COL334 Computer Networks

Assignment - 1

Aryan Jain, 2019CS10334

Q1) Networking Tools

a) Find the IP address of your machine. Try connecting to different service providers and notice the changes, if any, in the IP address of your machine.

i) IP of my system when connected to the internet using an Airtel wired connection
=> 192.168.2.7

ii) IP of my system when connected to the internet using an Airtel Hotpot
=> 192.168.8.25

iii) IP of my system when connected to the internet using a Jio Hotspot
=> 192.168.43.152

b) Find the IP address associated with www.google.com and www.facebook.com using nslookup. Change the DNS server (look for open DNS servers on the web) to use in the command and see how the IP address of the above domains change.

i) google.com

- DNS : ns1.google.com IP : 142.250.193.238
- DNS : ns2.google.com IP : 142.250.193.238
- DNS : 1.1.1.1 IP : 142.250.192.238 (non-authoritative)
- DNS : 192.168.2.1 IP : 142.250.193.238 (non-authoritative)
- DNS : b.ns.facebook.com IP REFUSED

ii) facebook.com

- DNS : ns1.google.com IP : REFUSED
- DNS : b.ns.facebook.com IP : 157.240.198.35
- DNS : 1.1.1.1 IP : 157.240.198.35 (non-authoritative)
- DNS : 192.168.2.1 IP : 157.240.198.35 (non-authoritative)

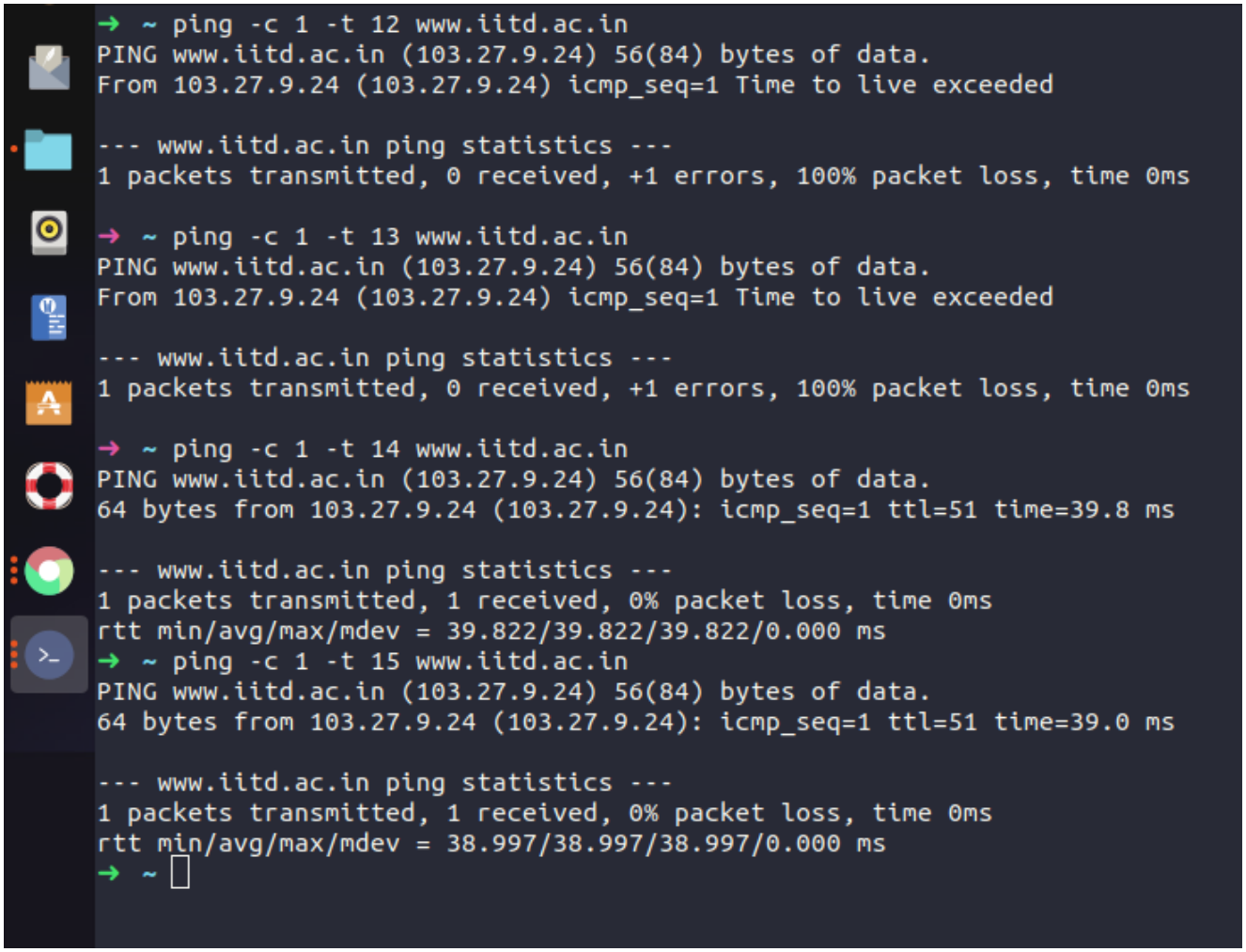
c) ping the IP address of www.iitd.ac.in. Send the ping packets with different packet sizes, TTL values, etc. What is the maximum size of ping packets that you are able to send? Is this size the same for the domains mentioned in part (b)?

