



Faculty of Computer Science

CSCI 6708 – Advanced Topics in Network Security

Name: Arka Ghosh

Banner ID: B00911033

Assignment: 01

Part 1

1.

```
Command Prompt
Microsoft Windows [Version 10.0.19043.1466]
(c) Microsoft Corporation. All rights reserved.

C:\Users\User>ping -n 10 www.google.com

Pinging www.google.com [142.251.40.228] with 32 bytes of data:
Reply from 142.251.40.228: bytes=32 time=19ms TTL=118
Reply from 142.251.40.228: bytes=32 time=19ms TTL=118
Reply from 142.251.40.228: bytes=32 time=19ms TTL=118
Reply from 142.251.40.228: bytes=32 time=19ms TTL=118
Reply from 142.251.40.228: bytes=32 time=19ms TTL=118
Reply from 142.251.40.228: bytes=32 time=19ms TTL=118
Reply from 142.251.40.228: bytes=32 time=19ms TTL=118
Reply from 142.251.40.228: bytes=32 time=30ms TTL=118
Reply from 142.251.40.228: bytes=32 time=45ms TTL=118

Ping statistics for 142.251.40.228:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 19ms, Maximum = 45ms, Average = 22ms

C:\Users\User>
```

The Wireshark packet capture shows a series of ICMP Echo (ping) requests and replies. The source IP is 192.168.2.48 and the destination IP is 142.251.40.228. The capture shows 10 successful pings and one failed ping due to 'Destination unreachable (Port unreachable)'.

No.	Time	Source	Destination	Protocol	Length	Identification	Info
2988	7.980577	192.168.2.48	142.251.40.228	ICMP	74	0x2990 (10640)	Echo (ping) request id=0x0001, seq=2025/59655, ttl=128 (reply in 2989)
2989	8.000386	142.251.40.228	192.168.2.48	ICMP	74	0x0000 (0)	Echo (ping) reply id=0x0001, seq=2025/59655, ttl=118 (request in 2988)
2993	8.996969	192.168.2.48	142.251.40.228	ICMP	74	0x2991 (10641)	Echo (ping) request id=0x0001, seq=2026/59911, ttl=128 (reply in 2994)
2994	9.016543	142.251.40.228	192.168.2.48	ICMP	74	0x0000 (0)	Echo (ping) reply id=0x0001, seq=2026/59911, ttl=118 (request in 2993)
3001	10.006593	192.168.2.48	142.251.40.228	ICMP	74	0x2992 (10642)	Echo (ping) request id=0x0001, seq=2027/60167, ttl=128 (reply in 3002)
3002	10.026328	142.251.40.228	192.168.2.48	ICMP	74	0x0000 (0)	Echo (ping) reply id=0x0001, seq=2027/60167, ttl=118 (request in 3001)
3212	11.025209	192.168.2.48	142.251.40.228	ICMP	74	0x2993 (10643)	Echo (ping) request id=0x0001, seq=2028/60423, ttl=128 (reply in 3213)
3213	11.044708	142.251.40.228	192.168.2.48	ICMP	74	0x0000 (0)	Echo (ping) reply id=0x0001, seq=2028/60423, ttl=118 (request in 3212)
3234	12.036167	192.168.2.48	142.251.40.228	ICMP	74	0x2994 (10644)	Echo (ping) request id=0x0001, seq=2029/60679, ttl=128 (reply in 3235)
3235	12.055936	142.251.40.228	192.168.2.48	ICMP	74	0x0000 (0)	Echo (ping) reply id=0x0001, seq=2029/60679, ttl=118 (request in 3234)
3264	13.043801	192.168.2.48	142.251.40.228	ICMP	74	0x2995 (10645)	Echo (ping) request id=0x0001, seq=2030/60935, ttl=128 (reply in 3266)
3266	13.063373	142.251.40.228	192.168.2.48	ICMP	74	0x0000 (0)	Echo (ping) reply id=0x0001, seq=2030/60935, ttl=118 (request in 3264)
3365	14.058159	192.168.2.48	142.251.40.228	ICMP	74	0x2996 (10646)	Echo (ping) request id=0x0001, seq=2031/61191, ttl=128 (reply in 3367)
3367	14.077629	142.251.40.228	192.168.2.48	ICMP	74	0x0000 (0)	Echo (ping) reply id=0x0001, seq=2031/61191, ttl=118 (request in 3365)
3379	15.068340	192.168.2.48	142.251.40.228	ICMP	74	0x2997 (10647)	Echo (ping) request id=0x0001, seq=2032/61447, ttl=128 (reply in 3382)
3382	15.087890	142.251.40.228	192.168.2.48	ICMP	74	0x0000 (0)	Echo (ping) reply id=0x0001, seq=2032/61447, ttl=118 (request in 3379)
19215	15.934889	192.168.2.48	142.166.166.166	ICMP	198	0xa952 (43346), 0x254e (9550)	Destination unreachable (Port unreachable)
24461	16.079842	192.168.2.48	142.251.40.228	ICMP	74	0x2998 (10648)	Echo (ping) request id=0x0001, seq=2033/61703, ttl=128 (reply in 25126)
25126	16.110392	142.251.40.228	192.168.2.48	ICMP	74	0x0000 (0)	Echo (ping) reply id=0x0001, seq=2033/61703, ttl=118 (request in 24461)
58686	17.093356	192.168.2.48	142.251.40.228	ICMP	74	0x2999 (10649)	Echo (ping) request id=0x0001, seq=2034/61959, ttl=128 (reply in 60299)

Frame 2988: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{44286BF3-2CA1-4BD0-85BF-ADC16C9D1554}, id 0
> Ethernet II, Src: IntelCor_91:bd:01 (0c:54:15:91:bd:01), Dst: Sagemcom_5f:74:e0 (b0:bb:e5:5f:74:e0)
> Internet Protocol Version 4, Src: 192.168.2.48, Dst: 142.251.40.228
v Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x4572 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 2025 (0x07e9)
Sequence Number (LE): 59655 (0xe907)
[Response frame: 2989]
> Data (32 bytes)

0000 b0 bb e5 5f 74 e0 0c 54 15 91 bd 01 08 00 45 00 ...t.t.t.t.t.t.t.t
0010 00 3c 29 90 00 00 00 01 96 79 c0 a8 02 30 8e fb ...<.....y...0...
0020 28 e4 08 00 45 72 00 01 07 e9 61 62 63 64 65 66 (...Er...-abcdef

The IP address of the host is 192.168.2.48.

