Name : Shriram Karpoora Sundara Pandian

Course : CSEC 600 Introduction to Cyber Security

Title : Packet Sniffing

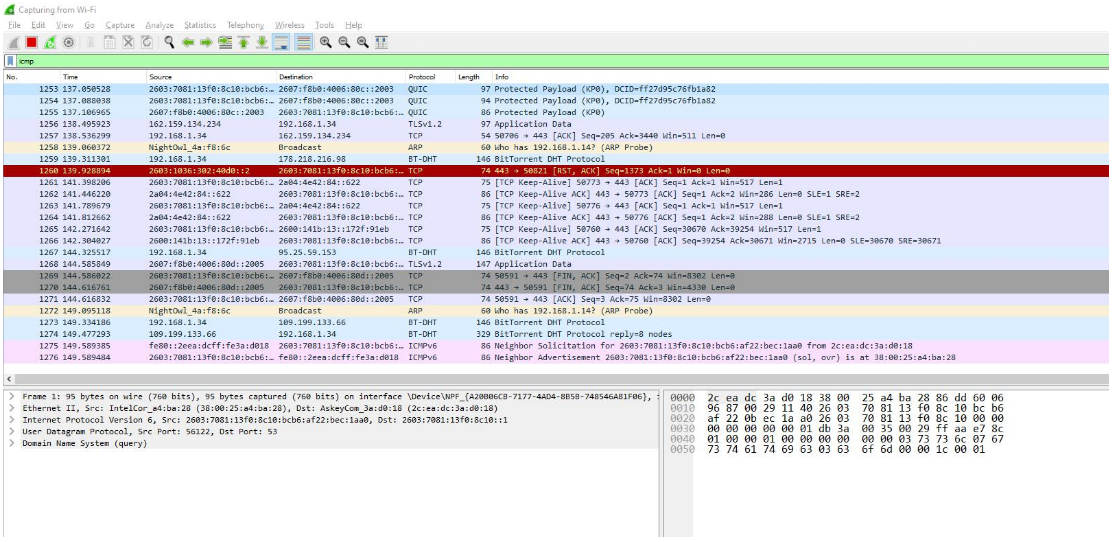
Lab : 6

Chapter : 7 (Routing)

Exercise 7. 01 :

Step 1 :

A.

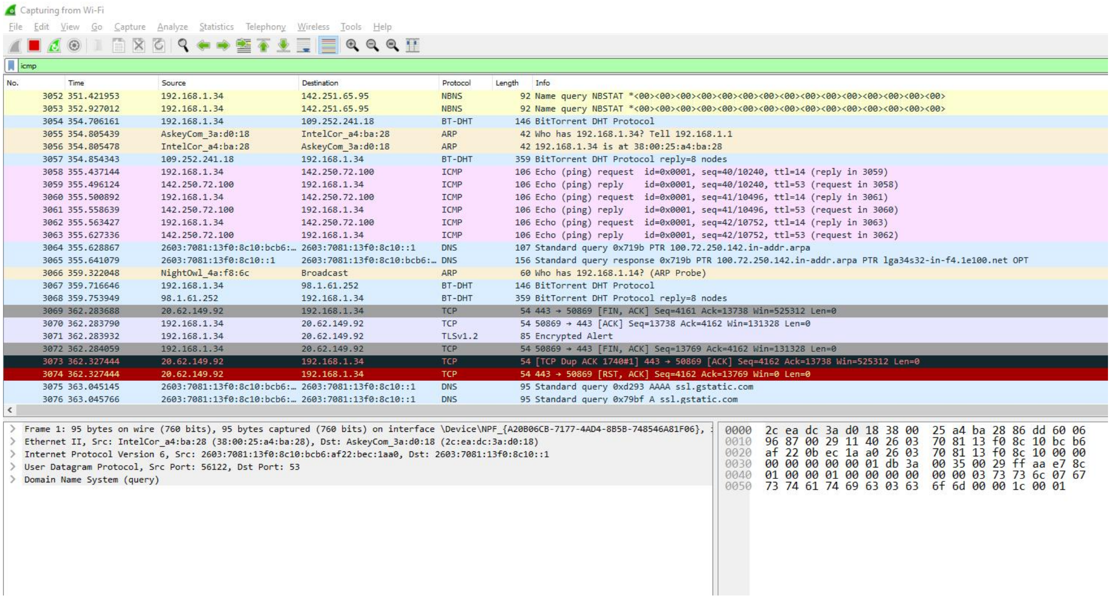

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

```
No.   Time        Source                       Destination                  Protocol Length Info
 1253 137.050528  2603:7081:13f0:8c10:bcb6:…   2607:f8b0:4006:80c::2003     QUIC       97 Protected Payload (KP0), DCID=ff27d95c76fb1a82
 1254 137.088038  2603:7081:13f0:8c10:bcb6:…   2607:f8b0:4006:80c::2003     QUIC       94 Protected Payload (KP0), DCID=ff27d95c76fb1a82
 1255 137.106965  2607:f8b0:4006:80c::2003     2603:7081:13f0:8c10:bcb6:…   QUIC       86 Protected Payload (KP0)
 1256 138.495923  162.159.134.234              192.168.1.34                 TLSv1.2    97 Application Data
 1257 138.536299  192.168.1.34                 162.159.134.234              TCP        54 50706 → 443 [ACK] Seq=205 Ack=3440 Win=511 Len=0
 1258 139.060372  NightOwl_4a:f8:6c            Broadcast                    ARP        60 Who has 192.168.1.14? (ARP Probe)
 1259 139.311301  192.168.1.34                 178.218.216.98               BT-DHT    146 BitTorrent DHT Protocol
 1260 139.928894  2603:1036:302:40d0::2        2603:7081:13f0:8c10:bcb6:…   TCP        74 443 → 50821 [RST, ACK] Seq=1373 Ack=1 Win=0 Len=0
 1261 141.398206  2603:7081:13f0:8c10:bcb6:…   2a04:4e42:84::622            TCP        75 [TCP Keep-Alive] 50773 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=1
 1262 141.446220  2a04:4e42:84::622            2603:7081:13f0:8c10:bcb6:…   TCP        86 [TCP Keep-Alive ACK] 443 → 50773 [ACK] Seq=1 Ack=2 Win=286 Len=0 SLE=1 SRE=2
 1263 141.789679  2603:7081:13f0:8c10:bcb6:…   2a04:4e42:84::622            TCP        75 [TCP Keep-Alive] 50776 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=1
 1264 141.812662  2a04:4e42:84::622            2603:7081:13f0:8c10:bcb6:…   TCP        86 [TCP Keep-Alive ACK] 443 → 50776 [ACK] Seq=1 Ack=2 Win=288 Len=0 SLE=1 SRE=2
 1265 142.271642  2603:7081:13f0:8c10:bcb6:…   2600:141b:13::172f:91eb      TCP        75 [TCP Keep-Alive] 50760 → 443 [ACK] Seq=30670 Ack=39254 Win=517 Len=1
 1266 142.304027  2600:141b:13::172f:91eb      2603:7081:13f0:8c10:bcb6:…   TCP        86 [TCP Keep-Alive ACK] 443 → 50760 [ACK] Seq=39254 Ack=30671 Win=2715 Len=0 SLE=30670 SRE=30671
 1267 144.325517  192.168.1.34                 95.25.59.153                 BT-DHT    146 BitTorrent DHT Protocol
 1268 144.585849  2607:f8b0:4006:80d::2005     2603:7081:13f0:8c10:bcb6:…   TLSv1.2   147 Application Data
 1269 144.586022  2603:7081:13f0:8c10:bcb6:…   2607:f8b0:4006:80d::2005     TCP        74 50591 → 443 [FIN, ACK] Seq=2 Ack=74 Win=8302 Len=0
 1270 144.616761  2607:f8b0:4006:80d::2005     2603:7081:13f0:8c10:bcb6:…   TCP        74 443 → 50591 [FIN, ACK] Seq=74 Ack=3 Win=4330 Len=0
 1271 144.616832  2603:7081:13f0:8c10:bcb6:…   2607:f8b0:4006:80d::2005     TCP        74 50591 → 443 [ACK] Seq=3 Ack=75 Win=8302 Len=0
 1272 149.095118  NightOwl_4a:f8:6c            Broadcast                    ARP        60 Who has 192.168.1.14? (ARP Probe)
 1273 149.334186  192.168.1.34                 109.199.133.66               BT-DHT    146 BitTorrent DHT Protocol
 1274 149.477293  109.199.133.66               192.168.1.34                 BT-DHT    329 BitTorrent DHT Protocol reply=8 nodes
 1275 149.589385  fe80::2eea:dcff:fe3a:d018    2603:7081:13f0:8c10:bcb6:…   ICMPv6     86 Neighbor Solicitation for 2603:7081:13f0:8c10:bcb6:af22:bec:1aa0 from 2c:ea:dc:3a:d0:18
 1276 149.589484  2603:7081:13f0:8c10:bcb6:…   fe80::2eea:dcff:fe3a:d018    ICMPv6     86 Neighbor Advertisement 2603:7081:13f0:8c10:bcb6:af22:bec:1aa0 (sol, ovr) is at 38:00:25:a4:ba:28
```

```
> Frame 1: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface \Device\NPF_{A20B06CB-7177-4AD4-8B5B-748546A81F06},
> Ethernet II, Src: IntelCor_a4:ba:28 (38:00:25:a4:ba:28), Dst: AskeyCom_3a:d0:18 (2c:ea:dc:3a:d0:18)
> Internet Protocol Version 6, Src: 2603:7081:13f0:8c10:bcb6:af22:bec:1aa0, Dst: 2603:7081:13f0:8c10::1
> User Datagram Protocol, Src Port: 56122, Dst Port: 53
> Domain Name System (query)
```

```
0000  2c ea dc 3a d0 18 38 00  25 a4 ba 28 86 dd 60 06
0010  96 87 00 29 11 40 26 03  70 81 13 f0 8c 10 bc b6
0020  af 22 0b ec 1a a0 26 03  70 81 13 f0 8c 10 00 00
0030  00 00 00 00 00 01 db 3a  00 35 00 29 ff aa e7 8c
0040  01 00 00 01 00 00 00 00  00 00 03 73 73 6c 07 67
0050  73 74 61 74 69 63 03 63  6f 6d 00 00 1c 00 01
```

