COL 334 Assignment 1

Rayyan Shahid

August 2021

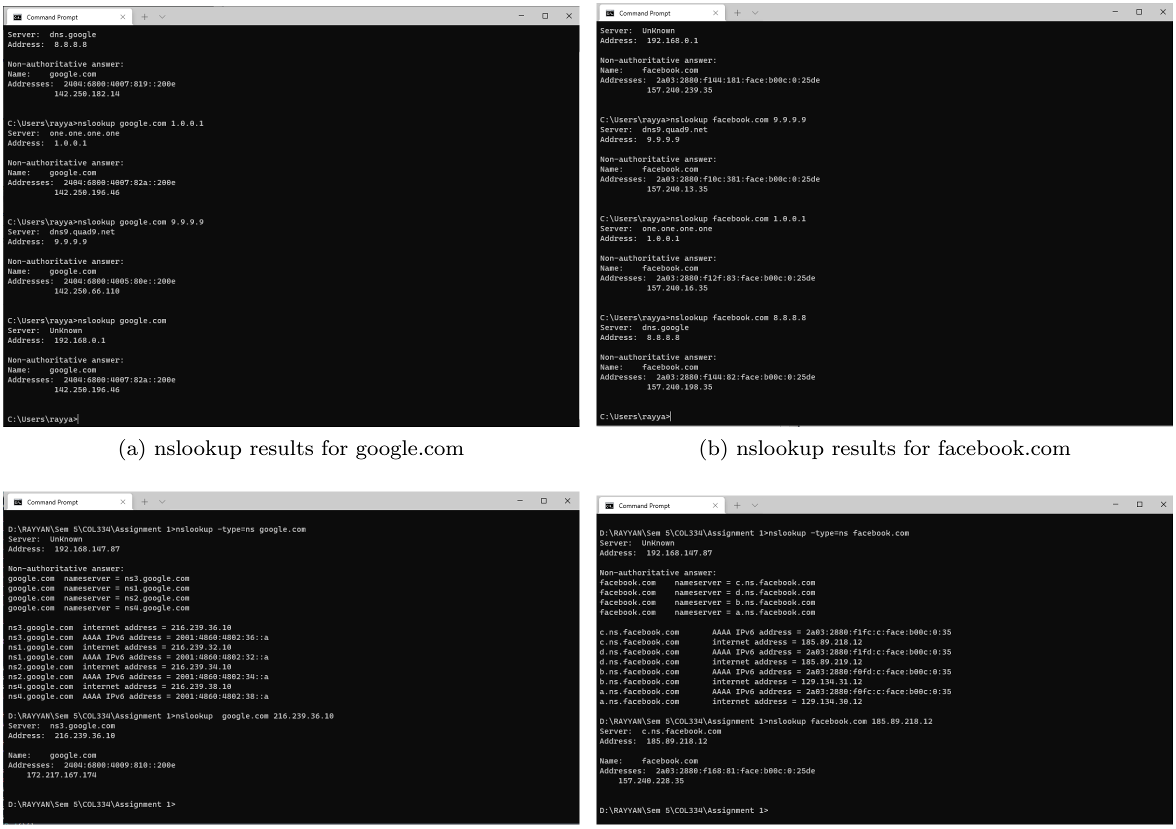
1. Networking Tools

a.

The public IPv4 address : 103.199.182.114 (RailWire), 27.61.109.43(Airtel)
The private IPv4 address : 192.168.147.218 (Airtel, Wireless LAN adapter Wi-Fi), 192.168.0.139 (RailWire, Ethernet adapter Ethernet), 192.168.0.218 (RailWire, Wireless LAN adapter Wi-Fi)

The public IP address changes when the ISP changes. The private IP addresses are assigned locally by the router for the different network interfaces connected to it. Thus, even for the same network interface (i.e Wireless LAN adapter Wi-Fi in the above case), the private IP addresses can be different for different ISPs/Network.

b.



```
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4007:819::200e
          142.250.182.14


C:\Users\rayya>nslookup google.com 1.0.0.1
Server:  one.one.one.one
Address:  1.0.0.1

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4007:82a::200e
          142.250.196.46


C:\Users\rayya>nslookup google.com 9.9.9.9
Server:  dns9.quad9.net
Address:  9.9.9.9

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4005:80e::200e
          142.250.66.110


C:\Users\rayya>nslookup google.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4007:82a::200e
          142.250.196.46


C:\Users\rayya>
```

(a) nslookup results for google.com

```
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    facebook.com
Addresses:  2a03:2880:f144:181:face:b00c:0:25de
          157.240.239.35


C:\Users\rayya>nslookup facebook.com 9.9.9.9
Server:  dns9.quad9.net
Address:  9.9.9.9

Non-authoritative answer:
Name:    facebook.com
Addresses:  2a03:2880:f10c:381:face:b00c:0:25de
          157.240.13.35


C:\Users\rayya>nslookup facebook.com 1.0.0.1
Server:  one.one.one.one
Address:  1.0.0.1

Non-authoritative answer:
Name:    facebook.com
Addresses:  2a03:2880:f12f:83:face:b00c:0:25de
          157.240.16.35


C:\Users\rayya>nslookup facebook.com 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    facebook.com
Addresses:  2a03:2880:f144:82:face:b00c:0:25de
          157.240.198.35


C:\Users\rayya>
```

