COL334 - Computer Networks

Abhishek kumar
2019CS10458
`Assignment 1`

August 22, 2021

1. Networking Tools

(a) Using normal Broadband, IP address is 192.168.1.19
Using my mobile hotspot, IP address is 192.168.43.83
This ip address is the private ip address assigned by ISP inside the same network. For getting the public ip address of the network, we can use **curl -s -4 https://icanhazip.com**.
The public IP for:
wifi -> 117.214.106.18
mobile hotspot -> 223.187.152.120

(b)
i. Using my default local DNS server
   - IP address of www.google.com - 142.250.193.100
   - IP address of www.facebook.com - 157.240.228.35

ii. Using Google Public DNS (8.8.8.8)
   - IP address of www.google.com - 172.217.163.196
   - IP address of www.facebook.com - 157.240.1.35

iii. Using Cloudfare DNS (1.1.1.1)
   - IP address of www.google.com - 216.58.196.164
   - IP address of www.facebook.com - 31.13.79.35

Different DNS server has different ip to domain record. So different DNS server provide different ip for same domain name. Each domain has multiple ip address to prevent traffic.

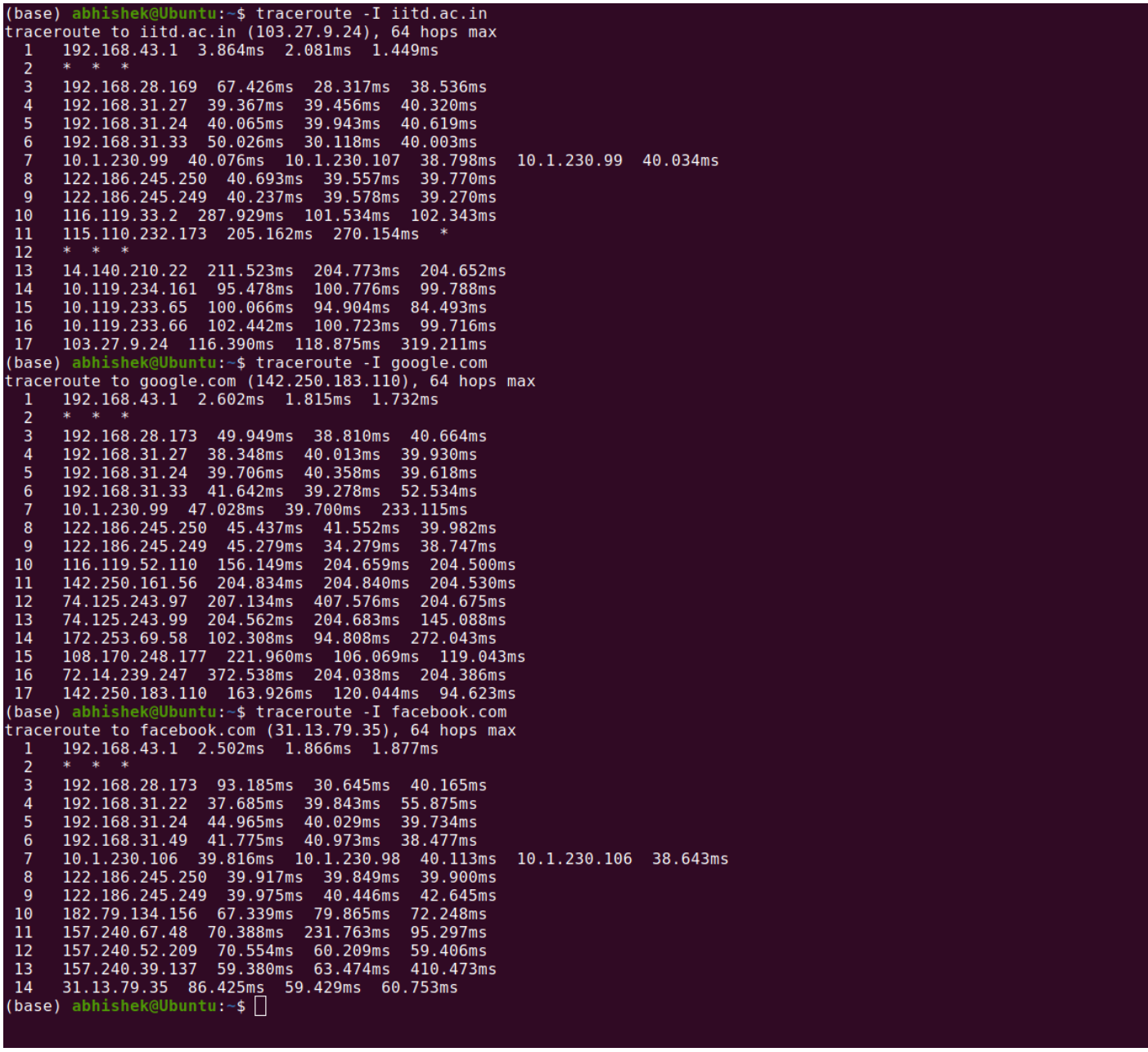
(c)
- www.iitd.ac.in
  i. Maximum size of packet sent = 34552 (34552+28) with rtt = 80 ms. Normally ping fragments the data so maximum size can be greater than MTU. We need to clearly specify the command if we don't want to fragment the data sent. With "-M do" (Don't fragment the data) flag, the maximum size of packet sent was 1432 (1432+28) bytes.
  ii. Minimum ttl so that packet was successfully sent = 21
- google.com
  i. Maximum size of packet sent = 68 (68+28) with rtt = 53 ms
  ii. Minimum ttl so that packet was successfully sent = 13
- facebook.com
  i. Maximum size of packet sent = 1432 (1432+28) with rtt = 52.5 ms
  ii. Minimum ttl so that packet was successfully sent = 16