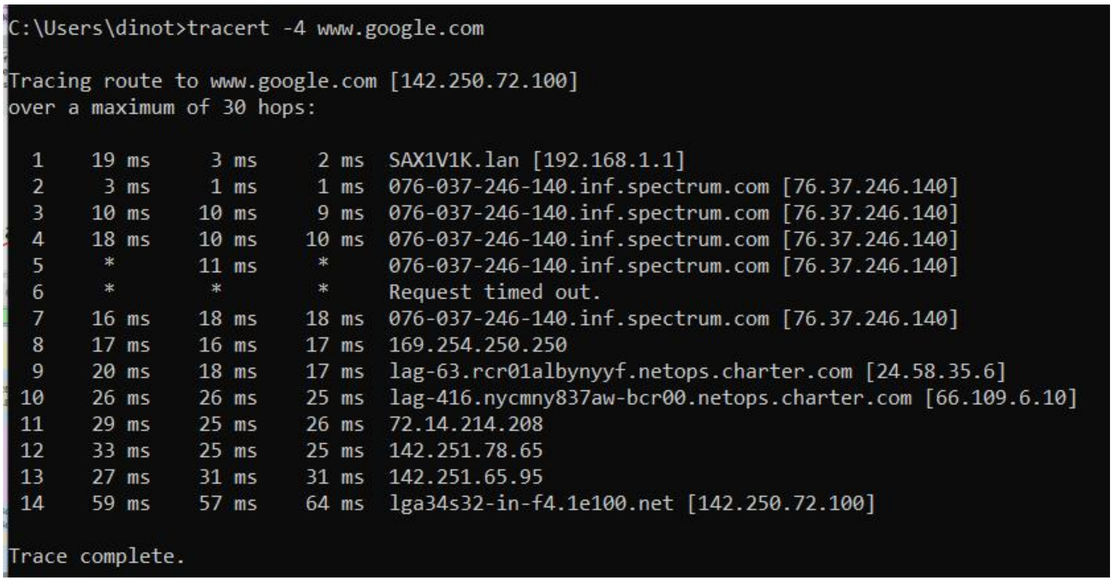
B. While running tracert the wireshark shows these responses :


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

```
No.   Time        Source                       Destination                  Protocol Length Info
 3052 351.421953  192.168.1.34                 142.251.65.95                NBNS       92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
 3053 352.927012  192.168.1.34                 142.251.65.95                NBNS       92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
 3054 354.706161  192.168.1.34                 109.252.241.18               BT-DHT    146 BitTorrent DHT Protocol
 3055 354.805439  AskeyCom_3a:d0:18            IntelCor_a4:ba:28            ARP        42 Who has 192.168.1.34? Tell 192.168.1.1
 3056 354.805478  IntelCor_a4:ba:28            AskeyCom_3a:d0:18            ARP        42 192.168.1.34 is at 38:00:25:a4:ba:28
 3057 354.854343  109.252.241.18               192.168.1.34                 BT-DHT    359 BitTorrent DHT Protocol reply=8 nodes
 3058 355.437144  192.168.1.34                 142.250.72.100               ICMP      106 Echo (ping) request  id=0x0001, seq=40/10240, ttl=14 (reply in 3059)
 3059 355.496124  142.250.72.100               192.168.1.34                 ICMP      106 Echo (ping) reply    id=0x0001, seq=40/10240, ttl=53 (request in 3058)
 3060 355.500892  192.168.1.34                 142.250.72.100               ICMP      106 Echo (ping) request  id=0x0001, seq=41/10496, ttl=14 (reply in 3061)
 3061 355.558639  142.250.72.100               192.168.1.34                 ICMP      106 Echo (ping) reply    id=0x0001, seq=41/10496, ttl=53 (request in 3060)
 3062 355.563427  192.168.1.34                 142.250.72.100               ICMP      106 Echo (ping) request  id=0x0001, seq=42/10752, ttl=14 (reply in 3063)
 3063 355.627336  142.250.72.100               192.168.1.34                 ICMP      106 Echo (ping) reply    id=0x0001, seq=42/10752, ttl=53 (request in 3062)
 3064 355.628867  2603:7081:13f0:8c10:bcb6:…   2603:7081:13f0:8c10::1       DNS       107 Standard query 0x719b PTR 100.72.250.142.in-addr.arpa
 3065 355.641079  2603:7081:13f0:8c10::1       2603:7081:13f0:8c10:bcb6:…   DNS       156 Standard query response 0x719b PTR 100.72.250.142.in-addr.arpa PTR lga34s32-in-f4.1e100.net OPT
 3066 359.322048  NightOwl_4a:f8:6c            Broadcast                    ARP        60 Who has 192.168.1.14? (ARP Probe)
 3067 359.716646  192.168.1.34                 98.1.61.252                  BT-DHT    146 BitTorrent DHT Protocol
 3068 359.753949  98.1.61.252                  192.168.1.34                 BT-DHT    359 BitTorrent DHT Protocol reply=8 nodes
 3069 362.283688  20.62.149.92                 192.168.1.34                 TCP        54 443 → 50869 [FIN, ACK] Seq=4161 Ack=13738 Win=525312 Len=0
 3070 362.283790  192.168.1.34                 20.62.149.92                 TCP        54 50869 → 443 [ACK] Seq=13738 Ack=4162 Win=131328 Len=0
 3071 362.283932  192.168.1.34                 20.62.149.92                 TLSv1.2    85 Encrypted Alert
 3072 362.284059  192.168.1.34                 20.62.149.92                 TCP        54 50869 → 443 [FIN, ACK] Seq=13769 Ack=4162 Win=131328 Len=0
 3073 362.327444  20.62.149.92                 192.168.1.34                 TCP        54 [TCP Dup ACK 1740#1] 443 → 50869 [ACK] Seq=4162 Ack=13738 Win=525312 Len=0
 3074 362.327444  20.62.149.92                 192.168.1.34                 TCP        54 443 → 50869 [RST, ACK] Seq=4162 Ack=13769 Win=0 Len=0
 3075 363.045145  2603:7081:13f0:8c10:bcb6:…   2603:7081:13f0:8c10::1       DNS        95 Standard query 0xd293 AAAA ssl.gstatic.com
 3076 363.045766  2603:7081:13f0:8c10:bcb6:…   2603:7081:13f0:8c10::1       DNS        95 Standard query 0x79bf A ssl.gstatic.com
```

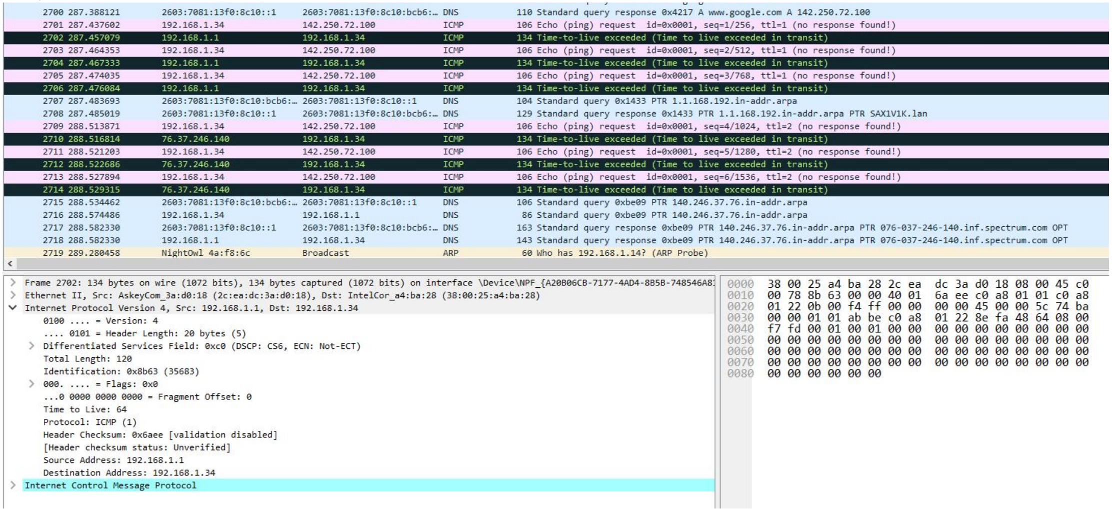
```
> Frame 1: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface \Device\NPF_{A20B06CB-7177-4AD4-8B5B-748546A81F06},
> Ethernet II, Src: IntelCor_a4:ba:28 (38:00:25:a4:ba:28), Dst: AskeyCom_3a:d0:18 (2c:ea:dc:3a:d0:18)
> Internet Protocol Version 6, Src: 2603:7081:13f0:8c10:bcb6:af22:bec:1aa0, Dst: 2603:7081:13f0:8c10::1
> User Datagram Protocol, Src Port: 56122, Dst Port: 53
> Domain Name System (query)
```

```
0000  2c ea dc 3a d0 18 38 00  25 a4 ba 28 86 dd 60 06
0010  96 87 00 29 11 40 26 03  70 81 13 f0 8c 10 bc b6
0020  af 22 0b ec 1a a0 26 03  70 81 13 f0 8c 10 00 00
0030  00 00 00 00 00 01 db 3a  00 35 00 29 ff aa e7 8c
0040  01 00 00 01 00 00 00 00  00 00 03 73 73 6c 07 67
0050  73 74 61 74 69 63 03 63  6f 6d 00 00 1c 00 01
```



```
C:\Users\dinot>tracert -4 www.google.com

Tracing route to www.google.com [142.250.72.100]
over a maximum of 30 hops:

  1    19 ms     3 ms     2 ms  SAX1V1K.lan [192.168.1.1]
  2     3 ms     1 ms     1 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  3    10 ms    10 ms     9 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  4    18 ms    10 ms    10 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  5     *       11 ms     *     076-037-246-140.inf.spectrum.com [76.37.246.140]
  6     *        *        *     Request timed out.
  7    16 ms    18 ms    18 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  8    17 ms    16 ms    17 ms  169.254.250.250
  9    20 ms    18 ms    17 ms  lag-63.rcr01albynyyf.netops.charter.com [24.58.35.6]
 10    26 ms    26 ms    25 ms  lag-416.nycmny837aw-bcr00.netops.charter.com [66.109.6.10]
 11    29 ms    25 ms    26 ms  72.14.214.208
 12    33 ms    25 ms    25 ms  142.251.78.65
 13    27 ms    31 ms    31 ms  142.251.65.95
 14    59 ms    57 ms    64 ms  lga34s32-in-f4.1e100.net [142.250.72.100]

Trace complete.
```