The IP address of the destination is 142.168.40.228.

2. The ICMP Type and Code number in the above request packet are in the following:

- Type: 8
- Code: 0

ICMP type is used to determine the purpose for which ICMP Packet is used. ICMP Type 8 indicates “Echo”. Type 8 is set in the ICMP header of an echo packet [1]. This type 8 is a query that is sent from the source to a potential destination address to determine whether the device is available or not [2]. As there is no code defined, the code is always set to 0 in the header in case of an ICMP echo packet [1].

3. Internet Control Message Protocol or ICMP is a network layer protocol which is used for transmitting the network layer information between hosts and routers. It is not meant to communicate information between application layer processes [3]. This is why an ICMP packet doesn’t have source and destination source address. In each ICMP packet, there is a “Type” and “Code” combination that determines which messages are being sent or received. As all the ICMP packets are interpreted by the network software, there is no need of port addresses to route the message to application layer process [3].

4. The other fields that the ICMP request packet have are in the following with the values of each field:

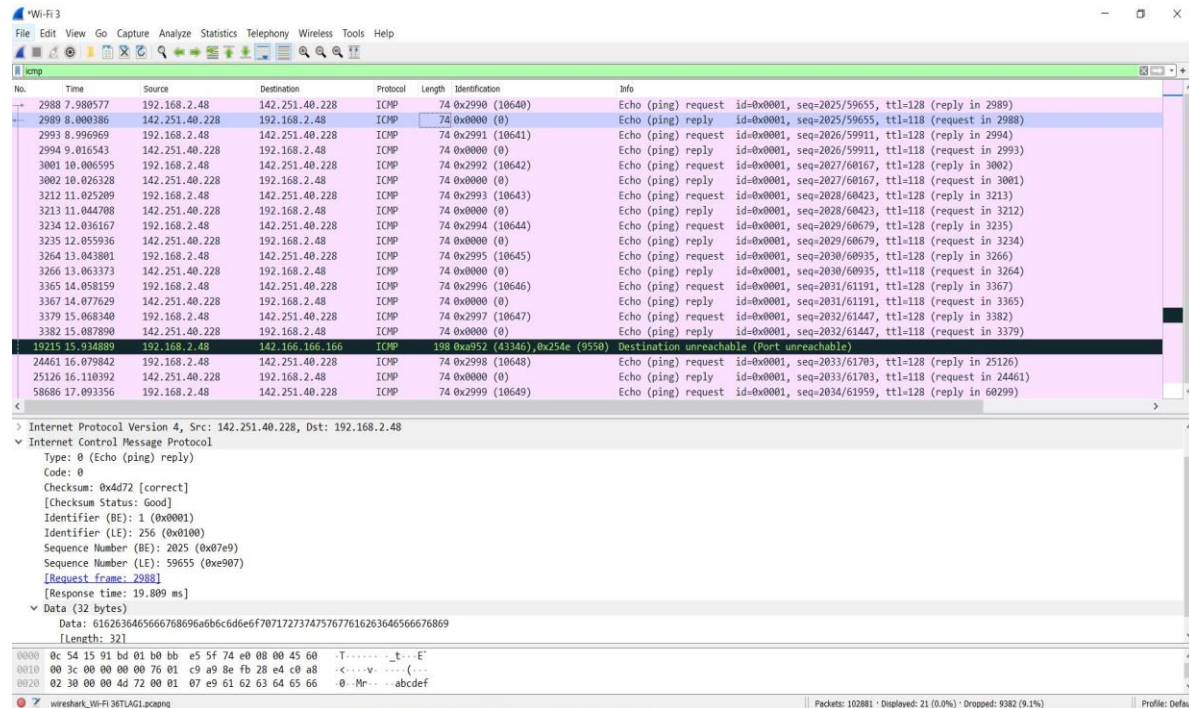
- Checksum: 0x4572
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence Number (BE): 2025 (0x07e9)
- Sequence Number (LE): 59655 (0xe907)

There is also a Data (32 bytes) with drop down menu whose value is:

- Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

5.

Wireshark Capture of the Reply Packet:



The Type and code in the reply packet are in the following:

- Type: 0
- Code: 0

As mentioned above, the ICMP type is used to determine the purpose for which the ICMP packet is used. So here, Type 0 indicates “Echo Reply”. Upon receiving the Echo message, the destination replies with an Echo Reply (Type 0) which means the device is available [2]. As there is no code defined, the code is always set to 0 in the header in case of an ICMP echo reply packet [1].

6. The other fields that the ICMP reply packet have are in the following with the values of each field:

Checksum: 0x4d72

- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence Number (BE): 2025 (0x07e9)
- Sequence Number (LE): 59655 (0xe907)

There is also a Data (32 bytes) with drop down menu whose value is:

- Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

Part 2

1. The server that I use for this question is Google. The highest packet size accepted by this server is 1464.

2. Here's are the two screenshots of the Windows Terminal and Wireshark Capture:

First Screenshot with 1464 Packet Size:

```

C:\Users\User>ping www.google.com -l 1460

Pinging www.google.com [142.251.41.4] with 1460 bytes of data:
Reply from 142.251.41.4: bytes=68 (sent 1460) time=20ms TTL=118
Reply from 142.251.41.4: bytes=68 (sent 1460) time=20ms TTL=118
Reply from 142.251.41.4: bytes=68 (sent 1460) time=20ms TTL=118
Reply from 142.251.41.4: bytes=68 (sent 1460) time=20ms TTL=118

Ping statistics for 142.251.41.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 20ms, Average = 20ms

C:\Users\User>ping www.google.com -l 1464

Pinging www.google.com [142.251.41.4] with 1464 bytes of data:
Reply from 142.251.41.4: bytes=68 (sent 1464) time=20ms TTL=118
Reply from 142.251.41.4: bytes=68 (sent 1464) time=20ms TTL=118
Reply from 142.251.41.4: bytes=68 (sent 1464) time=20ms TTL=118
Reply from 142.251.41.4: bytes=68 (sent 1464) time=20ms TTL=118

Ping statistics for 142.251.41.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 20ms, Average = 20ms