i) www.iitd.ac.in

- The maximum size of ping packets that we are able to send is 1464 bytes, which translates to 1472 bytes when we include the ICMP header.

```
→ ~ ping -c 1 -s 1460 www.iitd.ac.in
PING www.iitd.ac.in (103.27.9.24) 1460(1488) bytes of data.
1468 bytes from 103.27.9.24 (103.27.9.24): icmp_seq=1 ttl=51 time=40.7 ms

--- www.iitd.ac.in ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 40.665/40.665/40.665/0.000 ms
→ ~
→ ~
→ ~ ping -c 1 -s 1464 www.iitd.ac.in
PING www.iitd.ac.in (103.27.9.24) 1464(1492) bytes of data.
1472 bytes from 103.27.9.24 (103.27.9.24): icmp_seq=1 ttl=51 time=40.4 ms

--- www.iitd.ac.in ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 40.407/40.407/40.407/0.000 ms
→ ~
→ ~
→ ~ ping -c 1 -s 1465 www.iitd.ac.in
PING www.iitd.ac.in (103.27.9.24) 1465(1493) bytes of data.

--- www.iitd.ac.in ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

→ ~
→ ~
→ ~ ping -c 1 -s 1470 www.iitd.ac.in
PING www.iitd.ac.in (103.27.9.24) 1470(1498) bytes of data.

--- www.iitd.ac.in ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

→ ~
```

- The minimum TTL which returns a successful response is 14. Which means that the packet makes 14 hops when going from my system to the iitd server.



```
➜  ~ ping -c 1 -t 12 www.iitd.ac.in
PING www.iitd.ac.in (103.27.9.24) 56(84) bytes of data.
From 103.27.9.24 (103.27.9.24) icmp_seq=1 Time to live exceeded

--- www.iitd.ac.in ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms

➜  ~ ping -c 1 -t 13 www.iitd.ac.in
PING www.iitd.ac.in (103.27.9.24) 56(84) bytes of data.
From 103.27.9.24 (103.27.9.24) icmp_seq=1 Time to live exceeded

--- www.iitd.ac.in ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms

➜  ~ ping -c 1 -t 14 www.iitd.ac.in
PING www.iitd.ac.in (103.27.9.24) 56(84) bytes of data.
64 bytes from 103.27.9.24 (103.27.9.24): icmp_seq=1 ttl=51 time=39.8 ms

--- www.iitd.ac.in ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 39.822/39.822/39.822/0.000 ms
➜  ~ ping -c 1 -t 15 www.iitd.ac.in
PING www.iitd.ac.in (103.27.9.24) 56(84) bytes of data.
64 bytes from 103.27.9.24 (103.27.9.24): icmp_seq=1 ttl=51 time=39.0 ms

--- www.iitd.ac.in ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 38.997/38.997/38.997/0.000 ms
➜  ~
```

ii) www.google.com

- The maximum size of ping packets that we are able to send is 68 bytes, which translates to 76 bytes when we include the ICMP header.

```
➜  ~ ping -c 1 -s 68 www.google.com
PING www.google.com (142.250.77.132) 68(96) bytes of data.
76 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_sec

--- www.google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 50.341/50.341/50.341/0.000 ms
➜  ~ ping -c 1 -s 69 www.google.com
PING www.google.com (142.250.77.132) 69(97) bytes of data.

--- www.google.com ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

- The minimum TTL which returns a successful response is 11. Which means that the packet makes 11 hops when going from my system to the iitd server.