Step 2 :



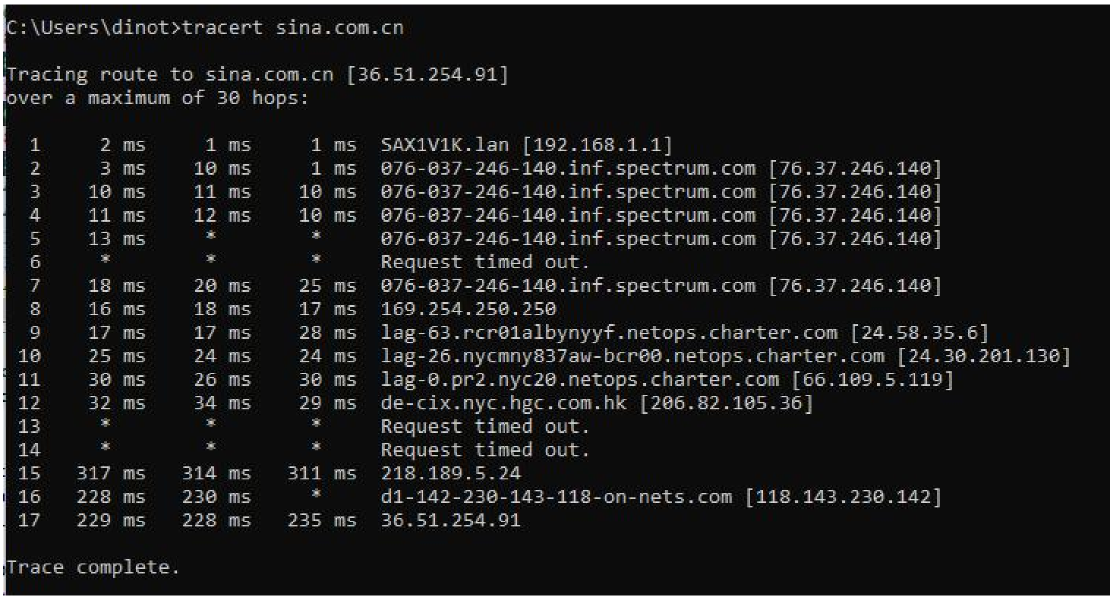
```
   2700 287.388121   2603:7081:13f0:8c10::1        2603:7081:13f0:8c10:bcb6:… DNS    110 Standard query response 0x4217 A www.google.com A 142.250.72.100
   2701 287.437602   192.168.1.34                  142.250.72.100             ICMP   106 Echo (ping) request  id=0x0001, seq=1/256, ttl=1 (no response found!)
   2702 287.457079   192.168.1.1                   192.168.1.34               ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
   2703 287.464353   192.168.1.34                  142.250.72.100             ICMP   106 Echo (ping) request  id=0x0001, seq=2/512, ttl=1 (no response found!)
   2704 287.467333   192.168.1.1                   192.168.1.34               ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
   2705 287.474035   192.168.1.34                  142.250.72.100             ICMP   106 Echo (ping) request  id=0x0001, seq=3/768, ttl=1 (no response found!)
   2706 287.476084   192.168.1.1                   192.168.1.34               ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
   2707 287.483693   2603:7081:13f0:8c10:bcb6:…    2603:7081:13f0:8c10::1     DNS    104 Standard query 0x1433 PTR 1.1.168.192.in-addr.arpa
   2708 287.485019   2603:7081:13f0:8c10::1        2603:7081:13f0:8c10:bcb6:… DNS    129 Standard query response 0x1433 PTR 1.1.168.192.in-addr.arpa PTR SAX1V1K.lan
   2709 288.513871   192.168.1.34                  142.250.72.100             ICMP   106 Echo (ping) request  id=0x0001, seq=4/1024, ttl=2 (no response found!)
   2710 288.516814   76.37.246.140                 192.168.1.34               ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
   2711 288.521203   192.168.1.34                  142.250.72.100             ICMP   106 Echo (ping) request  id=0x0001, seq=5/1280, ttl=2 (no response found!)
   2712 288.522686   76.37.246.140                 192.168.1.34               ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
   2713 288.527894   192.168.1.34                  142.250.72.100             ICMP   106 Echo (ping) request  id=0x0001, seq=6/1536, ttl=2 (no response found!)
   2714 288.529315   76.37.246.140                 192.168.1.34               ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
   2715 288.534462   2603:7081:13f0:8c10:bcb6:…    2603:7081:13f0:8c10::1     DNS    106 Standard query 0xbe09 PTR 140.246.37.76.in-addr.arpa
   2716 288.574486   192.168.1.34                  192.168.1.1                DNS     86 Standard query 0xbe09 PTR 140.246.37.76.in-addr.arpa
   2717 288.582330   2603:7081:13f0:8c10::1        2603:7081:13f0:8c10:bcb6:… DNS    163 Standard query response 0xbe09 PTR 140.246.37.76.in-addr.arpa PTR 076-037-246-140.inf.spectrum.com OPT
   2718 288.582330   192.168.1.1                   192.168.1.34               DNS    143 Standard query response 0xbe09 PTR 140.246.37.76.in-addr.arpa PTR 076-037-246-140.inf.spectrum.com OPT
   2719 289.280458   NightOwl 4a:f8:6c             Broadcast                  ARP     60 Who has 192.168.1.14? (ARP Probe)
```

```
> Frame 2702: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF_{A20B06CB-7177-4AD4-8B5B-748546A8
> Ethernet II, Src: AskeyCom_3a:d0:18 (2c:ea:dc:3a:d0:18), Dst: IntelCor_a4:ba:28 (38:00:25:a4:ba:28)
v Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.34
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
      Total Length: 120
      Identification: 0x8b63 (35683)
    > 000. .... = Flags: 0x0
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 64
      Protocol: ICMP (1)
      Header Checksum: 0x6aee [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.1.1
      Destination Address: 192.168.1.34
> Internet Control Message Protocol
```

```
0000  38 00 25 a4 ba 28 2c ea  dc 3a d0 18 08 00 45 c0
0010  00 78 8b 63 00 00 40 01  6a ee c0 a8 01 01 c0 a8
0020  01 22 0b 00 f4 ff 00 00  00 00 45 00 00 5c 74 ba
0030  00 00 01 01 ab be c0 a8  01 22 8e fa 48 64 08 00
0040  f7 fd 00 01 00 01 00 00  00 00 00 00 00 00 00 00
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0080  00 00 00 00 00 00
```

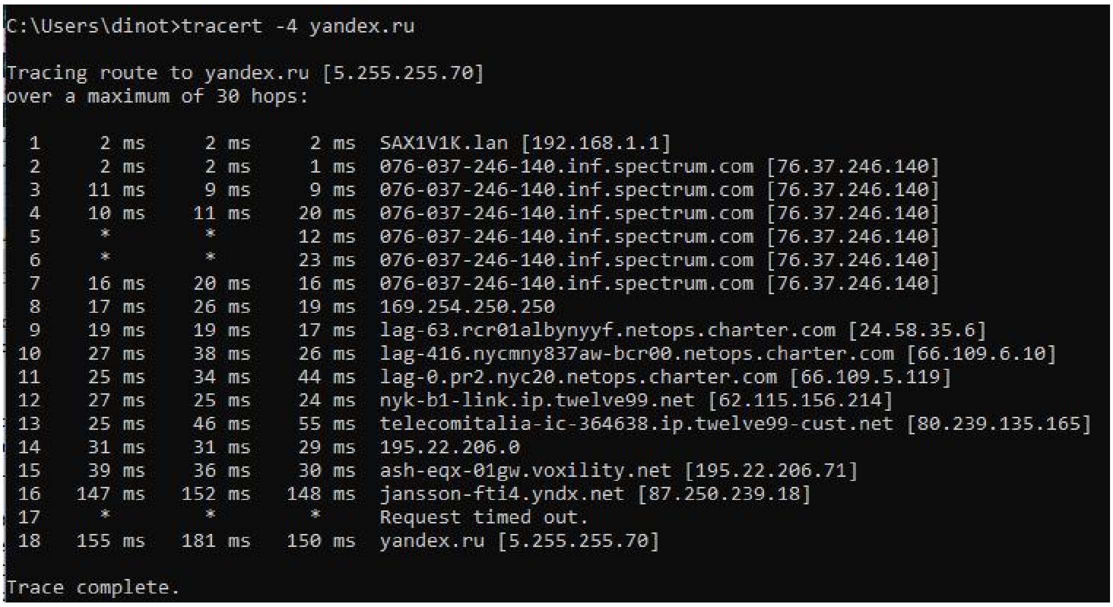
Step 3 :

A.