```

No.	Time	Source	Destination	Protocol	Length	Identification	Info
133	13.398386	192.168.2.48	142.251.41.4	ICMP	1506	0x7d7d (32125)	Echo (ping) request id=0x0001, seq=2199/38664, ttl=128
134	13.418985	142.251.41.4	192.168.2.48	ICMP	110	0x0000 (0)	Echo (ping) reply id=0x0001, seq=2199/38664, ttl=118
150	14.413990	192.168.2.48	142.251.41.4	ICMP	1506	0x7d7e (32126)	Echo (ping) request id=0x0001, seq=2200/38920, ttl=128
151	14.434834	142.251.41.4	192.168.2.48	ICMP	110	0x0000 (0)	Echo (ping) reply id=0x0001, seq=2200/38920, ttl=118
173	15.418369	192.168.2.48	142.251.41.4	ICMP	1506	0x7d7f (32127)	Echo (ping) request id=0x0001, seq=2201/39176, ttl=128
174	15.438845	142.251.41.4	192.168.2.48	ICMP	110	0x0000 (0)	Echo (ping) reply id=0x0001, seq=2201/39176, ttl=118
179	16.437279	192.168.2.48	142.251.41.4	ICMP	1506	0x7d80 (32128)	Echo (ping) request id=0x0001, seq=2202/39432, ttl=128
180	16.457809	142.251.41.4	192.168.2.48	ICMP	110	0x0000 (0)	Echo (ping) reply id=0x0001, seq=2202/39432, ttl=118

> Frame 133: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interface \Device\NPF_{44286BF3-2CA1-4BD0-85BF-ADC16C9D1554}, id 0 > Ethernet II, Src: IntelCor_91:bd:01 (0c:54:15:91:bd:01), Dst: Sagemcom_5f:74:e0 (b0:bb:e5:5f:74:e0) > Internet Protocol Version 4, Src: 192.168.2.48, Dst: 142.251.41.4 > Internet Control Message Protocol Type: 8 (Echo (ping) request) Code: 0 Checksum: 0x0582 [correct] [Checksum Status: Good] Identifier (BE): 1 (0x0001) Identifier (LE): 256 (0x0100) Sequence Number (BE): 2199 (0x0897) Sequence Number (LE): 39664 (0x0700)	
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

2nd Screenshot with 1465 Packet Size:

```
Command Prompt

C:\Users\User>ping www.google.com -l 1465

Pinging www.google.com [142.251.41.4] with 1465 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 142.251.41.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\User>
```

Wi-Fi 3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Identification	Info
23	4.118772	192.168.2.48	142.251.41.4	ICMP	1507	0x7d81 (32129)	Echo (ping) request id=0x0001, seq=2203/39688, ttl=128
93	8.847923	192.168.2.48	142.251.41.4	ICMP	1507	0x7d82 (32130)	Echo (ping) request id=0x0001, seq=2204/39944, ttl=128
118	13.853513	192.168.2.48	142.251.41.4	ICMP	1507	0x7d83 (32131)	Echo (ping) request id=0x0001, seq=2205/40200, ttl=128
160	18.843350	192.168.2.48	142.251.41.4	ICMP	1507	0x7d84 (32132)	Echo (ping) request id=0x0001, seq=2206/40456, ttl=128

< >

> Frame 23: 1507 bytes on wire (12056 bits), 1507 bytes captured (12056 bits) on interface \Device\NPF_{44286BF3-2CA1-4BD0-85BF-ADC16C9D1554}, id 0

> Ethernet II, Src: IntelCor_91:bd:01 (0c:54:15:91:bd:01), Dst: Sagemcom_5f:74:e0 (b0:bb:e5:5f:74:e0)

> Internet Protocol Version 4, Src: 192.168.2.48, Dst: 142.251.41.4

▼ Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x957d [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence Number (BE): 2203 (0x089b)

Sequence Number (LE): 20600 (0x5080)

0020 29 04 08 00 95 7d 00 01 08 9b 51 62 63 64 65 66).... abcdef

0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmnopqrstuv

wireshark_Wi-Fi 3X1WSF1.pcapng Packets: 215 · Displayed: 4 (1.9%) Profile: Default

From both of these screenshots, there were both Echo request and echo reply ICMP packet in the Wireshark capture while pinging with 1464 Packet Size. But while pinging with 1465 packet size, there is no reply packet from the destination. This means the server dropped the packet.

3. Web servers prevent large pings because an oversized ping can cause the system to freeze, crash or reboot. A correct IPv4 packet can be as large as 65,535 bytes [4]. When a packet is sent larger than this, it violates the IP. As a result, the attacker transmit packets in fragments, resulting in an oversized packets when the targeted victim tries to resemble it [4]. Because of this, there happens a buffer overflow that can result into a system crash. This is why servers use firewalls to drop oversized and unnecessary ping or ICMP packets.

Part 3

1.

Traceroute Result:

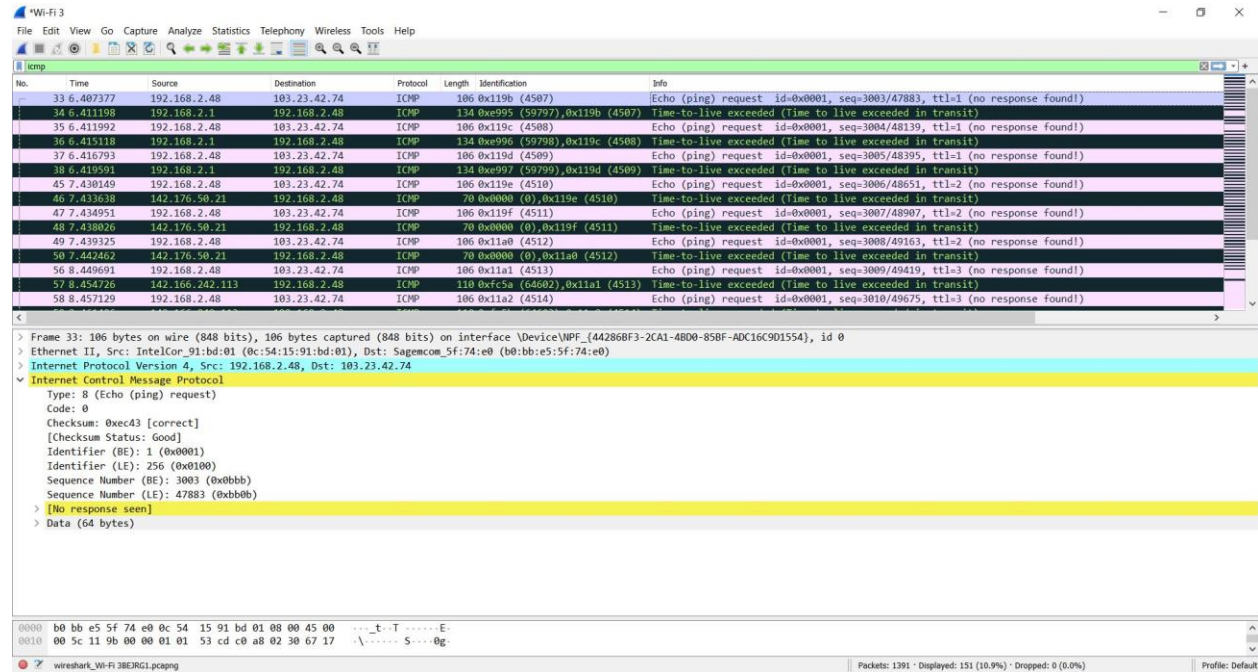
```
Command Prompt
C:\Users\User>tracert www.aust.edu

Tracing route to www.aust.edu [103.23.42.74]
over a maximum of 30 hops:

  0  3 ms    3 ms    2 ms  mynetwork [192.168.2.1]
  1  3 ms    3 ms    3 ms  loop0.8gw.ba19.hlfx.ns.aliant.net [142.176.50.21]
  2  5 ms    4 ms    3 ms  be16-181.cr01.hlfx.ns.aliant.net [142.166.242.113]
  3  22 ms   21 ms   21 ms  be19.bx02.nycm.ny.aliant.net [207.231.227.62]
  4  *        *        *      Request timed out.
  5  32 ms   32 ms  31 ms  ae2.3611.edge2.NewYork6.level3.net [4.69.209.82]
  6  *        *        *      Request timed out.
  7  32 ms   32 ms  32 ms  be3295.ccr42.jfk02.atlas.cogentco.com [154.54.80.1]
  8  103 ms  103 ms  103 ms  be3628.ccr42.par01.atlas.cogentco.com [154.54.27.170]
  9  129 ms  115 ms  114 ms  be2780.ccr32.mrs02.atlas.cogentco.com [154.54.72.226]
 10  114 ms  114 ms  114 ms  be2752.ccr22.mrs01.atlas.cogentco.com [154.54.38.33]
 11  114 ms  114 ms  114 ms  be2346.agr21.mrs01.atlas.cogentco.com [154.54.38.174]
 12  252 ms  254 ms  252 ms  bscc1.demarc.cogentco.com [149.14.126.122]
 13  252 ms  251 ms  251 ms  103-16-152-73-noc.bscc1.com [103.16.152.73]
 14  257 ms  257 ms  257 ms  103-16-152-81-noc.bscc1.com [103.16.152.81]
 15  257 ms  258 ms  257 ms  103-16-155-58-noc.bscc1.com [103.16.155.58]
 16  262 ms  262 ms  261 ms  103.9.136.206
 17  263 ms  263 ms  263 ms  103.9.136.202
 18  257 ms  257 ms  259 ms  eth-11-gulshan-1-rtr.intercloud.com.bd [103.248.12.138]
 19  263 ms  263 ms  262 ms  eth-11-shanta-tower-rtr.intercloud.com.bd [163.53.149.34]
 20  263 ms  262 ms  265 ms  103.23.42.42
 21  258 ms  374 ms  257 ms  103.23.42.68
 22  *        *        *      Request timed out.
 23  *        *        *      Request timed out.
 24  *        *        *      Request timed out.
 25  *        *        *      Request timed out.
 26  *        *        *      Request timed out.
 27  *        *        *      Request timed out.
 28  *        *        *      Request timed out.
 29  *        *        *      Request timed out.
 30  *        *        *      Request timed out.

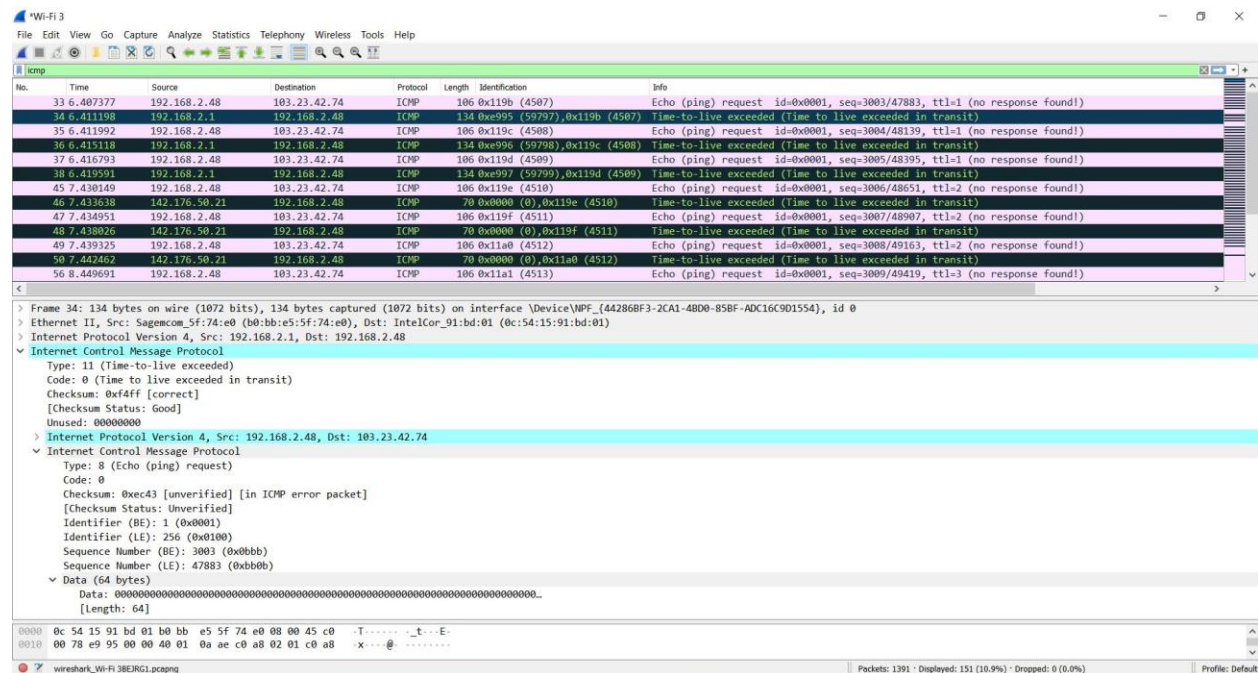
Trace complete.
```

Wireshark Capture of Request Packet:



The ICMP request packet is the same as the one I captured in the ping command. It has the same fields.