(b) nslookup results for facebook.com

```
D:\RAYYAN\Sem 5\COL334\Assignment 1>nslookup -type=ns google.com
Server:  UnKnown
Address:  192.168.147.87

Non-authoritative answer:
google.com  nameserver = ns3.google.com
google.com  nameserver = ns1.google.com
google.com  nameserver = ns2.google.com
google.com  nameserver = ns4.google.com

ns3.google.com  internet address = 216.239.36.10
ns3.google.com  AAAA IPv6 address = 2001:4860:4802:36::a
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  AAAA IPv6 address = 2001:4860:4802:32::a
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  AAAA IPv6 address = 2001:4860:4802:34::a
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  AAAA IPv6 address = 2001:4860:4802:38::a

D:\RAYYAN\Sem 5\COL334\Assignment 1>nslookup  google.com 216.239.36.10
Server:  ns3.google.com
Address:  216.239.36.10

Name:    google.com
Addresses:  2404:6800:4009:810::200e
    172.217.167.174


D:\RAYYAN\Sem 5\COL334\Assignment 1>
```

(c) nslookup authoritative results for google.com

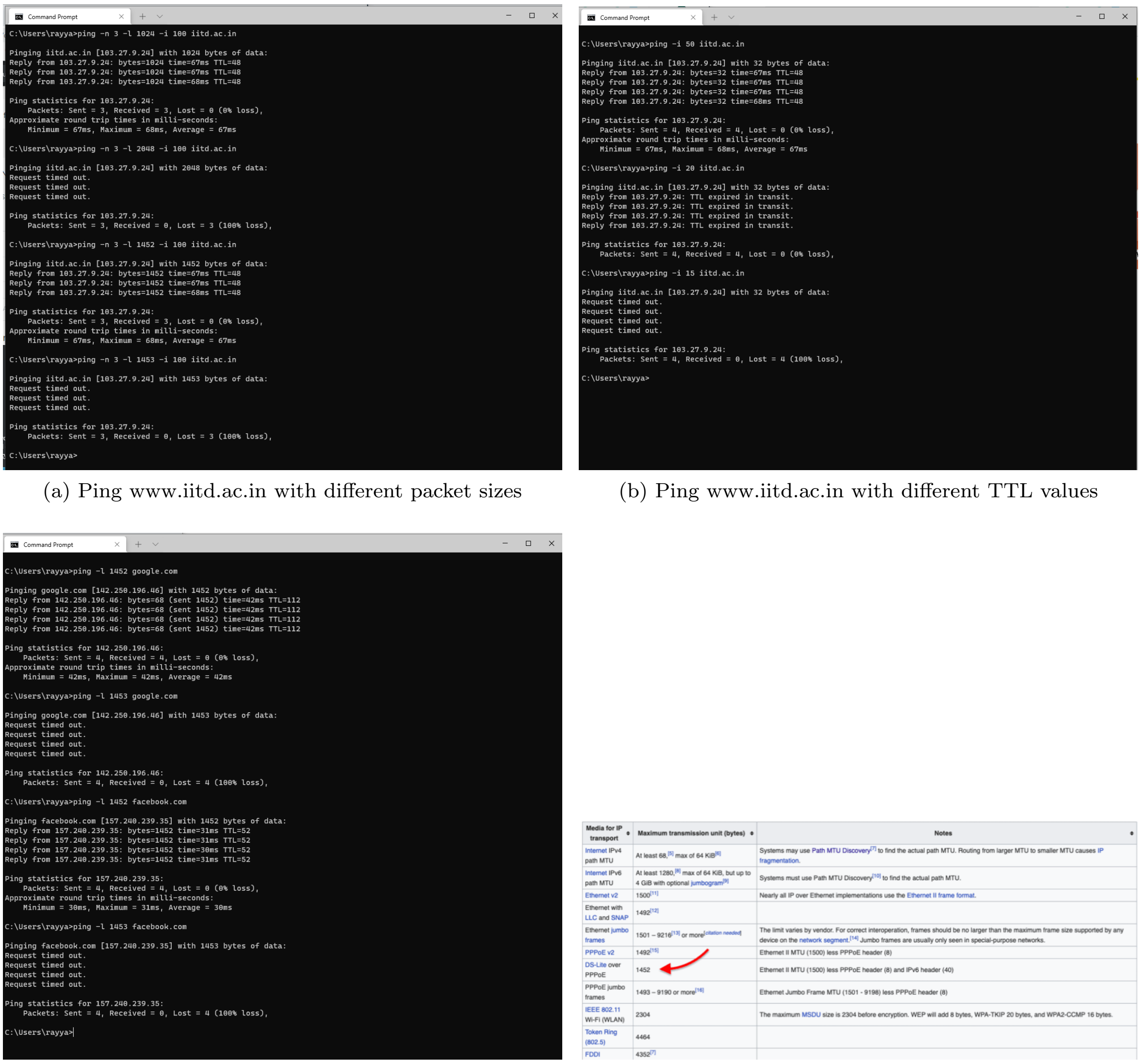
```
D:\RAYYAN\Sem 5\COL334\Assignment 1>nslookup -type=ns facebook.com
Server:  UnKnown
Address:  192.168.147.87

Non-authoritative answer:
facebook.com    nameserver = c.ns.facebook.com
facebook.com    nameserver = d.ns.facebook.com
facebook.com    nameserver = b.ns.facebook.com
facebook.com    nameserver = a.ns.facebook.com

c.ns.facebook.com       AAAA IPv6 address = 2a03:2880:f1fc:c:face:b00c:0:35
c.ns.facebook.com       internet address = 185.89.218.12
d.ns.facebook.com       AAAA IPv6 address = 2a03:2880:f1fd:c:face:b00c:0:35
d.ns.facebook.com       internet address = 185.89.219.12
b.ns.facebook.com       AAAA IPv6 address = 2a03:2880:f0fd:c:face:b00c:0:35
b.ns.facebook.com       internet address = 129.134.31.12
a.ns.facebook.com       AAAA IPv6 address = 2a03:2880:f0fc:c:face:b00c:0:35
a.ns.facebook.com       internet address = 129.134.30.12

D:\RAYYAN\Sem 5\COL334\Assignment 1>nslookup facebook.com 185.89.218.12
Server:  c.ns.facebook.com
Address:  185.89.218.12

Name:    facebook.com
Addresses:  2a03:2880:f168:81:face:b00c:0:25de
    157.240.228.35


D:\RAYYAN\Sem 5\COL334\Assignment 1>
```

