ASSIGNMENT – 1

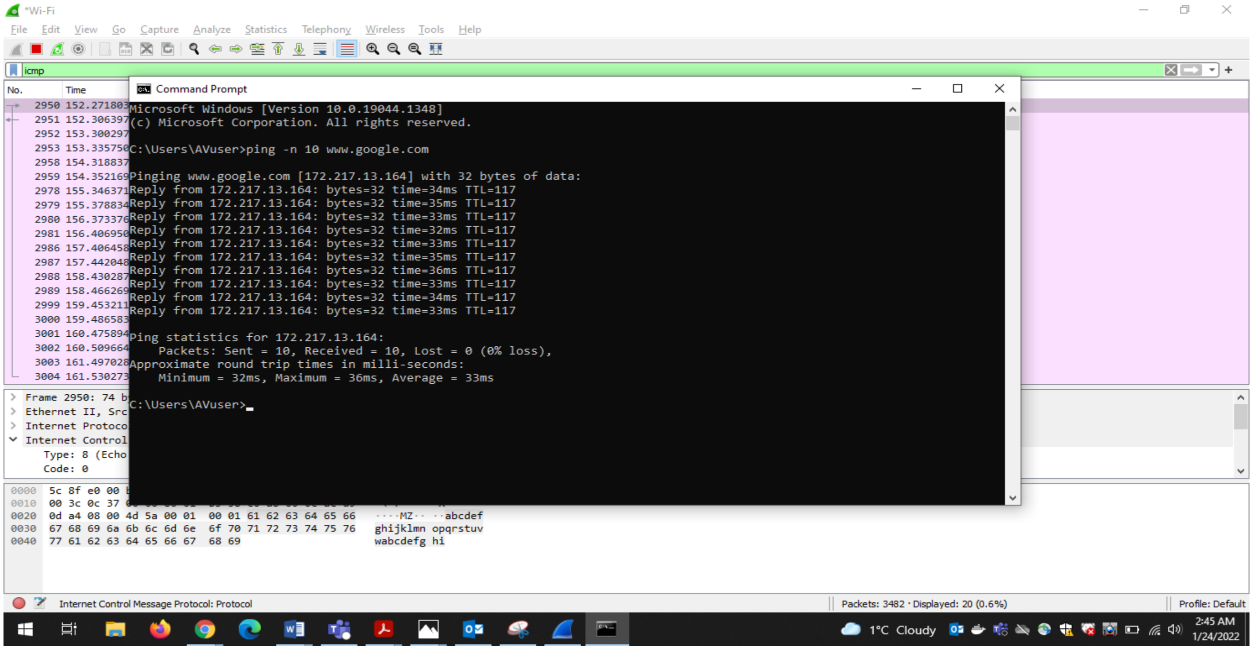
CSCI-6708 Advanced Network Security

Sumit Singh

B00882103

Sm435410@dal.ca

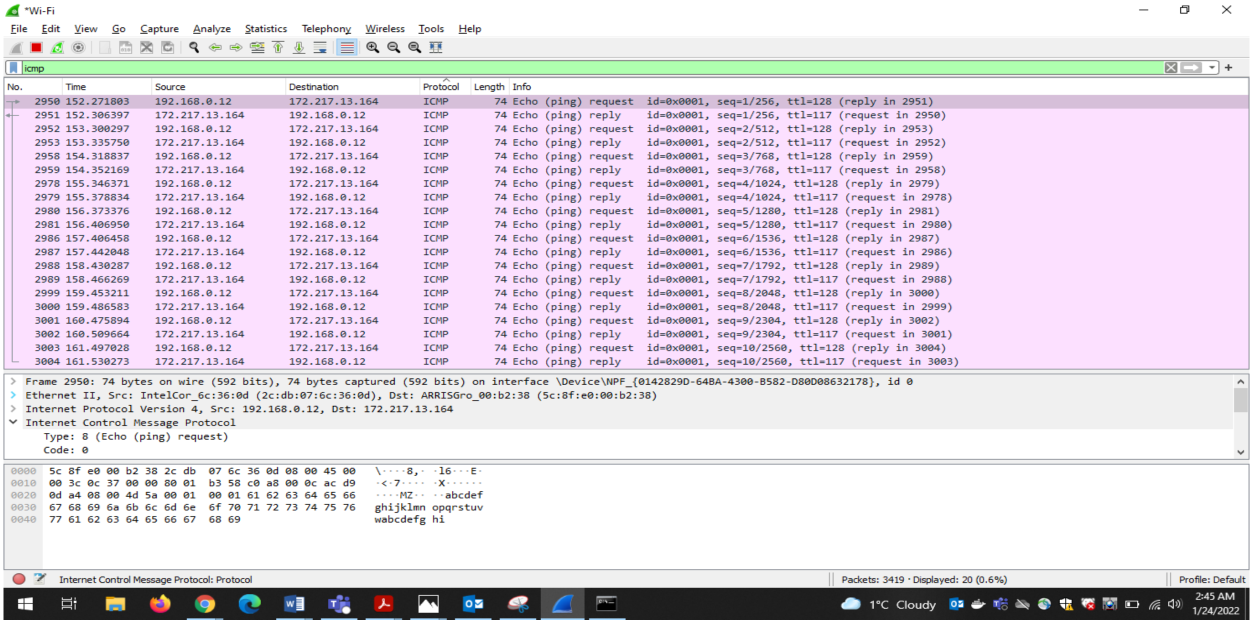
PART 1


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time
Command Prompt

```
Microsoft Windows [Version 10.0.19044.1348]
(c) Microsoft Corporation. All rights reserved.

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

Pinging www.google.com [172.217.13.164] with 32 bytes of data:
Reply from 172.217.13.164: bytes=32 time=34ms TTL=117
Reply from 172.217.13.164: bytes=32 time=35ms TTL=117
Reply from 172.217.13.164: bytes=32 time=33ms TTL=117
Reply from 172.217.13.164: bytes=32 time=32ms TTL=117
Reply from 172.217.13.164: bytes=32 time=33ms TTL=117
Reply from 172.217.13.164: bytes=32 time=35ms TTL=117
Reply from 172.217.13.164: bytes=32 time=36ms TTL=117
Reply from 172.217.13.164: bytes=32 time=33ms TTL=117
Reply from 172.217.13.164: bytes=32 time=34ms TTL=117
Reply from 172.217.13.164: bytes=32 time=33ms TTL=117

Ping statistics for 172.217.13.164:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 32ms, Maximum = 36ms, Average = 33ms

C:\Users\AVuser>_
```

```
Internet Control Message Protocol: Protocol
Packets: 3482 · Displayed: 20 (0.6%)
Profile: Default
```

1°C Cloudy
2:45 AM
1/24/2022


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

```
No.  Time        Source          Destination     Protocol Length Info
2950 152.271803  192.168.0.12    172.217.13.164  ICMP     74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (reply in 2951)
2951 152.306397  172.217.13.164  192.168.0.12    ICMP     74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=117 (request in 2950)
2952 153.300297  192.168.0.12    172.217.13.164  ICMP     74 Echo (ping) request  id=0x0001, seq=2/512, ttl=128 (reply in 2953)
2953 153.335750  172.217.13.164  192.168.0.12    ICMP     74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=117 (request in 2952)
2958 154.318837  192.168.0.12    172.217.13.164  ICMP     74 Echo (ping) request  id=0x0001, seq=3/768, ttl=128 (reply in 2959)
2959 154.352169  172.217.13.164  192.168.0.12    ICMP     74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=117 (request in 2958)
2978 155.346371  192.168.0.12    172.217.13.164  ICMP     74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=128 (reply in 2979)
2979 155.378834  172.217.13.164  192.168.0.12    ICMP     74 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=117 (request in 2978)
2980 156.373376  192.168.0.12    172.217.13.164  ICMP     74 Echo (ping) request  id=0x0001, seq=5/1280, ttl=128 (reply in 2981)
2981 156.406950  172.217.13.164  192.168.0.12    ICMP     74 Echo (ping) reply    id=0x0001, seq=5/1280, ttl=117 (request in 2980)
2986 157.406458  192.168.0.12    172.217.13.164  ICMP     74 Echo (ping) request  id=0x0001, seq=6/1536, ttl=128 (reply in 2987)
2987 157.442048  172.217.13.164  192.168.0.12    ICMP     74 Echo (ping) reply    id=0x0001, seq=6/1536, ttl=117 (request in 2986)
2988 158.430287  192.168.0.12    172.217.13.164  ICMP     74 Echo (ping) request  id=0x0001, seq=7/1792, ttl=128 (reply in 2989)
2989 158.466269  172.217.13.164  192.168.0.12    ICMP     74 Echo (ping) reply    id=0x0001, seq=7/1792, ttl=117 (request in 2988)
2999 159.453211  192.168.0.12    172.217.13.164  ICMP     74 Echo (ping) request  id=0x0001, seq=8/2048, ttl=128 (reply in 3000)
3000 159.486583  172.217.13.164  192.168.0.12    ICMP     74 Echo (ping) reply    id=0x0001, seq=8/2048, ttl=117 (request in 2999)
3001 160.475894  192.168.0.12    172.217.13.164  ICMP     74 Echo (ping) request  id=0x0001, seq=9/2304, ttl=128 (reply in 3002)
3002 160.509664  172.217.13.164  192.168.0.12    ICMP     74 Echo (ping) reply    id=0x0001, seq=9/2304, ttl=117 (request in 3001)
3003 161.497028  192.168.0.12    172.217.13.164  ICMP     74 Echo (ping) request  id=0x0001, seq=10/2560, ttl=128 (reply in 3004)
3004 161.530273  172.217.13.164  192.168.0.12    ICMP     74 Echo (ping) reply    id=0x0001, seq=10/2560, ttl=117 (request in 3003)
```

```
> Frame 2950: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{0142829D-64BA-4300-B582-D80D08632178}, id 0
> Ethernet II, Src: IntelCor_6c:36:0d (2c:db:07:6c:36:0d), Dst: ARRISGro_00:b2:38 (5c:8f:e0:00:b2:38)
> Internet Protocol Version 4, Src: 192.168.0.12, Dst: 172.217.13.164
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
```

