Computer Networks - Assignment 1

Aniket Gupta
Entry No - 2019CS10327

August 22, 2021

1 Networking Tools

1. **IP address using ipconfig**
   The IP address of my was not static. It was different with different service providers.
   - IP address obtained with RELIANCE JIO - 192.168.43.85
   - IP address obtained with AIRTEL - 192.168.43.173

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::48f7:be2e:40f7:d94c%2
   IPv4 Address. . . . . . . . . . . : 192.168.43.173
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.43.1
```

Figure 1: IP address with Airtel

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:4063:220d:80c0:48f7:be2e:40f7:d94c
   Temporary IPv6 Address. . . . . . : 2409:4063:220d:80c0:d4cb:7004:34cb:5b1e
   Link-local IPv6 Address . . . . . : fe80::48f7:be2e:40f7:d94c%2
   IPv4 Address. . . . . . . . . . . : 192.168.43.85
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::acd2:3bff:feb9:575b%2
                                       192.168.43.1
```

Figure 2: IP address with Reliance Jio

Reason for varying IP addresses:
The IP address keeps changing because the ISP generally provides "Dynamic IP address" instead of "Static IP address". One of the main reasons for this is that if one decides to move across town, he/she can still keep the previous ISP and there would be no need to go through the hassle of rerouting the "Static IP address".

2. **nslookup**
   IP address of www.google.com -
   - IPv4 Address - 142.250.193.36
   - IPv6 Address - 2404:6800:4002:81a::2004

   IP address of www.facebook.com -
   - IPv4 Address - 157.240.198.35
   - IPv6 Address - 2a03:2880:f144:82:face:b00c:0:25de

```
PS C:\Users\gupta> nslookup www.google.com ns1.google.com
Server:  ns1.google.com
Address:  216.239.32.10

Name:    www.google.com
Addresses:  2404:6800:4002:81a::2004
          142.250.193.36
```

```
PS C:\Users\gupta> nslookup www.facebook.com
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    star-mini.c10r.facebook.com
Addresses:  2a03:2880:f144:82:face:b00c:0:25de
          157.240.198.35
Aliases:  www.facebook.com
```

On changing the DNS server, the IP address of the above domains were also changing.

IP address of www.google.com on changing DNS servers:

(a) DNS server used - dns9.quad9.net (9.9.9.9)
- IPv4 Address - 172.217.24.68
- IPv6 Address - 2404:6800:4005:804::2004

(b) DNS server used - one.one.one.one (1.1.1.1)
- IPv4 Address - 142.250.196.36
- IPv6 Address - 2404:6800:4007:82a::2004

```
PS C:\Users\gupta> nslookup www.google.com 9.9.9.9
Server:  dns9.quad9.net
Address:  9.9.9.9

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4005:804::2004
          172.217.24.68
```

```
PS C:\Users\gupta> nslookup www.google.com 1.1.1.1
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4007:82a::2004
          142.250.196.36
```

IP address of www.facebook.com on changing DNS servers:

(a) DNS server used - dns9.quad9.net (9.9.9.9)
- IPv4 Address - 157.240.13.35
- IPv6 Address - 2a03:2880:f10c:283:face:b00c:0:25de

(b) DNS server used - one.one.one.one (1.1.1.1)
- IPv4 Address - 157.240.16.35
- IPv6 Address - 2a03:2880:f12f:183:face:b00c:0:25de

```
PS C:\Users\gupta> nslookup www.facebook.com 9.9.9.9
Server:  dns9.quad9.net
Address:  9.9.9.9

Non-authoritative answer:
Name:    star-mini.c10r.facebook.com
Addresses:  2a03:2880:f10c:283:face:b00c:0:25de
          157.240.13.35
Aliases:  www.facebook.com
```

```
PS C:\Users\gupta> nslookup www.facebook.com 1.1.1.1
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:    star-mini.c10r.facebook.com
Addresses:  2a03:2880:f12f:183:face:b00c:0:25de
          157.240.16.35
Aliases:  www.facebook.com
```