(d) nslookup authoritative results for iitd.ac.in

Figure 1: nslookup results

It is observed that on using different DNS servers, the IP addresses of the domains change. This is because large companies like Google and Facebook have large network traffic and thus have many different servers to serve the network requests. The IP addresses we see correspond to different servers and based on the current network traffic, IP addresses of different servers are returned by different DNS servers and/or at different times.

c.



```
C:\Users\rayya>ping -n 3 -l 1024 -i 100 iitd.ac.in

Pinging iitd.ac.in [103.27.9.24] with 1024 bytes of data:
Reply from 103.27.9.24: bytes=1024 time=67ms TTL=48
Reply from 103.27.9.24: bytes=1024 time=67ms TTL=48
Reply from 103.27.9.24: bytes=1024 time=68ms TTL=48

Ping statistics for 103.27.9.24:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 67ms, Maximum = 68ms, Average = 67ms

C:\Users\rayya>ping -n 3 -l 2048 -i 100 iitd.ac.in

Pinging iitd.ac.in [103.27.9.24] with 2048 bytes of data:
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 103.27.9.24:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),

C:\Users\rayya>ping -n 3 -l 1452 -i 100 iitd.ac.in

Pinging iitd.ac.in [103.27.9.24] with 1452 bytes of data:
Reply from 103.27.9.24: bytes=1452 time=67ms TTL=48
Reply from 103.27.9.24: bytes=1452 time=67ms TTL=48
Reply from 103.27.9.24: bytes=1452 time=68ms TTL=48

Ping statistics for 103.27.9.24:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 67ms, Maximum = 68ms, Average = 67ms

C:\Users\rayya>ping -n 3 -l 1453 -i 100 iitd.ac.in

Pinging iitd.ac.in [103.27.9.24] with 1453 bytes of data:
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 103.27.9.24:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),

C:\Users\rayya>
```

(a) Ping www.iitd.ac.in with different packet sizes

```
C:\Users\rayya>ping -i 50 iitd.ac.in

Pinging iitd.ac.in [103.27.9.24] with 32 bytes of data:
Reply from 103.27.9.24: bytes=32 time=67ms TTL=48
Reply from 103.27.9.24: bytes=32 time=67ms TTL=48
Reply from 103.27.9.24: bytes=32 time=67ms TTL=48
Reply from 103.27.9.24: bytes=32 time=68ms TTL=48

Ping statistics for 103.27.9.24:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 67ms, Maximum = 68ms, Average = 67ms

C:\Users\rayya>ping -i 20 iitd.ac.in

Pinging iitd.ac.in [103.27.9.24] with 32 bytes of data:
Reply from 103.27.9.24: TTL expired in transit.
Reply from 103.27.9.24: TTL expired in transit.
Reply from 103.27.9.24: TTL expired in transit.
Reply from 103.27.9.24: TTL expired in transit.

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

C:\Users\rayya>ping -i 15 iitd.ac.in

Pinging 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),

C:\Users\rayya>
```

(b) Ping www.iitd.ac.in with different TTL values

```
C:\Users\rayya>ping -l 1452 google.com

Pinging google.com [142.250.196.46] with 1452 bytes of data:
Reply from 142.250.196.46: bytes=68 (sent 1452) time=42ms TTL=112
Reply from 142.250.196.46: bytes=68 (sent 1452) time=42ms TTL=112
Reply from 142.250.196.46: bytes=68 (sent 1452) time=42ms TTL=112
Reply from 142.250.196.46: bytes=68 (sent 1452) time=42ms TTL=112

Ping statistics for 142.250.196.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 42ms, Average = 42ms

C:\Users\rayya>ping -l 1453 google.com

Pinging google.com [142.250.196.46] with 1453 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 142.250.196.46:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\rayya>ping -l 1452 facebook.com

Pinging facebook.com [157.240.239.35] with 1452 bytes of data:
Reply from 157.240.239.35: bytes=1452 time=31ms TTL=52
Reply from 157.240.239.35: bytes=1452 time=31ms TTL=52
Reply from 157.240.239.35: bytes=1452 time=30ms TTL=52
Reply from 157.240.239.35: bytes=1452 time=31ms TTL=52

Ping statistics for 157.240.239.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 30ms, Maximum = 31ms, Average = 30ms

C:\Users\rayya>ping -l 1453 facebook.com

Pinging facebook.com [157.240.239.35] with 1453 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 157.240.239.35:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\rayya>
```