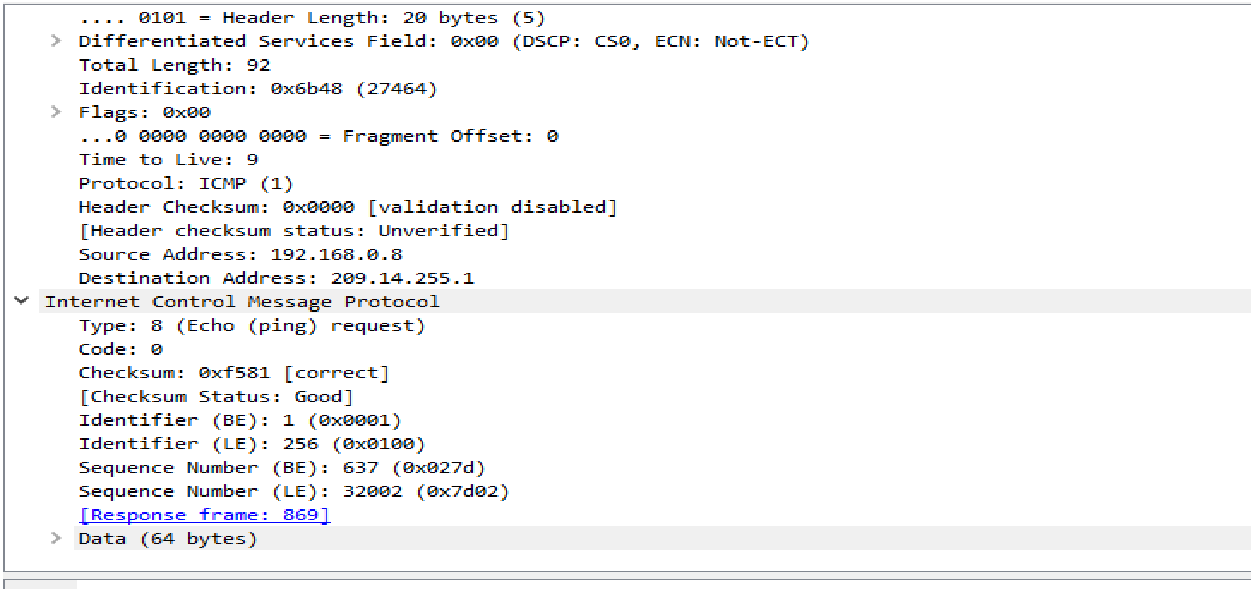
```
0000  5c 8f e0 00 b2 38 2c db  07 6c 36 0d 08 00 45 00   \····8,· ·l6···E·
0010  00 3c 0c 37 00 00 80 01  b3 58 c0 a8 00 0c ac d9   ·<·7···· ·X······
0020  0d a4 08 00 4d 5a 00 01  00 01 61 62 63 64 65 66   ····MZ·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

```
Internet Control Message Protocol: Protocol
Packets: 3419 · Displayed: 20 (0.6%)
Profile: Default
```

1. My IP address is :192.168.0.12
   Destination IP Address is: 172.217.13.164
2. ICMP type: 8 (Echo (ping) request)
   Code: 0
   Type specifies the type of ICMP message, like type 8 means request message and type 0 is used for a reply also type 3 for destination unreachable message.

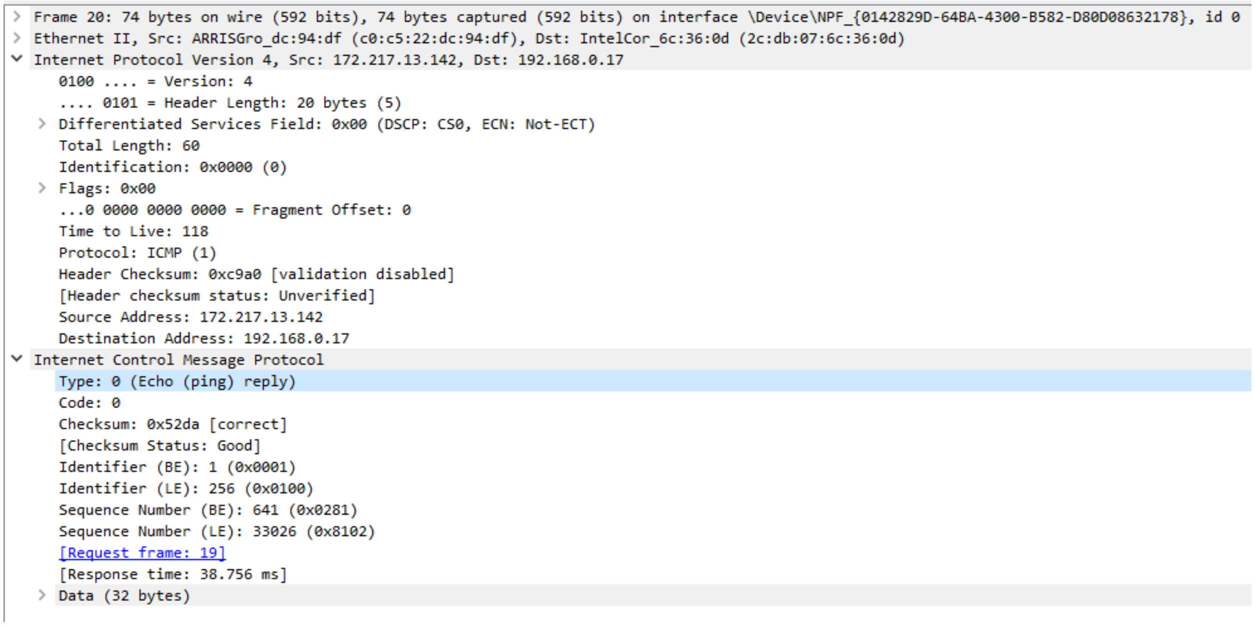
Code specifies what kind of ICMP message it is. Just for destination unreachable message we have 16 different codes. Code 0 means network was unreachable.

3. Port number are features of transport layer protocols such as TCP and UDP. ICMP packets do not have source and destination port number because it communicates network layer information between hosts and routers and not between application layer processes. Type and code combined is use to identify specific messages.
4. Following are the other fields in ICMP message and their values.



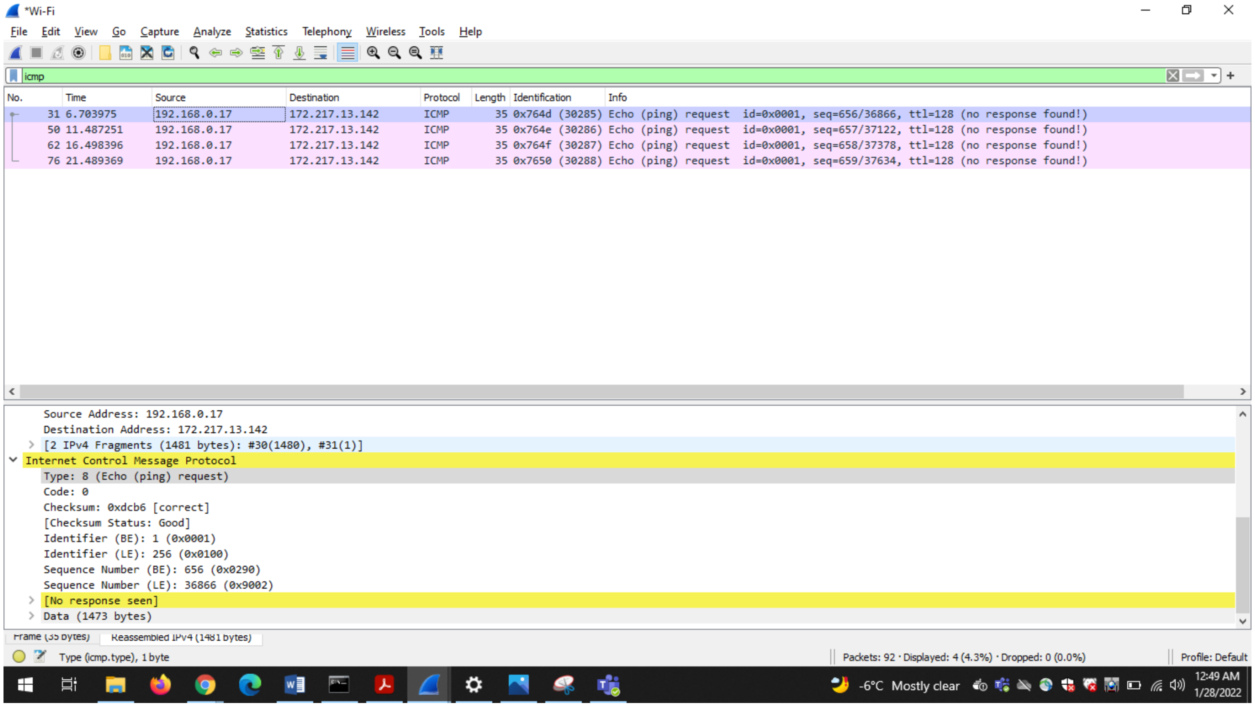
```
      .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 92
      Identification: 0x6b48 (27464)
    > Flags: 0x00
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 9
      Protocol: ICMP (1)
      Header Checksum: 0x0000 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.0.8
      Destination Address: 209.14.255.1
  v Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0xf581 [correct]
      [Checksum Status: Good]
      Identifier (BE): 1 (0x0001)
      Identifier (LE): 256 (0x0100)
      Sequence Number (BE): 637 (0x027d)
      Sequence Number (LE): 32002 (0x7d02)
      [Response frame: 869]
    > Data (64 bytes)
```

5. ICMP Type in reply packet is: 0 (Echo (ping) reply). ICMP message type 0 means Echo reply Code for ICMP reply packet is: 0. Code 0 for net is unreachable.
6. Following are the other fields in ICMP reply message with their values.



