DALHOUSIE UNIVERSITY

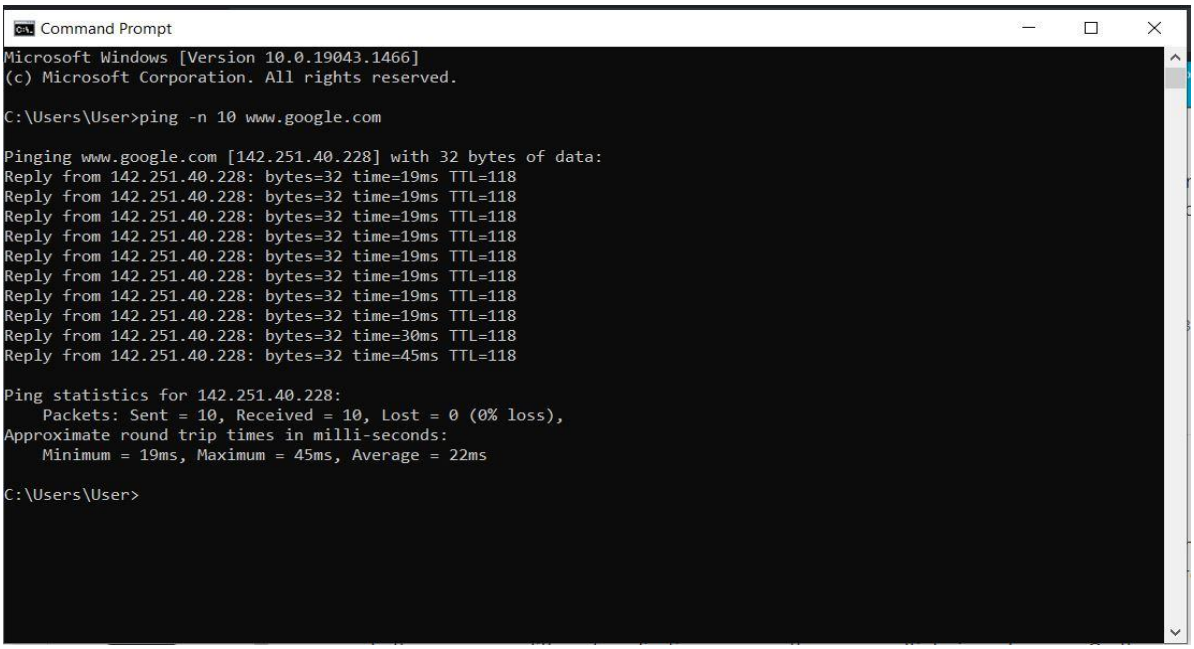
Faculty of Computer Science

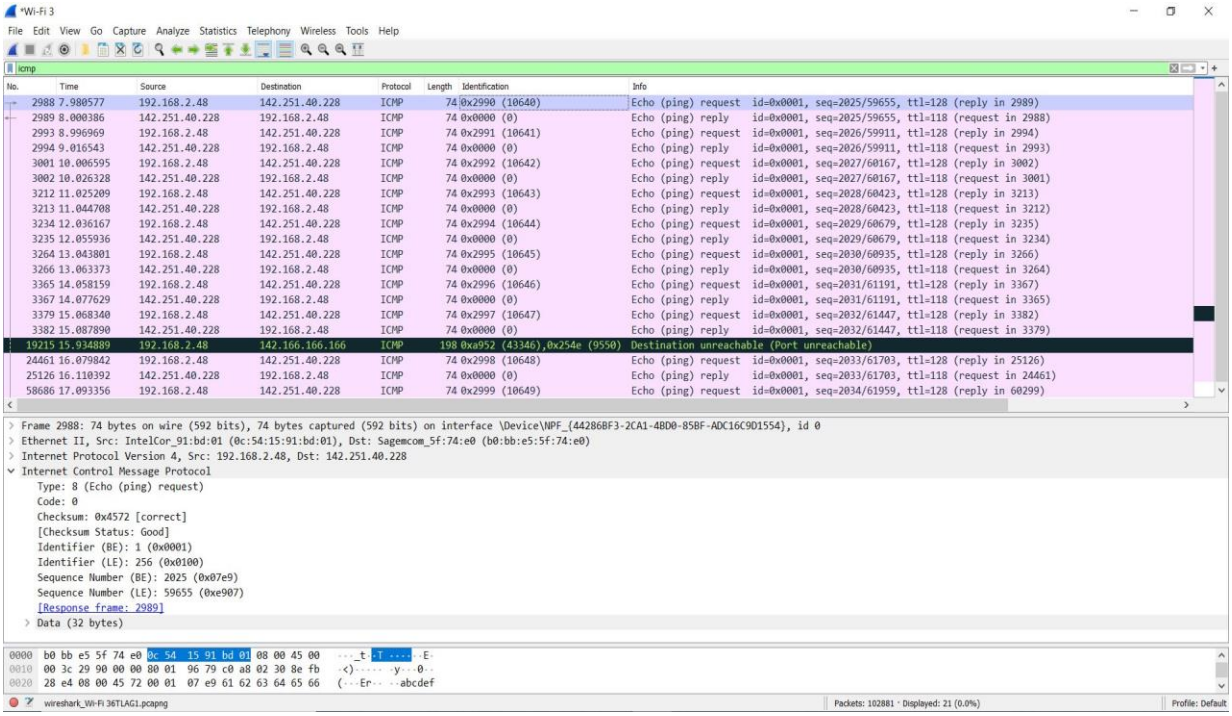
CSCI 6708 – Advanced Topics in Network Security

Name: Arka Ghosh
Banner ID: B00911033
Assignment: 01

Part 1

1.





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:

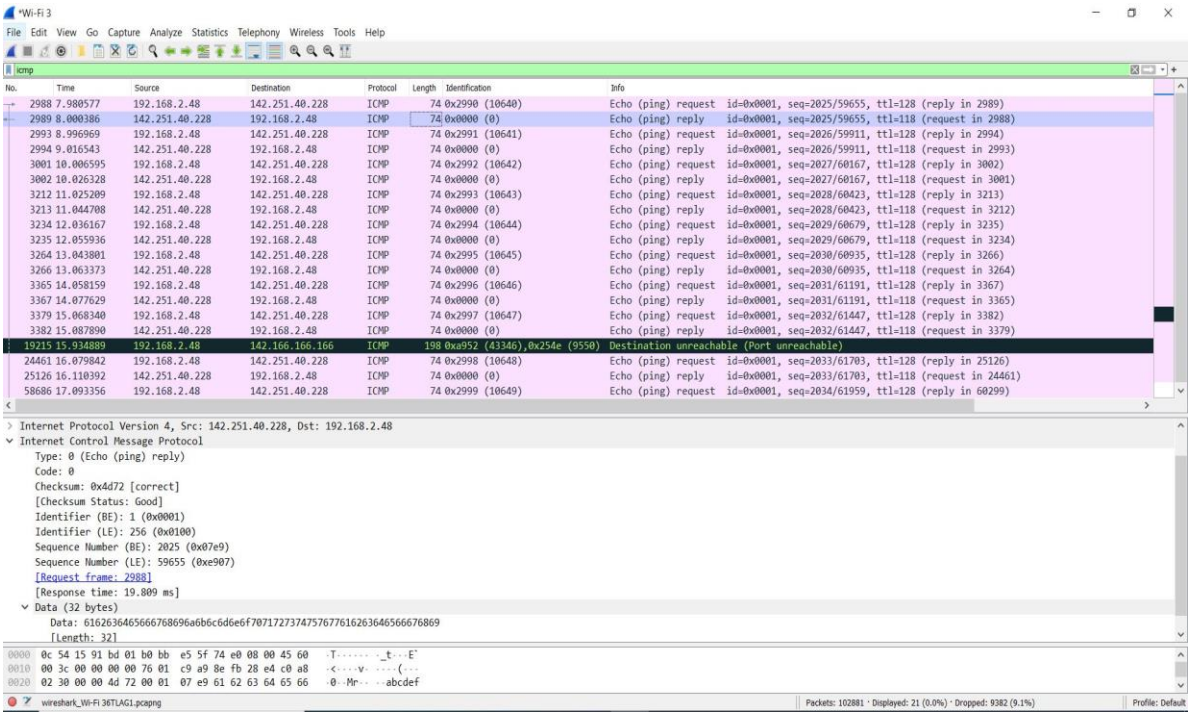
- Checksum: 0x4572
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence Number (BE): 2025 (0x07e9)
- Sequence Number (LE): 59655 (0xe907)

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

- Data: 6162636465666768696a6b6c6d6e6f707172737475767761626364656667686 9

5.