The maximum packet size that was successfully sent was different for different domains and the minimum ttl required for successful transmission was also different for different domains.The +28 bytes denotes the header of the packet sent.

(d) While using broadband
- When udp packets were sent no router other than gateway router was responding. So I used icmp packets. Most of the routers responded to while some were not responding.
- The routers to path iitd.ac.in has more non-responding routers as compared to google.com and facebook.com
- In ubuntu, traceroute automatically uses IPv4 address. There is another variant traceroute6

which uses IPv6 addresses. When tried traceroute6 with google.com, it showed the network is unreachable.
- For the unrespoding router, we can use find its address using ping with ttl value set to the number of hop which it took during traceroute to get to that router.

While using mobile hotspot
- The number of unresponding routers was very less (one or two).



```
(base) abhishek@Ubuntu:~$ traceroute -I iitd.ac.in
traceroute to iitd.ac.in (103.27.9.24), 64 hops max
  1   192.168.43.1  3.864ms  2.081ms  1.449ms
  2   *  *  *
  3   192.168.28.169  67.426ms  28.317ms  38.536ms
  4   192.168.31.27  39.367ms  39.456ms  40.320ms
  5   192.168.31.24  40.065ms  39.943ms  40.619ms
  6   192.168.31.33  50.026ms  30.118ms  40.003ms
  7   10.1.230.99  40.076ms  10.1.230.107  38.798ms  10.1.230.99  40.034ms
  8   122.186.245.250  40.693ms  39.557ms  39.770ms
  9   122.186.245.249  40.237ms  39.578ms  39.270ms
 10   116.119.33.2  287.929ms  101.534ms  102.343ms
 11   115.110.232.173  205.162ms  270.154ms  *
 12   *  *  *
 13   14.140.210.22  211.523ms  204.773ms  204.652ms
 14   10.119.234.161  95.478ms  100.776ms  99.788ms
 15   10.119.233.65  100.066ms  94.904ms  84.493ms
 16   10.119.233.66  102.442ms  100.723ms  99.716ms
 17   103.27.9.24  116.390ms  118.875ms  319.211ms
(base) abhishek@Ubuntu:~$ traceroute -I google.com
traceroute to google.com (142.250.183.110), 64 hops max
  1   192.168.43.1  2.602ms  1.815ms  1.732ms
  2   *  *  *
  3   192.168.28.173  49.949ms  38.810ms  40.664ms
  4   192.168.31.27  38.348ms  40.013ms  39.930ms
  5   192.168.31.24  39.706ms  40.358ms  39.618ms
  6   192.168.31.33  41.642ms  39.278ms  52.534ms
  7   10.1.230.99  47.028ms  39.700ms  233.115ms
  8   122.186.245.250  45.437ms  41.552ms  39.982ms
  9   122.186.245.249  45.279ms  34.279ms  38.747ms
 10   116.119.52.110  156.149ms  204.659ms  204.500ms
 11   142.250.161.56  204.834ms  204.840ms  204.530ms
 12   74.125.243.97  207.134ms  407.576ms  204.675ms
 13   74.125.243.99  204.562ms  204.683ms  145.088ms
 14   172.253.69.58  102.308ms  94.808ms  272.043ms
 15   108.170.248.177  221.960ms  106.069ms  119.043ms
 16   72.14.239.247  372.538ms  204.038ms  204.386ms
 17   142.250.183.110  163.926ms  120.044ms  94.623ms
(base) abhishek@Ubuntu:~$ traceroute -I facebook.com
traceroute to facebook.com (31.13.79.35), 64 hops max
  1   192.168.43.1  2.502ms  1.866ms  1.877ms
  2   *  *  *
  3   192.168.28.173  93.185ms  30.645ms  40.165ms
  4   192.168.31.22  37.685ms  39.843ms  55.875ms
  5   192.168.31.24  44.965ms  40.029ms  39.734ms
  6   192.168.31.49  41.775ms  40.973ms  38.477ms
  7   10.1.230.106  39.816ms  10.1.230.98  40.113ms  10.1.230.106  38.643ms
  8   122.186.245.250  39.917ms  39.849ms  39.900ms
  9   122.186.245.249  39.975ms  40.446ms  42.645ms
 10   182.79.134.156  67.339ms  79.865ms  72.248ms
 11   157.240.67.48  70.388ms  231.763ms  95.297ms
 12   157.240.52.209  70.554ms  60.209ms  59.406ms
 13   157.240.39.137  59.380ms  63.474ms  410.473ms
 14   31.13.79.35  86.425ms  59.429ms  60.753ms
(base) abhishek@Ubuntu:~$
```