```
> Frame 20: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{0142829D-64BA-4300-B582-D80D08632178}, id 0
> Ethernet II, Src: ARRISGro_dc:94:df (c0:c5:22:dc:94:df), Dst: IntelCor_6c:36:0d (2c:db:07:6c:36:0d)
v Internet Protocol Version 4, Src: 172.217.13.142, Dst: 192.168.0.17
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x0000 (0)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 118
    Protocol: ICMP (1)
    Header Checksum: 0xc9a0 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.217.13.142
    Destination Address: 192.168.0.17
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x52da [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 641 (0x0281)
    Sequence Number (LE): 33026 (0x8102)
    [Request frame: 19]
    [Response time: 38.756 ms]
  > Data (32 bytes)
```

Part 2:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

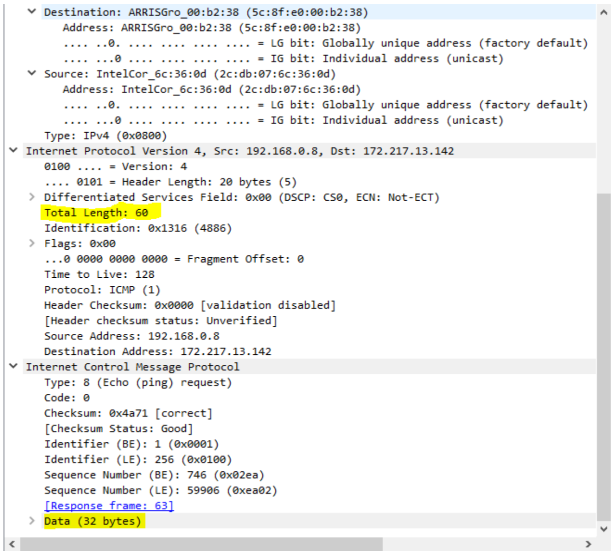
```
No.   Time       Source         Destination     Protocol Length Identification  Info
   31 6.703975   192.168.0.17   172.217.13.142  ICMP         35 0x764d (30285) Echo (ping) request  id=0x0001, seq=656/36866, ttl=128 (no response found!)
   50 11.487251  192.168.0.17   172.217.13.142  ICMP         35 0x764e (30286) Echo (ping) request  id=0x0001, seq=657/37122, ttl=128 (no response found!)
   62 16.498396  192.168.0.17   172.217.13.142  ICMP         35 0x764f (30287) Echo (ping) request  id=0x0001, seq=658/37378, ttl=128 (no response found!)
   76 21.489369  192.168.0.17   172.217.13.142  ICMP         35 0x7650 (30288) Echo (ping) request  id=0x0001, seq=659/37634, ttl=128 (no response found!)
```

```
    Source Address: 192.168.0.17
    Destination Address: 172.217.13.142
  > [2 IPv4 Fragments (1481 bytes): #30(1480), #31(1)]
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xdcb6 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 656 (0x0290)
    Sequence Number (LE): 36866 (0x9002)
  > [No response seen]
  > Data (1473 bytes)
```

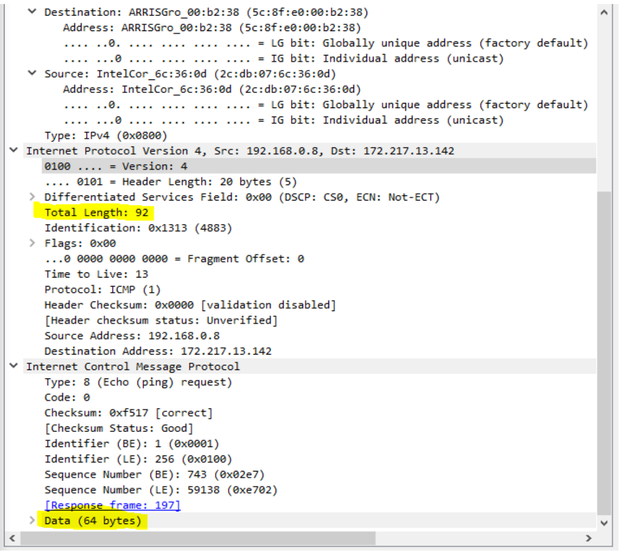
1. I was sending ping to google and its maximum packet size is 1472 bytes.
2. As we don't have any reply packets it seems packet is being dropped at the very beginning.
3. Web servers prevent large pings to avoid issues like ping of death. It has to do with DoS attack where an attacker can deliberately send IP packet with larger then 65536. Other reason is to avoid PING FLOOD problem, it is a simple denial-of-service attack where attacker overwhelms the server with ICMP request ping packets which will consume large amount of CPU for this operation and leads to server slowdown.

Part 3:

1. The only difference I see in their request message is data size



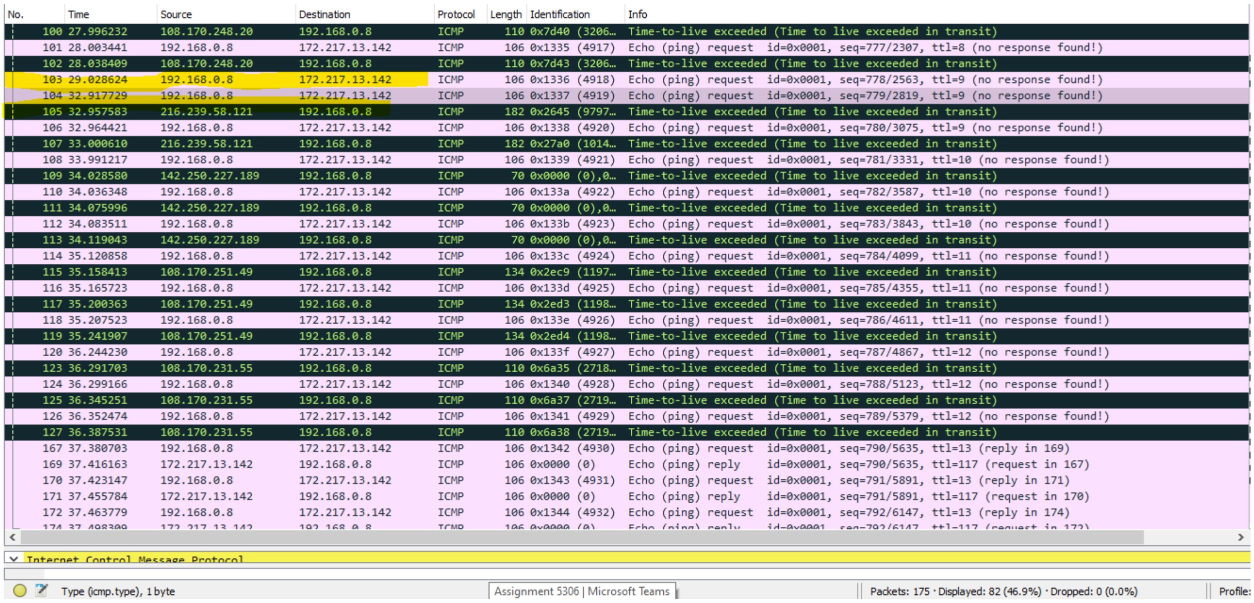
```
  v Destination: ARRISGro_00:b2:38 (5c:8f:e0:00:b2:38)
      Address: ARRISGro_00:b2:38 (5c:8f:e0:00:b2:38)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: IntelCor_6c:36:0d (2c:db:07:6c:36:0d)
      Address: IntelCor_6c:36:0d (2c:db:07:6c:36:0d)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.0.8, Dst: 172.217.13.142
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x1316 (4886)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.8
    Destination Address: 172.217.13.142
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4a71 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 746 (0x02ea)
    Sequence Number (LE): 59906 (0xea02)
    [Response frame: 63]
  > Data (32 bytes)
```