<u>Wireshark Capture of the Reply Packet:</u>



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:

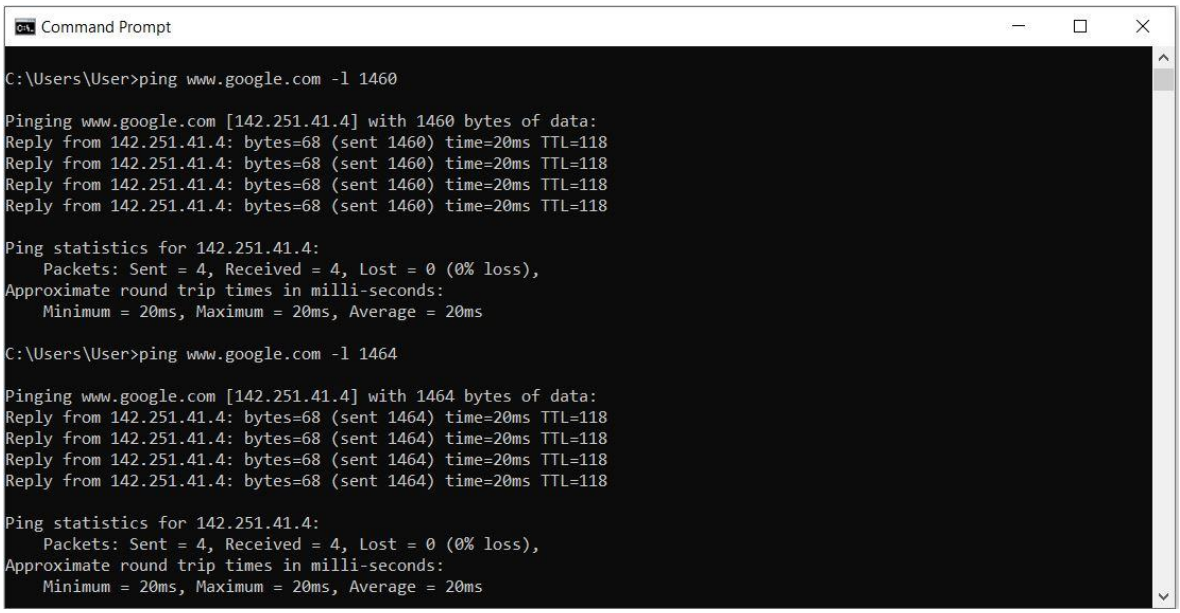
- Data: 6162636465666768696a6b6c6d6e6f707172737475767761626364656667686 9

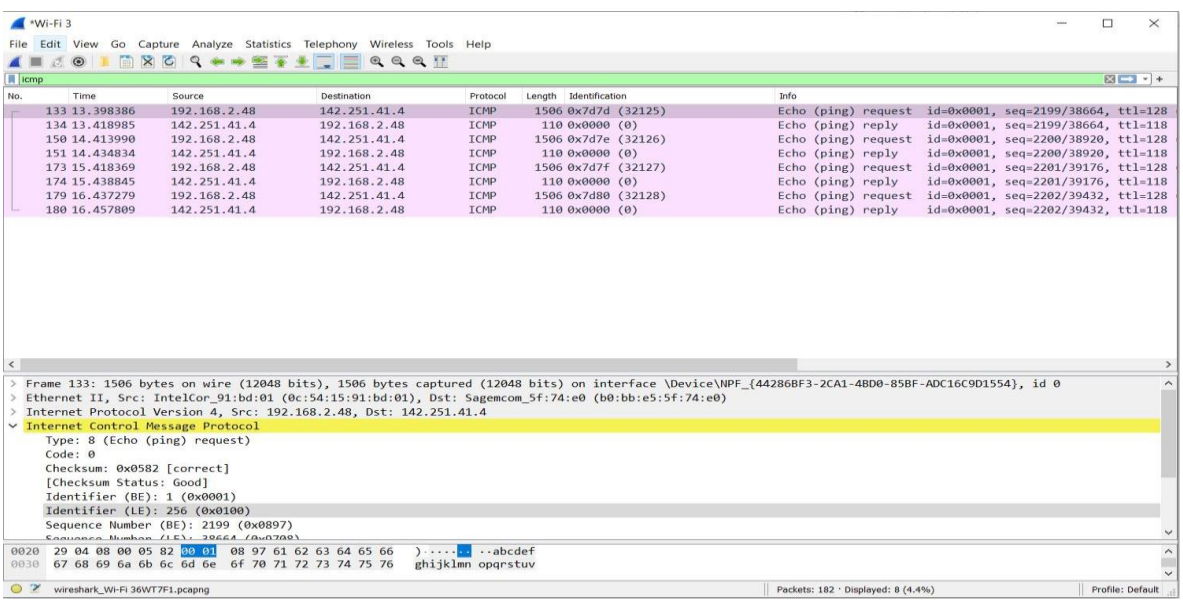
Part 2

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

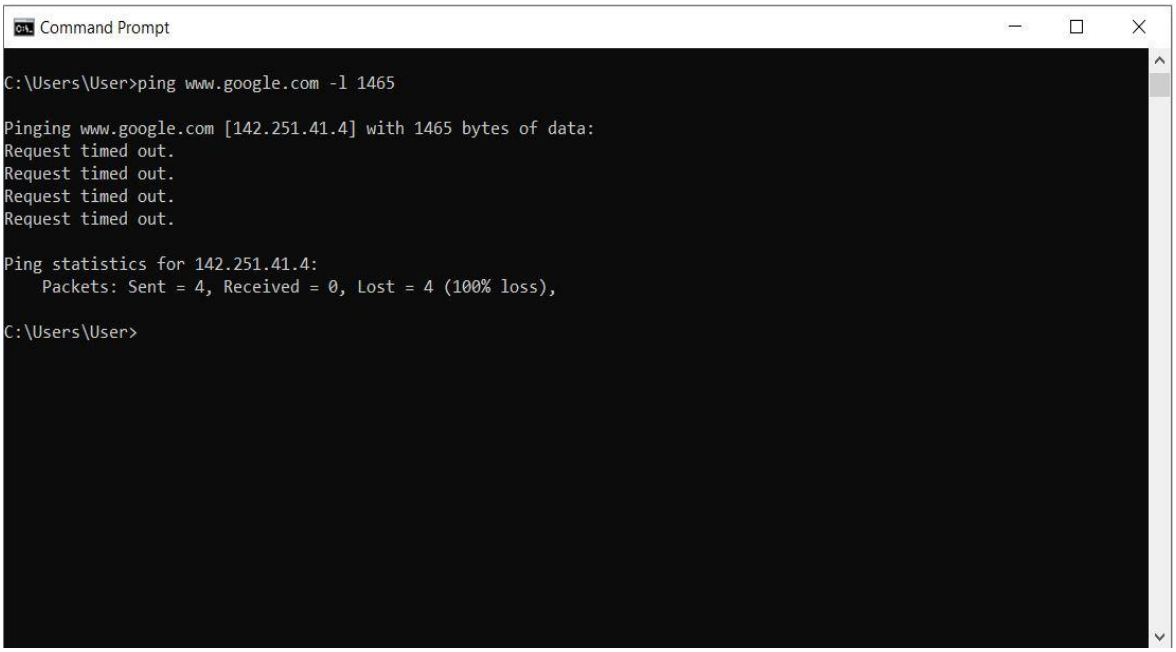
2. Here's are the two screenshots of the Windows Terminal and Wireshark Capture:

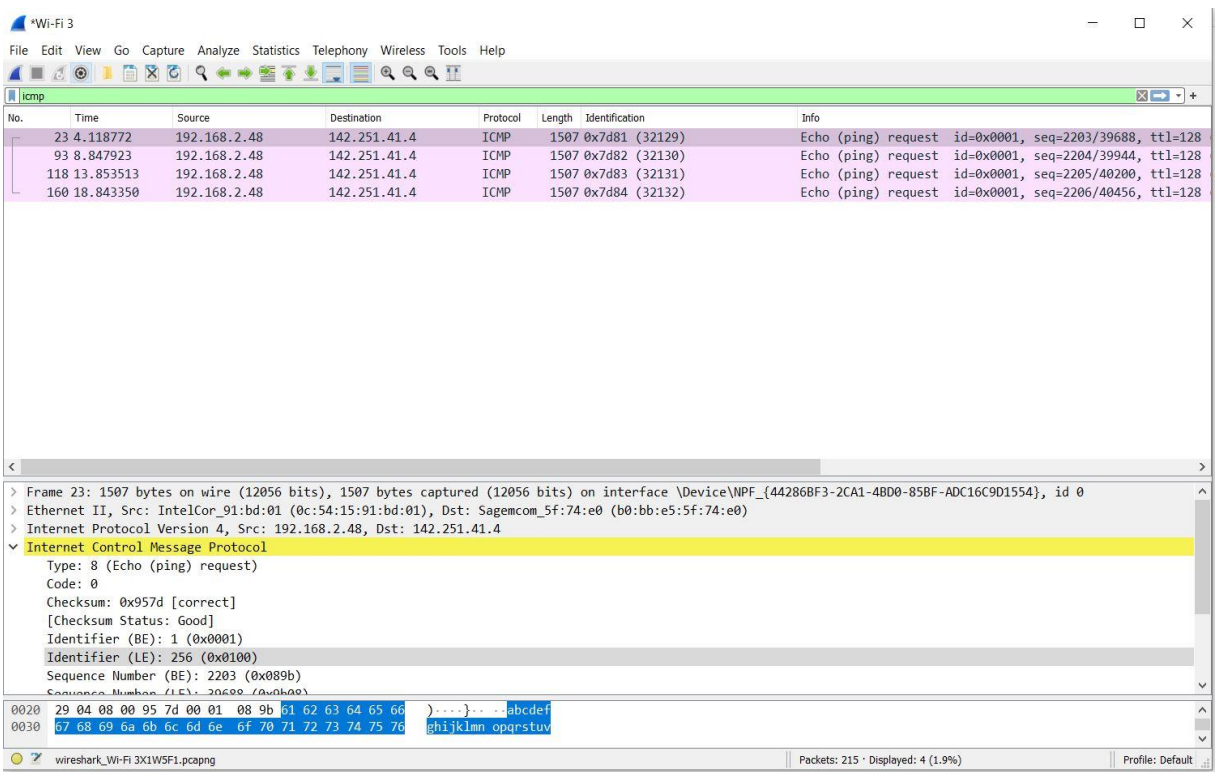
First Screenshot with 1464 Packet Size:





2nd Screenshot with 1465 Packet Size:





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.

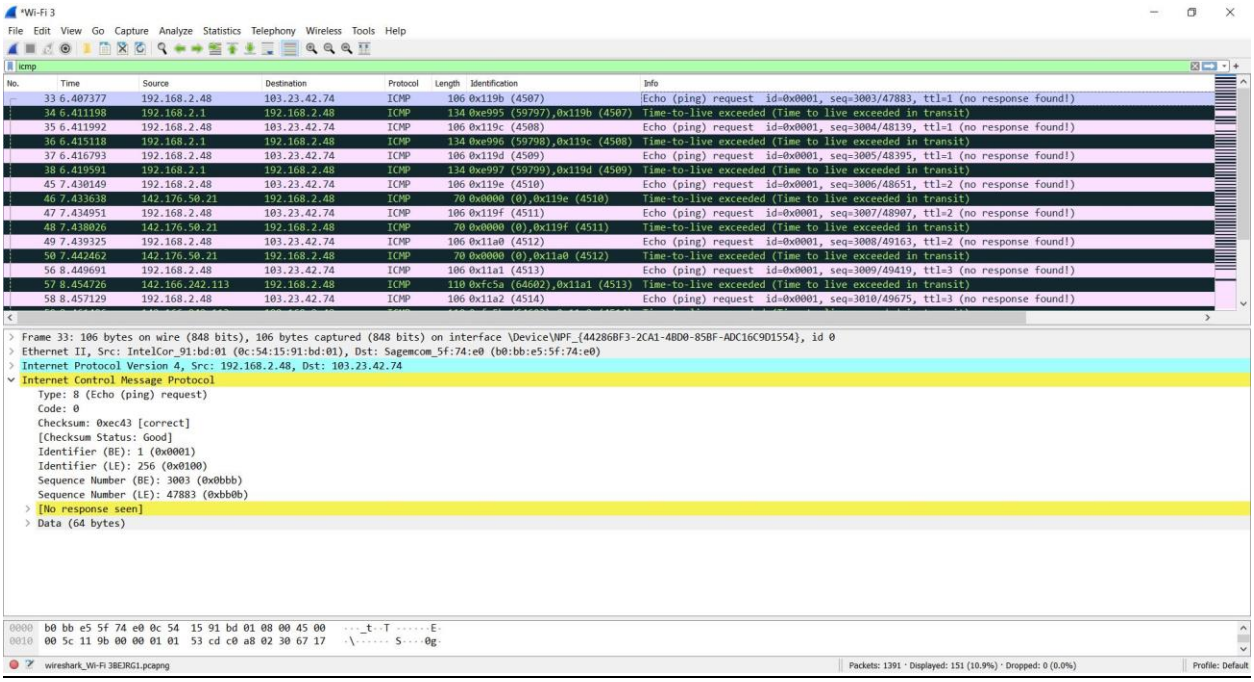
Part 3

1.