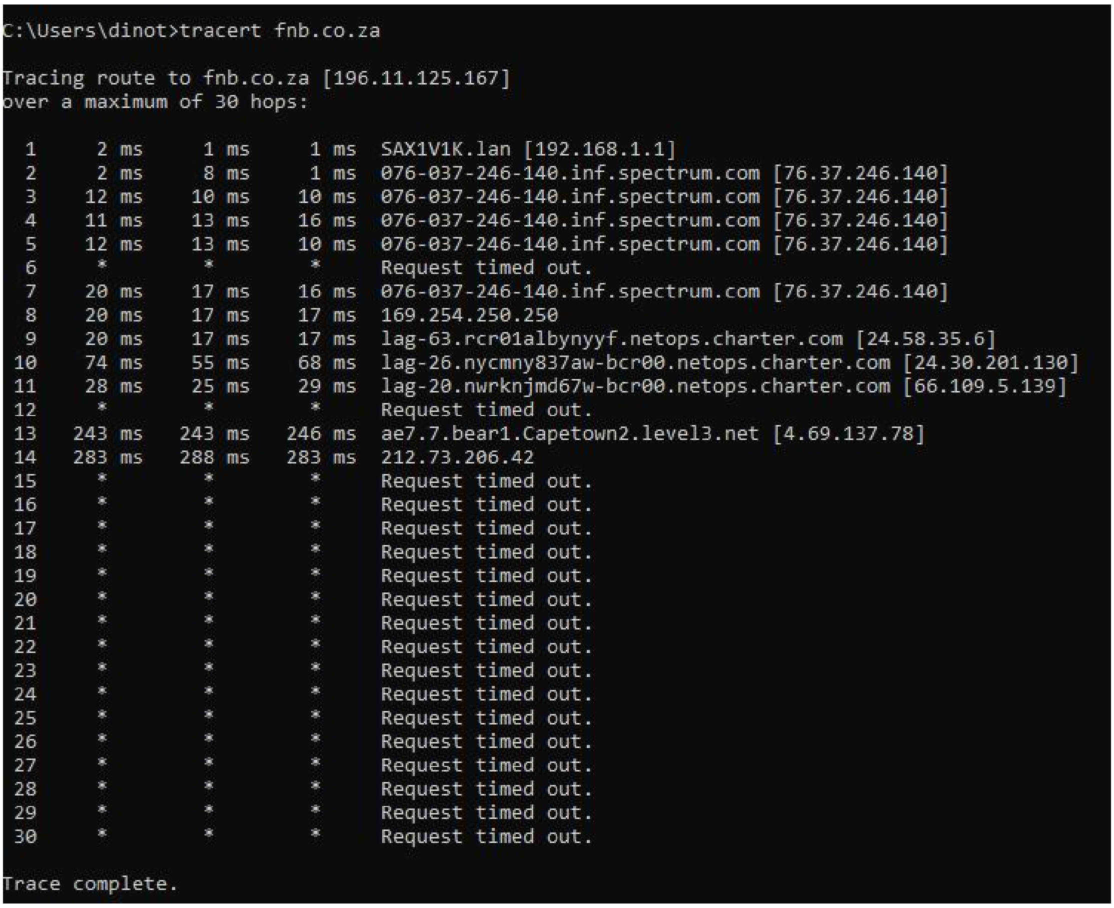
```
C:\Users\dinot>tracert sina.com.cn

Tracing route to sina.com.cn [36.51.254.91]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  SAX1V1K.lan [192.168.1.1]
  2     3 ms    10 ms     1 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  3    10 ms    11 ms    10 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  4    11 ms    12 ms    10 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  5    13 ms     *        *     076-037-246-140.inf.spectrum.com [76.37.246.140]
  6     *        *        *     Request timed out.
  7    18 ms    20 ms    25 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  8    16 ms    18 ms    17 ms  169.254.250.250
  9    17 ms    17 ms    28 ms  lag-63.rcr01albynyyf.netops.charter.com [24.58.35.6]
 10    25 ms    24 ms    24 ms  lag-26.nycmny837aw-bcr00.netops.charter.com [24.30.201.130]
 11    30 ms    26 ms    30 ms  lag-0.pr2.nyc20.netops.charter.com [66.109.5.119]
 12    32 ms    34 ms    29 ms  de-cix.nyc.hgc.com.hk [206.82.105.36]
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15   317 ms   314 ms   311 ms  218.189.5.24
 16   228 ms   230 ms     *     d1-142-230-143-118-on-nets.com [118.143.230.142]
 17   229 ms   228 ms   235 ms  36.51.254.91

Trace complete.
```

B.



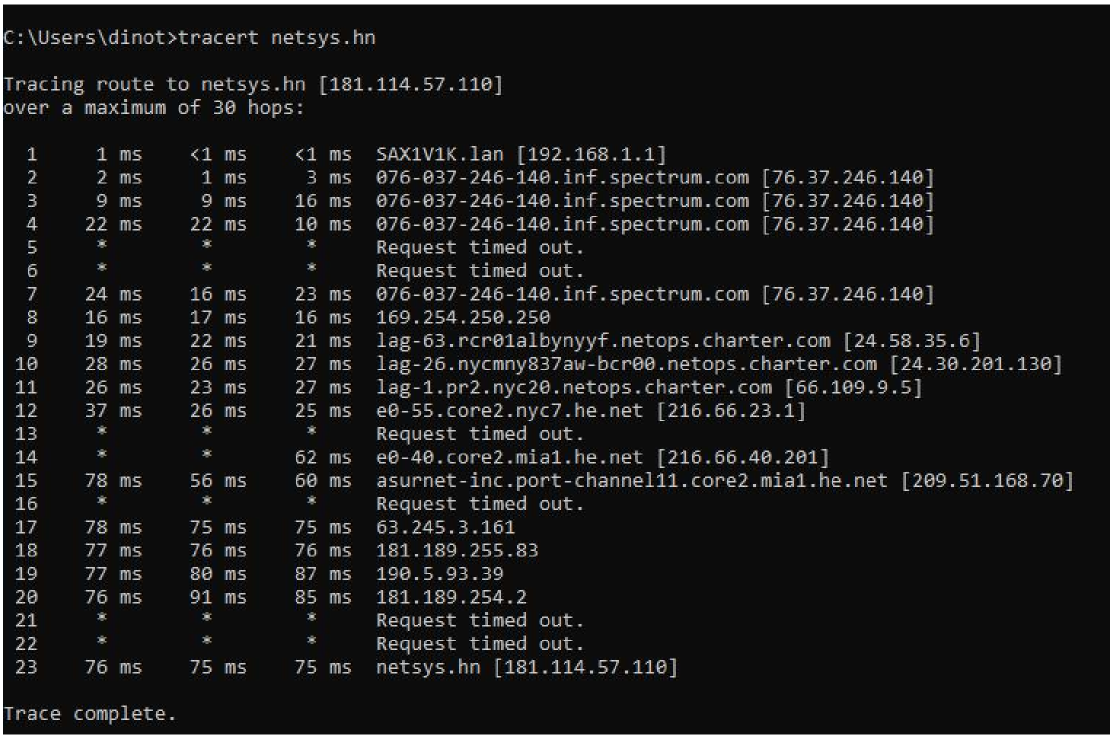
```
C:\Users\dinot>tracert -4 yandex.ru

Tracing route to yandex.ru [5.255.255.70]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  SAX1V1K.lan [192.168.1.1]
  2     2 ms     2 ms     1 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  3    11 ms     9 ms     9 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  4    10 ms    11 ms    20 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  5     *        *       12 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  6     *        *       23 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  7    16 ms    20 ms    16 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  8    17 ms    26 ms    19 ms  169.254.250.250
  9    19 ms    19 ms    17 ms  lag-63.rcr01albynyyf.netops.charter.com [24.58.35.6]
 10    27 ms    38 ms    26 ms  lag-416.nycmny837aw-bcr00.netops.charter.com [66.109.6.10]
 11    25 ms    34 ms    44 ms  lag-0.pr2.nyc20.netops.charter.com [66.109.5.119]
 12    27 ms    25 ms    24 ms  nyk-b1-link.ip.twelve99.net [62.115.156.214]
 13    25 ms    46 ms    55 ms  telecomitalia-ic-364638.ip.twelve99-cust.net [80.239.135.165]
 14    31 ms    31 ms    29 ms  195.22.206.0
 15    39 ms    36 ms    30 ms  ash-eqx-01gw.voxility.net [195.22.206.71]
 16   147 ms   152 ms   148 ms  jansson-fti4.yndx.net [87.250.239.18]
 17     *        *        *     Request timed out.
 18   155 ms   181 ms   150 ms  yandex.ru [5.255.255.70]

Trace complete.
```

C.



```
C:\Users\dinot>tracert fnb.co.za

Tracing route to fnb.co.za [196.11.125.167]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  SAX1V1K.lan [192.168.1.1]
  2     2 ms     8 ms     1 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  3    12 ms    10 ms    10 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  4    11 ms    13 ms    16 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  5    12 ms    13 ms    10 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  6     *        *        *     Request timed out.
  7    20 ms    17 ms    16 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  8    20 ms    17 ms    17 ms  169.254.250.250
  9    20 ms    17 ms    17 ms  lag-63.rcr01albynyyf.netops.charter.com [24.58.35.6]
 10    74 ms    55 ms    68 ms  lag-26.nycmny837aw-bcr00.netops.charter.com [24.30.201.130]
 11    28 ms    25 ms    29 ms  lag-20.nwrknjmd67w-bcr00.netops.charter.com [66.109.5.139]
 12     *        *        *     Request timed out.
 13   243 ms   243 ms   246 ms  ae7.7.bear1.Capetown2.level3.net [4.69.137.78]
 14   283 ms   288 ms   283 ms  212.73.206.42
 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.
```