Wireshark Capture of Reply Packet

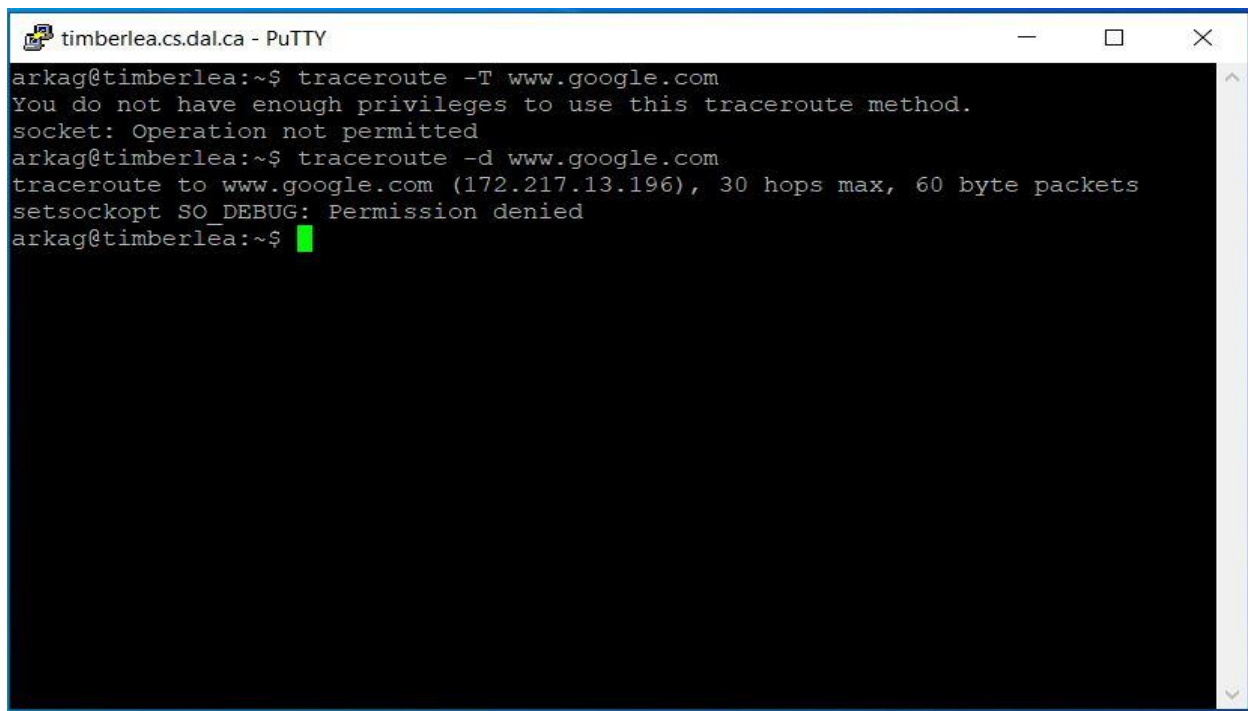


The fields with their values in this reply packet has been mentioned below:

- The fields of the ICMP request packet that has been added along with this above mentioned packet is mentioned below:

- 2.**

From the Windows terminal mentioned above, it can be seen that the first error packet is in the hop no. 5. The wireshark capture of that packet has been provided below:



```
timberlea.cs.dal.ca - PuTTY
arkag@timberlea:~$ traceroute -T www.google.com
You do not have enough privileges to use this traceroute method.
socket: Operation not permitted
arkag@timberlea:~$ traceroute -d www.google.com
traceroute to www.google.com (172.217.13.196), 30 hops max, 60 byte packets
setsockopt SO_DEBUG: Permission denied
arkag@timberlea:~$
```

4. `-s src_addr` is for choosing an alternative source address for outgoing packet. One can use the `-s src_addr` option to choose an alternative source address while running traceroute instead of the default one.

There is security issues with that option. It can lead into IP spoofing. IP spoofing is the creation of IP packets with an altered source address in order to either conceal the sender's identity or to impersonate a computer system [7]. Using `-s src_addr` option, an attacker can easily send packets with an altered source address.

Part 4

Experiment No. 1

Forward Path

Source	Command	Destination
<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6	<input type="radio"/> ping	<input checked="" type="radio"/> Your IP: 134.41.62.153
Anaheim, CA	<input checked="" type="radio"/> traceroute	<input type="radio"/> Another IP
	<input type="radio"/> show bgp route	<input type="radio"/> Sprint Site
<input type="button" value="Submit"/>		

Sprint Source: Anaheim, CA (sl-crs2-ana)
Your IP: 134.41.62.153
Performing: ICMP Traceroute
IP Version: IPv4

```
Tracing the route to hlfxn018gw-134-41-62-153.dhcp-dynamic.fibreop.ns.bellaliant.net (134.41.62.153)

 1 sl-crs2-ria-be10.sprintlink.net (144.232.22.71) 8 msec 10 msec
   sl-crs2-aj-be7.sprintlink.net (144.232.17.29) 15 msec
 2 sl-crs2-stk-bell.sprintlink.net (144.232.22.95) 23 msec
   sl-crs2-stk-be3.sprintlink.net (144.232.22.179) 15 msec
   sl-crs2-stk-bell.sprintlink.net (144.232.22.95) 15 msec
 3 sl-crs2-oro-be2.sprintlink.net (144.232.15.238) 15 msec 23 msec 23 msec
 4 sl-crs2-oma-be7.sprintlink.net (144.232.15.166) 51 msec 47 msec 47 msec
 5 sl-crs2-chi-be4.sprintlink.net (144.232.22.74) 58 msec 63 msec 55 msec
 6 sl-mst70-chi2-be17.sprintlink.net (144.232.2.94) 55 msec 55 msec 55 msec
 7 144.223.3.226 56 msec 55 msec 55 msec
 8 * * *
 9 * * *
10 *
```