<u>Traceroute Result:</u>

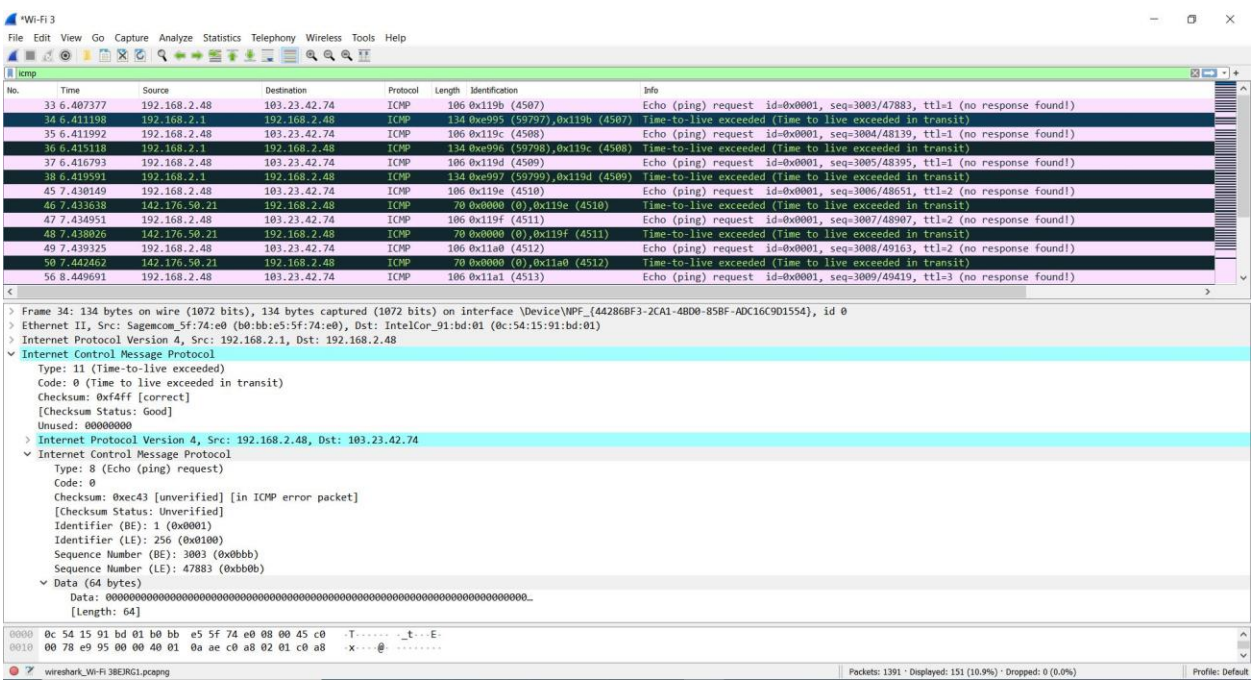
```
Command Prompt

C:\Users\User>tracert www.aust.edu

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

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



This ICMP reply packet differs from the one I captured with the ping command. This reply packet contains the ICMP request packet along with a 8bit IP header named Time-to-Live (TTL). In the traceroute, the source sends the first packet with a TTL value of 1. When the packet reaches at the router's end, TTL value is decremented by 1 by the router and the router sends back an ICMP TTL Exceeded message to the source [5].