3. **ping**

Pinging www.iitd.ac.in with different packet sizes:

```
PS C:\Users\gupta> ping -l 64 www.iitd.ac.in

Pinging www.iitd.ac.in [103.27.9.24] with 64 bytes of data:
Reply from 103.27.9.24: bytes=64 time=57ms TTL=49
Reply from 103.27.9.24: bytes=64 time=64ms TTL=49
Reply from 103.27.9.24: bytes=64 time=100ms TTL=49
Reply from 103.27.9.24: bytes=64 time=100ms TTL=49

Ping statistics for 103.27.9.24:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 57ms, Maximum = 100ms, Average = 80ms
```

```
PS C:\Users\gupta> ping -l 128 www.iitd.ac.in

Pinging www.iitd.ac.in [103.27.9.24] with 128 bytes of data:
Reply from 103.27.9.24: bytes=128 time=87ms TTL=49
Reply from 103.27.9.24: bytes=128 time=91ms TTL=49
Reply from 103.27.9.24: bytes=128 time=63ms TTL=49
Reply from 103.27.9.24: bytes=128 time=66ms TTL=49

Ping statistics for 103.27.9.24:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 63ms, Maximum = 91ms, Average = 76ms
```

Figure 3: Pinging www.iitd.ac.in with packet sizes of 64 and 128 bytes

Pinging www.iitd.ac.in with different TTL values:

```
PS C:\Users\gupta> ping -i 10 www.iitd.ac.in

Pinging www.iitd.ac.in [103.27.9.24] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 103.27.9.24:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
PS C:\Users\gupta> ping -i 30 www.iitd.ac.in

Pinging www.iitd.ac.in [103.27.9.24] with 32 bytes of data:
Reply from 103.27.9.24: bytes=32 time=66ms TTL=49
Reply from 103.27.9.24: bytes=32 time=61ms TTL=49
Reply from 103.27.9.24: bytes=32 time=68ms TTL=49
Reply from 103.27.9.24: bytes=32 time=218ms TTL=49

Ping statistics for 103.27.9.24:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 61ms, Maximum = 218ms, Average = 103ms
```

Figure 4: Pinging www.iitd.ac.in with packet TTL values of 10 and 30

Maximum packet size that could be sent to www.iitd.ac.in:

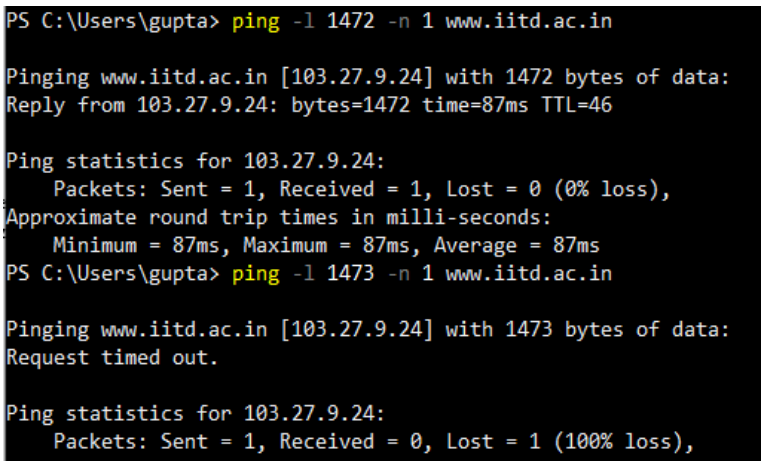


Figure 5: Maximum packet size that could be sent to www.iitd.ac.in

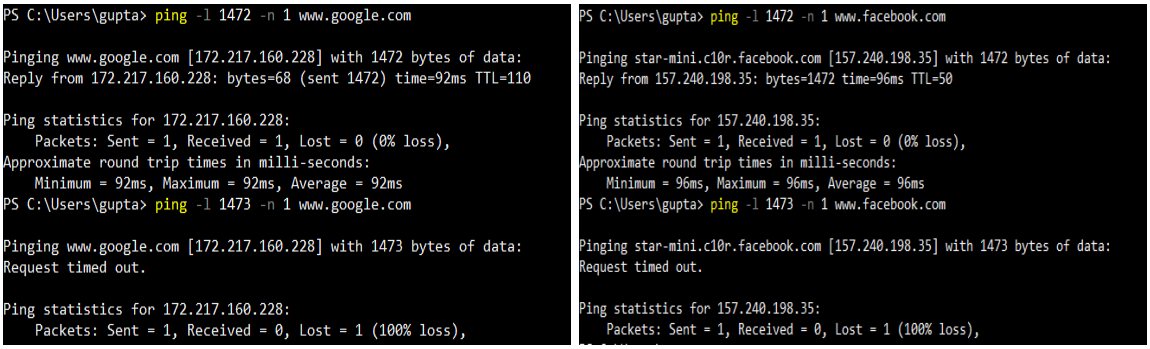


Figure 6: Maximum packet size that could be sent to www.google.com and www.facebook.com

Observation: Note that in Figure 5 and Figure 6, I am able to ping with packet size of 1472 bytes but not with 1473 bytes for all the three domains. For all the three domains, the maximum size of ping packet that I am able to send is 1472 bytes.
The maximum amount of data that can be placed in a single segment without fragmentation is limited by Maximum Transmission Unit (MTU). Most link-layer protocols have an MTU of 1500 bytes. The maximum amount of data that can be put in one segment (Maximum Segment Size) can be obtained be subtracting the size of header from MTU. The header size in this case appears to be of around 28 bytes.

4. **tracert**
tracert for **www.iitd.ac.in** with multiple ISPs

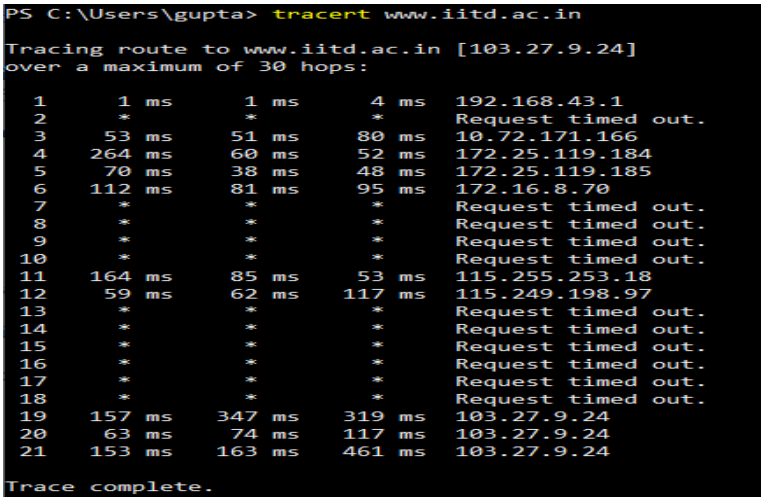


Figure 7: tracert for www.iitd.ac.in using Reliance Jio ISP

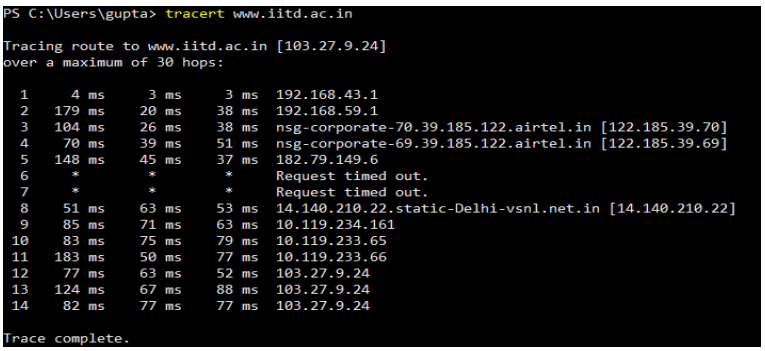


Figure 8: tracert for www.iitd.ac.in using Airtel ISP

Observations:

- The route taken to reach **www.iitd.ac.in** is different for the two ISPs.
- Many routers in the path were not responding on using the Reliance Jio ISP. When I switched to Airtel, no. of hops in the route decreased and more no. of routers started responding.