Completed - Thu Jan 27 12:09:41 EST 2022

Backward Path

```
Command Prompt

C:\Users\User>tracert 144.232.22.71

Tracing route to sl-crs2-ria-be10.sprintlink.net [144.232.22.71]
over a maximum of 30 hops:

 1  2 ms    2 ms    2 ms  mynetwork [192.168.2.1]
 2  3 ms    6 ms    4 ms  loop0.8gw.ba19.hlfx.ns.aliant.net [142.176.50.21]
 3  4 ms    3 ms    4 ms  ae17-182.cr02.hlfx.ns.aliant.net [142.166.242.117]
 4  4 ms    4 ms    3 ms  hg-0-2-0-0-50.cr01.hlfx.ns.aliant.net [142.166.149.93]
 5  22 ms   22 ms   22 ms  be19.bx02.nycm.ny.aliant.net [207.231.227.62]
 6  22 ms   29 ms   24 ms  ae20.cr3-nyc6.ip4.gtt.net [209.120.140.5]
 7  * * *
 8  * * *   Request timed out.
 9  * * *   Request timed out.
10 * * *   Request timed out.
11 * * *   Request timed out.
12 * * *   Request timed out.
13 * * *   Request timed out.
14 * * *   Request timed out.
15 * * *   Request timed out.
16 * * *   Request timed out.
17 * * *   Request timed out.
18 * * *   Request timed out.
19 * * *   Request timed out.
20 * * *   Request timed out.
21 * * *   Request timed out.
22 * * *   Request timed out.
23 * * *   Request timed out.
24 * * *   Request timed out.
25 * * *   Request timed out.
26 * * *   Request timed out.
27 * * *   Request timed out.
28 * * *   Request timed out.
29 * * *   Request timed out.
30 * * *   Request timed out.

Trace complete.

C:\Users\User>
```

Experiment No. 2

Forward Path

Looking GlassHome > Looking Glass

Source
☒ IPv4 ☐ IPv6

Rio De Janeiro, Brazil

Command
☐ ping
☒ traceroute
☐ show bgp route

Destination
☒ Your IP: 134.41.62.153
☐ Another IP
☐ Sprint Site

Submit

Sprint Source: Rio De Janeiro, Brazil (sl-mpe01-rio)
Your IP: 134.41.62.153
Performing: ICMP Traceroute
IP Version: IPv4

```
Tracing the route to hlfxs018gw-134-41-62-153.dhcp-dynamic.fibreop.ns.bellalliant.net (134.41.62.153)

 1  sl-crs2-mia-gi0-9-4-0.sprintlink.net (144.232.4.170) 111 msec  111 msec  112 msec
 2  sl-crs2-atl-be19.sprintlink.net (144.232.0.130) 123 msec  127 msec  127 msec
 3  sl-crs2-nsh-be6.sprintlink.net (144.232.17.73) 130 msec  132 msec  128 msec
 4  sl-crs2-roa-be2.sprintlink.net (144.232.2.125) 135 msec  132 msec  136 msec
 5  sl-crs2-chi-be6.sprintlink.net (144.232.22.70) 137 msec  136 msec  141 msec
 6  sl-mst70-chi2-be17.sprintlink.net (144.232.2.94) 135 msec  136 msec  135 msec
 7  144.223.3.226 135 msec  135 msec  135 msec
 8  * * *
 9  * * *
10  *
```

Completed - Thu Jan 27 12:17:47 EST 2022

Reverse Path

```
Select Command Prompt

C:\Users\User>tracert 144.232.4.170

Tracing route to sl-crs2-mia-gi0-9-4-0.sprintlink.net [144.232.4.170]
over a maximum of 30 hops:

 1    4 ms    2 ms    2 ms    mynetwork [192.168.2.1]
 2   11 ms    5 ms    6 ms    loop0.8gw.ba19.hlfx.ns.aliant.net [142.176.50.21]
 3    7 ms    3 ms    4 ms    be16-181.cr01.hlfx.ns.aliant.net [142.166.242.113]
 4   22 ms   21 ms   22 ms    be19.bx02.nycm.ny.aliant.net [207.231.227.62]
 5   28 ms   28 ms   23 ms    ae20.cr3-nyc6.ip4.gtt.net [209.120.140.5]
 6    *      *      *      Request timed out.
 7    *      *      *      Request timed out.
 8    *      *      *      Request timed out.
 9    *      *      *      Request timed out.
10   *      *      *      Request timed out.
11   *      *      *      Request timed out.
12   *      *      *      Request timed out.
13   *      *      *      Request timed out.
14   *      *      *      Request timed out.
15   *      *      *      Request timed out.
16   *      *      *      Request timed out.
17   *      *      *      Request timed out.
18   *      *      *      Request timed out.
19   *      *      *      Request timed out.
20   *      *      *      Request timed out.
21   *      *      *      Request timed out.
22   *      *      *      Request timed out.
23   *      *      *      Request timed out.
24   *      *      *      Request timed out.
25   *      *      *      Request timed out.
26   *      *      *      Request timed out.
27   *      *      *      Request timed out.
28   *      *      *      Request timed out.
29   *      *      *      Request timed out.
30   *      *      *      Request timed out.

Trace complete.

C:\Users\User>
```


Experiment No. 3

Forward Path

Looking Glass

Home > Looking Glass

Source

☒ IPv4 ☐ IPv6

Dusseldorf, Germany

Command

☐ ping
☒ traceroute
☐ show bgp route

Destination

☒ Your IP: 134.41.62.153
☐ Another IP
☐ Sprint Site

Submit

Sprint Source: Dusseldorf, Germany (sl-mpe01-dus)
Your IP: 134.41.62.153
Performing: ICMP Traceroute
IP Version: IPv4

Tracing the route to hlfxns018gw-134-41-62-153.dhcp-dynamic.fibreop.ns.bellaliant.net (134.41.62.153)