```
  v Destination: ARRISGro_00:b2:38 (5c:8f:e0:00:b2:38)
      Address: ARRISGro_00:b2:38 (5c:8f:e0:00:b2:38)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: IntelCor_6c:36:0d (2c:db:07:6c:36:0d)
      Address: IntelCor_6c:36:0d (2c:db:07:6c:36:0d)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.0.8, Dst: 172.217.13.142
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x1313 (4883)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 13
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.8
    Destination Address: 172.217.13.142
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf517 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 743 (0x02e7)
    Sequence Number (LE): 59138 (0xe702)
    [Response frame: 197]
  > Data (64 bytes)
```

Difference is same for reply packet too. Few other differences that can be observed in reply packet is response time for ping is greater and as tracert has multiple types of reply packet, few of them have ICMP reply time as 11.

2.



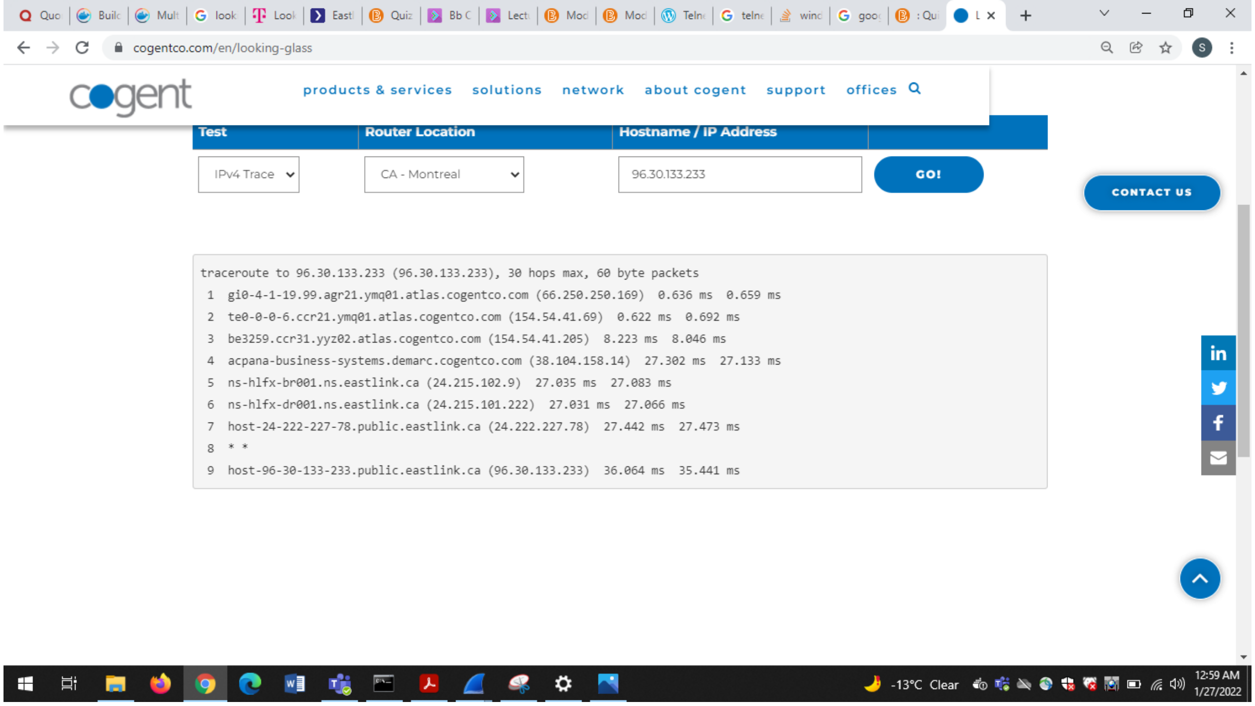
```
No.    Time       Source           Destination      Protocol  Length Identification  Info
   100 27.996232  108.170.248.20   192.168.0.8      ICMP       110 0x7d40 (3206…  Time-to-live exceeded (Time to live exceeded in transit)
   101 28.003441  192.168.0.8      172.217.13.142   ICMP       106 0x1335 (4917)  Echo (ping) request  id=0x0001, seq=777/2307, ttl=8 (no response found!)
   102 28.038409  108.170.248.20   192.168.0.8      ICMP       110 0x7d43 (3206…  Time-to-live exceeded (Time to live exceeded in transit)
   103 29.028624  192.168.0.8      172.217.13.142   ICMP       106 0x1336 (4918)  Echo (ping) request  id=0x0001, seq=778/2563, ttl=9 (no response found!)
   104 32.917729  192.168.0.8      172.217.13.142   ICMP       106 0x1337 (4919)  Echo (ping) request  id=0x0001, seq=779/2819, ttl=9 (no response found!)
   105 32.957583  216.239.58.121   192.168.0.8      ICMP       182 0x2645 (9797…  Time-to-live exceeded (Time to live exceeded in transit)
   106 32.964421  192.168.0.8      172.217.13.142   ICMP       106 0x1338 (4920)  Echo (ping) request  id=0x0001, seq=780/3075, ttl=9 (no response found!)
   107 33.000610  216.239.58.121   192.168.0.8      ICMP       182 0x27a0 (1014…  Time-to-live exceeded (Time to live exceeded in transit)
   108 33.991217  192.168.0.8      172.217.13.142   ICMP       106 0x1339 (4921)  Echo (ping) request  id=0x0001, seq=781/3331, ttl=10 (no response found!)
   109 34.028580  142.250.227.189  192.168.0.8      ICMP        70 0x0000 (0),0…  Time-to-live exceeded (Time to live exceeded in transit)
   110 34.036348  192.168.0.8      172.217.13.142   ICMP       106 0x133a (4922)  Echo (ping) request  id=0x0001, seq=782/3587, ttl=10 (no response found!)
   111 34.075996  142.250.227.189  192.168.0.8      ICMP        70 0x0000 (0),0…  Time-to-live exceeded (Time to live exceeded in transit)
   112 34.083511  192.168.0.8      172.217.13.142   ICMP       106 0x133b (4923)  Echo (ping) request  id=0x0001, seq=783/3843, ttl=10 (no response found!)
   113 34.119043  142.250.227.189  192.168.0.8      ICMP        70 0x0000 (0),0…  Time-to-live exceeded (Time to live exceeded in transit)
   114 35.120858  192.168.0.8      172.217.13.142   ICMP       106 0x133c (4924)  Echo (ping) request  id=0x0001, seq=784/4099, ttl=11 (no response found!)
   115 35.158413  108.170.251.49   192.168.0.8      ICMP       134 0x2ec9 (1197…  Time-to-live exceeded (Time to live exceeded in transit)
   116 35.165723  192.168.0.8      172.217.13.142   ICMP       106 0x133d (4925)  Echo (ping) request  id=0x0001, seq=785/4355, ttl=11 (no response found!)
   117 35.200363  108.170.251.49   192.168.0.8      ICMP       134 0x2ed3 (1198…  Time-to-live exceeded (Time to live exceeded in transit)
   118 35.207523  192.168.0.8      172.217.13.142   ICMP       106 0x133e (4926)  Echo (ping) request  id=0x0001, seq=786/4611, ttl=11 (no response found!)
   119 35.241907  108.170.251.49   192.168.0.8      ICMP       134 0x2ed4 (1198…  Time-to-live exceeded (Time to live exceeded in transit)
   120 36.244230  192.168.0.8      172.217.13.142   ICMP       106 0x133f (4927)  Echo (ping) request  id=0x0001, seq=787/4867, ttl=12 (no response found!)
   123 36.291703  108.170.231.55   192.168.0.8      ICMP       110 0x6a35 (2718…  Time-to-live exceeded (Time to live exceeded in transit)
   124 36.299166  192.168.0.8      172.217.13.142   ICMP       106 0x1340 (4928)  Echo (ping) request  id=0x0001, seq=788/5123, ttl=12 (no response found!)
   125 36.345251  108.170.231.55   192.168.0.8      ICMP       110 0x6a37 (2719…  Time-to-live exceeded (Time to live exceeded in transit)
   126 36.352474  192.168.0.8      172.217.13.142   ICMP       106 0x1341 (4929)  Echo (ping) request  id=0x0001, seq=789/5379, ttl=12 (no response found!)
   127 36.387531  108.170.231.55   192.168.0.8      ICMP       110 0x6a38 (2719…  Time-to-live exceeded (Time to live exceeded in transit)
   167 37.380703  192.168.0.8      172.217.13.142   ICMP       106 0x1342 (4930)  Echo (ping) request  id=0x0001, seq=790/5635, ttl=13 (reply in 169)
   169 37.416163  172.217.13.142   192.168.0.8      ICMP       106 0x0000 (0)     Echo (ping) reply    id=0x0001, seq=790/5635, ttl=117 (request in 167)
   170 37.423147  192.168.0.8      172.217.13.142   ICMP       106 0x1343 (4931)  Echo (ping) request  id=0x0001, seq=791/5891, ttl=13 (reply in 171)
   171 37.455784  172.217.13.142   192.168.0.8      ICMP       106 0x0000 (0)     Echo (ping) reply    id=0x0001, seq=791/5891, ttl=117 (request in 170)
   172 37.463779  192.168.0.8      172.217.13.142   ICMP       106 0x1344 (4932)  Echo (ping) request  id=0x0001, seq=792/6147, ttl=13 (reply in 174)
   174 37.498309  172.217.13.142   192.168.0.8      ICMP       106 0x0000 (0)     Echo (ping) reply    id=0x0001, seq=792/6147, ttl=117 (request in 172)

∨ Internet Control Message Protocol

Type (icmp.type), 1 byte    Assignment 5306 | Microsoft Teams    Packets: 175 · Displayed: 82 (46.9%) · Dropped: 0 (0.0%)    Profile:
```

There are few error responses in tracert command, the one highlighted yield to * error in traceroute but has no error packer. And those in the black color are time-to-live exceeded error packets which has ICMP message type 11.

3. -T: option in linux is used for making use of TCP SYNC for the requests. I cannot find an alternative for this command in windows so I was unable to execute it.
   -d: option in unix version is used to enable debugging. But where as in windows it is used for not resolving address to hostname. There is no alternative in windows to -d, so I am unable to execute this command.
4. -S srcaddr option in linux enable use of IPv6 only source address, it makes use of ipv6 address given in command as source address. This option has few security issues as it results in address spoofing

Part 4:

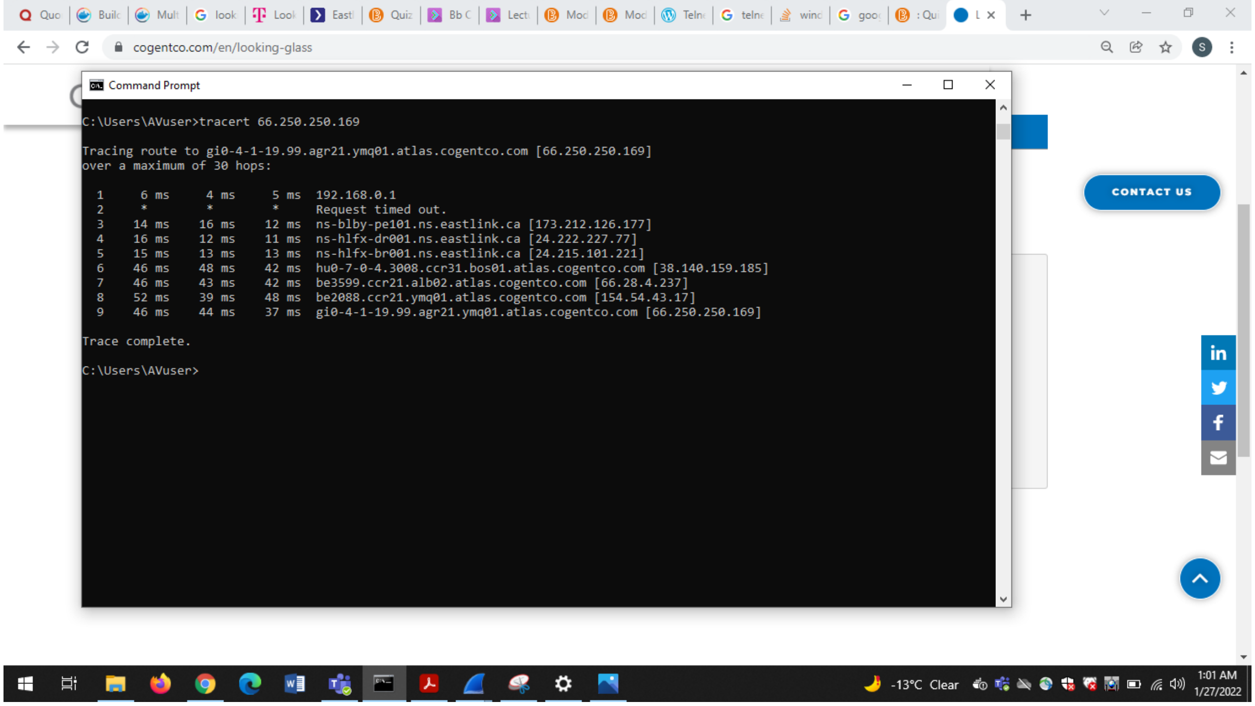
1. Cogentco server for north America.
   Forward path:



Test: IPv4 Trace
Router Location: CA - Montreal
Hostname / IP Address: 96.30.133.233