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

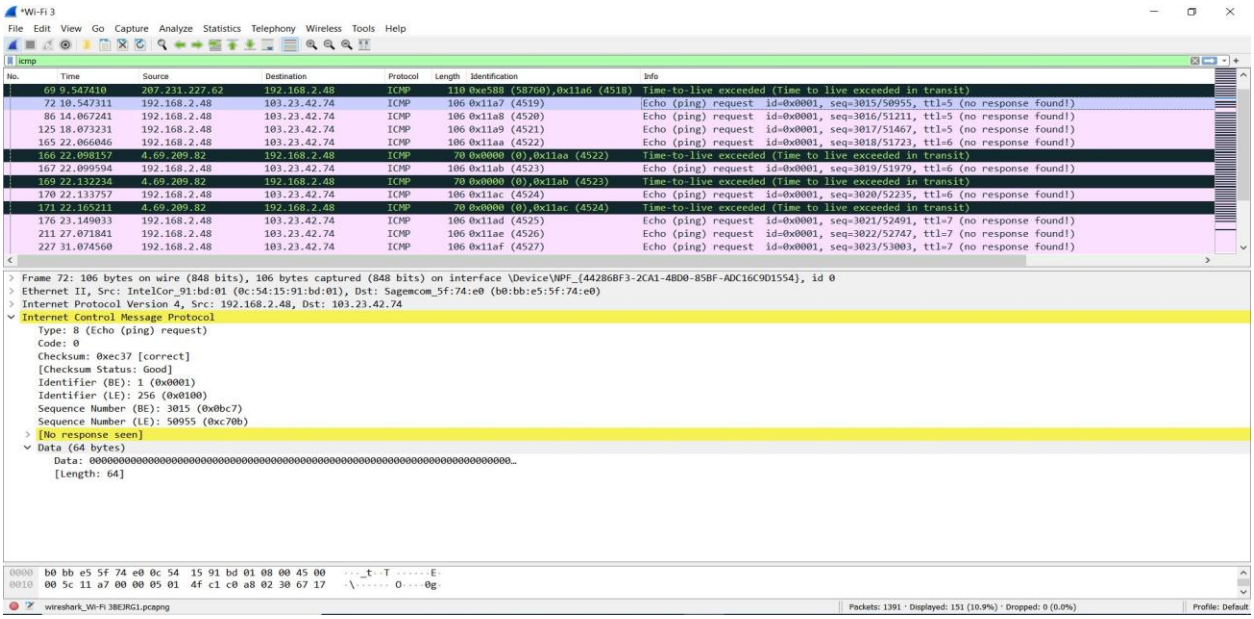
- Type: 11
- Code: 0
- Checksum: 0xf4ff
- Unused: 00000000

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

- Type: 8
- Code: 0
- Checksum: 0xec43
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence Number (BE): 3003 (0x0bbb)
- Sequence Number (LE): 47883 (0xbb0b)
  Data (64 bytes)
- Data:
  0000000000000000000000000000000000000000000000000000000000000000000000000000
  …

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:

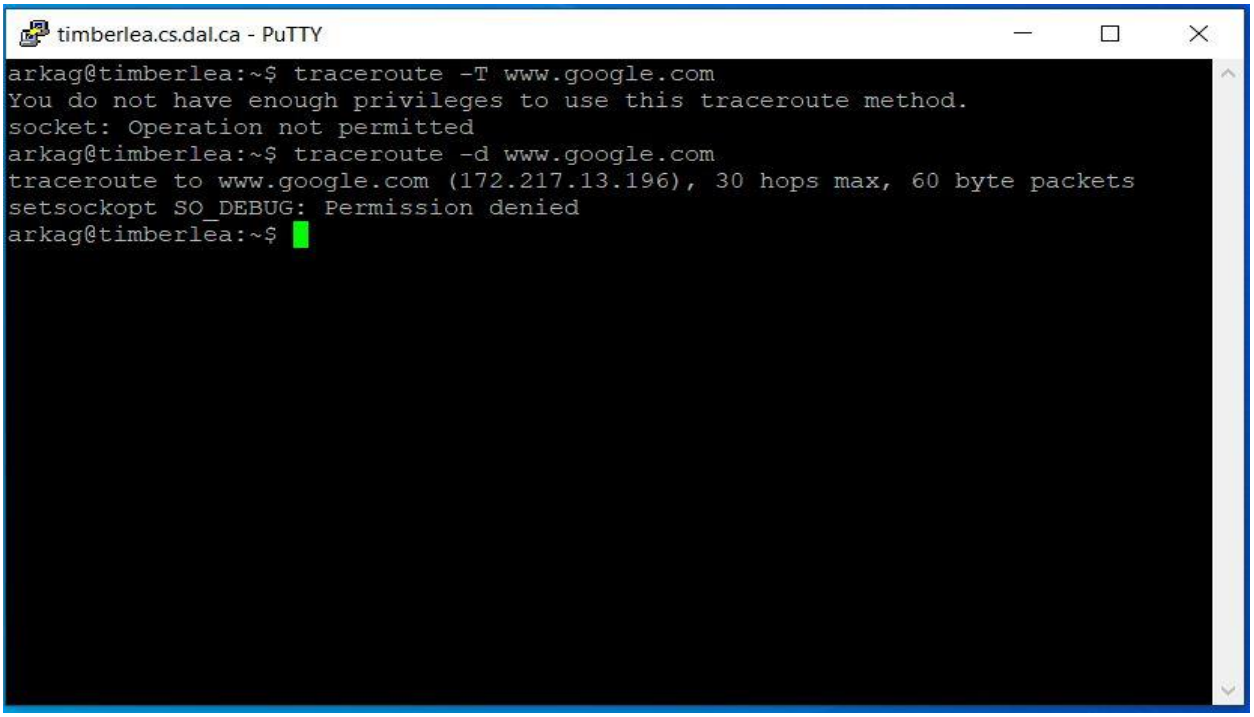


The error packet has the same field as the one I got with ping command. The fields in that packet is mentioned below with their values:

- Type: 8
- Code: 0
- Checksum: 0xec37 [correct]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence Number (BE): 3015 (0x0bc7)
- Sequence Number (LE): 50955 (0xc70b)
  Data (64 bytes)
    - Data: 0000000000000000000000000000000000000000000000000000000000000000000000000000…

3. –T is for using TCP SYN for probing and –d is for enabling socket level debugging in Unix server.