1 sl-mpe71-fra-gi0-6-0-13.sprintlink.net (213.206.129.112) 6 msec 5 msec 5 msec
2 sl-mpe71-ams-hu0-0-0-1.sprintlink.net (213.206.129.27) 11 msec 12 msec 12 msec
3 sl-mpe70-ams-be10.sprintlink.net (217.149.32.42) 11 msec 12 msec 12 msec
4 sl-mpe70-lon-be3.sprintlink.net (213.206.129.15) 17 msec 17 msec 17 msec
5 sl-crs1-nyc-be7.sprintlink.net (144.232.9.113) 86 msec 88 msec 88 msec
6 sl-crs1-akr-be21.sprintlink.net (144.232.22.64) 107 msec 110 msec 106 msec
7 sl-crs1-chi-be2.sprintlink.net (144.232.18.5) 112 msec 112 msec 114 msec
8 sl-mst70-chi2-be16.sprintlink.net (144.232.2.92) 108 msec 109 msec 109 msec
9 144.223.3.226 109 msec 109 msec 108 msec
10 * * *
11 * * *

Completed - Thu Jan 27 20:01:17 EST 2022

Reverse Path

Command Prompt

C:\Users\User>tracert 213.206.129.112

Tracing route to sl-mpe71-fra-gi0-6-0-13.sprintlink.net [213.206.129.112]
over a maximum of 30 hops:

1 2 ms 3 ms 3 ms mynetwork [192.168.2.1]
2 7 ms 14 ms 15 ms loop0.8gw.ba19.hlfx.ns.aliant.net [142.176.50.21]
3 3 ms 3 ms 4 ms ae17-182.cr02.hlfx.ns.aliant.net [142.166.242.117]
4 6 ms 5 ms 6 ms hg-0-2-0-0-50.cr01.hlfx.ns.aliant.net [142.166.149.93]
5 23 ms 22 ms 22 ms be19.bx02.nycm.ny.aliant.net [207.231.227.62]
6 22 ms 22 ms 30 ms ae20.cr3-nyc6.ip4.gtt.net [209.120.140.5]
7 * * * Request timed out.
8 * * * Request timed out.
9 * * * Request timed out.
10 * * * Request timed out.
11 * * * Request timed out.
12 * * * Request timed out.
13 * * * Request timed out.
14 * * * Request timed out.
15 * * * Request timed out.
16 * * * Request timed out.
17 * * * Request timed out.
18 * * * Request timed out.
19 * * * Request timed out.
20 * * * Request timed out.
21 * * * Request timed out.
22 * * * Request timed out.
23 * * * Request timed out.
24 * * * Request timed out.
25 * * * Request timed out.
26 * * * Request timed out.
27 * * * Request timed out.
28 * * * Request timed out.
29 * * * Request timed out.
30 * * * Request timed out.

Trace complete.

Experiment No. 4

Forward Path

Looking Glass

Home > Looking Glass

Source

☒ IPv4 ☐ IPv6

Tokyo, Japan

Command

☐ ping
☒ traceroute
☐ show bgp route

Destination

☒ Your IP: 134.41.62.153
☐ Another IP
☐ Sprint Site

Submit

Sprint Source: Tokyo, Japan (sl-mpe11-tok)
Your IP: 134.41.62.153
Performing: ICMP Traceroute
IP Version: IPv4

Tracing the route to hlfxns018gw-134-41-62-153.dhcp-dynamic.fibreop.ns.bellaliant.net (134.41.62.153)

```
 1 sl-mpe70-tok-gi0-7-0-23.sprintlink.net (203.222.36.70) 4 msec 1 msec 2 msec
 2 sl-mpe71-tok-be1.sprintlink.net (203.222.36.49) 2 msec 2 msec 2 msec
 3 sl-crs2-sj-be8.sprintlink.net (144.232.0.80) 100 msec 102 msec 103 msec
 4 sl-crs2-stk-be3.sprintlink.net (144.232.22.179) 105 msec 100 msec 105 msec
 5 sl-crs2-oro-be2.sprintlink.net (144.232.15.238) 103 msec 102 msec 103 msec
 6 sl-crs2-oma-be7.sprintlink.net (144.232.15.166) 136 msec 130 msec 130 msec
 7 sl-crs2-chi-be4.sprintlink.net (144.232.22.74) 141 msec 141 msec 136 msec
 8 sl-mst70-chi2-be17.sprintlink.net (144.232.2.94) 138 msec 136 msec 136 msec
 9 144.223.3.226 135 msec 138 msec 136 msec
10 * * *
11 * * *
12 *
```

Completed - Thu Jan 27 19:23:22 EST 2022

Reverse Path

Command Prompt

C:\Users\User>tracert 203.222.36.70

Tracing route to sl-mpe70-tok-gi0-7-0-23.sprintlink.net [203.222.36.70]
over a maximum of 30 hops:

1	3 ms	2 ms	2 ms	mynetwork [192.168.2.1]
2	3 ms	4 ms	3 ms	loop0.8gw.ba19.hlfx.ns.aliant.net [142.176.50.21]
3	4 ms	3 ms	3 ms	ae17-182.cr02.hlfx.ns.aliant.net [142.166.242.117]
4	3 ms	3 ms	3 ms	hg-0-2-0-0-50.cr01.hlfx.ns.aliant.net [142.166.149.93]
5	22 ms	22 ms	22 ms	be19.bx02.nycm.ny.aliant.net [207.231.227.62]
6	22 ms	21 ms	21 ms	ae20.cr3-nyc6.ip4.gtt.net [209.120.140.5]
7	*	*	*	Request timed out.
8	*	*	*	Request timed out.
9	*	*	*	Request timed out.
10	*	*	*	Request timed out.
11	*	*	*	Request timed out.
12	*	*	*	Request timed out.
13	*	*	*	Request timed out.
14	*	*	*	Request timed out.
15	*	*	*	Request timed out.
16	*	*	*	Request timed out.
17	*	*	*	Request timed out.
18	*	*	*	Request timed out.
19	*	*	*	Request timed out.
20	*	*	*	Request timed out.
21	*	*	*	Request timed out.
22	*	*	*	Request timed out.
23	*	*	*	Request timed out.
24	*	*	*	Request timed out.
25	*	*	*	Request timed out.
26	*	*	*	Request timed out.
27	*	*	*	Request timed out.
28	*	*	*	Request timed out.
29	*	*	*	Request timed out.
30	*	*	*	Request timed out.