(c) Ping google.com and facebook.com with different packet sizes

Media for IP transport	Maximum transmission unit (bytes)	Notes
Internet IPv4 path MTU	At least 68,[5] max of 64 KiB[6]	Systems may use Path MTU Discovery[7] to find the actual path MTU. Routing from larger MTU to smaller MTU causes IP fragmentation.
Internet IPv6 path MTU	At least 1280,[8] max of 64 KiB, but up to 4 GiB with optional jumbogram[9]	Systems must use Path MTU Discovery[10] to find the actual path MTU.
Ethernet v2	1500[11]	Nearly all IP over Ethernet implementations use the Ethernet II frame format.
Ethernet with LLC and SNAP	1492[12]	
Ethernet jumbo frames	1501 – 9216[13] or more[citation needed]	The limit varies by vendor. For correct interoperation, frames should be no larger than the maximum frame size supported by any device on the network segment.[14] Jumbo frames are usually only seen in special-purpose networks.
PPPoE v2	1492[15]	Ethernet II MTU (1500) less PPPoE header (8)
DS-Lite over PPPoE	1452	Ethernet II MTU (1500) less PPPoE header (8) and IPv6 header (40)
PPPoE jumbo frames	1493 – 9190 or more[16]	Ethernet Jumbo Frame MTU (1501 - 9198) less PPPoE header (8)
IEEE 802.11 Wi-Fi (WLAN)	2304	The maximum MSDU size is 2304 before encryption. WEP will add 8 bytes, WPA-TKIP 20 bytes, and WPA2-CCMP 16 bytes.
Token Ring (802.5)	4464	
FDDI	4352[7]	

(d) Maximum Packet size

Figure 2: Ping with different options

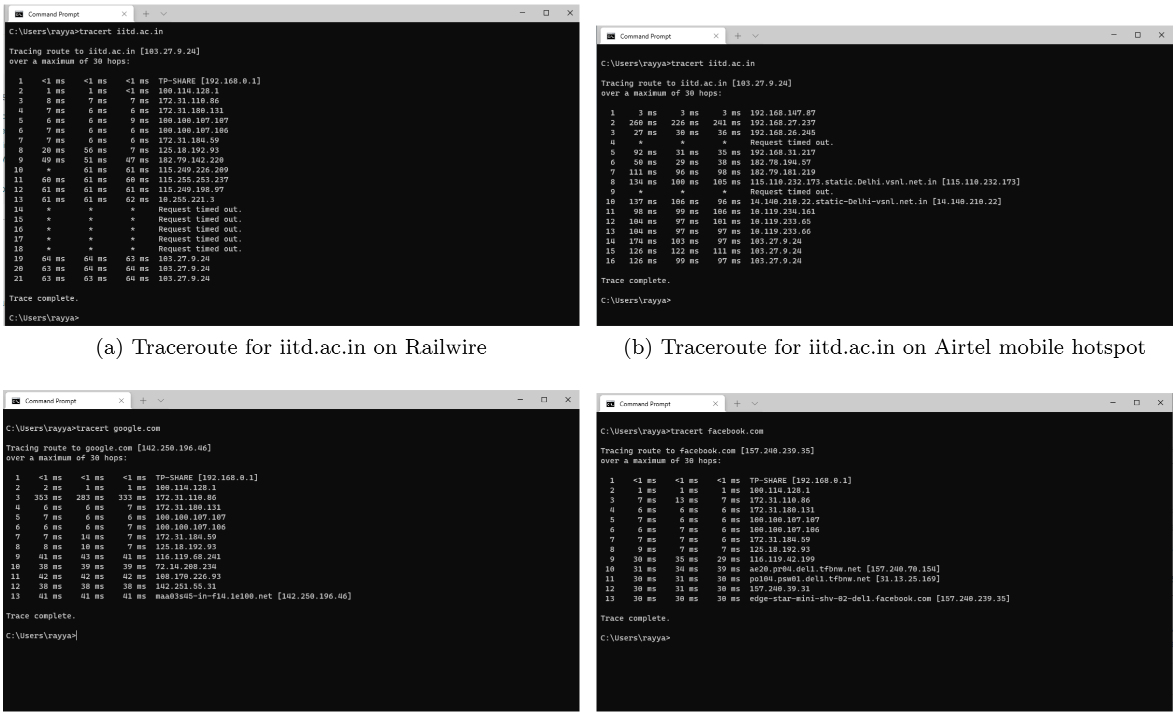
It is observed that the maximum allowed packet size is 1452 Bytes. For values larger than this, we get “Request timed out” message.

When TTL value is large, the Ping command works as expected, returning the round trip times for the sent packets. For lower values, we get the message “TTL expired in transit”, implying that a larger value of TTL was required for the complete transmission of packet from source to destination. We also get a message “Request timed out” message for some values of TTL, implying that the node at which the TTL expired did not send back the packet to the source. Increasing the time-out value using the option `/w <timeout>` might help in some cases. However, the result was the same when used for iitd.ac.in.