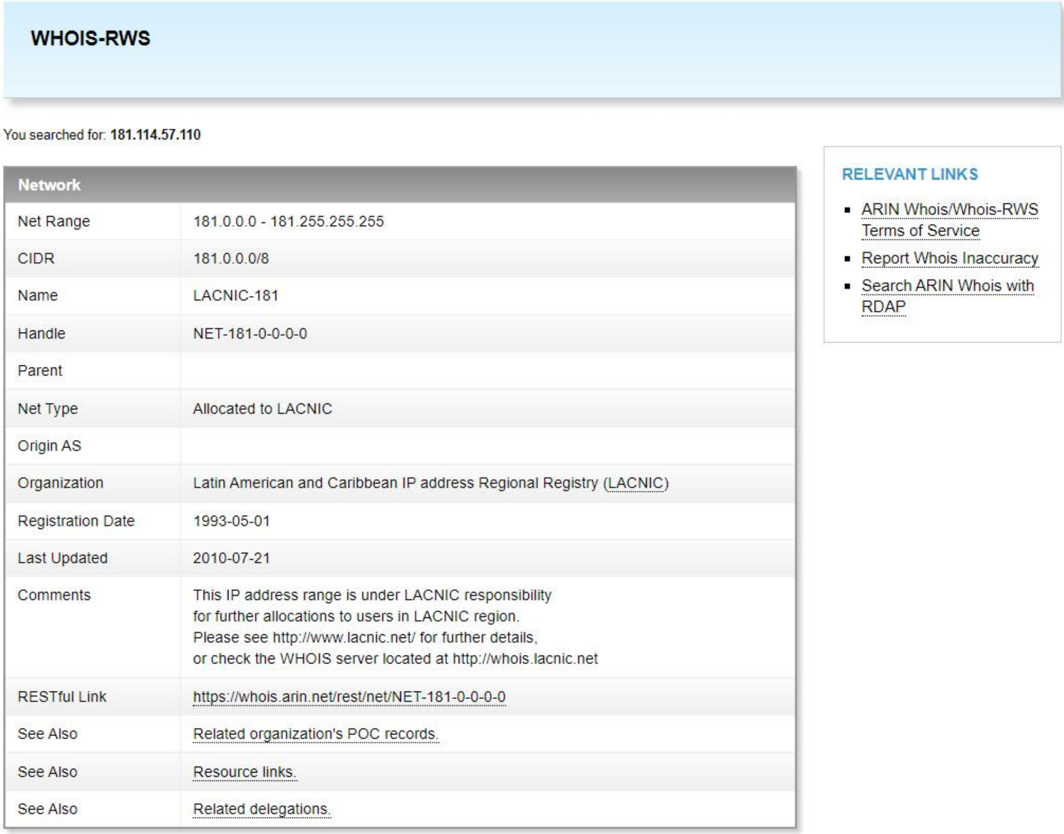
D.



```
C:\Users\dinot>tracert netsys.hn

Tracing route to netsys.hn [181.114.57.110]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  SAX1V1K.lan [192.168.1.1]
  2     2 ms     1 ms     3 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  3     9 ms     9 ms    16 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  4    22 ms    22 ms    10 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7    24 ms    16 ms    23 ms  076-037-246-140.inf.spectrum.com [76.37.246.140]
  8    16 ms    17 ms    16 ms  169.254.250.250
  9    19 ms    22 ms    21 ms  lag-63.rcr01albynyyf.netops.charter.com [24.58.35.6]
 10    28 ms    26 ms    27 ms  lag-26.nycmny837aw-bcr00.netops.charter.com [24.30.201.130]
 11    26 ms    23 ms    27 ms  lag-1.pr2.nyc20.netops.charter.com [66.109.9.5]
 12    37 ms    26 ms    25 ms  e0-55.core2.nyc7.he.net [216.66.23.1]
 13     *        *        *     Request timed out.
 14     *        *       62 ms  e0-40.core2.mia1.he.net [216.66.40.201]
 15    78 ms    56 ms    60 ms  asurnet-inc.port-channel11.core2.mia1.he.net [209.51.168.70]
 16     *        *        *     Request timed out.
 17    78 ms    75 ms    75 ms  63.245.3.161
 18    77 ms    76 ms    76 ms  181.189.255.83
 19    77 ms    80 ms    87 ms  190.5.93.39
 20    76 ms    91 ms    85 ms  181.189.254.2
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23    76 ms    75 ms    75 ms  netsys.hn [181.114.57.110]

Trace complete.
```

E.

I. Tracert netsys.hn



WHOIS-RWS

You searched for: **181.114.57.110**

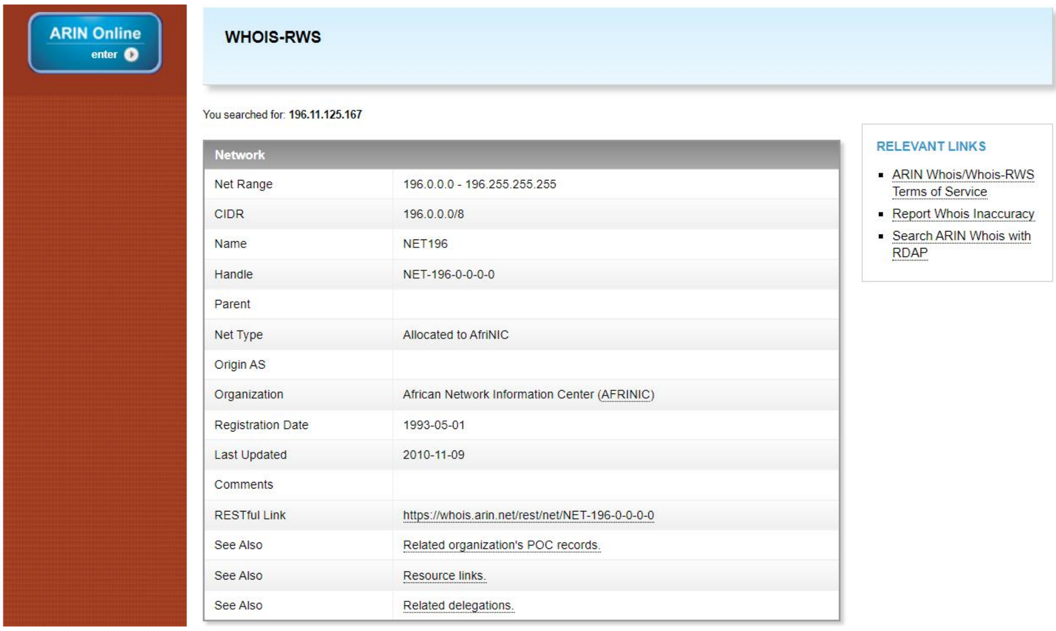
Network	
Net Range	181.0.0.0 - 181.255.255.255
CIDR	181.0.0.0/8
Name	LACNIC-181
Handle	NET-181-0-0-0-0
Parent	
Net Type	Allocated to LACNIC
Origin AS	
Organization	Latin American and Caribbean IP address Regional Registry (LACNIC)
Registration Date	1993-05-01
Last Updated	2010-07-21
Comments	This IP address range is under LACNIC responsibility for further allocations to users in LACNIC region. Please see http://www.lacnic.net/ for further details, or check the WHOIS server located at http://whois.lacnic.net
RESTful Link	https://whois.arin.net/rest/net/NET-181-0-0-0-0
See Also	Related organization's POC records.
See Also	Resource links.
See Also	Related delegations.

RELEVANT LINKS

- ARIN Whois/Whois-RWS Terms of Service
- Report Whois Inaccuracy
- Search ARIN Whois with RDAP

II.

tracert fnb.co.za



WHOIS-RWS

You searched for: **196.11.125.167**

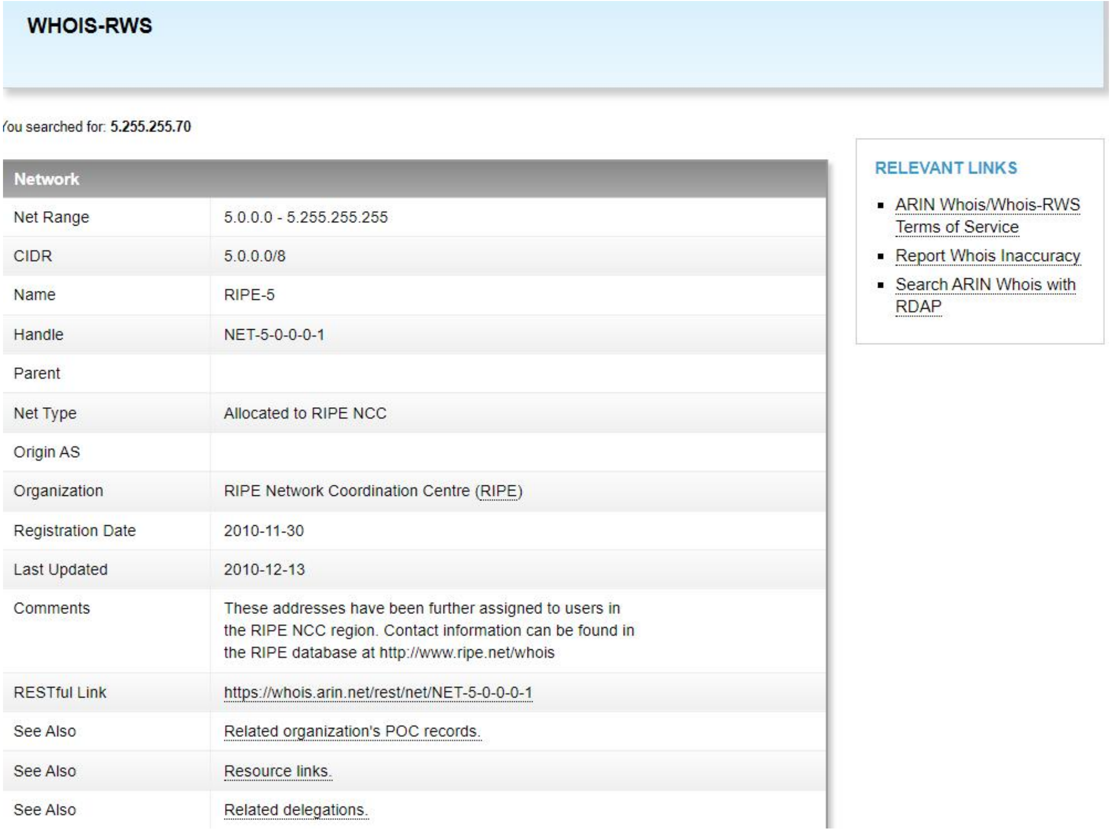
Network	
Net Range	196.0.0.0 - 196.255.255.255
CIDR	196.0.0.0/8
Name	NET196
Handle	NET-196-0-0-0-0
Parent	
Net Type	Allocated to AfriNIC
Origin AS	
Organization	African Network Information Center (AFRINIC)
Registration Date	1993-05-01
Last Updated	2010-11-09
Comments	
RESTful Link	https://whois.arin.net/rest/net/NET-196-0-0-0-0
See Also	Related organization's POC records.
See Also	Resource links.
See Also	Related delegations.