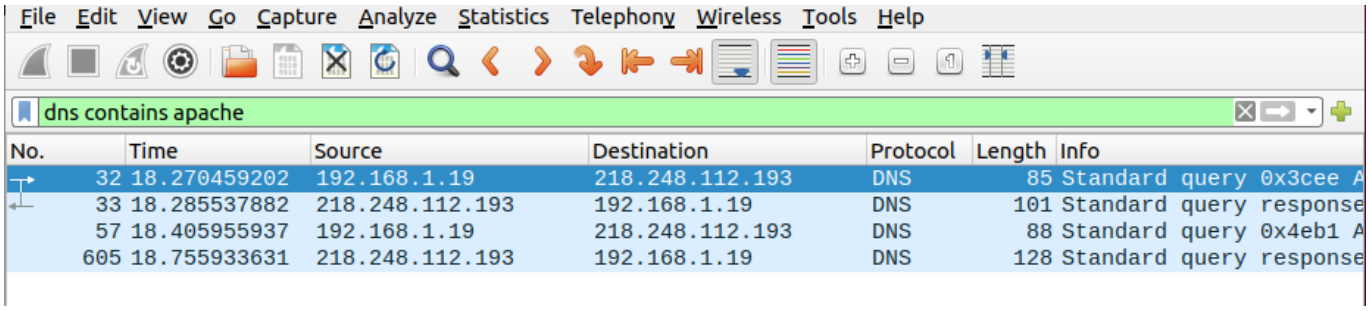
Figure 1: With Mobile hotspot

```
(base) abhishek@Ubuntu:~$ traceroute -I iitd.ac.in
traceroute to iitd.ac.in (103.27.9.24), 64 hops max
  1   192.168.1.1  1.159ms  1.154ms  1.093ms
  2   117.214.104.1  2.241ms  3.848ms  1.769ms
  3   218.248.100.205  2.059ms  1.893ms  1.887ms
  4   218.248.115.134  3.050ms  2.368ms  1.609ms
  5   *  *  *
  6   *  *  *
  7   *  *  *
  8   *  *  *
  9   *  *  *
 10   *  *  *
 11   *  *  *
 12   10.200.116.137  53.922ms  53.647ms  55.062ms
 13   172.24.18.17  55.294ms  55.829ms  54.476ms
 14   10.255.221.35  55.151ms  54.508ms  57.323ms
 15   *  *  *
 16   *  *  *
 17   *  *  *
 18   *  *  *
 19   103.27.9.24  75.603ms  73.511ms  73.644ms
(base) abhishek@Ubuntu:~$ traceroute -I google.com
traceroute to google.com (142.250.67.46), 64 hops max
  1   192.168.1.1  1.126ms  1.040ms  0.937ms
  2   117.214.104.1  1.783ms  1.672ms  2.109ms
  3   218.248.100.205  1.602ms  2.030ms  1.795ms
  4   218.248.111.98  6.058ms  5.747ms  5.548ms
  5   *  *  *
  6   *  *  *
  7   142.250.160.182  55.424ms  54.460ms  53.398ms
  8   172.253.69.189  52.775ms  52.792ms  52.552ms
  9   108.170.251.107  50.886ms  51.359ms  51.836ms
 10   142.250.63.117  58.497ms  51.530ms  57.516ms
 11   72.14.239.11  52.222ms  53.135ms  52.611ms
 12   74.125.242.129  55.284ms  53.245ms  53.642ms
 13   142.250.228.83  55.799ms  57.170ms  53.092ms
 14   142.250.67.46  52.338ms  52.725ms  52.589ms
(base) abhishek@Ubuntu:~$ traceroute -I facebook.com
traceroute to facebook.com (157.240.1.35), 64 hops max
  1   192.168.1.1  1.218ms  1.576ms  1.164ms
  2   117.214.104.1  1.840ms  1.895ms  4.192ms
  3   218.248.100.205  1.628ms  1.866ms  1.911ms
  4   218.248.111.94  3.354ms  2.139ms  2.795ms
  5   *  *  *
  6   *  *  *
  7   157.240.67.178  17.167ms  38.301ms  29.134ms
  8   129.134.104.213  17.701ms  26.815ms  21.666ms
  9   157.240.38.197  15.588ms  15.745ms  15.306ms
 10   157.240.1.35  15.834ms  16.220ms  16.100ms
(base) abhishek@Ubuntu:~$
```