The maximum allowed packet size is 1452 Bytes for google.com and facebook.com. This is the same as that for iitd.ac.in.

Ethernet has the MTU (maximum transmission unit) size of 1500 Bytes. Out of this, PPPoE header takes up 8 Bytes and the IPv6 header takes 40 Bytes. The remaining 1452 Bytes is the largest allowed packet size (also called the Maximum Segment Size).

d.



```
C:\Users\rayya>tracert iitd.ac.in

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

  1    <1 ms    <1 ms    <1 ms  TP-SHARE [192.168.0.1]
  2     1 ms     1 ms    <1 ms  100.114.128.1
  3     8 ms     7 ms     7 ms  172.31.110.86
  4     7 ms     6 ms     6 ms  172.31.180.131
  5     6 ms     6 ms     9 ms  100.100.107.107
  6     7 ms     6 ms     6 ms  100.100.107.106
  7     7 ms     6 ms     6 ms  172.31.184.59
  8    20 ms    56 ms     7 ms  125.18.192.93
  9    49 ms    51 ms    47 ms  182.79.142.220
 10     *       61 ms    61 ms  115.249.226.209
 11    60 ms    61 ms    60 ms  115.255.253.237
 12    61 ms    61 ms    61 ms  115.249.198.97
 13    61 ms    61 ms    62 ms  10.255.221.3
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19    64 ms    64 ms    63 ms  103.27.9.24
 20    63 ms    64 ms    64 ms  103.27.9.24
 21    63 ms    63 ms    64 ms  103.27.9.24

Trace complete.

C:\Users\rayya>
```

(a) Traceroute for iitd.ac.in on Railwire

```
C:\Users\rayya>tracert iitd.ac.in

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

  1     3 ms     3 ms     3 ms  192.168.147.87
  2   260 ms   226 ms   241 ms  192.168.27.237
  3    27 ms    30 ms    36 ms  192.168.26.245
  4     *        *        *     Request timed out.
  5    92 ms    31 ms    35 ms  192.168.31.217
  6    50 ms    29 ms    38 ms  182.78.194.57
  7   111 ms    96 ms    98 ms  182.79.181.219
  8   134 ms   100 ms   105 ms  115.110.232.173.static.Delhi.vsnl.net.in [115.110.232.173]
  9     *        *        *     Request timed out.
 10   137 ms   106 ms    96 ms  14.140.210.22.static-Delhi-vsnl.net.in [14.140.210.22]
 11    98 ms    99 ms   106 ms  10.119.234.161
 12   104 ms    97 ms   101 ms  10.119.233.65
 13   104 ms    97 ms    97 ms  10.119.233.66
 14   174 ms   103 ms    97 ms  103.27.9.24
 15   126 ms   122 ms   111 ms  103.27.9.24
 16   126 ms    99 ms    97 ms  103.27.9.24

Trace complete.

C:\Users\rayya>
```

(b) Traceroute for iitd.ac.in on Airtel mobile hotspot

```
C:\Users\rayya>tracert google.com

Tracing route to google.com [142.250.196.46]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  TP-SHARE [192.168.0.1]
  2     2 ms     1 ms     1 ms  100.114.128.1
  3   353 ms   283 ms   333 ms  172.31.110.86
  4     6 ms     6 ms     7 ms  172.31.180.131
  5     7 ms     6 ms     6 ms  100.100.107.107
  6     6 ms     6 ms     7 ms  100.100.107.106
  7     7 ms    14 ms     7 ms  172.31.184.59
  8     8 ms    10 ms     7 ms  125.18.192.93
  9    41 ms    43 ms    41 ms  116.119.68.241
 10    38 ms    39 ms    39 ms  72.14.208.234
 11    42 ms    42 ms    42 ms  108.170.226.93
 12    38 ms    38 ms    38 ms  142.251.55.31
 13    41 ms    41 ms    41 ms  maa03s45-in-f14.1e100.net [142.250.196.46]

Trace complete.

C:\Users\rayya>
```

(c) Traceroute for google.com on railwire

```
C:\Users\rayya>tracert facebook.com

Tracing route to facebook.com [157.240.239.35]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  TP-SHARE [192.168.0.1]
  2     1 ms     1 ms     1 ms  100.114.128.1
  3     7 ms    13 ms     7 ms  172.31.110.86
  4     6 ms     6 ms     6 ms  172.31.180.131
  5     7 ms     6 ms     6 ms  100.100.107.107
  6     6 ms     7 ms     6 ms  100.100.107.106
  7     7 ms     7 ms     6 ms  172.31.184.59
  8     9 ms     7 ms     7 ms  125.18.192.93
  9    30 ms    35 ms    29 ms  116.119.42.199
 10    31 ms    34 ms    39 ms  ae20.pr04.del1.tfbnw.net [157.240.70.154]
 11    30 ms    31 ms    30 ms  po104.psw01.del1.tfbnw.net [31.13.25.169]
 12    30 ms    31 ms    30 ms  157.240.39.31
 13    30 ms    30 ms    30 ms  edge-star-mini-shv-02-del1.facebook.com [157.240.239.35]

Trace complete.

C:\Users\rayya>
```

(d) Traceroute for facebook.com on railwire

Figure 3: Traceroute

For Railwire, it is observed that hops numbered 14 to 18 are not responding and the message “Request timed out” is observed. Moreover, some private IP addresses are also observed in the hops numbered 1 and 13.