RELEVANT LINKS

- ARIN Whois/Whois-RWS Terms of Service
- Report Whois Inaccuracy
- Search ARIN Whois with RDAP

III.

tracert -4 yandex.ru



WHOIS-RWS

You searched for: **5.255.255.70**

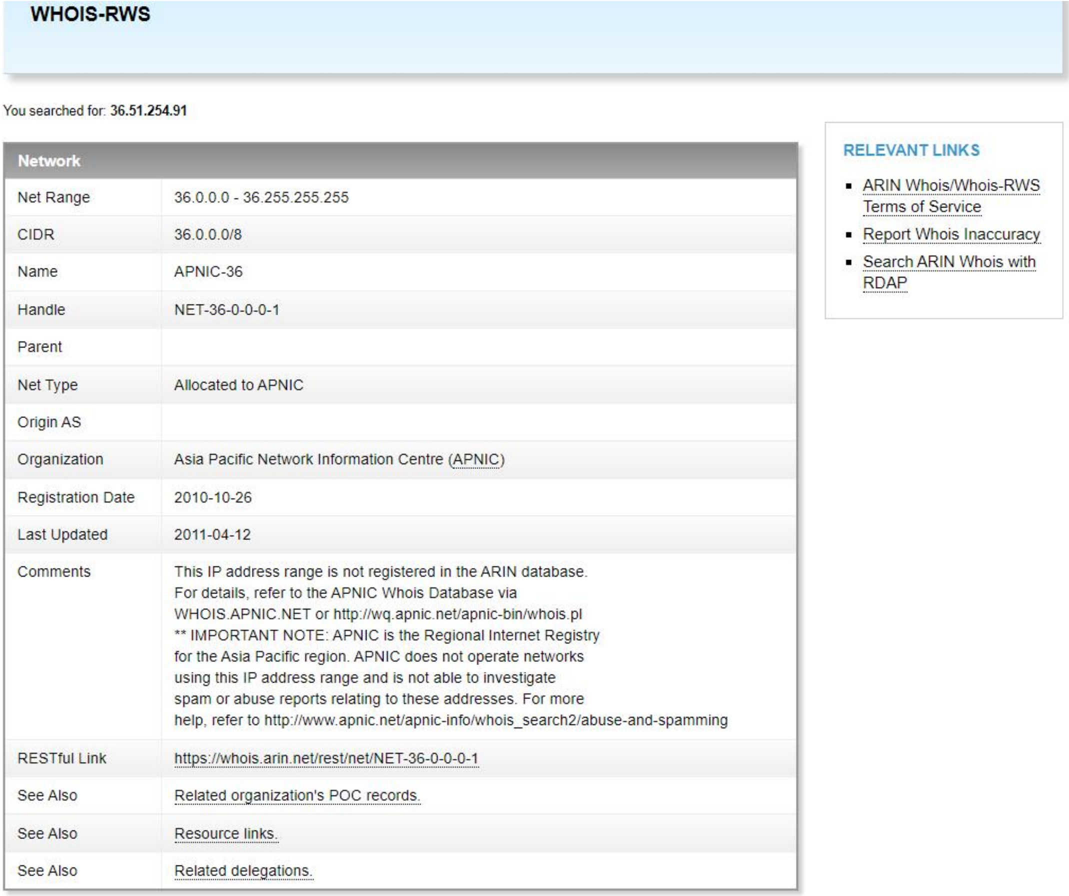
Network	
Net Range	5.0.0.0 - 5.255.255.255
CIDR	5.0.0.0/8
Name	RIPE-5
Handle	NET-5-0-0-0-1
Parent	
Net Type	Allocated to RIPE NCC
Origin AS	
Organization	RIPE Network Coordination Centre (RIPE)
Registration Date	2010-11-30
Last Updated	2010-12-13
Comments	These addresses have been further assigned to users in the RIPE NCC region. Contact information can be found in the RIPE database at http://www.ripe.net/whois
RESTful Link	https://whois.arin.net/rest/net/NET-5-0-0-0-1
See Also	Related organization's POC records.
See Also	Resource links.
See Also	Related delegations.

RELEVANT LINKS

- ARIN Whois/Whois-RWS Terms of Service
- Report Whois Inaccuracy
- Search ARIN Whois with RDAP

IV.

tracert sina.com.cn



WHOIS-RWS

You searched for: **36.51.254.91**

Network	
Net Range	36.0.0.0 - 36.255.255.255
CIDR	36.0.0.0/8
Name	APNIC-36
Handle	NET-36-0-0-0-1
Parent	
Net Type	Allocated to APNIC
Origin AS	
Organization	Asia Pacific Network Information Centre (APNIC)
Registration Date	2010-10-26
Last Updated	2011-04-12
Comments	This IP address range is not registered in the ARIN database. For details, refer to the APNIC Whois Database via WHOIS.APNIC.NET or http://wq.apnic.net/apnic-bin/whois.pl ** IMPORTANT NOTE: APNIC is the Regional Internet Registry for the Asia Pacific region. APNIC does not operate networks using this IP address range and is not able to investigate spam or abuse reports relating to these addresses. For more help, refer to http://www.apnic.net/apnic-info/whois_search2/abuse-and-spamming
RESTful Link	https://whois.arin.net/rest/net/NET-36-0-0-0-1
See Also	Related organization's POC records.
See Also	Resource links.
See Also	Related delegations.

RELEVANT LINKS

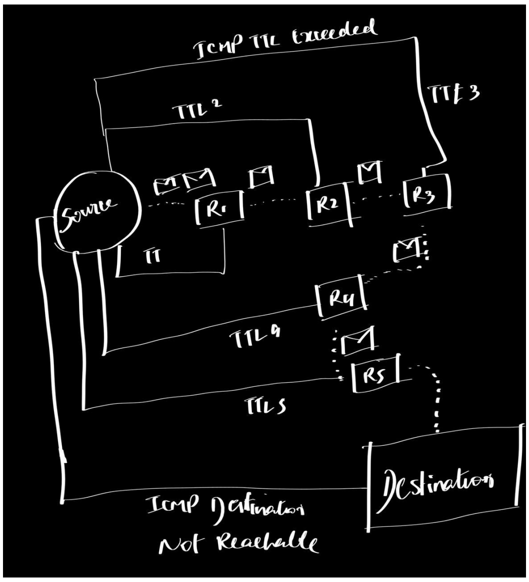
- ARIN Whois/Whois-RWS Terms of Service
- Report Whois Inaccuracy
- Search ARIN Whois with RDAP

F.

Almost all the hops are around 14 to 18 but the hop to South Africa is 30 which is considerably lot of hop than rest of them, as we can see lot of Request timed out is a reason after 15 with lot of asterisks. May be the there are lot of filters going on filtering ICMP request and not allowing for replies is the case.

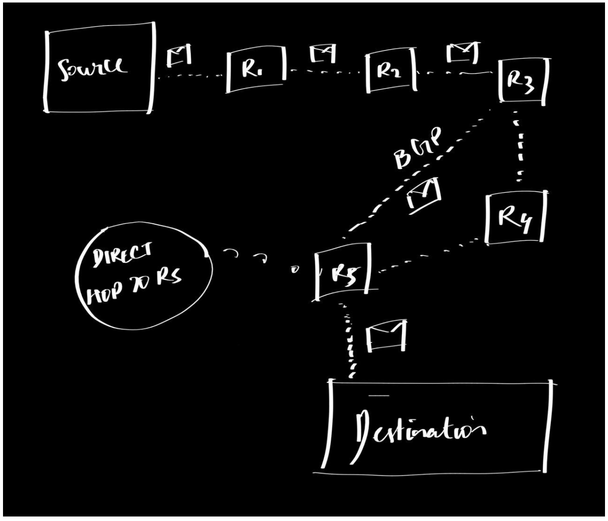
Step 4 :

A.

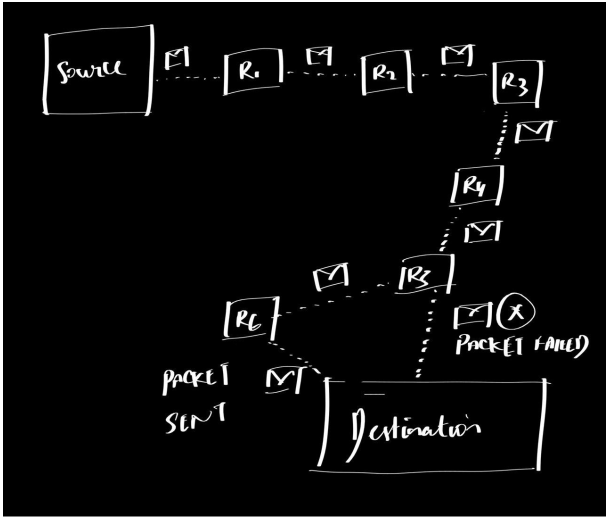


B.

Five routers to four routers, instead of going from r3 to r4 to r5, it directly passed from r3 to r5.



Instead of using five routers, here extra r6 needed for packet or frame delivery.

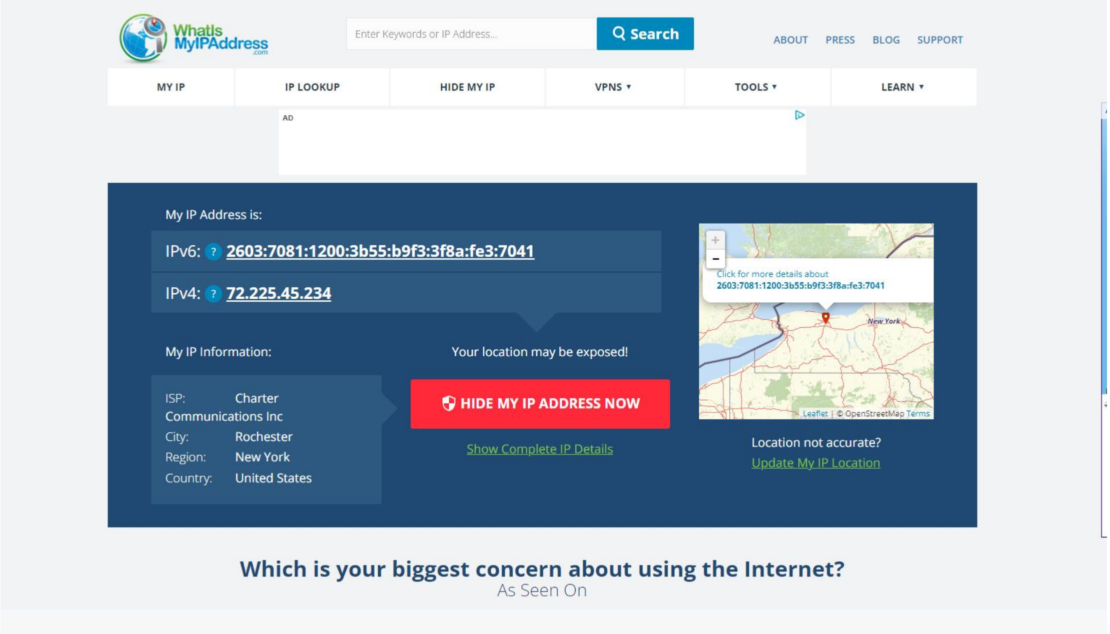


C. I got some anomalous value from trace routing above websites from four different regions, I found of maximum 314 ms I got from the above website especially from South Africa.