Trace complete.

C:\Users\User>

Experiment No. 5

Forward Path

Source

☒ IPv4 ☐ IPv6

Melbourne, Australia

Command

☐ ping
☒ traceroute
☐ show bgp route

Destination

☒ Your IP: 134.41.62.153
☐ Another IP
☐ Sprint Site

Submit

Sprint Source: Melbourne, Australia (sl-mpe01-mel)
Your IP: 134.41.62.153
Performing: ICMP Traceroute
IP Version: IPv4

Tracing the route to hlfkna018gw-134-41-62-153.dhcp-dynamic.fibreop.na.bellaliant.net (134.41.62.153)

```
1 sl-mpe70-syd2-gi0-3-0-9.sprintlink.net (203.222.33.164) 14 msec 13 msec 12 msec
2 sl-mpe01-syd-gi0-0-1-9.sprintlink.net (203.222.33.104) 16 msec 15 msec 15 msec
3 sl-mpe02-ana-gi0-0-0-0.sprintlink.net (203.222.33.20) 152 msec 151 msec 152 msec
4 sl-crs1-ana-te0-3-0-3.sprintlink.net (144.232.16.157) 153 msec
  sl-crs2-ana-te0-3-0-3.sprintlink.net (144.232.16.155) 151 msec 152 msec
5 sl-crs2-aj-be7.sprintlink.net (144.232.17.29) 160 msec
  sl-crs1-ria-bel0.sprintlink.net (144.232.22.69) 160 msec
  sl-crs2-aj-be7.sprintlink.net (144.232.17.29) 160 msec
6 sl-crs2-stk-be3.sprintlink.net (144.232.22.179) 164 msec
  sl-crs2-stk-bel1.sprintlink.net (144.232.22.95) 168 msec 166 msec
7 sl-crs1-oro-be2.sprintlink.net (144.232.15.236) 166 msec 168 msec 168 msec
8 sl-crs1-cma-be7.sprintlink.net (144.232.15.164) 200 msec
  sl-crs2-cma-be7.sprintlink.net (144.232.15.166) 199 msec 193 msec
9 sl-crs2-chi-be4.sprintlink.net (144.232.22.74) 203 msec 202 msec
  sl-crs1-chi-be4.sprintlink.net (144.232.22.72) 204 msec
10 sl-mat70-chi2-bel16.sprintlink.net (144.232.2.92) 201 msec 201 msec
  sl-mat70-chi2-bel17.sprintlink.net (144.232.2.94) 200 msec
11 144.223.3.226 201 msec 200 msec 200 msec
12 * * *
13 * * *
```

Reverse Path

Command Prompt

C:\Users\User>tracert 203.222.33.164

Tracing route to sl-mpe70-syd2-gi0-3-0-9.sprintlink.net [203.222.33.164]
over a maximum of 30 hops:

```
 1      3 ms      2 ms      4 ms    mynetwork [192.168.2.1]
 2      4 ms      4 ms     13 ms    loop0.8gw.ba19.hlfk.ns.aliant.net [142.176.50.21]
 3      4 ms      4 ms      6 ms    be16-181.cr01.hlfk.ns.aliant.net [142.166.242.113]
 4     21 ms     21 ms     21 ms    be19.bx02.nycm.ny.aliant.net [207.231.227.62]
 5     29 ms     29 ms     21 ms    ae20.cr3-nyc6.ip4.gtt.net [209.120.140.5]
 6      *      *      *      Request timed out.
 7      *      *      *      Request timed out.
 8      *      *      *      Request timed out.
 9      *      *      *      Request timed out.
10     *      *      *      Request timed out.
11     *      *      *      Request timed out.
12     *      *      *      Request timed out.
13     *      *      *      Request timed out.
14     *      *      *      Request timed out.
15     *      *      *      Request timed out.
16     *      *      *      Request timed out.
17     *      *      *      Request timed out.
18     *      *      *      Request timed out.
19     *      *      *      Request timed out.
20     *      *      *      Request timed out.
21     *      *      *      Request timed out.
22     *      *      *      Request timed out.
23     *      *      *      Request timed out.
24     *      *      *      Request timed out.
25     *      *      *      Request timed out.
26     *      *      *      Request timed out.
27     *      *      *      Request timed out.
28     *      *      *      Request timed out.
29     *      *      *      Request timed out.
30     *      *      *      Request timed out.
```

Trace complete.

Five of the above mentioned experiments couldn't give a full traceroute result. Both the forward and reverse traceroute in the 5 experiment start giving error packets from the after a few hops. I have tried running this traceroute command turning my Firewall off but it fails to reach to the destination.

References

- [1]. Network Direction. 2022. *ICMP Types - Network Direction*. [online] Available at: <https://networkdirection.net/articles/network-theory/icmptypes>.
- [2]. SearchNetworking. 2022. *What is ICMP (Internet Control Message Protocol)? - Definition from WhatIs.com*. [online] Available at: <https://www.techtarget.com/searchnetworking/definition/ICMP>.
- [3] Howtouselinux. 2022. *Exploring ICMP Port Number with Example - Howtouselinux*. [online] Available at: <https://www.howtouselinux.com/post/icmp-port-number>.
- [4] A. Mitra, "What are Ping Flood and Ping of Death?", 2017. [Online]. Available: <https://www.thesecuritybuddy.com/dos-ddos-prevention/what-are-ping-flood-and-ping-of-death/>.
- [5] J. Lévesque, "What is a Traceroute and How Do Traceroutes Work? | Obkio", *Obkio*, 2022. [Online]. Available: <https://obkio.com/blog/traceroutes-what-are-they-and-how-do-they-work/>.
- [6] "17 traceroute command examples to Identify Network Problems in Linux/Unix | CyberITHub", *CyberITHub*, 2022. [Online]. Available: <https://www.cyberithub.com/traceroute-command-examples-in-linux-unix/>.
- [7] A. Sarangam, "IP Spoofing - A Comprehensive Guide For 2021", *Jigsaw Academy*, 2021. [Online]. Available: <https://www.jigsawacademy.com/blogs/cyber-security/what-is-ip-spoofing/>.