```
➜  ~ ping -c 1 -t 12 www.google.com
PING www.google.com (142.250.77.164) 56(84) bytes of data.
64 bytes from maa05s17-in-f4.1e100.net (142.250.77.164): icmp_seq=1 ttl=117

--- www.google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 51.988/51.988/51.988/0.000 ms
➜  ~ ping -c 1 -t 11 www.google.com
PING www.google.com (142.250.77.164) 56(84) bytes of data.

--- www.google.com ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

iii) www.facebook.com

- The maximum size of ping packets that we are able to send is 1464 bytes, which translates to 1472 bytes when we include the ICMP header.

```
➜  ~ ping -c 1 -s 1464 www.facebook.com
PING star-mini.c10r.facebook.com (157.240.16.35) 1464(1492) bytes of data.
1472 bytes from edge-star-mini-shv-01-bom1.facebook.com (157.240.16.35): icmp_seq=

--- star-mini.c10r.facebook.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 38.215/38.215/38.215/0.000 ms
➜  ~ ping -c 1 -s 1465 www.facebook.com
PING star-mini.c10r.facebook.com (157.240.16.35) 1465(1493) bytes of data.

--- star-mini.c10r.facebook.com ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

- The minimum TTL which returns a successful response is 8. Which means that the packet makes 8 hops when going from my system to the iitd server.

```
➜  ~ ping -c 1 -t 8 www.facebook.com
PING star-mini.c10r.facebook.com (157.240.198.35) 56(84) bytes of data.

--- star-mini.c10r.facebook.com ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

➜  ~ ping -c 1 -t 9 www.facebook.com
PING star-mini.c10r.facebook.com (157.240.198.35) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-01-del1.facebook.com (157.240.198.35): icmp_seq=1 ttl

--- star-mini.c10r.facebook.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 11.691/11.691/11.691/0.000 ms
➜  ~
```

d) Run traceroute via two or more service providers for www.iitd.ac.in. If your ISP blocks packets on the path to www.iitd.ac.in ..... to reply?

I use the command `$ traceroute -4 -I www.iitd.ac.in` to obtain the below results

→ I use the flags -4 to force IPv4 tracerouting

→ I use the -I flag to use icmp packets instead of udp as it leads to responses from much more routers compared to udp.

i) Airtel Ethernet:

- We observe that routers at positions 2, 7, 8, 9, 10, 11 do not acknowledge the packets in the given time period

```
➜  ~ traceroute -4 -I www.iitd.ac.in
traceroute to www.iitd.ac.in (103.27.9.24), 30 hops max, 60 byte packets
 1  _gateway (192.168.2.1)  2.317 ms  3.062 ms  3.727 ms
 2  * * *
 3  abts-north-dynamic-255.111.57.27.airtelbroadband.in (27.57.111.255)  10.818
ms  11.671 ms  12.554 ms
 4  nsg-corporate-57.77.186.122.airtel.in (122.186.77.57)  15.243 ms  15.493 ms
  15.958 ms
 5  182.79.153.91 (182.79.153.91)  22.871 ms  23.080 ms  23.257 ms
 6  115.110.232.173.static.Delhi.vsnl.net.in (115.110.232.173)  24.574 ms  14.8
59 ms  16.192 ms
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  103.27.9.24 (103.27.9.24)  38.138 ms  37.933 ms  38.037 ms
13  103.27.9.24 (103.27.9.24)  38.406 ms  37.900 ms  38.032 ms
14  103.27.9.24 (103.27.9.24)  37.616 ms  37.974 ms  38.043 ms
➜  ~
```

ii) Jio hotspot:

- We observe that routers at positions 2, 7, 8, 9, 10, 11 do not acknowledge the packets in the given time period

