COL334 – Assignment 1

Satyam Kumar Modi – 2019CS50448

1. (a) IP Address when connected to home router : 192.168.29.252
IP Address when connected to mobile hotspot: 192.168.43.252
The IP Address reported are private IP addresses allocated by the router used.

(b) IP address for www.google.com
i. 127.0.0.53 – 172.217.27.164
ii. 8.8.8.8 – 142.250.193.196
iii. 8.8.4.4 – 172.217.166.196

IP address for www.facebook.com
i. 127.0.0.53 – 157.240.239.35
ii. 8.8.8.8 – 157.240.239.35
iii. 8.8.4.4 – 157.240.239.35

(c) Maximum size that could be sent using ping was 1500 bytes(including header size) to www.iitd.ac.in
This was irrespective of the dns server used. We noted that few routers had no response to the ping request. The reason might be that they may have dropped the arrived ICMP packets. May be the routers don't want to display any details

(d) Traceroute for iitd.ac.in
i. Router

traceroute to iitd.ac.in (103.27.9.24), 64 hops max
1 192.168.29.1 7.417ms 2.601ms 6.078ms
2 10.2.232.1 6.232ms 4.668ms 5.051ms
3 172.26.12.225 6.036ms 7.669ms 6.341ms
4 192.168.86.238 5.506ms 192.168.86.240 9.772ms 192.168.86.238 5.315ms
5 172.26.104.52 9.157ms 9.689ms 5.004ms
6 172.26.104.147 10.053ms 9.636ms 9.566ms
7 192.168.85.52 9.966ms 192.168.85.54 10.815ms 192.168.85.52 7.650ms
8 192.168.85.55 5.880ms 9.911ms 9.866ms
9 172.16.24.29 27.113ms 24.235ms 24.285ms
10 172.26.12.230 24.570ms 24.382ms 25.046ms
11 172.16.4.199 24.121ms 20.651ms 19.693ms
12 172.16.4.115 38.139ms 38.902ms 40.401ms
13 172.16.2.48 34.996ms 33.504ms 36.222ms
14 115.255.253.18 46.247ms 50.315ms 48.457ms
15 115.249.198.97 50.175ms 49.457ms 50.175ms
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 103.27.9.24 172.990ms 108.686ms 201.969ms

ii. Mobile Hotspot

traceroute to iitd.ac.in (103.27.9.24), 64 hops max

```
1   *  192.168.43.1  4.006ms  3.441ms
2   *  *  *
3   10.72.46.83  265.473ms  204.645ms  204.765ms
4   172.25.44.183  204.671ms  204.828ms  204.637ms
5   172.26.55.98  204.765ms  *  273.430ms
6   172.25.7.6  204.609ms  204.692ms  204.498ms
7   *  *  *
8   *  *  *
9   *  *  *
10   *  *  *
11   *  *  *
12   *  *  *
13   *  *  *
14   115.249.198.97  219.506ms  204.590ms  204.759ms
15   *  *  *
16   *  *  *
17   *  *  *
18   *  *  *
19   *  *  *
20   *  *  *
21   103.27.9.24  222.111ms  204.594ms  204.643ms
```

The asterisk seen can be attributed to the fact that those routers don't respond to such packets and may be they don't want to disclose their routing details.

Use -4 flag to force it to use Ipv4 address.

One can change the responding time by using the "-w" flag in traceroute command. Also, we can use the "-I" flag in case few router's firewall block the UDP packets arrived (used in default case) to force it to use ICMP packets.

One can alos notice the changing address at some hop, this was due to the fact that the packet might have chosen some other route.

2. (a) 0.0353 s

(b) 30 packets. Individual requests is sent for each object while requesting for the webpage. First, the css and the required js files are requested, then comes the image and html file.

(c) 1.6457s

(d) No, there were no http request packets found in case of http://cse.iitd.ac.in as the webpage used https protocol which is encrypted with ssl. It was easier for http://apache.org because it used no security layer on its top, so sniffing the http packets were easier.

One can view the https packet data using "ssl" filter but that will be in encrypted form.