Figure 9: www.facebook.com is using IPv6 addresses by default with Reliance Jio ISP

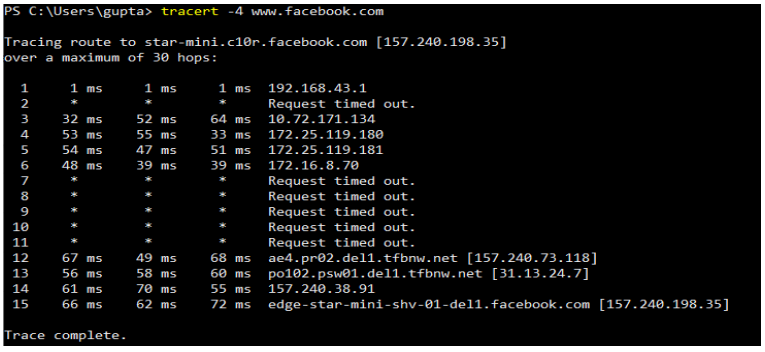


Figure 10: Using tracert -4 www.facebook.com forces tracert to use IPv4 addresses

Observations:

- With Reliance Jio ISP, **www.facebook.com** was using IPv6 addresses by default. To force it to use IPv4, I used the command **tracert -4 www.facebook.com**
- None of the IP addresses observed on the routes to different hosts were private.
- Some of the routers on the path were not replying.

Changes in the tracert for some of the missing routers:

- In case of Windows 10 OS, the only change that I could do to get reply from more routers is to change the ISP (see Figure 6 and Figure 7 above). But, in this case, the route taken itself changes.

- Increasing the wait time (by using -w flag) made some of the routers, that were not replying earlier, to respond.
- When I tried traceroute on Linux, few routers were replying on sending the default UDP packets. Sending ICMP packets (using -I flag) increased the number of routers that were replying.

Figure 11: On LINUX system - traceroute www.google.com (sending default UDP packets)

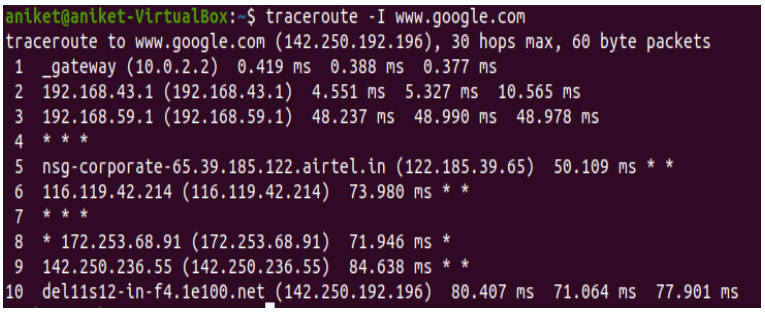


Figure 12: On LINUX system - traceroute -I www.google.com (sending ICMP packets)

2 Packet Analysis

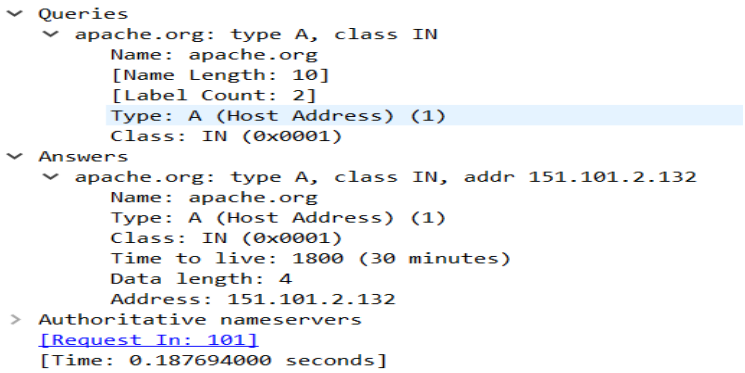
1. **dns** filter for packets grabbed while visiting **http://apache.org/**

   (a) There were multiple DNS requests and response.

