Assignment 1

COL334

22nd August

Aman Kumar

2019CS10324

1. Networking Tools

a. Getting familiar with IP address

The IP address I found from the first service provider: (IIT Delhi WIFI)

```
Link-local IPv6 Address . . . . . : fe80::916a:a914:2c9e:10d8%6(Preferred)
IPv4 Address. . . . . . . . . . . : 10.184.15.253(Preferred)
```

And from the second service provider: (mobile hotspot)

```
IPv6 Address. . . . . . . . . . . : 2405:204:1010:39b5:916a:a914:2c9e:10d8(Preferred)
Temporary IPv6 Address. . . . . . : 2405:204:1010:39b5:6db1:e321:ef88:4579(Preferred)
Link-local IPv6 Address . . . . . : fe80::916a:a914:2c9e:10d8%6(Preferred)
IPv4 Address. . . . . . . . . . . : 192.168.43.72(Preferred)
```

We can clearly see both IP addresses are different. This happens because we use the public IP address of whatever network we are on. The IP address of the “My” laptop doesn’t belong to my laptop—it belongs to the network I am connected to. My laptop is just borrowing it for a while.

b. Effect of changing DNS server on IP addresses

The IP address associated with www.google.com and www.facebook.com are:

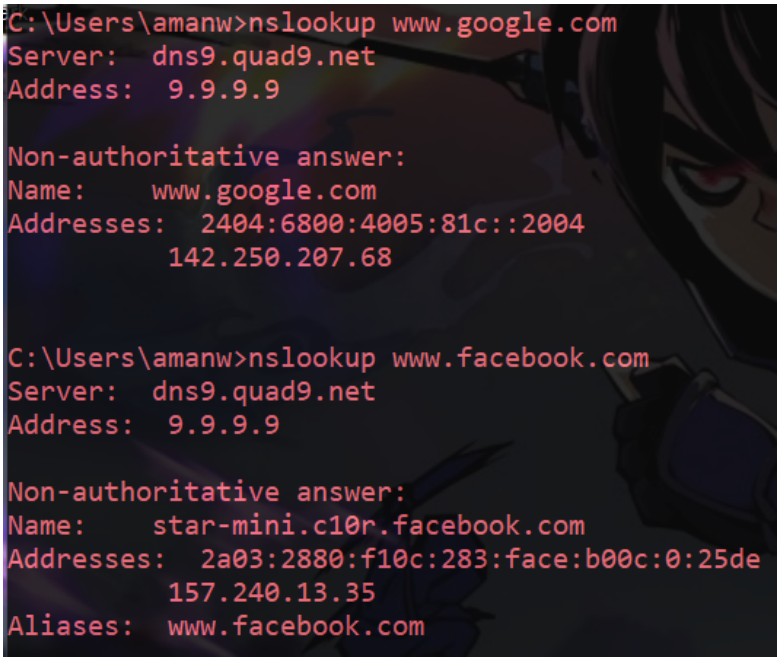
```
C:\Users\amanw>nslookup www.google.com
Server:  dns1.cc.iitd.ac.in
Address:  10.10.2.2

Non-authoritative answer:
Name:    www.google.com.ac.in
Addresses:  ::ffff:146.112.61.110
          146.112.61.110


C:\Users\amanw>nslookup www.facebook.com
Server:  dns1.cc.iitd.ac.in
Address:  10.10.2.2

Non-authoritative answer:
Name:    www.facebook.com.ac.in
Addresses:  ::ffff:146.112.61.110
          146.112.61.110
```