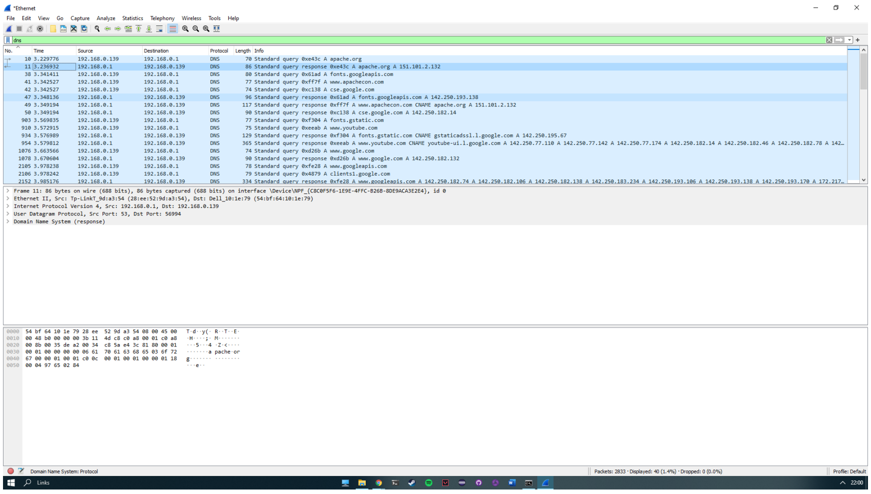
For Airtel, it is observed that hops numbered 4 and 9 are not responding and the message “Request timed out” is observed. Moreover, some private IP addresses are also observed in the hops numbered 1, 2, 3, 5, 11, 12 and 13.

We don’t observe any IPv6 paths in traceroute. However, to force the traceroute command to use IPv4 paths, we can use the option `-4`.

For google.com and facebook.com, all the intermediate nodes in traceroute are responding.

2. Packet Analysis

a.



dns

```
No.  Time     Source         Destination    Protocol Length Info
  10 3.229776 192.168.0.139  192.168.0.1    DNS       70 Standard query 0xe43c A apache.org
  11 3.236932 192.168.0.1    192.168.0.139  DNS       86 Standard query response 0xe43c A apache.org A 151.101.2.132
  38 3.341411 192.168.0.139  192.168.0.1    DNS       80 Standard query 0x61ad A fonts.googleapis.com
  41 3.342527 192.168.0.139  192.168.0.1    DNS       77 Standard query 0xff7f A www.apachecon.com
  42 3.342527 192.168.0.139  192.168.0.1    DNS       74 Standard query 0xc138 A cse.google.com
  47 3.348136 192.168.0.1    192.168.0.139  DNS       96 Standard query response 0x61ad A fonts.googleapis.com A 142.250.193.138
  49 3.349194 192.168.0.1    192.168.0.139  DNS      117 Standard query response 0xff7f A www.apachecon.com CNAME apache.org A 151.101.2.132
  50 3.349194 192.168.0.1    192.168.0.139  DNS       90 Standard query response 0xc138 A cse.google.com A 142.250.182.14
 903 3.569835 192.168.0.139  192.168.0.1    DNS       77 Standard query 0xf304 A fonts.gstatic.com
 910 3.572915 192.168.0.139  192.168.0.1    DNS       75 Standard query 0xeeab A www.youtube.com
 934 3.576989 192.168.0.1    192.168.0.139  DNS      129 Standard query response 0xf304 A fonts.gstatic.com CNAME gstaticadssl.l.google.com A 142.250.195.67
 954 3.579812 192.168.0.1    192.168.0.139  DNS      365 Standard query response 0xeeab A www.youtube.com CNAME youtube-ui.l.google.com A 142.250.77.110 A 142.250.77.142 A 142.250.77.174 A 142.250.182.14 A 142.250.182.46 A 142.250.182.78 A 142…
1076 3.663566 192.168.0.139  192.168.0.1    DNS       74 Standard query 0xd26b A www.google.com
1078 3.670604 192.168.0.1    192.168.0.139  DNS       90 Standard query response 0xd26b A www.google.com A 142.250.182.132
2105 3.978238 192.168.0.139  192.168.0.1    DNS       78 Standard query 0xfe28 A www.googleapis.com
2106 3.978242 192.168.0.139  192.168.0.1    DNS       79 Standard query 0x4879 A clients1.google.com
2152 3.985176 192.168.0.1    192.168.0.139  DNS      334 Standard query response 0xfe28 A www.googleapis.com A 142.250.182.74 A 142.250.182.106 A 142.250.182.138 A 142.250.183.234 A 142.250.193.106 A 142.250.193.138 A 142.250.193.170 A 172.217…
```

```
> Frame 11: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{C8C0F5F6-1E9E-4FFC-B26B-8DE9ACA3E2E4}, id 0
> Ethernet II, Src: Tp-LinkT_9d:a3:54 (28:ee:52:9d:a3:54), Dst: Dell_10:1e:79 (54:bf:64:10:1e:79)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.139
> User Datagram Protocol, Src Port: 53, Dst Port: 56994
> Domain Name System (response)
```

```
0000  54 bf 64 10 1e 79 28 ee  52 9d a3 54 08 00 45 00   T·d··y(· R··T··E·
0010  00 48 b0 00 00 00 3b 11  4d c8 c0 a8 00 01 c0 a8   ·H····;· M·······
0020  00 8b 00 35 de a2 00 34  c8 5a e4 3c 81 80 00 01   ···5···4 ·Z·<····
0030  00 01 00 00 00 00 06 61  70 61 63 68 65 03 6f 72   ·······a pache·or
0040  67 00 00 01 00 01 c0 0c  00 01 00 01 00 00 01 18   g······· ········
0050  00 04 97 65 02 84                                  ···e··
```