Figure 2: With Wifi

2. Packet Analysis using Wireshark

(a) The time taken for DNS request-response to complete was 0.485 seconds.



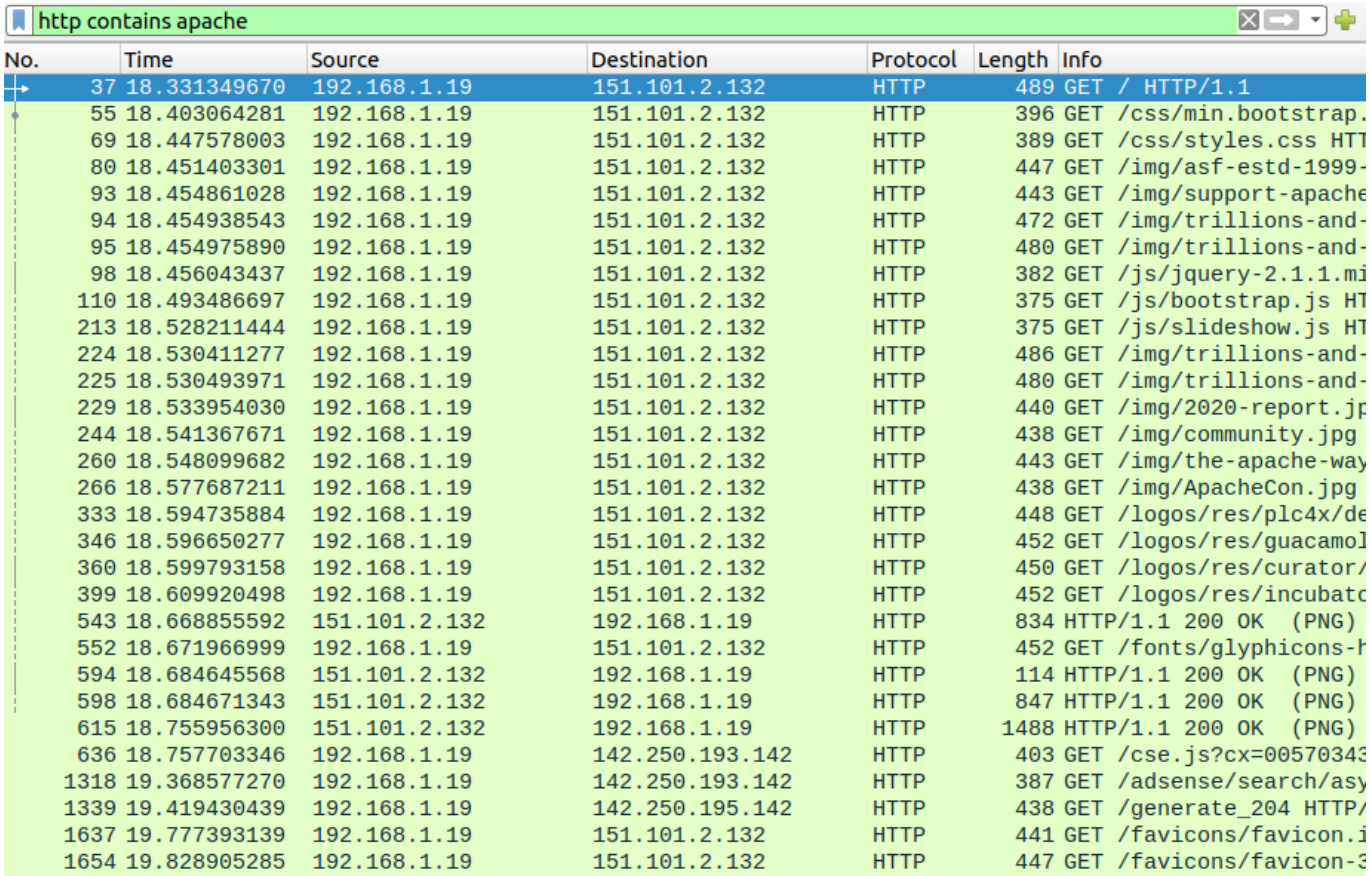
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns contains apache