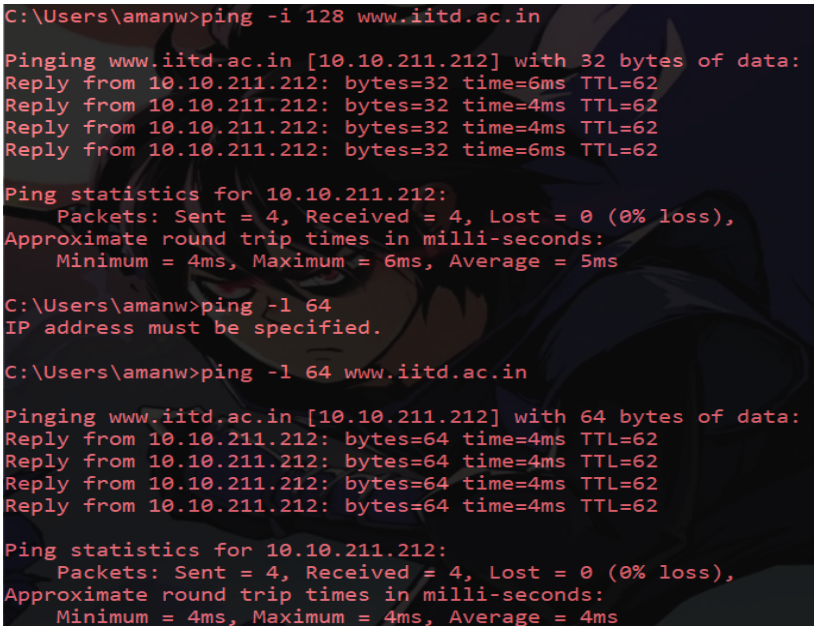
After changing the DNS server to “9.9.9.9”:



We get different addresses for the various DNS servers. This happens because many websites use multiple IP addresses (distributing the load on multiple servers) and a DNS server is a dictionary that store addresses associated with any website. Thus different DNS servers can store different addresses.

c. Pinging IP address with different packet sizes and TLL values

Pinging www.iitd.ac.in:



```
C:\Users\amanw>ping -l 103200 www.iitd.ac.in
Bad value for option -l, valid range is from 0 to 65500.

C:\Users\amanw>ping -l 65500 www.iitd.ac.in

Pinging www.iitd.ac.in [10.10.211.212] with 65500 bytes of data:
Reply from 10.10.211.212: bytes=65500 time=18ms TTL=62
Reply from 10.10.211.212: bytes=65500 time=84ms TTL=62
Reply from 10.10.211.212: bytes=65500 time=13ms TTL=62
Reply from 10.10.211.212: bytes=65500 time=14ms TTL=62

Ping statistics for 10.10.211.212:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 84ms, Average = 32ms
```

www.iitd.ac.in can handle the maximum possible packet size by my OS(65500 bytes). But in the case of www.google.com, and www.facebook.com it can take a total packet size of 1472 bytes. Snapshots are attached below:

```
C:\Users\amanw>ping -l 1472 www.google.com

Pinging www.google.com [142.250.194.228] with 1472 bytes of data:
Reply from 142.250.194.228: bytes=68 (sent 1472) time=6ms TTL=118
Reply from 142.250.194.228: bytes=68 (sent 1472) time=7ms TTL=118
Reply from 142.250.194.228: bytes=68 (sent 1472) time=6ms TTL=118
Reply from 142.250.194.228: bytes=68 (sent 1472) time=6ms TTL=118

Ping statistics for 142.250.194.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 7ms, Average = 6ms

C:\Users\amanw>ping -l 1473 www.google.com

Pinging www.google.com [142.250.194.228] with 1473 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 142.250.194.228:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\Users\amanw>ping -l 1473 www.facebook.com

Pinging star-mini.c10r.facebook.com [157.240.16.35] with 1473 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 157.240.16.35:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\amanw>ping -l 1472 www.facebook.com

Pinging star-mini.c10r.facebook.com [157.240.16.35] with 1472 bytes of data:
Reply from 157.240.16.35: bytes=1472 time=30ms TTL=54
Reply from 157.240.16.35: bytes=1472 time=27ms TTL=54
Reply from 157.240.16.35: bytes=1472 time=29ms TTL=54
Reply from 157.240.16.35: bytes=1472 time=27ms TTL=54

Ping statistics for 157.240.16.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 27ms, Maximum = 30ms, Average = 28ms
```

Maximum packet size depend on routers through which the packet travel. Different routers have different packet size limit. The absolute limitation on TCP packet size is 64K (65535 bytes). The MTU

(Maximum Transmission Unit) for Ethernet, for instance, is 1500 bytes. That's why we arre seeing different result for different website.