```
traceroute to 96.30.133.233 (96.30.133.233), 30 hops max, 60 byte packets
 1  gi0-4-1-19.99.agr21.ymq01.atlas.cogentco.com (66.250.250.169)  0.636 ms  0.659 ms
 2  te0-0-0-6.ccr21.ymq01.atlas.cogentco.com (154.54.41.69)  0.622 ms  0.692 ms
 3  be3259.ccr31.yyz02.atlas.cogentco.com (154.54.41.205)  8.223 ms  8.046 ms
 4  acpana-business-systems.demarc.cogentco.com (38.104.158.14)  27.302 ms  27.133 ms
 5  ns-hlfx-br001.ns.eastlink.ca (24.215.102.9)  27.035 ms  27.083 ms
 6  ns-hlfx-dr001.ns.eastlink.ca (24.215.101.222)  27.031 ms  27.066 ms
 7  host-24-222-227-78.public.eastlink.ca (24.222.227.78)  27.442 ms  27.473 ms
 8  * *
 9  host-96-30-133-233.public.eastlink.ca (96.30.133.233)  36.064 ms  35.441 ms
```

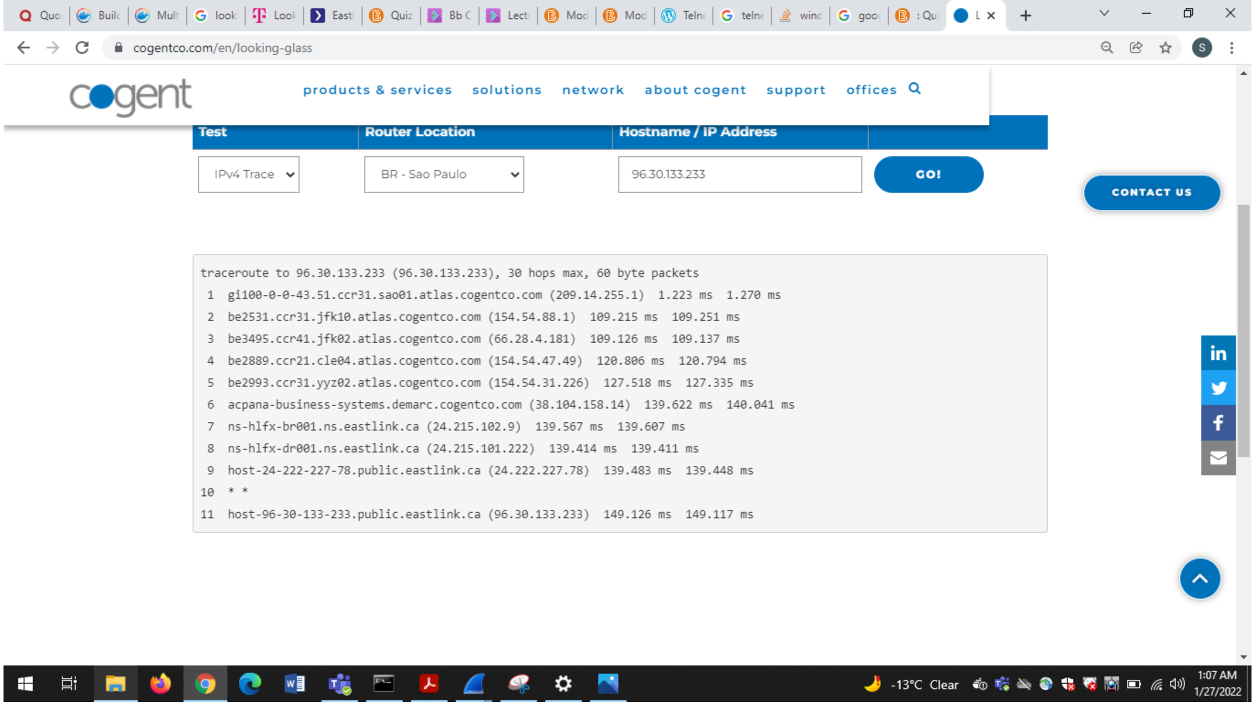
Reverse path:



```
C:\Users\AVuser>tracert 66.250.250.169

Tracing route to gi0-4-1-19.99.agr21.ymq01.atlas.cogentco.com [66.250.250.169]
over a maximum of 30 hops:

  1     6 ms     4 ms     5 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3    14 ms    16 ms    12 ms  ns-blby-pe101.ns.eastlink.ca [173.212.126.177]
  4    16 ms    12 ms    11 ms  ns-hlfx-dr001.ns.eastlink.ca [24.222.227.77]
  5    15 ms    13 ms    13 ms  ns-hlfx-br001.ns.eastlink.ca [24.215.101.221]
  6    46 ms    48 ms    42 ms  hu0-7-0-4.3008.ccr31.bos01.atlas.cogentco.com [38.140.159.185]
  7    46 ms    43 ms    42 ms  be3599.ccr21.alb02.atlas.cogentco.com [66.28.4.237]
  8    52 ms    39 ms    48 ms  be2088.ccr21.ymq01.atlas.cogentco.com [154.54.43.17]
  9    46 ms    44 ms    37 ms  gi0-4-1-19.99.agr21.ymq01.atlas.cogentco.com [66.250.250.169]

Trace complete.

C:\Users\AVuser>
```

2. Cogentco server for South America

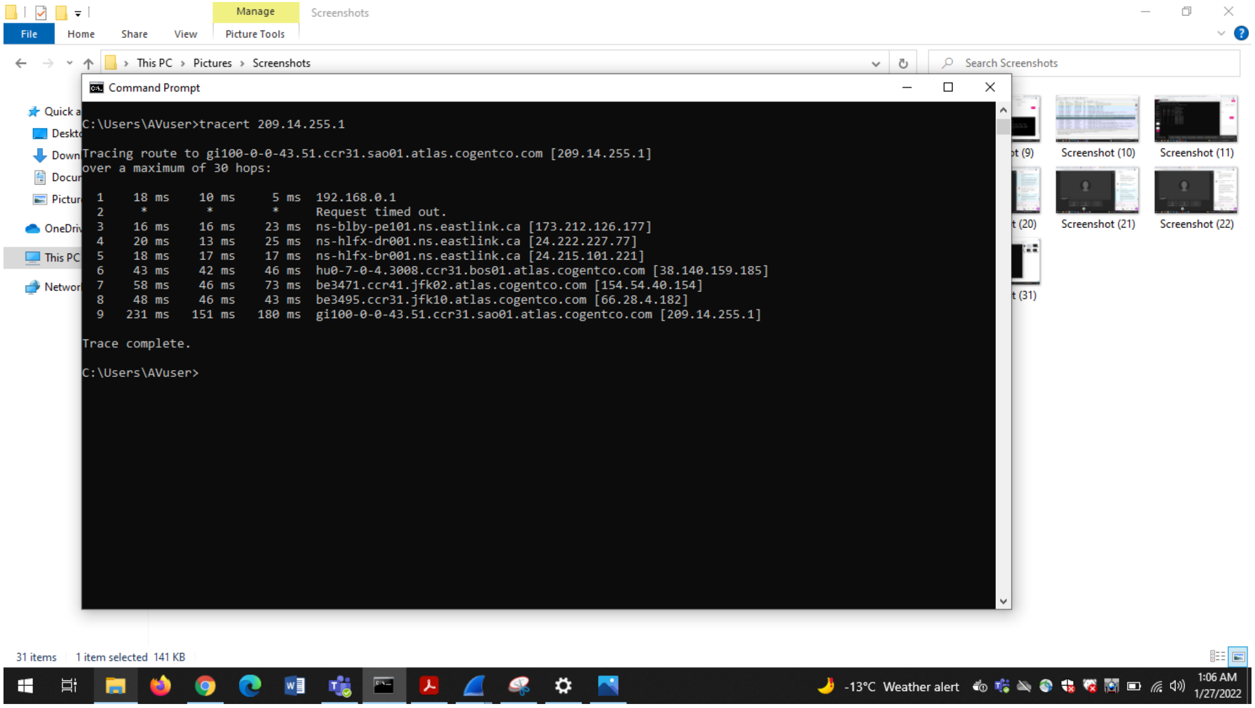
Forward path:



Test: IPv4 Trace
Router Location: BR - Sao Paulo
Hostname / IP Address: 96.30.133.233

```
traceroute to 96.30.133.233 (96.30.133.233), 30 hops max, 60 byte packets
 1  gi100-0-0-43.51.ccr31.sao01.atlas.cogentco.com (209.14.255.1)  1.223 ms  1.270 ms
 2  be2531.ccr31.jfk10.atlas.cogentco.com (154.54.88.1)  109.215 ms  109.251 ms
 3  be3495.ccr41.jfk02.atlas.cogentco.com (66.28.4.181)  109.126 ms  109.137 ms
 4  be2889.ccr21.cle04.atlas.cogentco.com (154.54.47.49)  120.806 ms  120.794 ms
 5  be2993.ccr31.yyz02.atlas.cogentco.com (154.54.31.226)  127.518 ms  127.335 ms
 6  acpana-business-systems.demarc.cogentco.com (38.104.158.14)  139.622 ms  140.041 ms
 7  ns-hlfx-br001.ns.eastlink.ca (24.215.102.9)  139.567 ms  139.607 ms
 8  ns-hlfx-dr001.ns.eastlink.ca (24.215.101.222)  139.414 ms  139.411 ms
 9  host-24-222-227-78.public.eastlink.ca (24.222.227.78)  139.483 ms  139.448 ms
10  * *
11  host-96-30-133-233.public.eastlink.ca (96.30.133.233)  149.126 ms  149.117 ms
```

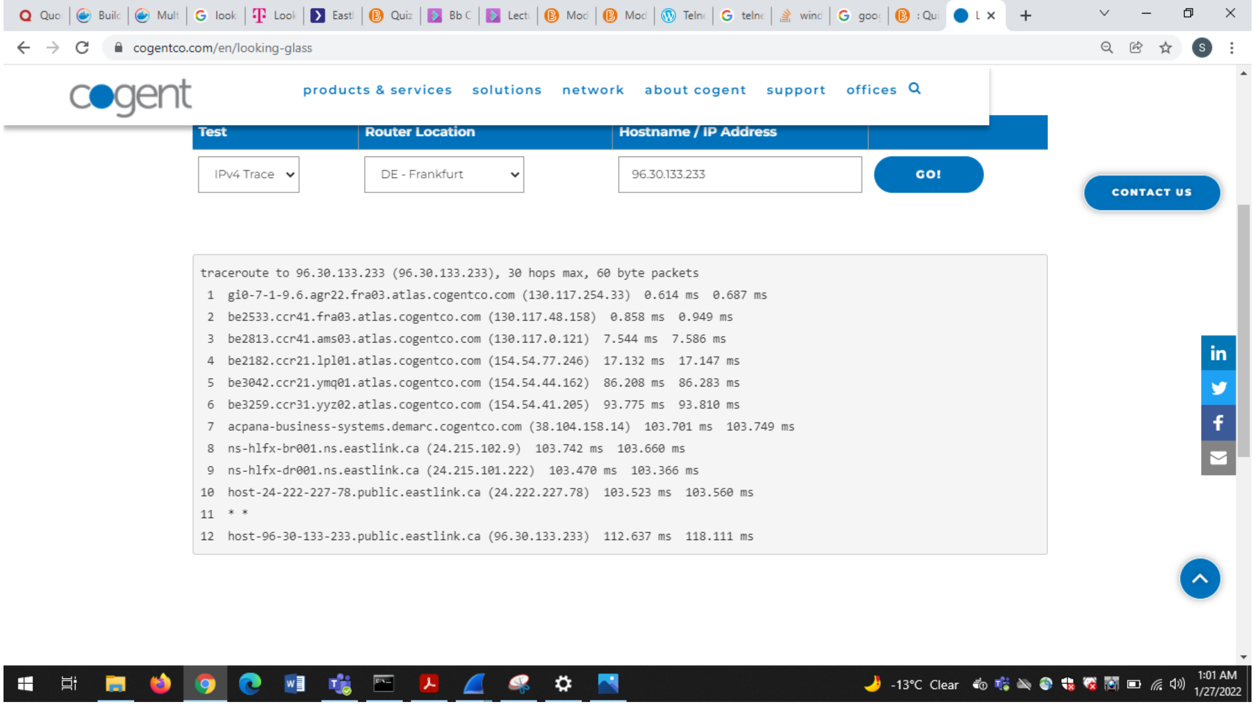
Reverse path:



```
C:\Users\AVuser>tracert 209.14.255.1

Tracing route to gi100-0-0-43.51.ccr31.sao01.atlas.cogentco.com [209.14.255.1]
over a maximum of 30 hops:

  1    18 ms    10 ms     5 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3    16 ms    16 ms    23 ms  ns-blby-pe101.ns.eastlink.ca [173.212.126.177]
  4    20 ms    13 ms    25 ms  ns-hlfx-dr001.ns.eastlink.ca [24.222.227.77]
  5    18 ms    17 ms    17 ms  ns-hlfx-br001.ns.eastlink.ca [24.215.101.221]
  6    43 ms    42 ms    46 ms  hu0-7-0-4.3008.ccr31.bos01.atlas.cogentco.com [38.140.159.185]
  7    58 ms    46 ms    73 ms  be3471.ccr41.jfk02.atlas.cogentco.com [154.54.40.154]
  8    48 ms    46 ms    43 ms  be3495.ccr31.jfk10.atlas.cogentco.com [66.28.4.182]
  9   231 ms   151 ms   180 ms  gi100-0-0-43.51.ccr31.sao01.atlas.cogentco.com [209.14.255.1]

Trace complete.

C:\Users\AVuser>
```

3. Cogentco server for Europe

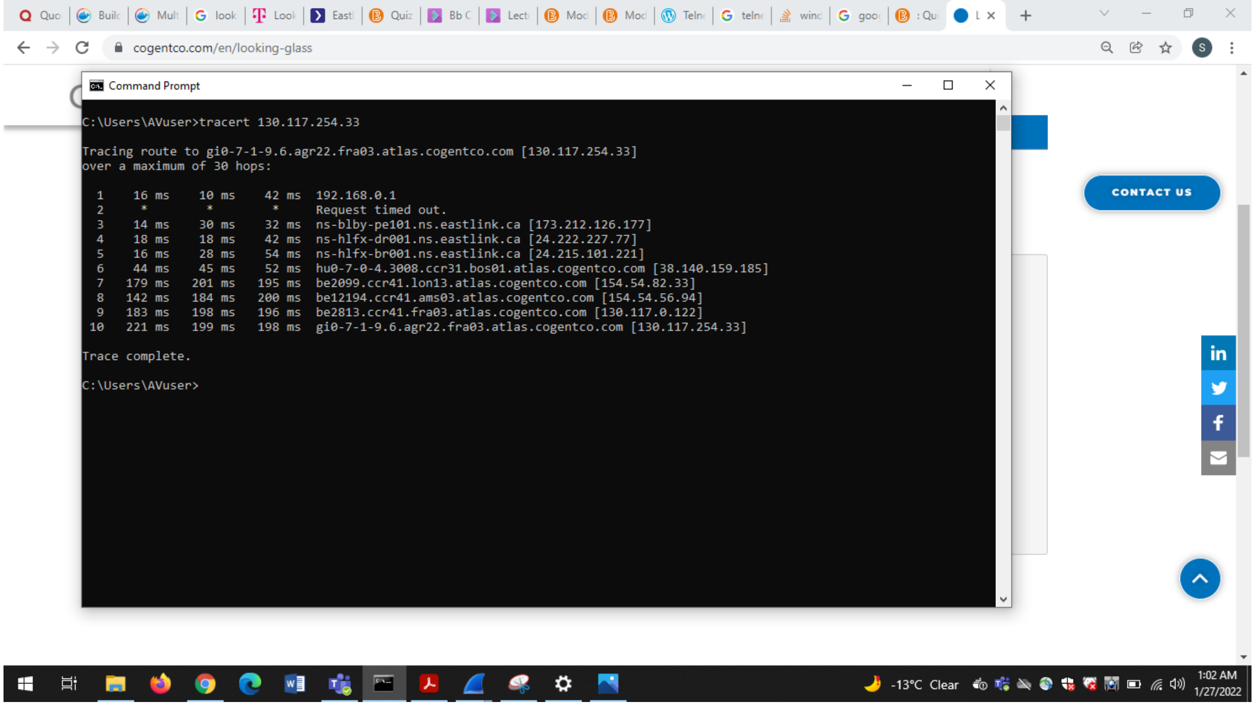
Forward path:



Test	Router Location	Hostname / IP Address	
IPv4 Trace	DE - Frankfurt	96.30.133.233	GO!

```
traceroute to 96.30.133.233 (96.30.133.233), 30 hops max, 60 byte packets
 1  gi0-7-1-9.6.agr22.fra03.atlas.cogentco.com (130.117.254.33)  0.614 ms  0.687 ms
 2  be2533.ccr41.fra03.atlas.cogentco.com (130.117.48.158)  0.858 ms  0.949 ms
 3  be2813.ccr41.ams03.atlas.cogentco.com (130.117.0.121)  7.544 ms  7.586 ms
 4  be2182.ccr21.lpl01.atlas.cogentco.com (154.54.77.246)  17.132 ms  17.147 ms
 5  be3042.ccr21.ymq01.atlas.cogentco.com (154.54.44.162)  86.208 ms  86.283 ms
 6  be3259.ccr31.yyz02.atlas.cogentco.com (154.54.41.205)  93.775 ms  93.810 ms
 7  acpana-business-systems.demarc.cogentco.com (38.104.158.14)  103.701 ms  103.749 ms
 8  ns-hlfx-br001.ns.eastlink.ca (24.215.102.9)  103.742 ms  103.660 ms
 9  ns-hlfx-dr001.ns.eastlink.ca (24.215.101.222)  103.470 ms  103.366 ms
10  host-24-222-227-78.public.eastlink.ca (24.222.227.78)  103.523 ms  103.560 ms
11  * *
12  host-96-30-133-233.public.eastlink.ca (96.30.133.233)  112.637 ms  118.111 ms
```

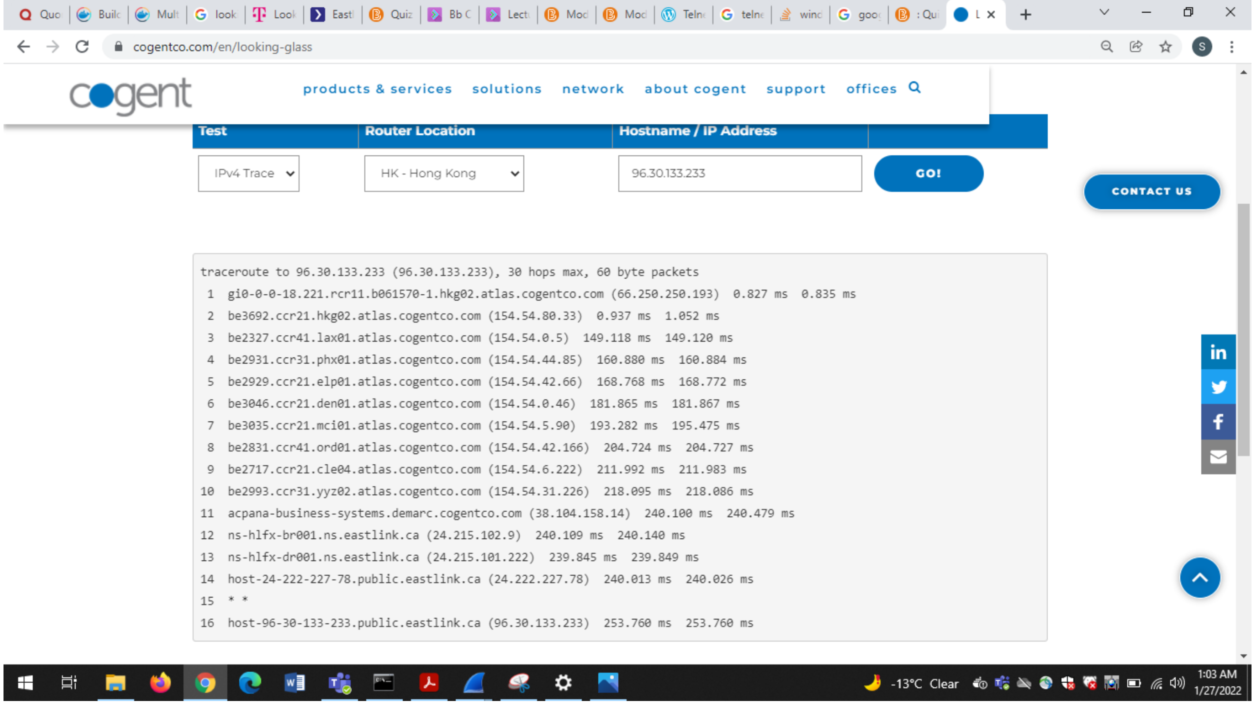
Reverse path:



```
C:\Users\AVuser>tracert 130.117.254.33

Tracing route to gi0-7-1-9.6.agr22.fra03.atlas.cogentco.com [130.117.254.33]
over a maximum of 30 hops:

  1    16 ms    10 ms    42 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3    14 ms    30 ms    32 ms  ns-blby-pe101.ns.eastlink.ca [173.212.126.177]
  4    18 ms    18 ms    42 ms  ns-hlfx-dr001.ns.eastlink.ca [24.222.227.77]
  5    16 ms    28 ms    54 ms  ns-hlfx-br001.ns.eastlink.ca [24.215.101.221]
  6    44 ms    45 ms    52 ms  hu0-7-0-4.3008.ccr31.bos01.atlas.cogentco.com [38.140.159.185]
  7   179 ms   201 ms   195 ms  be2099.ccr41.lon13.atlas.cogentco.com [154.54.82.33]
  8   142 ms   184 ms   200 ms  be12194.ccr41.ams03.atlas.cogentco.com [154.54.56.94]
  9   183 ms   198 ms   196 ms  be2813.ccr41.fra03.atlas.cogentco.com [130.117.0.122]
 10   221 ms   199 ms   198 ms  gi0-7-1-9.6.agr22.fra03.atlas.cogentco.com [130.117.254.33]

Trace complete.