No.	Time	Source	Destination	Protocol	Length	Info
32	18.270459202	192.168.1.19	218.248.112.193	DNS	85	Standard query 0x3cee A
33	18.285537882	218.248.112.193	192.168.1.19	DNS	101	Standard query response
57	18.405955937	192.168.1.19	218.248.112.193	DNS	88	Standard query 0x4eb1 A
605	18.755933631	218.248.112.193	192.168.1.19	DNS	128	Standard query response

Figure 3: DNS request-response http://www.apache.org/

(b) The number of http requests sent was approximately 30. The server sends objects of a webpages in chunks not complete webpage at one time. The browser renders as soon as an object arrives and leave spaces for those objects which is yet to arrive. As soon as the remaining objects arrive they are put at the respective places in webpage. It was also observed that text, css and javascript(essential) files were received earlier and images and videos (heavy files) were received later.



http contains apache

No.	Time	Source	Destination	Protocol	Length	Info
37	18.331349670	192.168.1.19	151.101.2.132	HTTP	489	GET / HTTP/1.1
55	18.403064281	192.168.1.19	151.101.2.132	HTTP	396	GET /css/min.bootstrap.
69	18.447578003	192.168.1.19	151.101.2.132	HTTP	389	GET /css/styles.css HTT
80	18.451403301	192.168.1.19	151.101.2.132	HTTP	447	GET /img/asf-estd-1999-
93	18.454861028	192.168.1.19	151.101.2.132	HTTP	443	GET /img/support-apache
94	18.454938543	192.168.1.19	151.101.2.132	HTTP	472	GET /img/trillions-and-
95	18.454975890	192.168.1.19	151.101.2.132	HTTP	480	GET /img/trillions-and-
98	18.456043437	192.168.1.19	151.101.2.132	HTTP	382	GET /js/jquery-2.1.1.mi
110	18.493486697	192.168.1.19	151.101.2.132	HTTP	375	GET /js/bootstrap.js HT
213	18.528211444	192.168.1.19	151.101.2.132	HTTP	375	GET /js/slideshow.js HT
224	18.530411277	192.168.1.19	151.101.2.132	HTTP	486	GET /img/trillions-and-
225	18.530493971	192.168.1.19	151.101.2.132	HTTP	480	GET /img/trillions-and-
229	18.533954030	192.168.1.19	151.101.2.132	HTTP	440	GET /img/2020-report.jp
244	18.541367671	192.168.1.19	151.101.2.132	HTTP	438	GET /img/community.jpg
260	18.548099682	192.168.1.19	151.101.2.132	HTTP	443	GET /img/the-apache-way
266	18.577687211	192.168.1.19	151.101.2.132	HTTP	438	GET /img/ApacheCon.jpg
333	18.594735884	192.168.1.19	151.101.2.132	HTTP	448	GET /logos/res/plc4x/de
346	18.596650277	192.168.1.19	151.101.2.132	HTTP	452	GET /logos/res/guacamol
360	18.599793158	192.168.1.19	151.101.2.132	HTTP	450	GET /logos/res/curator/
399	18.609920498	192.168.1.19	151.101.2.132	HTTP	452	GET /logos/res/incubato