The minimum TTL for www.facebook.com is 11.

```
C:\Users\amanw>ping -i 11 www.facebook.com

Pinging star-mini.c10r.facebook.com [157.240.16.35] with 32 bytes of data:
Reply from 157.240.16.35: bytes=32 time=28ms TTL=54
Reply from 157.240.16.35: bytes=32 time=27ms TTL=54
Reply from 157.240.16.35: bytes=32 time=28ms TTL=54
Reply from 157.240.16.35: bytes=32 time=27ms TTL=54

Ping statistics for 157.240.16.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 27ms, Maximum = 28ms, Average = 27ms

C:\Users\amanw>ping -i 10 www.facebook.com

Pinging star-mini.c10r.facebook.com [157.240.16.35] with 32 bytes of data:
Reply from 173.252.67.69: TTL expired in transit.
Reply from 173.252.67.69: TTL expired in transit.
Reply from 173.252.67.69: TTL expired in transit.
Reply from 173.252.67.69: TTL expired in transit.

Ping statistics for 157.240.16.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

The minimum TTL for www.iitd.ac.in is 3:

```
C:\Users\amanw>ping -i 3 www.iitd.ac.in

Pinging www.iitd.ac.in [10.10.211.212] with 32 bytes of data:
Reply from 10.10.211.212: bytes=32 time=5ms TTL=62
Reply from 10.10.211.212: bytes=32 time=4ms TTL=62
Reply from 10.10.211.212: bytes=32 time=4ms TTL=62
Reply from 10.10.211.212: bytes=32 time=3ms TTL=62

Ping statistics for 10.10.211.212:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 5ms, Average = 4ms

C:\Users\amanw>ping -i 2 www.iitd.ac.in

Pinging www.iitd.ac.in [10.10.211.212] with 32 bytes of data:
Reply from 10.254.236.18: TTL expired in transit.
Reply from 10.254.236.18: TTL expired in transit.
Reply from 10.254.236.18: TTL expired in transit.
Reply from 10.254.236.18: TTL expired in transit.

Ping statistics for 10.10.211.212:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

The minimum TTL for www.google.com is 9:

```
C:\Users\amanw>ping -i 8 www.google.com

Pinging www.google.com [142.250.194.228] with 32 bytes of data:
Reply from 142.251.52.215: TTL expired in transit.
Reply from 142.251.52.215: TTL expired in transit.
Reply from 142.251.52.215: TTL expired in transit.
Reply from 142.251.52.215: TTL expired in transit.

Ping statistics for 142.250.194.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\amanw>ping -i 9 www.google.com

Pinging www.google.com [142.250.194.228] with 32 bytes of data:
Reply from 142.250.194.228: bytes=32 time=6ms TTL=118
Reply from 142.250.194.228: bytes=32 time=7ms TTL=118
Reply from 142.250.194.228: bytes=32 time=8ms TTL=118
Reply from 142.250.194.228: bytes=32 time=8ms TTL=118

Ping statistics for 142.250.194.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 8ms, Average = 7ms
```

d. Tracerouting www.iitd.ac.in

Tracerouting using IIT Delhi WIFI:

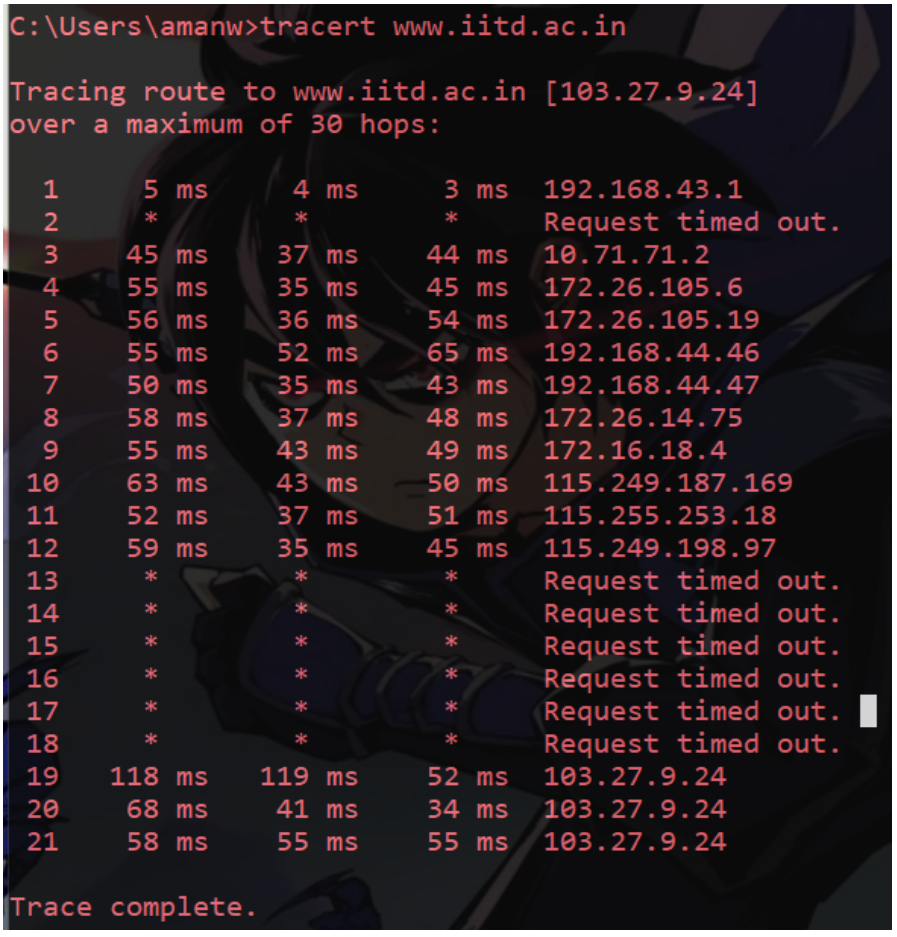
```
C:\Users\amanw>tracert www.iitd.ac.in

Tracing route to www.iitd.ac.in [10.10.211.212]
over a maximum of 30 hops:

  1     4 ms     4 ms     3 ms  10.184.0.14
  2     5 ms     4 ms     5 ms  10.254.236.18
  3     4 ms     3 ms     4 ms  www.iitd.ac.in [10.10.211.212]

Trace complete.
```

Tracerouting using mobile hotspot(Airtel 4G):



```
C:\Users\amanw>tracert www.iitd.ac.in

Tracing route to www.iitd.ac.in [103.27.9.24]
over a maximum of 30 hops:

  1     5 ms     4 ms     3 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3    45 ms    37 ms    44 ms  10.71.71.2
  4    55 ms    35 ms    45 ms  172.26.105.6
  5    56 ms    36 ms    54 ms  172.26.105.19
  6    55 ms    52 ms    65 ms  192.168.44.46
  7    50 ms    35 ms    43 ms  192.168.44.47
  8    58 ms    37 ms    48 ms  172.26.14.75
  9    55 ms    43 ms    49 ms  172.16.18.4
 10    63 ms    43 ms    50 ms  115.249.187.169
 11    52 ms    37 ms    51 ms  115.255.253.18
 12    59 ms    35 ms    45 ms  115.249.198.97
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19   118 ms   119 ms    52 ms  103.27.9.24
 20    68 ms    41 ms    34 ms  103.27.9.24
 21    58 ms    55 ms    55 ms  103.27.9.24

Trace complete.
```

Observations:

- In case of mine, I am getting only IPV4 IP addresses.
- Asterisk (*) is in place of time taken in which IP address is taking too much time to response(Request timed out)
- Different route form different network provider.
- IP address of www.iitd.ac.in is also different because of different DNS server of different network provider.

2. Packet Analysis

DNS responses for http://apache.org:

dns contains apache

No.	Time	Source	Destination	Protocol	Length	Info
279	39.078213	10.184.15.253	10.10.2.2	DNS	70	Stand
280	39.105372	10.10.2.2	10.184.15.253	DNS	287	Stand
365	39.417935	10.184.15.253	10.10.2.2	DNS	77	Stand
439	39.444430	10.10.2.2	10.184.15.253	DNS	315	Stand

a. Time taken for the DNS request-response to complete is 39.444 - 39.078 = 0.366s

http responses for http://apache.org:

http contains apache

No.	Time	Source	Destination	Protocol	Length	Info
284	39.114871	10.184.15.253	151.101.2.132	HTTP	496	GET / HTTP/1.1
337	39.394332	10.184.15.253	151.101.2.132	HTTP	410	GET /css/min.boo
342	39.401685	10.184.15.253	151.101.2.132	HTTP	403	GET /css/styles
353	39.412904	10.184.15.253	151.101.2.132	HTTP	450	GET /img/asf-est
358	39.413996	10.184.15.253	151.101.2.132	HTTP	446	GET /img/support
359	39.414664	10.184.15.253	151.101.2.132	HTTP	475	GET /img/trillic
362	39.415598	10.184.15.253	151.101.2.132	HTTP	483	GET /img/trillic
436	39.443217	10.184.15.253	151.101.2.132	HTTP	396	GET /js/jquery-1
437	39.444051	10.184.15.253	151.101.2.132	HTTP	389	GET /js/bootstra
440	39.444456	10.184.15.253	151.101.2.132	HTTP	389	GET /js/slidesho
459	39.460582	10.184.15.253	151.101.2.132	HTTP	489	GET /img/trillic
460	39.460976	10.184.15.253	151.101.2.132	HTTP	483	GET /img/trillic
475	39.472512	10.184.15.253	151.101.2.132	HTTP	443	GET /img/2020-re
493	39.486268	10.184.15.253	151.101.2.132	HTTP	441	GET /img/communi
568	39.506543	10.184.15.253	151.101.2.132	HTTP	446	GET /img/the-apa
618	39.596722	10.184.15.253	151.101.2.132	HTTP	441	GET /img/Apache(
654	39.627483	10.184.15.253	151.101.2.132	HTTP	451	GET /logos/res/p
658	39.634111	10.184.15.253	151.101.2.132	HTTP	455	GET /logos/res/p
672	39.638817	151.101.2.132	10.184.15.253	HTTP	421	HTTP/1.1 200 OK
684	39.645600	151.101.2.132	10.184.15.253	HTTP	60	HTTP/1.1 200 OK
714	39.661793	10.184.15.253	151.101.2.132	HTTP	453	GET /logos/res/c
716	39.662242	10.184.15.253	151.101.2.132	HTTP	455	GET /logos/res/1
745	39.672475	151.101.2.132	10.184.15.253	HTTP	189	HTTP/1.1 200 OK
756	39.674876	151.101.2.132	10.184.15.253	HTTP	414	HTTP/1.1 200 OK
858	40.309245	10.184.15.253	142.250.193.46	HTTP	421	GET /cse.js?cx=(
866	40.561423	10.184.15.253	151.101.2.132	HTTP	462	GET /fonts/glypl
1758	41.324800	10.184.15.253	142.250.193.46	HTTP	405	GET /adsense/sea
1775	41.361653	10.184.15.253	216.58.196.110	HTTP	445	GET /generate_20
2103	42.212357	10.184.15.253	151.101.2.132	HTTP	444	GET /favicons/fa
2111	42.229819	10.184.15.253	151.101.2.132	HTTP	450	GET /favicons/fa

b. Total 30 http requests are generated.

c. Total time take to load the entire webpage is 42.229 - 39.078 = 3.151s

http responses for http://www.cse.iitd.ac.in:

http

No.	Time	Source	Destination	Protocol	Length	Info
237	17.626249	10.184.15.253	10.208.20.4	HTTP	504	GET / HTTP/1.1
240	17.629899	10.208.20.4	10.184.15.253	HTTP	261	HTTP/1.1 301 Moved Permanently (text/html)

We can see that there are only two request/responses (1 request, 1 response). This is because the http page http://www.cse.iitd.ac.in is ewsiewxrws ro https webpage and thus all the content object request are visible in the TLS/SSL filter and there is no http traffic. This can be seen clearly in the second response “301 Moved Permanently”.

3. Implementing Traceroute in python

My python code is printing IP addresses of all the hops and generating a plot of RTT(round trip time) vs hop number. Plot got saved in output.png.
Output for www.google.com:

```
amanw@DESKTOP-NO3631B MINGW64 ~/Desktop/C++
$ python -u "/c/Users/amanw/Desktop/C++/traceR.py"
Enter the domain name: www.google.com
IP addresses of all the hops:
10.184.0.14
10.255.1.34
10.119.233.65
10.1.207.69
10.119.234.162
72.14.194.160
108.170.251.97
142.251.52.215
142.250.194.228
```