Domain Name System: Protocol

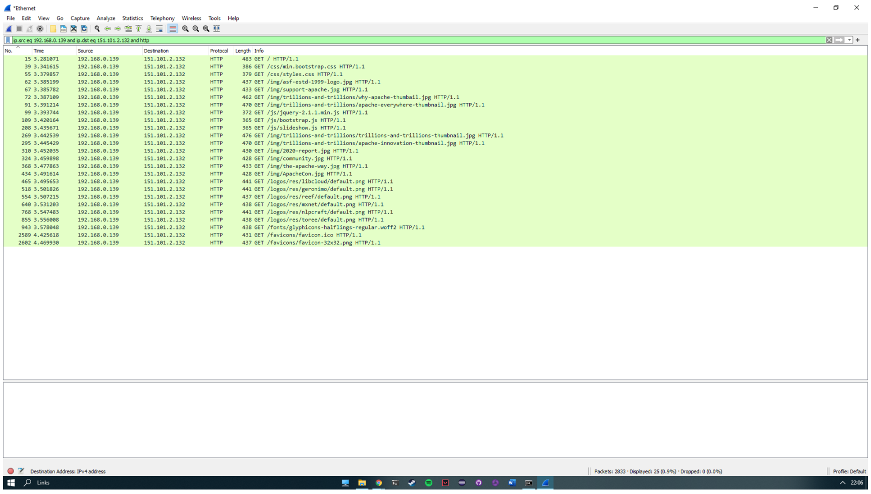
Packets: 2833 · Displayed: 40 (1.4%) · Dropped: 0 (0.0%)

Profile: Default

Figure 4: dns filter on the sniffed packets

DNS request time for apache.org = 3.229776, DNS response time = 3.236932
Thus, it took approximately 7 ms for the DNS request-response to complete. The source for the DNS response was the local router which explains the low delay.

b.

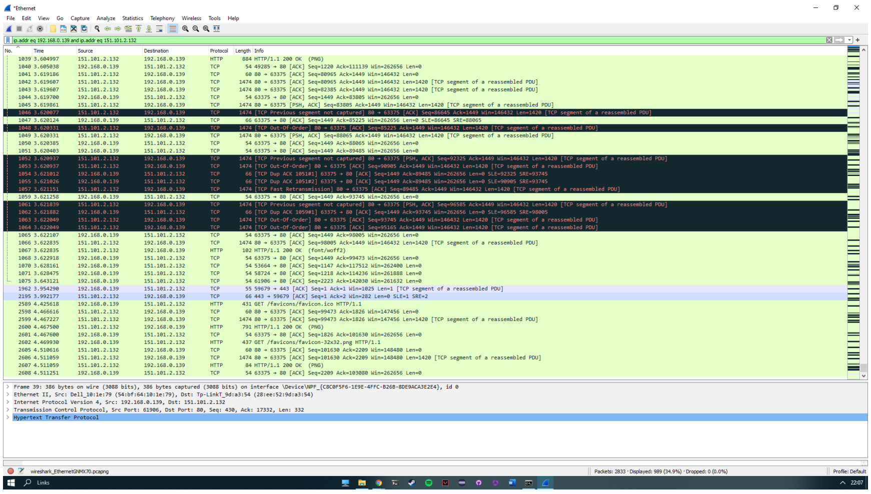


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.src eq 192.168.0.139 and ip.dst eq 151.101.2.132 and http