543	18.668855592	151.101.2.132	192.168.1.19	HTTP	834	HTTP/1.1 200 OK (PNG)
552	18.671966999	192.168.1.19	151.101.2.132	HTTP	452	GET /fonts/glyphicons-h
594	18.684645568	151.101.2.132	192.168.1.19	HTTP	114	HTTP/1.1 200 OK (PNG)
598	18.684671343	151.101.2.132	192.168.1.19	HTTP	847	HTTP/1.1 200 OK (PNG)
615	18.755956300	151.101.2.132	192.168.1.19	HTTP	1488	HTTP/1.1 200 OK (PNG)
636	18.757703346	192.168.1.19	142.250.193.142	HTTP	403	GET /cse.js?cx=00570343
1318	19.368577270	192.168.1.19	142.250.193.142	HTTP	387	GET /adsense/search/asy
1339	19.419430439	192.168.1.19	142.250.195.142	HTTP	438	GET /generate_204 HTTP/
1637	19.777393139	192.168.1.19	151.101.2.132	HTTP	441	GET /favicons/favicon.i
1654	19.828905285	192.168.1.19	151.101.2.132	HTTP	447	GET /favicons/favicon-3

Figure 4: HTTP request-response http://www.apache.org/

(c) The total time taken by webpage to load was 1.558 seconds.

(d) For http://www.cse.iitd.ac.in, when http filter was appplied there was a single response stating the 301 moved permanently. The http request of iitd uses https thus there was no traffic when

http filter was used. The traffic can be seen while using tls filter. www.apache.org uses both http and https thus there was a traffic in http for apache.org.

dns contains iitd

No.	Time	Source	Destination	Protocol	Length	Info
56	11.087641486	192.168.1.19	218.248.112.193	DNS	89	Standard query 0x1bd8 A
58	11.170093199	218.248.112.193	192.168.1.19	DNS	176	Standard query response

Figure 5: DNS request-response http://www.cse.iitd.ac.in/

http contains iitd

No.	Time	Source	Destination	Protocol	Length	Info
62	11.254366335	192.168.1.19	103.27.9.152	HTTP	493	GET / HTTP/1.1
64	11.339032145	103.27.9.152	192.168.1.19	HTTP	809	HTTP/1.1 301 Moved Perm

Figure 6: HTTP request-response http://www.cse.iitd.ac.in/

tls contains iitd

No.	Time	Source	Destination	Protocol	Length	Info
71	11.427273821	192.168.1.19	103.27.9.152	TLSv1.2	583	Client Hello
76	11.514213275	103.27.9.152	192.168.1.19	TLSv1.2	4162	Server Hello
78	11.515866048	103.27.9.152	192.168.1.19	TLSv1.2	445	Certificate, Server Key
101	11.888215693	192.168.1.19	103.27.9.152	TLSv1.2	594	Client Hello
102	11.888427586	192.168.1.19	103.27.9.152	TLSv1.2	594	Client Hello
103	11.888678168	192.168.1.19	103.27.9.152	TLSv1.2	594	Client Hello
111	11.892510178	192.168.1.19	103.27.9.152	TLSv1.2	594	Client Hello
112	11.892737808	192.168.1.19	103.27.9.152	TLSv1.2	594	Client Hello