C:\Users\AVuser>
```

4. Cogentco server for Asia

Forward path:

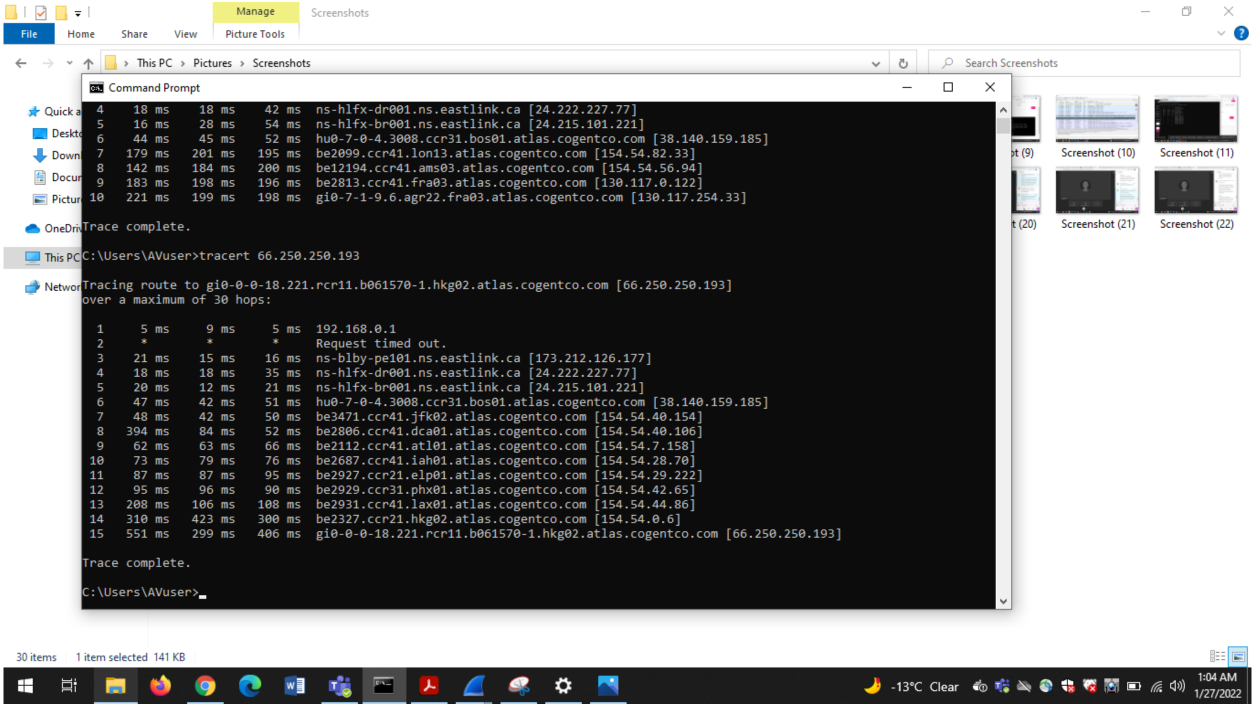


cogentco.com/en/looking-glass

Test	Router Location	Hostname / IP Address
IPv4 Trace	HK - Hong Kong	96.30.133.233

```
traceroute to 96.30.133.233 (96.30.133.233), 30 hops max, 60 byte packets
 1  gi0-0-0-18.221.rcr11.b061570-1.hkg02.atlas.cogentco.com (66.250.250.193)  0.827 ms  0.835 ms
 2  be3692.ccr21.hkg02.atlas.cogentco.com (154.54.80.33)  0.937 ms  1.052 ms
 3  be2327.ccr41.lax01.atlas.cogentco.com (154.54.0.5)  149.118 ms  149.120 ms
 4  be2931.ccr31.phx01.atlas.cogentco.com (154.54.44.85)  160.880 ms  160.884 ms
 5  be2929.ccr21.elp01.atlas.cogentco.com (154.54.42.66)  168.768 ms  168.772 ms
 6  be3046.ccr21.den01.atlas.cogentco.com (154.54.0.46)  181.865 ms  181.867 ms
 7  be3035.ccr21.mci01.atlas.cogentco.com (154.54.5.90)  193.282 ms  195.475 ms
 8  be2831.ccr41.ord01.atlas.cogentco.com (154.54.42.166)  204.724 ms  204.727 ms
 9  be2717.ccr21.cle04.atlas.cogentco.com (154.54.6.222)  211.992 ms  211.983 ms
10  be2993.ccr31.yyz02.atlas.cogentco.com (154.54.31.226)  218.095 ms  218.086 ms
11  acpana-business-systems.demarc.cogentco.com (38.104.158.14)  240.100 ms  240.479 ms
12  ns-hlfx-br001.ns.eastlink.ca (24.215.102.9)  240.109 ms  240.140 ms
13  ns-hlfx-dr001.ns.eastlink.ca (24.215.101.222)  239.845 ms  239.849 ms
14  host-24-222-227-78.public.eastlink.ca (24.222.227.78)  240.013 ms  240.026 ms
15  * *
16  host-96-30-133-233.public.eastlink.ca (96.30.133.233)  253.760 ms  253.760 ms
```

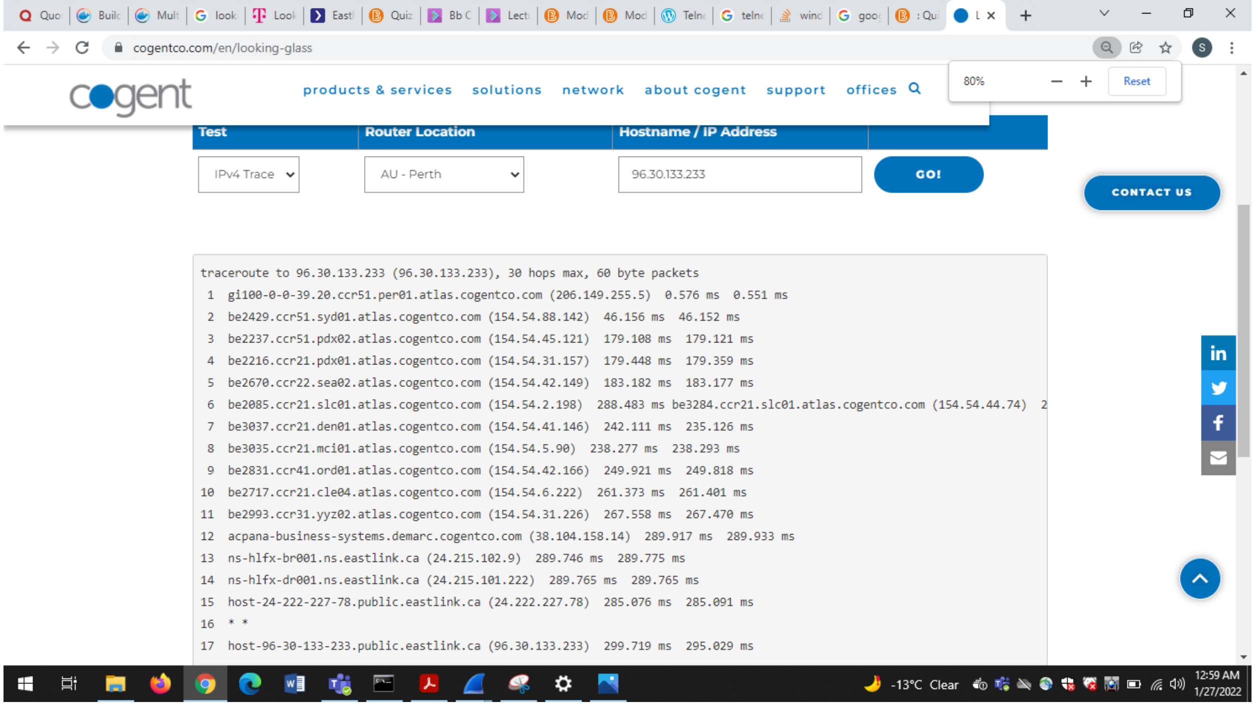
Reverse path:



```
  4    18 ms    18 ms    42 ms  ns-hlfx-dr001.ns.eastlink.ca [24.222.227.77]
  5    16 ms    28 ms    54 ms  ns-hlfx-br001.ns.eastlink.ca [24.215.101.221]
  6    44 ms    45 ms    52 ms  hu0-7-0-4.3008.ccr31.bos01.atlas.cogentco.com [38.140.159.185]
  7   179 ms   201 ms   195 ms  be2099.ccr41.lon13.atlas.cogentco.com [154.54.82.33]
  8   142 ms   184 ms   200 ms  be12194.ccr41.ams03.atlas.cogentco.com [154.54.56.94]
  9   183 ms   198 ms   196 ms  be2813.ccr41.fra03.atlas.cogentco.com [130.117.0.122]
 10   221 ms   199 ms   198 ms  gi0-7-1-9.6.agr22.fra03.atlas.cogentco.com [130.117.254.33]

Trace complete.

C:\Users\AVuser>tracert 66.250.250.193

Tracing route to gi0-0-0-18.221.rcr11.b061570-1.hkg02.atlas.cogentco.com [66.250.250.193]
over a maximum of 30 hops:

  1     5 ms     9 ms     5 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3    21 ms    15 ms    16 ms  ns-blby-pe101.ns.eastlink.ca [173.212.126.177]
  4    18 ms    18 ms    35 ms  ns-hlfx-dr001.ns.eastlink.ca [24.222.227.77]
  5    20 ms    12 ms    21 ms  ns-hlfx-br001.ns.eastlink.ca [24.215.101.221]
  6    47 ms    42 ms    51 ms  hu0-7-0-4.3008.ccr31.bos01.atlas.cogentco.com [38.140.159.185]
  7    48 ms    42 ms    50 ms  be3471.ccr41.jfk02.atlas.cogentco.com [154.54.40.154]
  8   394 ms    84 ms    52 ms  be2806.ccr41.dca01.atlas.cogentco.com [154.54.40.106]
  9    62 ms    63 ms    66 ms  be2112.ccr41.atl01.atlas.cogentco.com [154.54.7.158]
 10    73 ms    79 ms    76 ms  be2687.ccr41.iah01.atlas.cogentco.com [154.54.28.70]
 11    87 ms    87 ms    95 ms  be2927.ccr21.elp01.atlas.cogentco.com [154.54.29.222]
 12    95 ms    96 ms    90 ms  be2929.ccr31.phx01.atlas.cogentco.com [154.54.42.65]
 13   208 ms   106 ms   108 ms  be2931.ccr41.lax01.atlas.cogentco.com [154.54.44.86]
 14   310 ms   423 ms   300 ms  be2327.ccr21.hkg02.atlas.cogentco.com [154.54.0.6]
 15   551 ms   299 ms   406 ms  gi0-0-0-18.221.rcr11.b061570-1.hkg02.atlas.cogentco.com [66.250.250.193]

Trace complete.