   (b) There were 2 DNS queries of type A to get the IPv4 address and 1 DNS query of type AAAA to get the IPv6 address of the host (apache.org).

   (c) There were many other subsequent DNS queries for the different websites mentioned/used in the webpage.

- Time taken in the first type A request-response for apache.org host: 0.187694000 sec



- Time taken in the second type A request-response for apache.org host: 0.004123000 sec

```
Queries
  apache.org: type A, class IN
      Name: apache.org
      [Name Length: 10]
      [Label Count: 2]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
Answers
  apache.org: type A, class IN, addr 151.101.2.132
      Name: apache.org
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 1800 (30 minutes)
      Data length: 4
      Address: 151.101.2.132
  [Request In: 107]
  [Time: 0.004123000 seconds]
```

- Time taken in the type AAAA request-response for apache.org host: 0.098022000 sec

```
Queries
  apache.org: type AAAA, class IN
      Name: apache.org
      [Name Length: 10]
      [Label Count: 2]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
Answers
  apache.org: type AAAA, class IN, addr 2a04:4e42::644
      Name: apache.org
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      Time to live: 1800 (30 minutes)
      Data length: 16
      AAAA Address: 2a04:4e42::644
> Authoritative nameservers
  [Request In: 111]
  [Time: 0.098022000 seconds]
```

2. **http** filter for packets grabbed while visiting **http://apache.org/**

   - Total number of http packets grabbed = 64
   - Number of http request packets = 32
   - Number of http response packets = 32

   Structure of web-pages (based on observation on the packets grabbed)

   (a) It consists of a base HTML file which has multiple HTML elements.

   (b) The website, when visited, contains several images, link to several other websites, UI components etc.

   (c) The base HTML file generally has the relative paths to the CSS files, Javascript files, image files and other files if they are stored on the same server.

   (d) If the files required are not on the same server, then the HTML file contains the URLs that can be used to get to the server that contains the required file.

   Rendering of the web-page (based on observation on the packets grabbed)

   (a) The browser first made a DNS request (to any DNS server) to get the IP address of the server.

   (b) It then sent HTTP GET request to the server.

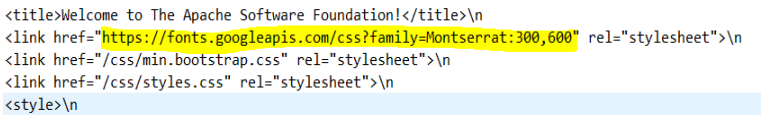
   (c) It received the base HTML file in response from the server.

   (d) It then sent multiple other HTTP GET request to the same server to get the files and images for whose the relative paths were mentioned in the base HTML page.

   (e) For the files that were not on the same server, browser first found the IP addresses of the servers (by making another DNS requests) that contain the files by using the URLs mentioned.

   (f) It then requested those servers for the required files and render those files after getting response.

3. Total time taken to download entire website (**http://apache.org/**)

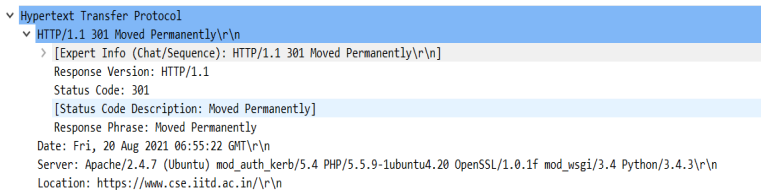


NOTE: To get the total time to download the entire website, we need the time when first DNS request is sent and when last content packet is received. Note that in this case, the base HTML file has reference to other hosts as well that use https protocol (see the figure above. It is a snap from the HTML file received in one of the HTTP responses. It contains reference to a host using HTTPS). The browser requests file/data from those hosts as well. The last content packet may or may not be an HTTP packet.

