure 7: Output at client

```
Sent Ping 8 Wed Mar 15 09:46:00 2023
Ping 8 Request Timed out

Sent Ping 9 Wed Mar 15 09:46:01 2023
Received PING 9 WED MAR 15 09:46:01 2023
RTT: 0.0014684200286865234 seconds

Sent Ping 10 Wed Mar 15 09:46:01 2023
Ping 10 Request Timed out

Average RTT =  0.00024473667144775390
Closing Socket ...
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop/CS315 CN_Lab/Submissions/Assignment 10$
```

Figure 8: Output at client