Exercise : 7. 02

Step 1 :

A.



My IP Address is:

IPv6: 2603:7081:1200:3b55:b9f3:3f8a:fe3:7041

IPv4: 72.225.45.234

My IP Information:

ISP: Charter Communications Inc

City: Rochester

Region: New York

Country: United States

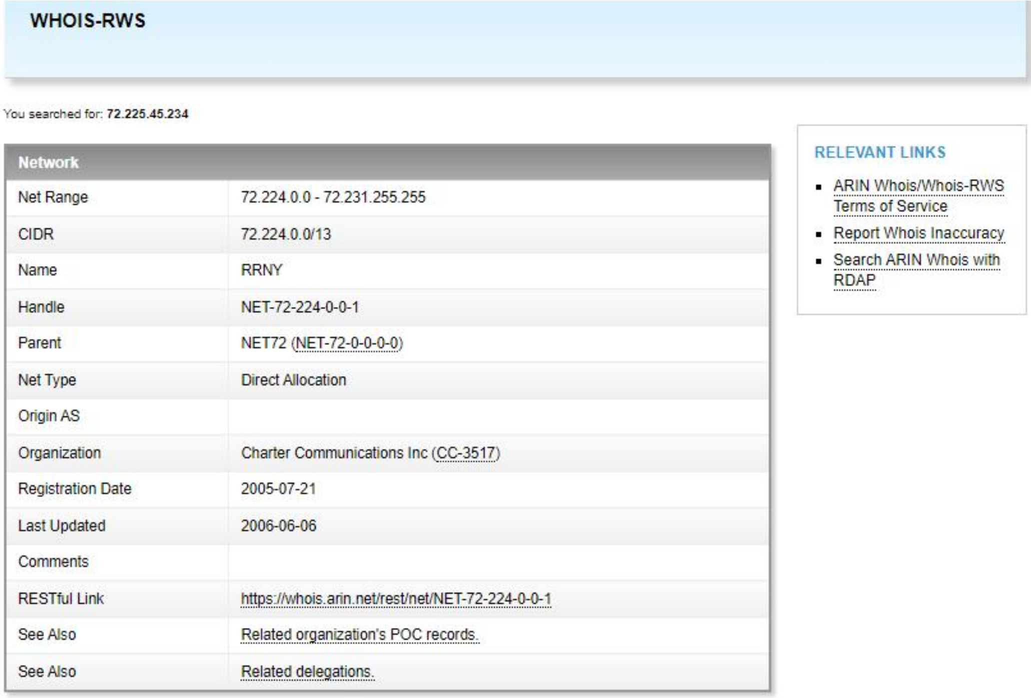
Your location may be exposed!

Location not accurate?

Which is your biggest concern about using the Internet?

As Seen On

B.


WHOIS-RWS

You searched for: **72.225.45.234**

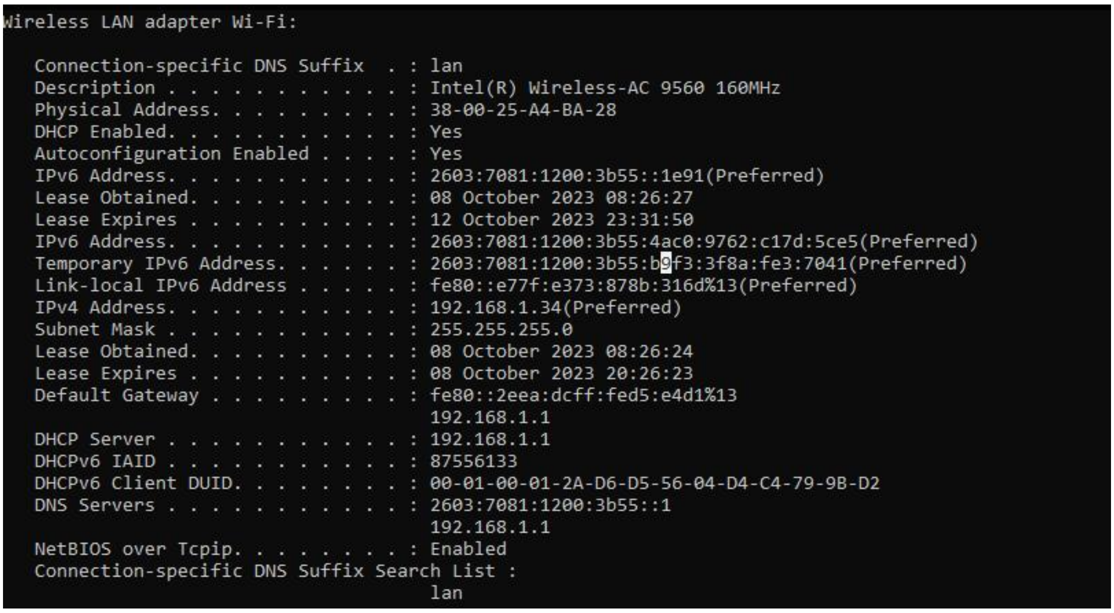
Network	
Net Range	72.224.0.0 - 72.231.255.255
CIDR	72.224.0.0/13
Name	RRNY
Handle	NET-72-224-0-0-1
Parent	NET72 (NET-72-0-0-0-0)
Net Type	Direct Allocation
Origin AS	
Organization	Charter Communications Inc (CC-3517)
Registration Date	2005-07-21
Last Updated	2006-06-06
Comments	
RESTful Link	https://whois.arin.net/rest/net/NET-72-224-0-0-1
See Also	Related organization's POC records.
See Also	Related delegations.

RELEVANT LINKS

- ARIN Whois/Whois-RWS Terms of Service
- Report Whois Inaccuracy
- Search ARIN Whois with RDAP

Step 2 :

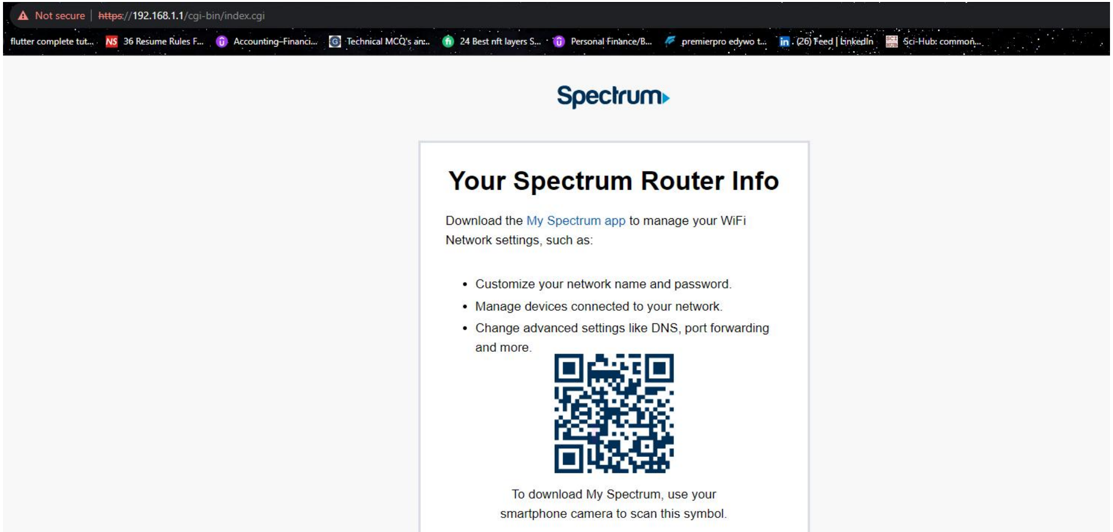
A.