I have used Timberlea for using both of the commands. I cannot run traceroute using these commands. Because the kernel doesn't support these command. The screenshot is attached below:



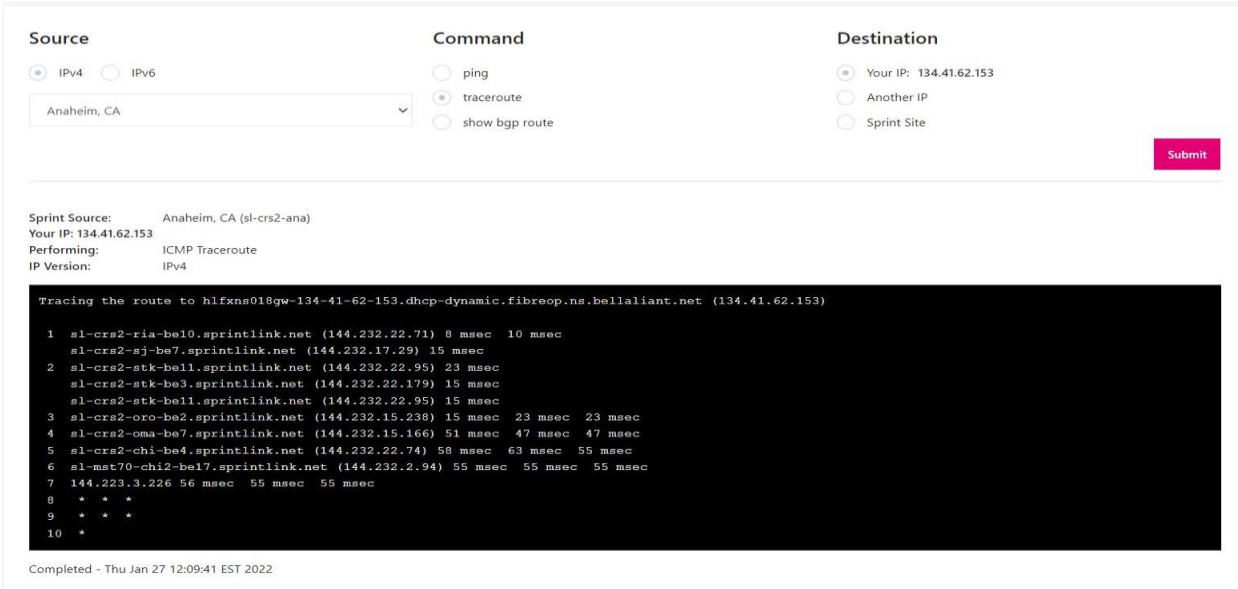
4. –s src_addr is for choosing an alternative source address for outgoing packet. One can use the –s src_addr option to choose an alternative source address while running traceroute instead of the default one.

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.

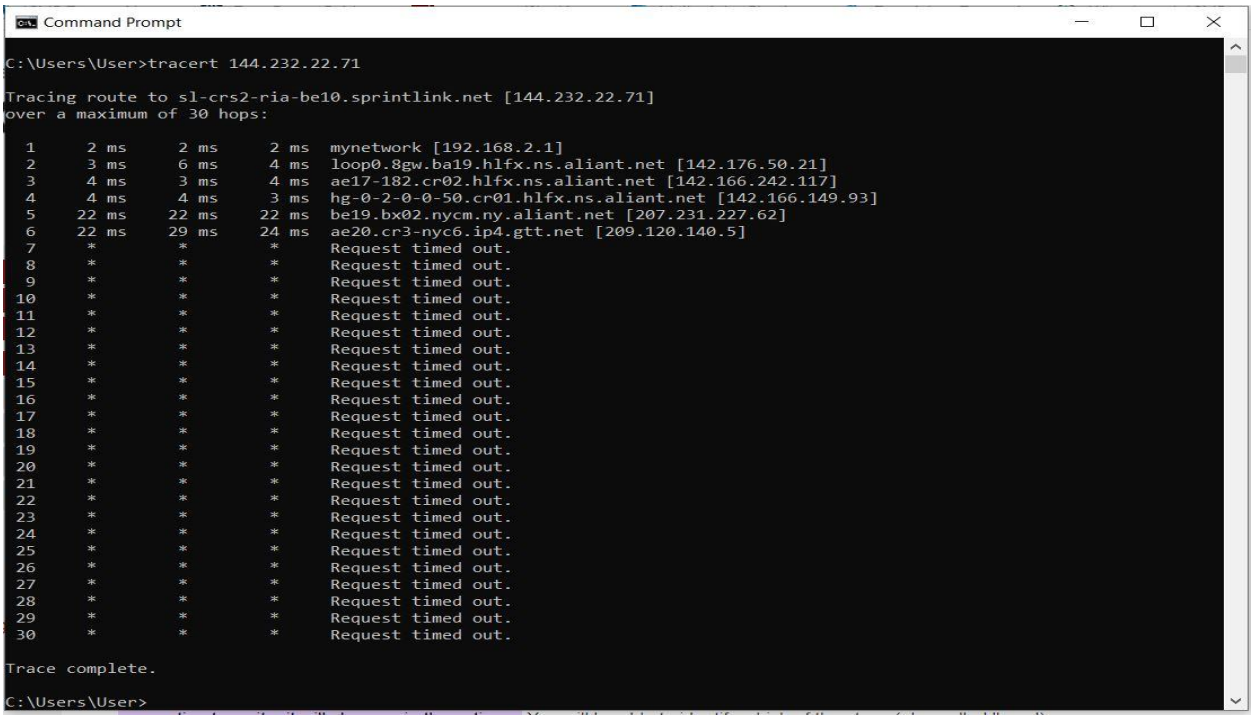
Part 4

Experiment No. 1

Forward Path