```
traceroute to www.iitd.ac.in (103.27.9.24), 30 hops max, 60 byte packets
 1  _gateway (192.168.43.1)  6.379 ms  6.673 ms  7.386 ms
 2  * * *
 3  10.72.91.18 (10.72.91.18)  46.295 ms  46.292 ms  46.288 ms
 4  192.168.48.157 (192.168.48.157)  46.288 ms  46.285 ms 192.168.48.153 (192.16
8.48.153)  45.424 ms
 5  172.26.103.229 (172.26.103.229)  45.416 ms  46.275 ms  46.271 ms
 6  172.26.102.179 (172.26.102.179)  47.679 ms  37.379 ms  37.348 ms
 7  172.25.107.231 (172.25.107.231)  37.423 ms  29.006 ms  39.223 ms
 8  172.25.107.230 (172.25.107.230)  38.748 ms  38.714 ms  39.430 ms
 9  172.16.26.5 (172.16.26.5)  45.457 ms  45.453 ms  45.449 ms
10  172.16.26.5 (172.16.26.5)  44.314 ms  43.287 ms  43.271 ms
11  115.110.210.37.static-Delhi.vsnl.net.in (115.110.210.37)  44.135 ms  44.123
ms  35.606 ms
12  * * *
13  14.140.210.22.static-Delhi-vsnl.net.in (14.140.210.22)  52.961 ms  48.214 ms
  47.956 ms
14  * * *
15  * * *
16  * * *
17  103.27.9.24 (103.27.9.24)  55.345 ms  38.050 ms  39.873 ms
18  103.27.9.24 (103.27.9.24)  46.864 ms  46.986 ms  35.796 ms
19  103.27.9.24 (103.27.9.24)  30.055 ms  39.585 ms  39.110 ms
```

Q2) Packet Analysis

a) Type A DNS requests correspond to the IPv4 address of the server, whereas Type AAAA DNS requests correspond to the IPv6 address.

Filter used : (dns.qry.name == "apache.org")&& (dns.flags == 0x8180)&&(dns)&&(!icmp)

(dns.qry.name == "apache.org")&& (dns.flags == 0x8180)&&(dns)&&(!icmp)

No.	Time	Source	Destination	Protocol	Length	DNS Response Time	Info
10	6.083…	8.8.8.8	192.168…	DNS	97	0.01875…	Standard query respons…
11	6.088…	8.8.8.8	192.168…	DNS	109	0.02362…	Standard query respons…
12	6.117…	192.168…	192.168…	DNS	109	0.05284…	Standard query respons…
14	6.130…	192.168…	192.168…	DNS	97	0.06590…	Standard query respons…
1…	6.411…	192.168…	192.168…	DNS	109	0.02318…	Standard query respons…

IPv4 DNS request-response time : 0.0188 seconds

IPv6 DNS request-response time : 0.0236 seconds

b) HTTP requests are found using the filter : (http.request.method == "GET")

(http.request.method == "GET")

No.	Time	Source	Destination	Protocol	Length	DNS Response Time	Info
18	6.14630…	192.168.2.7	151.101.2.…	HTTP	395		GET / HTTP/1.1
61	6.26249…	192.168.2.7	151.101.2.…	HTTP	359		GET /css/min.bootstrap.css HTTP/1.1
62	6.26283…	192.168.2.7	151.101.2.…	HTTP	352		GET /css/styles.css HTTP/1.1
135	6.36107…	192.168.2.7	151.101.2.…	HTTP	338		GET /js/bootstrap.js HTTP/1.1
145	6.37661…	192.168.2.7	151.101.2.…	HTTP	345		GET /js/jquery-2.1.1.min.js HTTP/1.1
150	6.37962…	192.168.2.7	151.101.2.…	HTTP	338		GET /js/slideshow.js HTTP/1.1
308	6.52736…	192.168.2.7	151.101.2.…	HTTP	367		GET /logos/res/xmlgraphics/default.png HTTP/1.1
309	6.52741…	192.168.2.7	151.101.2.…	HTTP	399		GET /img/trillions-and-trillions/trillions-and-trilli…
310	6.52744…	192.168.2.7	151.101.2.…	HTTP	351		GET /img/community.jpg HTTP/1.1
311	6.52747…	192.168.2.7	151.101.2.…	HTTP	360		GET /img/asf-estd-1999-logo.jpg HTTP/1.1
312	6.52749…	192.168.2.7	151.101.2.…	HTTP	393		GET /img/trillions-and-trillions/apache-everywhere-th…
396	6.57664…	192.168.2.7	142.250.19…	HTTP	370		GET /cse.js?cx=005703438322411770421:5mgshgrgx2u HTTP…
614	6.62519…	192.168.2.7	151.101.2.…	HTTP	365		GET /logos/res/incubator/default.png HTTP/1.1
1903	6.79240…	192.168.2.7	151.101.2.…	HTTP	442		GET /fonts/glyphicons-halflings-regular.woff2 HTTP/1.…
1904	6.79243…	192.168.2.7	151.101.2.…	HTTP	353		GET /img/2020-report.jpg HTTP/1.1
1905	6.79249…	192.168.2.7	151.101.2.…	HTTP	356		GET /img/support-apache.jpg HTTP/1.1
1906	6.79250…	192.168.2.7	151.101.2.…	HTTP	385		GET /img/trillions-and-trillions/why-apache-thumbail.…
1907	6.79253…	192.168.2.7	151.101.2.…	HTTP	361		GET /logos/res/flink/default.png HTTP/1.1
1908	6.79256…	192.168.2.7	151.101.2.…	HTTP	356		GET /img/the-apache-way.jpg HTTP/1.1