Figure 7: TLS request-response http://www.cse.iitd.ac.in/

3. Implemetation of Traceroute

I have used ping command in ubuntu to get the route of website. Python is used to obtain the information and process the output to get the RTT value. I have used matplotlib library to plot the graph between the RTT value vs Hop Number. The command to run the file is-

pyhton3 traceroute.py <DomainName>

The output and Graph for google.com is shown below

```
(base) abhishek@Ubuntu:~/Course/SEM 5/COL334 - Computer Networks/Computer-Networ
ks/Assignments/Assignment 1$ python3 traceroute.py google.com
ip of Website (172.217.166.110)
1       192.168.1.1     2.82
2       117.214.104.1   1.89
3       218.248.100.205 2.21
4       218.248.115.134 2.89
6       No reply         0.0
7       No reply         0.0
7       142.250.160.182 49.3
8       74.125.37.131   48.5
9       74.125.244.196  66.6
10      209.85.250.56   46.5
11      172.253.66.106  49.3
12      72.14.239.59    54.5
13      74.125.242.129  49.7
14      74.125.252.215  46.4
15      172.217.166.110 48.9
(base) abhishek@Ubuntu:~/Course/SEM 5/COL334 - Computer Networks/Computer-Networ
ks/Assignments/Assignment 1$
```

Figure 8: Traceroute of google.com

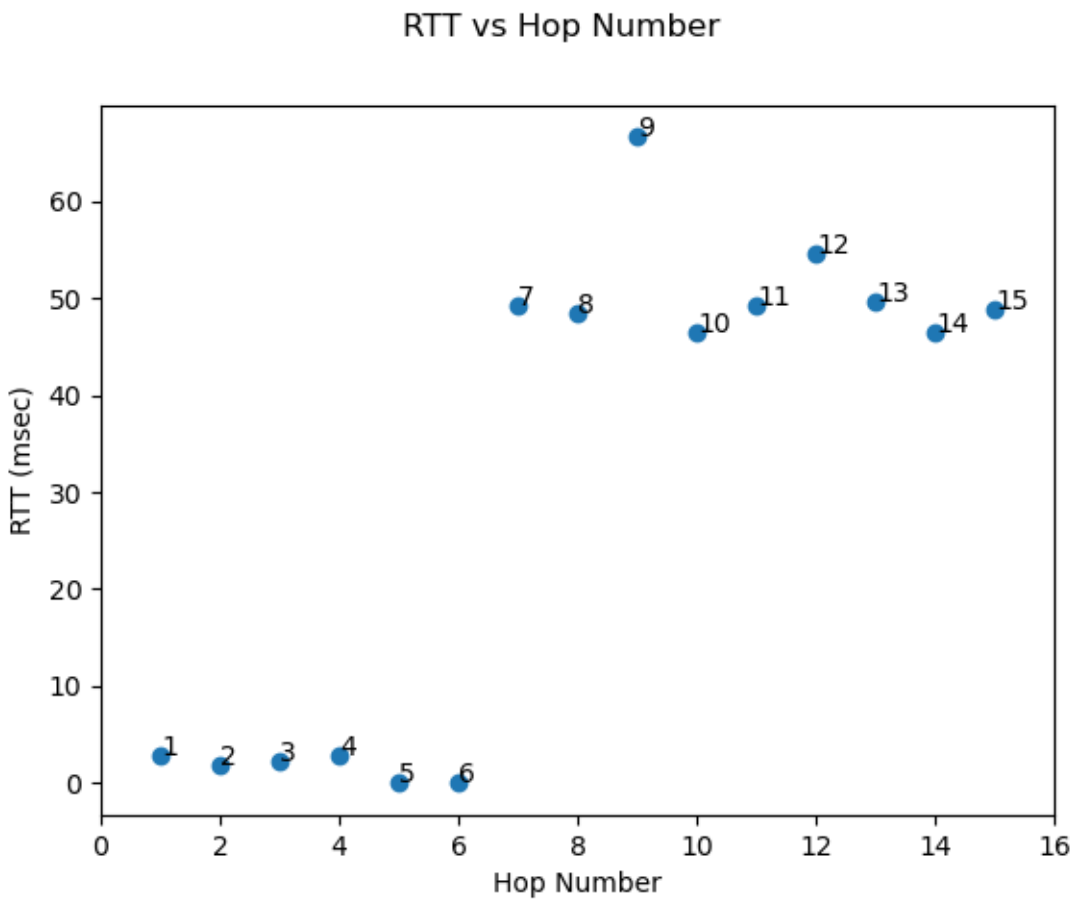


Figure 9: RTT vs Hop Number of google.com