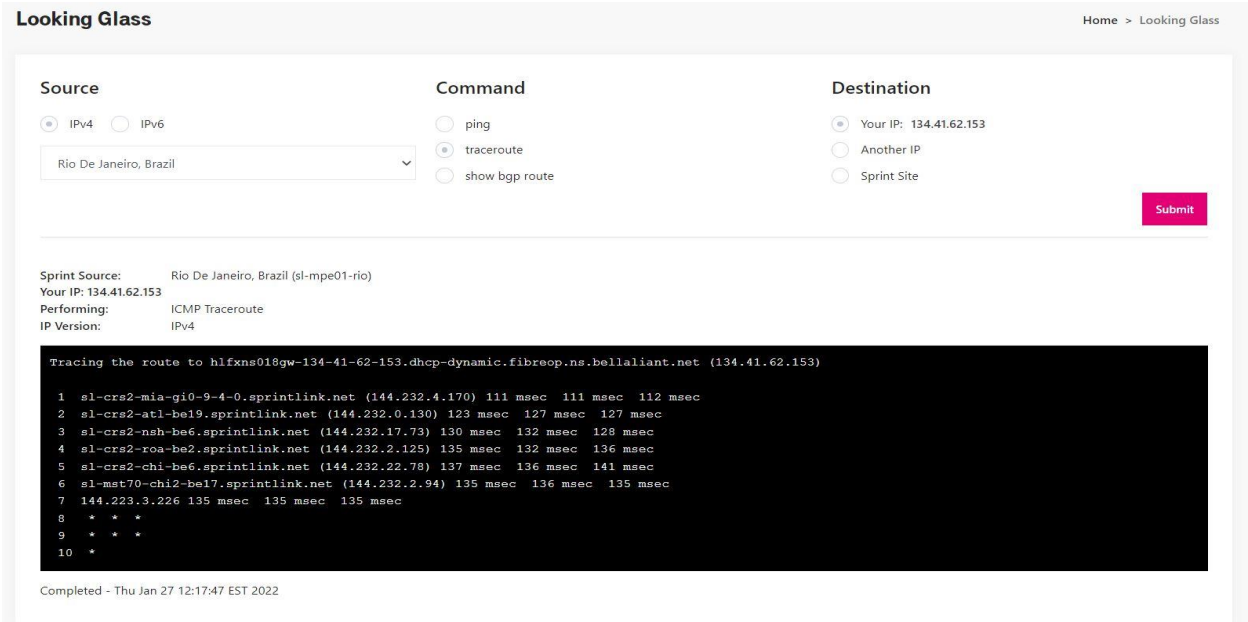


Backward Path

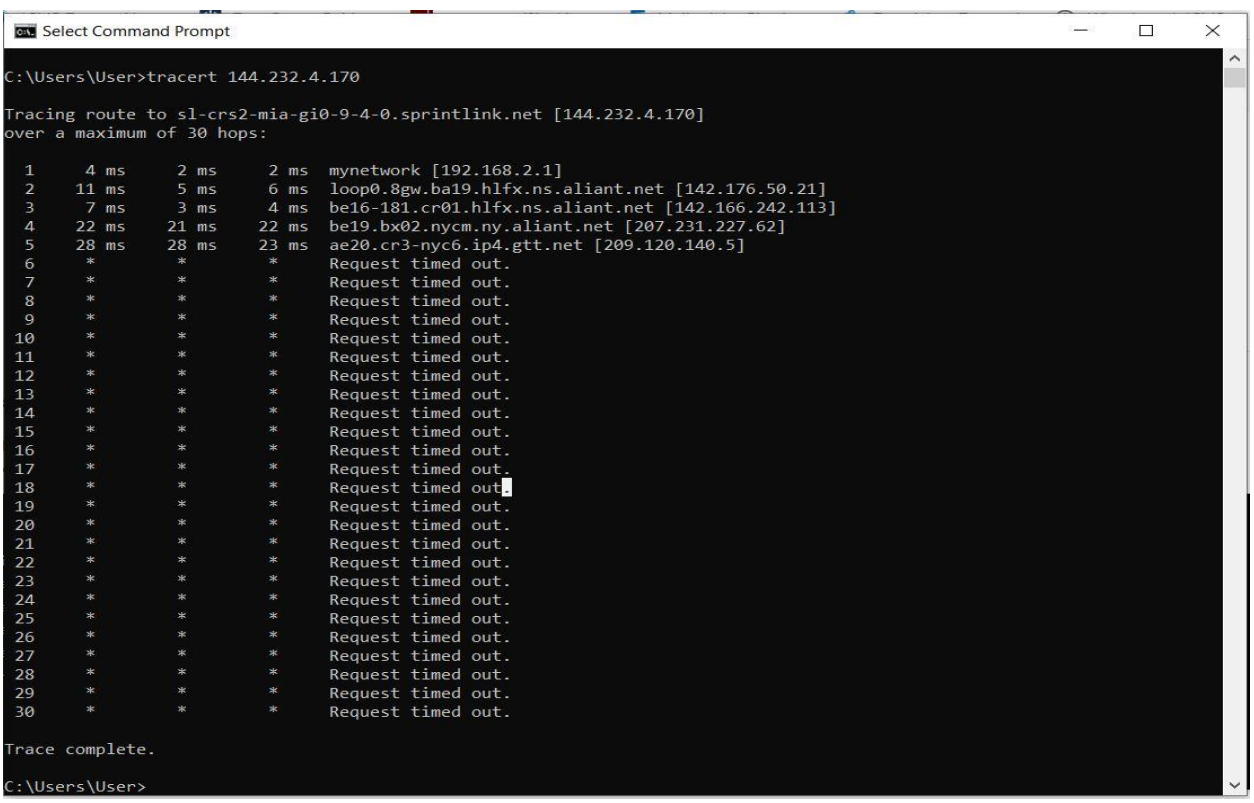


Experiment No. 2

Forward Path

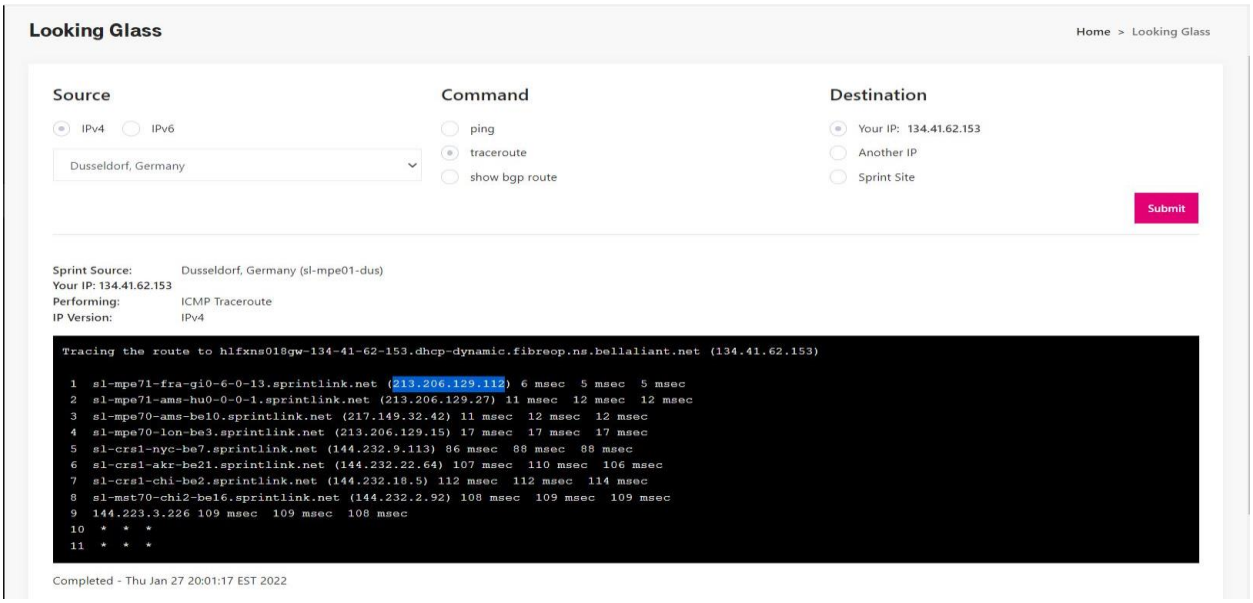


Reverse Path

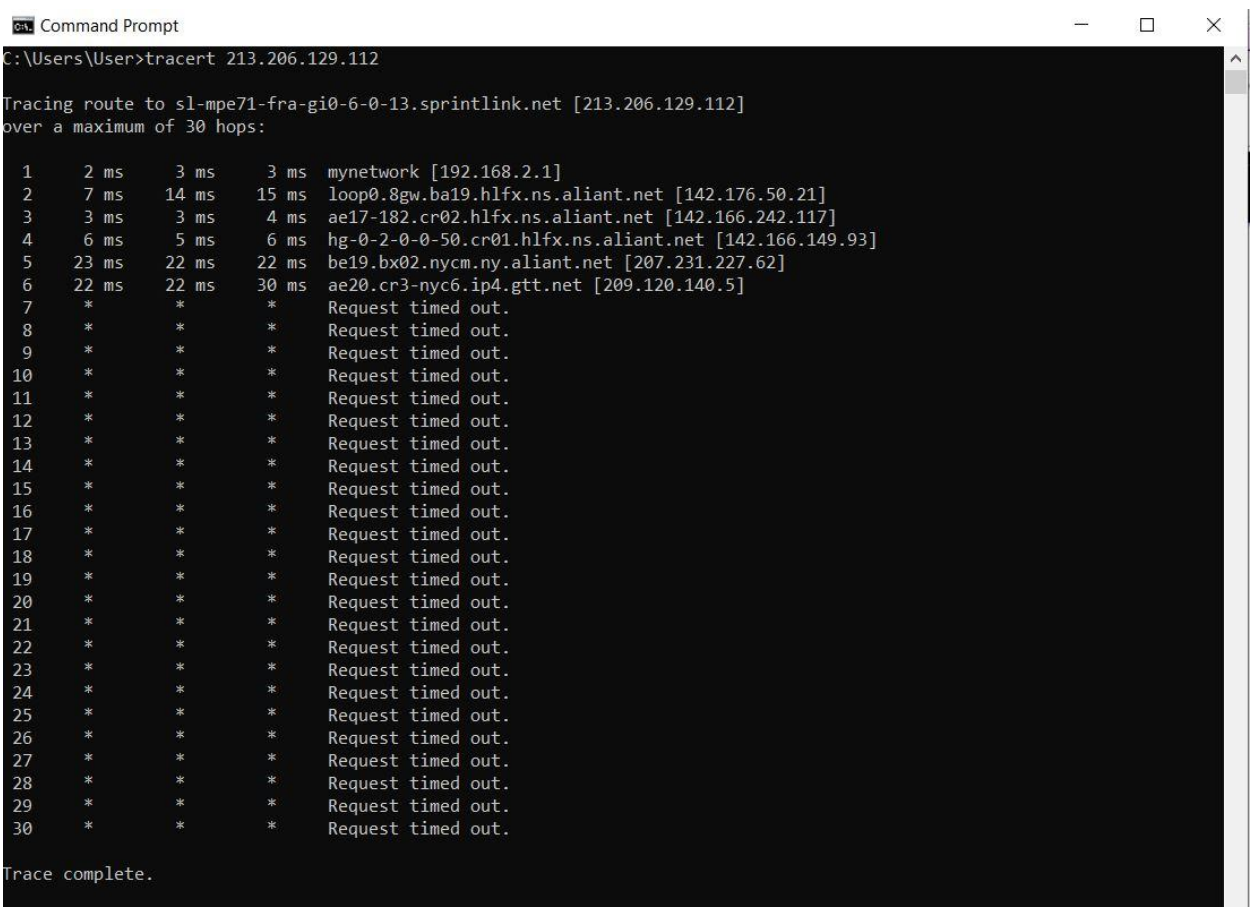


Experiment No. 3

Forward Path

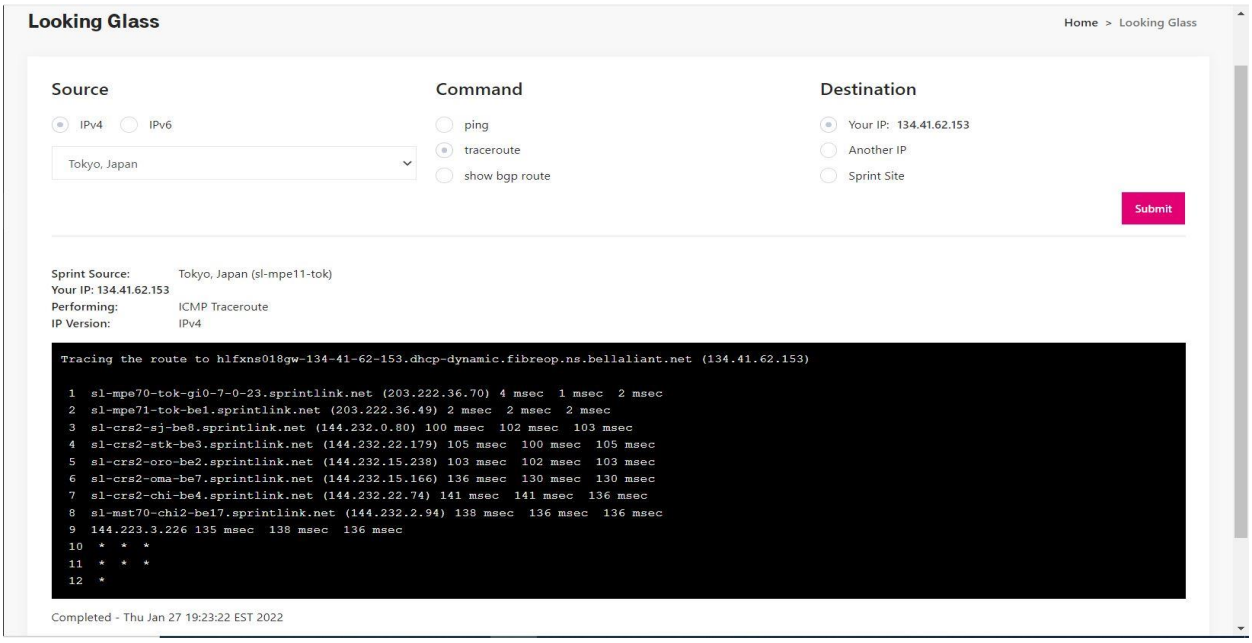


Reverse Path

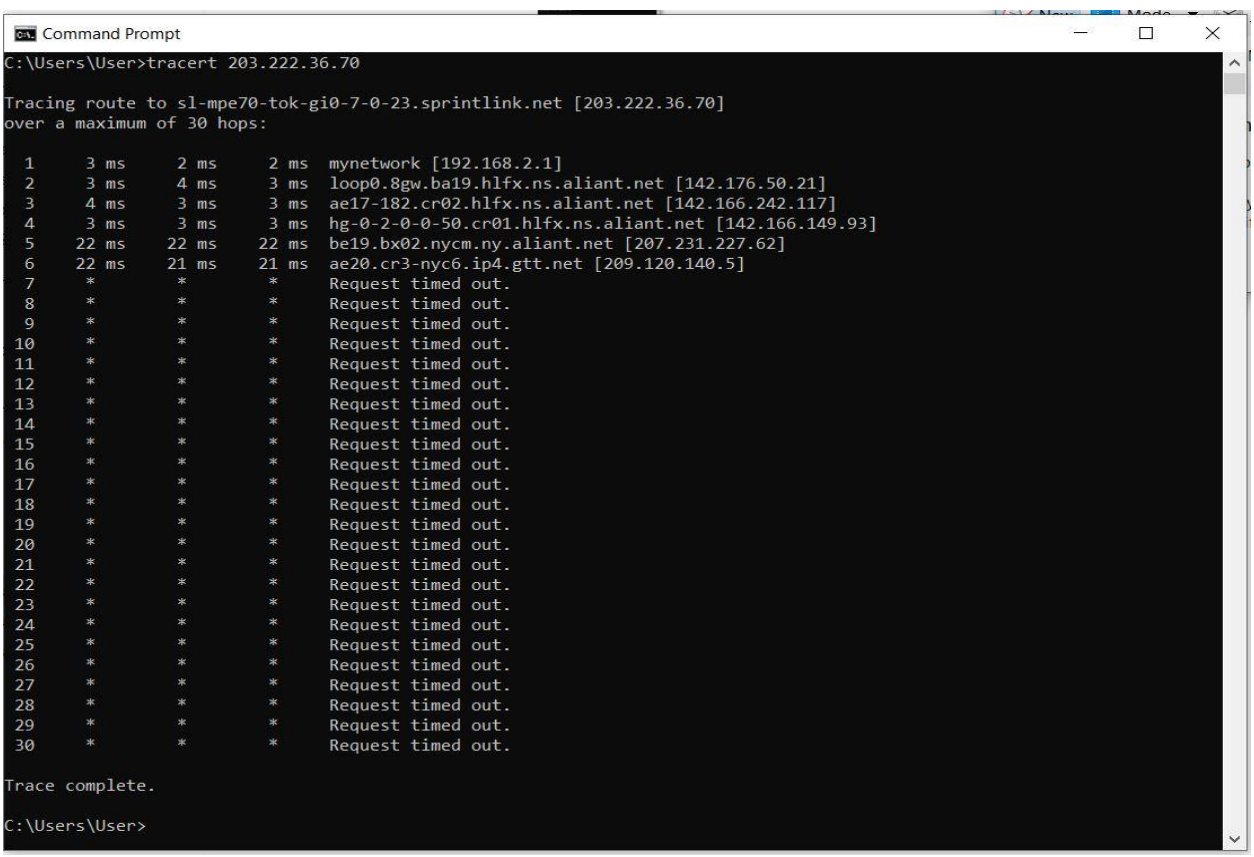


Experiment No. 4

Forward Path

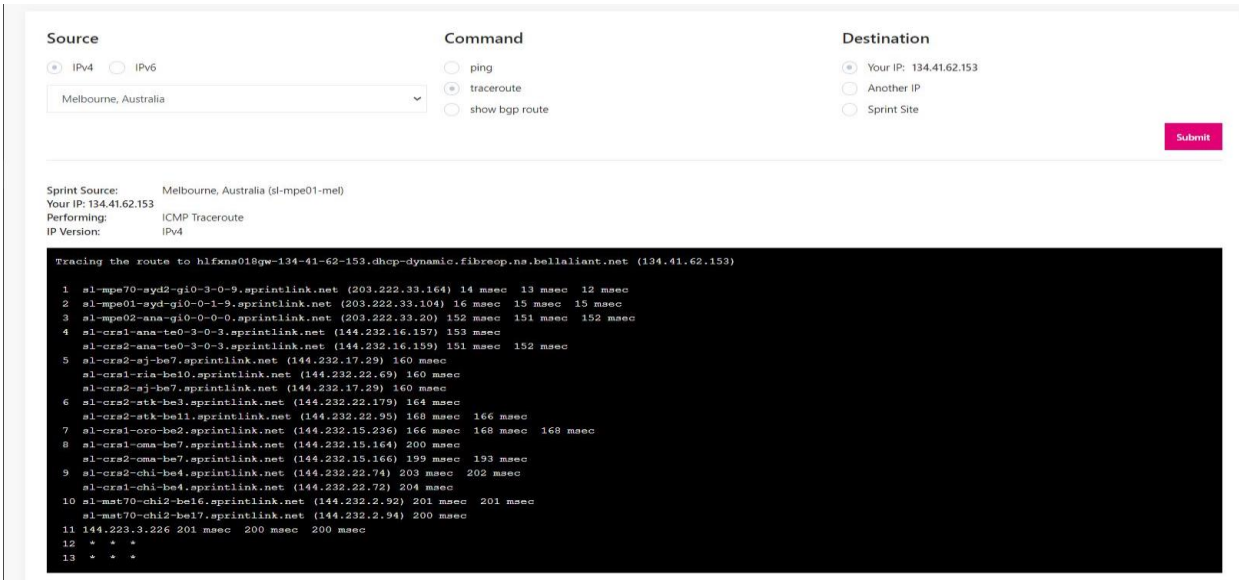


Reverse Path

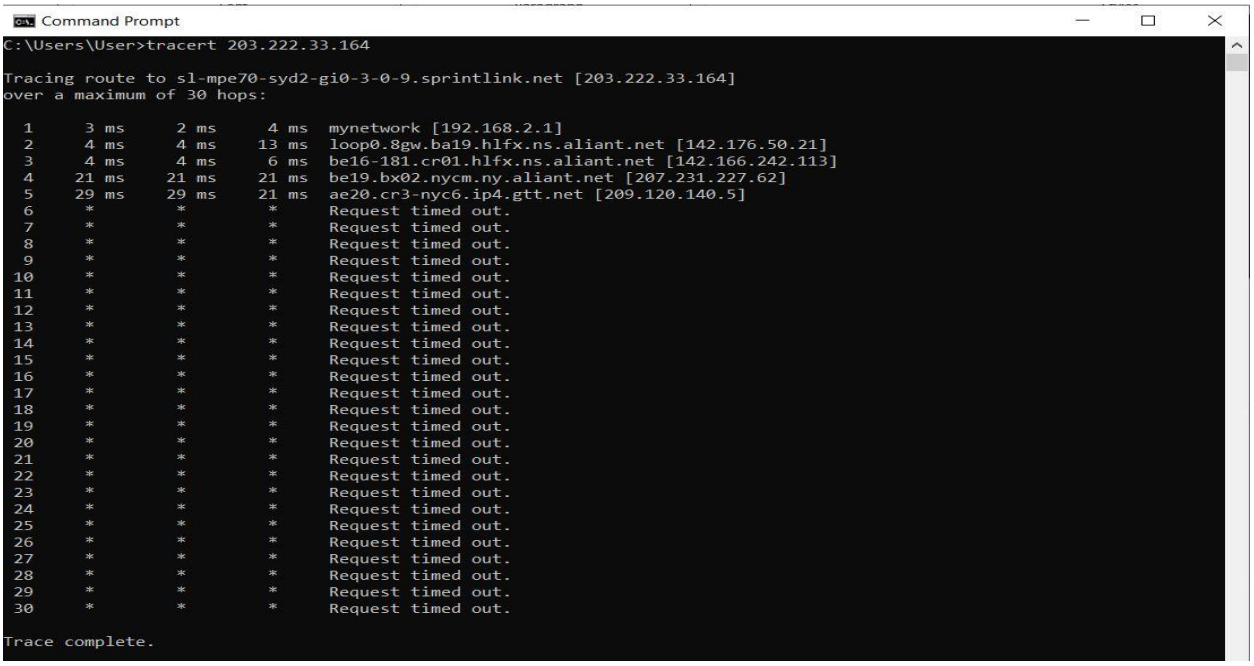


Experiment No. 5

Forward Path



Reverse Path



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/.