C:\Users\AVuser>_
```

5. Cogentco server for Australia

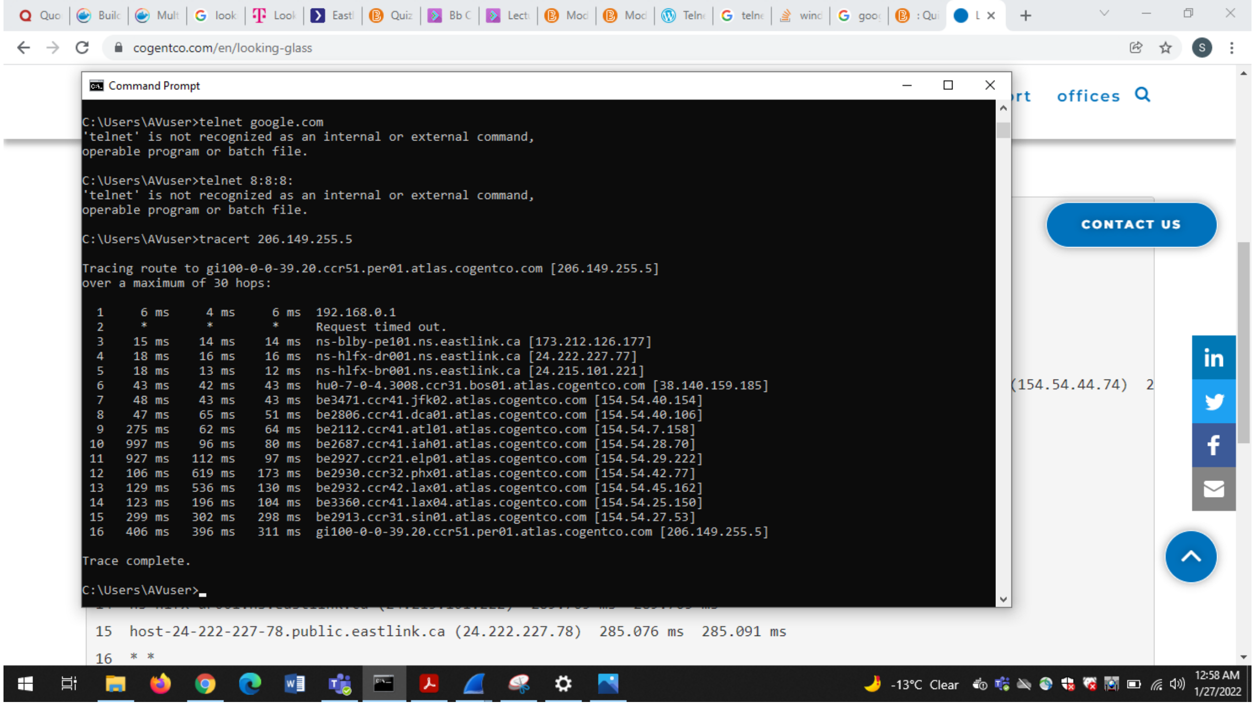
Forward path:



Test	Router Location	Hostname / IP Address
IPv4 Trace	AU - Perth	96.30.133.233

```
traceroute to 96.30.133.233 (96.30.133.233), 30 hops max, 60 byte packets
 1  gi100-0-0-39.20.ccr51.per01.atlas.cogentco.com (206.149.255.5)  0.576 ms  0.551 ms
 2  be2429.ccr51.syd01.atlas.cogentco.com (154.54.88.142)  46.156 ms  46.152 ms
 3  be2237.ccr51.pdx02.atlas.cogentco.com (154.54.45.121)  179.108 ms  179.121 ms
 4  be2216.ccr21.pdx01.atlas.cogentco.com (154.54.31.157)  179.448 ms  179.359 ms
 5  be2670.ccr22.sea02.atlas.cogentco.com (154.54.42.149)  183.182 ms  183.177 ms
 6  be2085.ccr21.slc01.atlas.cogentco.com (154.54.2.198)  288.483 ms be3284.ccr21.slc01.atlas.cogentco.com (154.54.44.74)  2
 7  be3037.ccr21.den01.atlas.cogentco.com (154.54.41.146)  242.111 ms  235.126 ms
 8  be3035.ccr21.mci01.atlas.cogentco.com (154.54.5.90)  238.277 ms  238.293 ms
 9  be2831.ccr41.ord01.atlas.cogentco.com (154.54.42.166)  249.921 ms  249.818 ms
10  be2717.ccr21.cle04.atlas.cogentco.com (154.54.6.222)  261.373 ms  261.401 ms
11  be2993.ccr31.yyz02.atlas.cogentco.com (154.54.31.226)  267.558 ms  267.470 ms
12  acpana-business-systems.demarc.cogentco.com (38.104.158.14)  289.917 ms  289.933 ms
13  ns-hlfx-br001.ns.eastlink.ca (24.215.102.9)  289.746 ms  289.775 ms
14  ns-hlfx-dr001.ns.eastlink.ca (24.215.101.222)  289.765 ms  289.765 ms
15  host-24-222-227-78.public.eastlink.ca (24.222.227.78)  285.076 ms  285.091 ms
16  * *
17  host-96-30-133-233.public.eastlink.ca (96.30.133.233)  299.719 ms  295.029 ms
```

Reverse path:



```
C:\Users\AVuser>telnet google.com
'telnet' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\AVuser>telnet 8:8:8:
'telnet' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\AVuser>tracert 206.149.255.5

Tracing route to gi100-0-0-39.20.ccr51.per01.atlas.cogentco.com [206.149.255.5]
over a maximum of 30 hops:

  1     6 ms     4 ms     6 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3    15 ms    14 ms    14 ms  ns-blby-pe101.ns.eastlink.ca [173.212.126.177]
  4    18 ms    16 ms    16 ms  ns-hlfx-dr001.ns.eastlink.ca [24.222.227.77]
  5    18 ms    13 ms    12 ms  ns-hlfx-br001.ns.eastlink.ca [24.215.101.221]
  6    43 ms    42 ms    43 ms  hu0-7-0-4.3008.ccr31.bos01.atlas.cogentco.com [38.140.159.185]
  7    48 ms    43 ms    43 ms  be3471.ccr41.jfk02.atlas.cogentco.com [154.54.40.154]
  8    47 ms    65 ms    51 ms  be2806.ccr41.dca01.atlas.cogentco.com [154.54.40.106]
  9   275 ms    62 ms    64 ms  be2112.ccr41.atl01.atlas.cogentco.com [154.54.7.158]
 10   997 ms    96 ms    80 ms  be2687.ccr41.iah01.atlas.cogentco.com [154.54.28.70]
 11   927 ms   112 ms    97 ms  be2927.ccr21.elp01.atlas.cogentco.com [154.54.29.222]
 12   106 ms   619 ms   173 ms  be2930.ccr32.phx01.atlas.cogentco.com [154.54.42.77]
 13   129 ms   536 ms   130 ms  be2932.ccr42.lax01.atlas.cogentco.com [154.54.45.162]
 14   123 ms   196 ms   104 ms  be3360.ccr41.lax04.atlas.cogentco.com [154.54.25.150]
 15   299 ms   302 ms   298 ms  be2913.ccr31.sin01.atlas.cogentco.com [154.54.27.53]
 16   406 ms   396 ms   311 ms  gi100-0-0-39.20.ccr51.per01.atlas.cogentco.com [206.149.255.5]

Trace complete.

C:\Users\AVuser>_
```

(154.54.44.74) 2
15 host-24-222-227-78.public.eastlink.ca (24.222.227.78) 285.076 ms 285.091 ms
16 * *

The major difference that I can see between reverse and forward path is turnaround time. And number of hops are different from reverse to forward, forward path has more .no of hops. When looked at wired shark we see icmp messages for reverse but not for forward because it may be handled by other protocols at the server end.

References:

[1]M. Pramatarov, "Traceroute command and its options - ClouDNS Blog", *ClouDNS Blog*, 2022. [Online]. Available: https://www.cloudns.net/blog/traceroute-command-tracert/. [Accessed: 28- Jan- 2022]

[2]"ShieldSquare Captcha", *Networklessons.com*, 2022. [Online]. Available: https://networklessons.com/cisco/ccie-routing-switching-written/icmp-internet-control-message-protocol#:~:text=ICMP%20(Internet%20Control%20Message%20Protocol)%20is%20a%20network%20protocol%20used,for%20diagnostics%20and%20network%20management.&text=For%20example%2C%20type%208%20is,of%20ICMP%20message%20it%20is. [Accessed: 28- Jan- 2022]

[3]W. numbers?, B. Wankhede, R. Trunk, W. Tigger and R. Maupin, "Why doesn’t ICMP use port numbers?", *Network Engineering Stack Exchange*, 2022. [Online]. Available: https://networkengineering.stackexchange.com/questions/50955/why-doesn-t-icmp-use-port-numbers. [Accessed: 28- Jan- 2022]

[4]"Internet Control Message Protocol (ICMP) Parameters", *Iana.org*, 2022. [Online]. Available: https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml#icmp-parameters-codes-0. [Accessed: 28- Jan- 2022]

[5]"ICMP (Internet Control Message Protocol)", *NetworkLessons.com*, 2022. [Online]. Available: https://networklessons.com/cisco/ccie-routing-switching-written/icmp-internet-control-message-protocol#:~:text=A%20good%20example%20is%20the,error%20message%20to%20the%20source.&text=When%20you%20see%20code%200,the%20destination%20host%20was%20unreachable. [Accessed: 28- Jan- 2022]

[6]W. &#39;ping&#39;?, V. M and A. Waters, "Why do companies block 'ping'?", *Super User*, 2022. [Online]. Available: https://superuser.com/questions/318870/why-do-companies-block-ping#:~:text=It%20has%20to%20do%20with,allowed%20by%20the%20IP%20protocol. [Accessed: 28- Jan- 2022]

[7]S. PING?, M. Jefferson and T. Pornin, "Security risk of PING?", *Information Security Stack Exchange*, 2022. [Online]. Available: https://security.stackexchange.com/questions/4440/security-risk-of-ping. [Accessed: 28- Jan- 2022]

[8]"Looking Glass", *Cogentco.com*, 2022. [Online]. Available: https://www.cogentco.com/en/looking-glass. [Accessed: 28- Jan- 2022]

[9]"What is a Denial-of-Service Attack?", *SearchSecurity*, 2022. [Online]. Available: https://searchsecurity.techtarget.com/definition/denial-of-service. [Accessed: 28- Jan- 2022]

[10]"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/. [Accessed: 28- Jan- 2022]