- Time at which first DNS request was sent - 7.728428 sec
- Approximate time at which the grabbing of packets stopped - 20.264863 sec
- Total time taken to download the website = 20.264863 - 7.728428 sec = 12.536435 sec

4. Packet trace for **http://www.cse.iitd.ac.in**

- There was almost no http traffic for http://www.cse.iitd.ac.in.

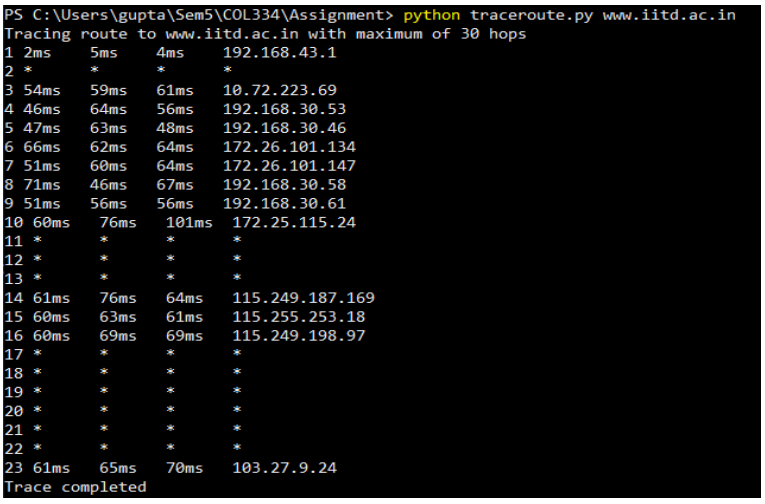


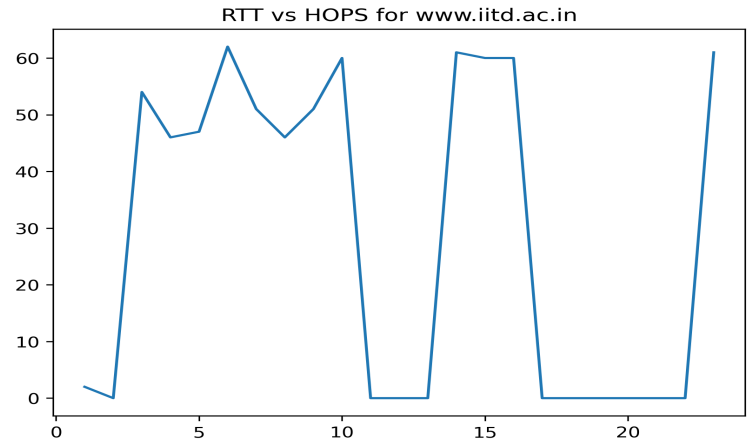
- It is because the host sent an http response stating that the website has been moved to https://www.cse.iitd.ac.in/. Thus, we are redirected to https://www.cse.iitd.ac.in/ which uses https and therfore it sends data packets encrypted with SSL which are not captured using http filter.
- In case of http://apache.org/, the host was using http protocol and was not encrypting the packets. Thus, it was easier in that case to grab the packets using http filter.

3 Traceroute Implementation using Ping

NOTE: I pinged each of the routers 3 times and took the minimum of the 3 rtt values for plotting, if the router replied and zero otherwise.