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : lan
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz
   Physical Address. . . . . . . . . : 38-00-25-A4-BA-28
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2603:7081:1200:3b55::1e91(Preferred)
   Lease Obtained. . . . . . . . . . : 08 October 2023 08:26:27
   Lease Expires . . . . . . . . . . : 12 October 2023 23:31:50
   IPv6 Address. . . . . . . . . . . : 2603:7081:1200:3b55:4ac0:9762:c17d:5ce5(Preferred)
   Temporary IPv6 Address. . . . . . : 2603:7081:1200:3b55:b9f3:3f8a:fe3:7041(Preferred)
   Link-local IPv6 Address . . . . . : fe80::e77f:e373:878b:316d%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.34(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 08 October 2023 08:26:24
   Lease Expires . . . . . . . . . . : 08 October 2023 20:26:23
   Default Gateway . . . . . . . . . : fe80::2eea:dcff:fed5:e4d1%13
                                       192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 87556133
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-D6-D5-56-04-D4-C4-79-9B-D2
   DNS Servers . . . . . . . . . . . : 2603:7081:1200:3b55::1
                                       192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       lan
```

B. From the Step 2a, the IPV6 temporary address is matching with a 1a. Both looks same, but IPV4 is not matching though.

Step 3.



Your Spectrum Router Info

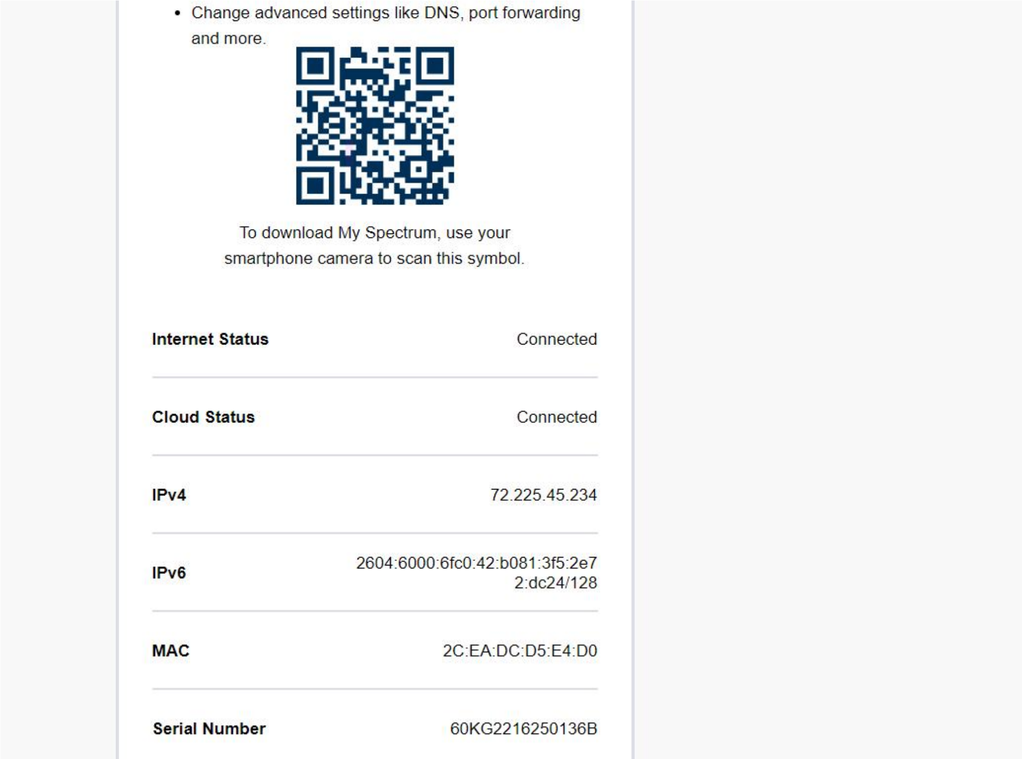
Download the My Spectrum app to manage your WiFi Network settings, such as:

- Customize your network name and password.
- Manage devices connected to your network.
- Change advanced settings like DNS, port forwarding and more.

To download My Spectrum, use your smartphone camera to scan this symbol.

A.

B.



- Change advanced settings like DNS, port forwarding and more.

To download My Spectrum, use your smartphone camera to scan this symbol.

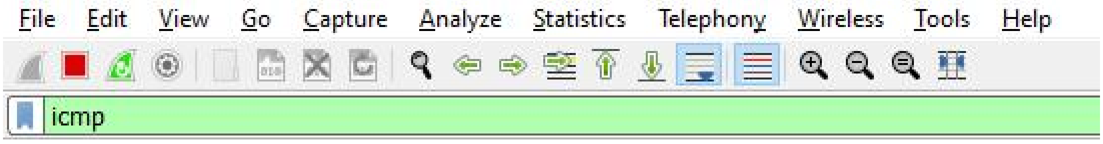
Internet Status	Connected
Cloud Status	Connected
IPv4	72.225.45.234
IPv6	2604:6000:6fc0:42:b081:3f5:2e7 2:dc24/128
MAC	2C:EA:DC:D5:E4:D0
Serial Number	60KG2216250136B

C.

For addressing the limitation of IPV4 addresses and for helping the ISP to connect to customers whom using IPV4 addresses. As internet is growing and devices too. It is necessary for CGNAT deployments.

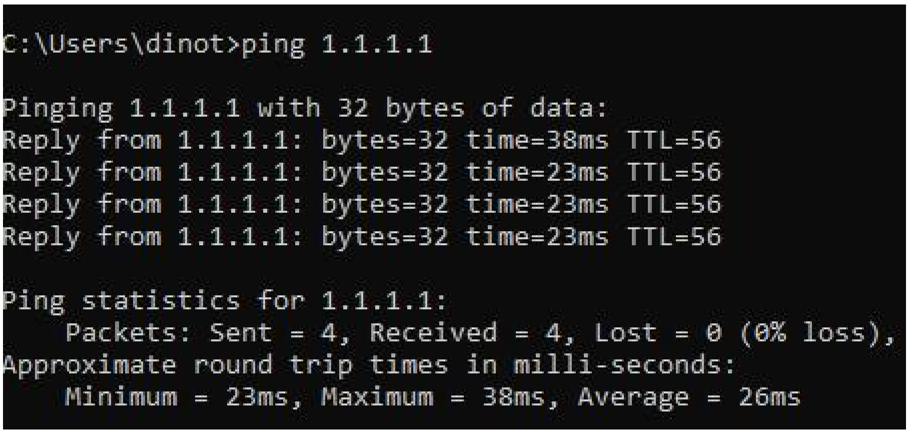
Step 4 :

A.



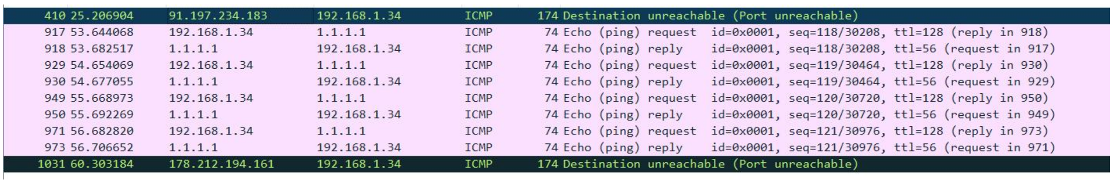
icmp

B.



```
C:\Users\dinot>ping 1.1.1.1

Pinging 1.1.1.1 with 32 bytes of data:
Reply from 1.1.1.1: bytes=32 time=38ms TTL=56
Reply from 1.1.1.1: bytes=32 time=23ms TTL=56
Reply from 1.1.1.1: bytes=32 time=23ms TTL=56
Reply from 1.1.1.1: bytes=32 time=23ms TTL=56

Ping statistics for 1.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 38ms, Average = 26ms
```

C.



```
 410 25.206904   91.197.234.183   192.168.1.34   ICMP   174 Destination unreachable (Port unreachable)
 917 53.644068   192.168.1.34     1.1.1.1        ICMP    74 Echo (ping) request  id=0x0001, seq=118/30208, ttl=128 (reply in 918)
 918 53.682517   1.1.1.1          192.168.1.34   ICMP    74 Echo (ping) reply    id=0x0001, seq=118/30208, ttl=56 (request in 917)
 929 54.654069   192.168.1.34     1.1.1.1        ICMP    74 Echo (ping) request  id=0x0001, seq=119/30464, ttl=128 (reply in 930)
 930 54.677055   1.1.1.1          192.168.1.34   ICMP    74 Echo (ping) reply    id=0x0001, seq=119/30464, ttl=56 (request in 929)
 949 55.668973   192.168.1.34     1.1.1.1        ICMP    74 Echo (ping) request  id=0x0001, seq=120/30720, ttl=128 (reply in 950)
 950 55.692269   1.1.1.1          192.168.1.34   ICMP    74 Echo (ping) reply    id=0x0001, seq=120/30720, ttl=56 (request in 949)
 971 56.682820   192.168.1.34     1.1.1.1        ICMP    74 Echo (ping) request  id=0x0001, seq=121/30976, ttl=128 (reply in 973)
 973 56.706652   1.1.1.1          192.168.1.34   ICMP    74 Echo (ping) reply    id=0x0001, seq=121/30976, ttl=56 (request in 971)
1031 60.303184   178.212.194.161  192.168.1.34   ICMP   174 Destination unreachable (Port unreachable)
```

SOURCE address for ICMP echo request : 192.168.1.34
DESTINATION address for ICMP echo reply : 192.168.1.34

D.
192.168.1.34 is used through out as source IP for my machine which is my private IP address, and other two address are shared IP address and Port translated address.

Step 5 :
A.
I unable to see port forwarding, my wifi not allowing to see it.
B.
C.

Exercise 7. 03 :
Step 1 :
SSID is service set identifier and my ssid is “SpectrumSetup-D0”. This SSID is my home routers provided by Spectrum.

Step 2 :
Guest network is not enabled in our home router to ensure the privacy of router, also it is residential wifi so no guest wifi configured.

Step 3 :
The frequency of this router is 5Ghz and it supports 2.4 Ghz too. It mainly works on 5Ghz to provide higher bandwidth.

Step 4 :
WPA2 is used for encryption for this wifi network, which I feel reasonably secure.

Step 5 :
It uses 802.11ax as it uses wifi 6 technology and wifi speed upto 960 MBps.

Step 6 :
I didn’t find any Quality of service to my knowledge but certain services can be implemented my restriced the websites which are harmful and not recommended like (Parental Controls) and restricting the public websites to reach the private data like (Prioritization) etc.

Step 7 :
WPA/WPA2 and port forwarding, Firewall rules, IDS, VPN etc are used in this network for ensuring security and firewall configurations.

Step 8 :
System monitoring and user management are the allowed by the system tools from administrative perspective.

Lab analysis :

1. Tracert and Ping is different in a way that ping allows user to know that the source sends packet and destination replied it or not, but tracert allows to see number of hops happened between source and destination. We can also see whether our ICMP request or reply is filtered or not.

2. The TTL is time to live field ensures the packet duration in between the hops and it has 1 byte value, and it is usually configured by the sender of packet.

3. The routes are designed for efficiency and based on Border Routing Protocols, so that the internal structure of the system makes all the routes to have similar hops in my opinion.

4. NAT is primarily used within a private or local network, such as a home or a small business network, to allow multiple devices to share a single public IP address. It helps conserve public IP addresses. Whereas CGNAT is used by Internet Service Providers (ISPs) and carriers to allow multiple customers to share a pool of public IP addresses. It's primarily used to address the shortage of public IPv4 addresses on a larger scale.

5. These factors are important while setting up SOHO :
I. Security and Privacy
II. Port Forwarding
III. Encryption
IV. Firewall
V. Guest wifi Access
VI. Bandwidth configuration
VII. Having good password for your SSID

Key Term Quiz

1. NAT
2. CGNAT
3. HOP
4. TRACERT
5. WPA2