2228	6.87298…	192.168.2.7	151.101.2.…	HTTP	393		GET /img/trillions-and-trillions/apache-innovation-th…
2360	6.88705…	192.168.2.7	151.101.2.…	HTTP	351		GET /img/ApacheCon.jpg HTTP/1.1
2369	6.88776…	192.168.2.7	151.101.2.…	HTTP	361		GET /logos/res/toree/default.png HTTP/1.1
2379	6.88929…	192.168.2.7	151.101.2.…	HTTP	363		GET /logos/res/griffin/default.png HTTP/1.1
2532	6.94861…	192.168.2.7	142.250.19…	HTTP	354		GET /adsense/search/async-ads.js HTTP/1.1
2846	7.00730…	192.168.2.7	142.250.19…	HTTP	354		GET /adsense/search/async-ads.js HTTP/1.1
2852	7.02126…	192.168.2.7	216.58.196…	HTTP	355		GET /generate_204 HTTP/1.1
3166	7.19280…	192.168.2.7	151.101.2.…	HTTP	362		GET /favicons/favicon-194x194.png HTTP/1.1
3167	7.19321…	192.168.2.7	151.101.2.…	HTTP	360		GET /favicons/favicon-16x16.png HTTP/1.1

28 GET requests are made while loading the page https://apache.org

From looking at the http packets it can be inferred that all images, stylesheets or files are stored as external links to files in the source code, and separate HTTP GET requests are made for every external file that is accessed or loaded.

Also, if we look at the response packets for these GET requests, if the files being returned are too large, it is sent as multiple packets and those packets are labelled as CONTINUATION.

c) First DNS query made at : 6.065 seconds

Last content packet delivered at : 7.272 seconds

Time taken to download the entire page : 1.208 seconds

d) We are not able to find much HTTP traffic when accessing “http://www.cse.iitd.ac.in/” because the cse iitd website now uses https. We can see the first HTTP request which tries to load the website, but we receive a 301 response and are redirected to the HTTPS website. From this point onward the website is loaded using OCSP packets which take care of the TLS protocols. On the other hand, “http://apache.org” uses HTTP packets, so we can easily access these packets.

http

No.	Time	Source	Destination	Protocol	Length	Info
63	3.5784…	192.168.2…	103.27.9.…	HT…	403	GET / HTTP/1.1
67	3.6168…	103.27.9.…	192.168.2…	HT…	809	HTTP/1.1 301 Mo…
113	3.7934…	192.168.2…	23.55.106…	OC…	487	Request
116	3.8291…	23.55.106…	192.168.2…	OC…	954	Response
1789	4.4823…	192.168.2…	172.217.1…	OC…	490	[TCP Previous s…
2032	4.5896…	172.217.1…	192.168.2…	OC…	767	Response
2840	5.0746…	192.168.2…	172.217.1…	OC…	490	Request
2853	5.1872…	172.217.1…	192.168.2…	OC…	767	Response
3012	5.3669…	192.168.2…	172.217.1…	OC…	491	Request
3045	5.3977…	192.168.2…	172.217.1…	OC…	491	Request
3051	5.4127…	192.168.2…	172.217.1…	OC…	491	Request
3056	5.4742…	172.217.1…	192.168.2…	OC…	768	Response
3067	5.4934…	172.217.1…	192.168.2…	OC…	768	Response
3074	5.5043…	172.217.1…	192.168.2…	OC…	768	Response

Q3) Implement Traceroute using Ping

Run the code using “python3 tracert.py” and then input the url, maximum permitted hops and timeout time when prompted.

```
➜ asgn1 python3 tracert.py
Enter server name or ip: www.iitd.ac.in
Enter maximum number of permitted (leave blank for default of 30 hops):
IP : 192.168.2.1    hops to this server : 1    round_trip_time : 1.28
This server does not respond
IP : 27.57.111.255    hops to this server : 3    round_trip_time : 6.10
IP : 122.186.77.57    hops to this server : 4    round_trip_time : 7.14
IP : 182.79.153.91    hops to this server : 5    round_trip_time : 14.5
IP : 115.110.232.173    hops to this server : 6    round_trip_time : 14.0
This server does not respond
This server does not respond
This server does not respond
This server does not respond
This server does not respond
IP : 103.27.9.24    hops to this server : 12    round_trip_time : 32.7
IP : 103.27.9.24    hops to this server : 13    round_trip_time : 32.9
IP : 103.27.9.24:    hops to this server : 14    round_trip_time : 32.3
➜ asgn1
```