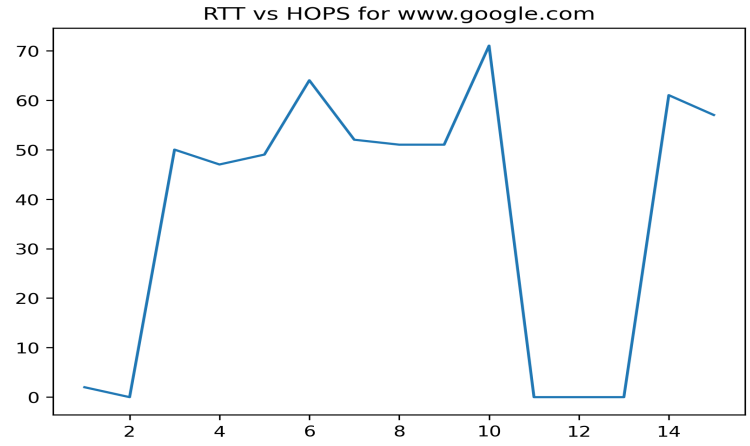
- Route tracing for www.iitd.ac.in





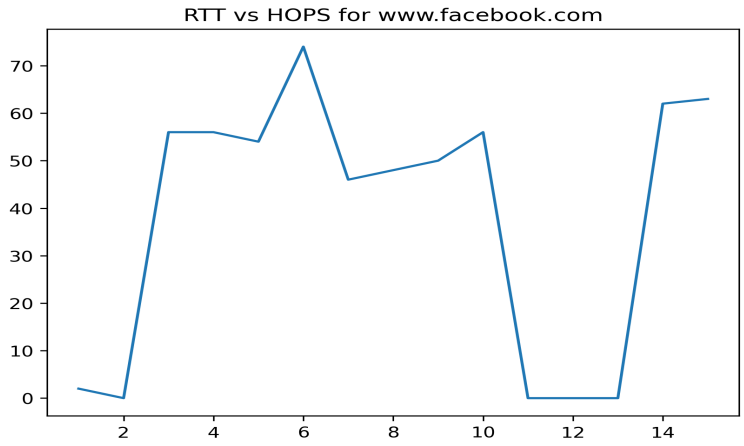
- Route tracing for www.google.com

```
PS C:\Users\gupta\Sem5\COL334\Assignment> python traceroute.py www.google.com
Tracing route to www.google.com with maximum of 30 hops
1 2ms    4ms    4ms    192.168.43.1
2 *      *      *      *
3 50ms   56ms   53ms   10.72.223.45
4 47ms   56ms   53ms   192.168.30.49
5 51ms   49ms   59ms   192.168.30.46
6 64ms   80ms   72ms   172.26.101.134
7 52ms   56ms   55ms   172.26.101.146
8 51ms   62ms   53ms   192.168.30.58
9 51ms   58ms   64ms   192.168.30.59
10 71ms   72ms   71ms   172.25.115.24
11 *      *      *      *
12 *      *      *      *
13 *      *      *      *
14 61ms   63ms   69ms   142.251.52.225
15 60ms   57ms   75ms   142.250.194.100
Trace completed
```



- Route tracing for www.facebook.com

```
PS C:\Users\gupta\Sem5\COL334\Assignment> python traceroute.py -h 30 -w 5000 www.facebook.com
Tracing route to www.facebook.com with maximum of 30 hops
1 2ms    4ms    4ms    192.168.43.1
2 *      *      *      *
3 56ms   60ms   68ms   10.72.223.45
4 56ms   67ms   72ms   192.168.30.53
5 54ms   63ms   57ms   192.168.30.48
6 75ms   76ms   74ms   172.26.101.134
7 46ms   62ms   56ms   172.26.101.146
8 48ms   54ms   50ms   192.168.30.54
9 50ms   59ms   54ms   192.168.30.55
10 56ms   83ms   70ms   172.25.115.24
11 *      *      *      *
12 *      *      *      *
13 *      *      *      *
14 62ms   76ms   64ms   173.252.67.147
15 63ms   75ms   73ms   157.240.198.35
Trace completed
```


RTT vs HOPS for www.facebook.com
70
60
50
40
30
20
10
0
2
4
6
8
10
12
14