No.   Time      Source          Destination     Protocol Length Info
   15 3.281071  192.168.0.139   151.101.2.132   HTTP     483 GET / HTTP/1.1
   39 3.341615  192.168.0.139   151.101.2.132   HTTP     386 GET /css/min.bootstrap.css HTTP/1.1
   55 3.379857  192.168.0.139   151.101.2.132   HTTP     379 GET /css/styles.css HTTP/1.1
   62 3.385199  192.168.0.139   151.101.2.132   HTTP     437 GET /img/asf-estd-1999-logo.jpg HTTP/1.1
   67 3.385782  192.168.0.139   151.101.2.132   HTTP     433 GET /img/support-apache.jpg HTTP/1.1
   72 3.387109  192.168.0.139   151.101.2.132   HTTP     462 GET /img/trillions-and-trillions/why-apache-thumbail.jpg HTTP/1.1
   91 3.391214  192.168.0.139   151.101.2.132   HTTP     470 GET /img/trillions-and-trillions/apache-everywhere-thumbnail.jpg HTTP/1.1
   99 3.393744  192.168.0.139   151.101.2.132   HTTP     372 GET /js/jquery-2.1.1.min.js HTTP/1.1
  109 3.420164  192.168.0.139   151.101.2.132   HTTP     365 GET /js/bootstrap.js HTTP/1.1
  208 3.435671  192.168.0.139   151.101.2.132   HTTP     365 GET /js/slideshow.js HTTP/1.1
  269 3.442539  192.168.0.139   151.101.2.132   HTTP     476 GET /img/trillions-and-trillions/trillions-and-trillions-thumbnail.jpg HTTP/1.1
  295 3.445429  192.168.0.139   151.101.2.132   HTTP     470 GET /img/trillions-and-trillions/apache-innovation-thumbnail.jpg HTTP/1.1
  310 3.452035  192.168.0.139   151.101.2.132   HTTP     430 GET /img/2020-report.jpg HTTP/1.1
  324 3.459898  192.168.0.139   151.101.2.132   HTTP     428 GET /img/community.jpg HTTP/1.1
  368 3.477863  192.168.0.139   151.101.2.132   HTTP     433 GET /img/the-apache-way.jpg HTTP/1.1
  434 3.491614  192.168.0.139   151.101.2.132   HTTP     428 GET /img/ApacheCon.jpg HTTP/1.1
  465 3.495653  192.168.0.139   151.101.2.132   HTTP     441 GET /logos/res/libcloud/default.png HTTP/1.1
  518 3.501826  192.168.0.139   151.101.2.132   HTTP     441 GET /logos/res/geronimo/default.png HTTP/1.1
  554 3.507215  192.168.0.139   151.101.2.132   HTTP     437 GET /logos/res/reef/default.png HTTP/1.1
  640 3.531203  192.168.0.139   151.101.2.132   HTTP     438 GET /logos/res/mxnet/default.png HTTP/1.1
  768 3.547483  192.168.0.139   151.101.2.132   HTTP     441 GET /logos/res/nlpcraft/default.png HTTP/1.1
  855 3.556008  192.168.0.139   151.101.2.132   HTTP     438 GET /logos/res/toree/default.png HTTP/1.1
  943 3.578048  192.168.0.139   151.101.2.132   HTTP     438 GET /fonts/glyphicons-halflings-regular.woff2 HTTP/1.1
 2589 4.425618  192.168.0.139   151.101.2.132   HTTP     431 GET /favicons/favicon.ico HTTP/1.1
 2602 4.469930  192.168.0.139   151.101.2.132   HTTP     437 GET /favicons/favicon-32x32.png HTTP/1.1

Destination Address: IPv4 address          Packets: 2833 · Displayed: 25 (0.9%) · Dropped: 0 (0.0%)          Profile: Default
```

Figure 5: HTTP GET requests

There are 25 HTTP GET requests. These HTTP requests give us some hint about how web-pages are structured. At first, the browser requests the HTML file for the web-page. On parsing the HTML, it recognizes any external references to CSS style-sheets, JavaScript files or any other media files like images, fonts, etc. Subsequently, the browser requests these files and parses them as and when they are received. In our case we find css files, JavaScript files, jpeg and png image files, ico for icons and woff2 for fonts. Each of these files are requested in a single HTTP GET request.



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

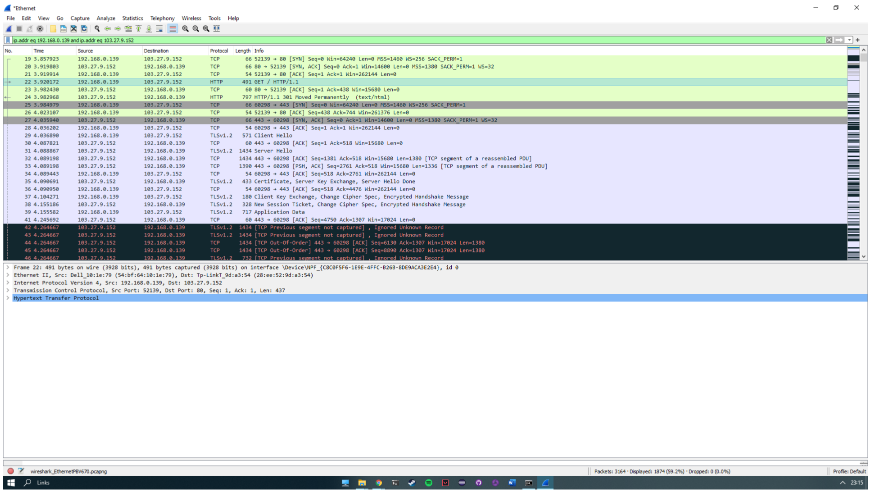
```
ip.addr eq 192.168.0.139 and ip.addr eq 151.101.2.132

No.   Time      Source          Destination     Protocol Length Info
 1039 3.604997  151.101.2.132   192.168.0.139   HTTP     884 HTTP/1.1 200 OK  (PNG)
 1040 3.605038  192.168.0.139   151.101.2.132   TCP       54 49285 → 80 [ACK] Seq=1220 Ack=111139 Win=262656 Len=0
 1041 3.619186  151.101.2.132   192.168.0.139   TCP       60 80 → 63375 [ACK] Seq=80965 Ack=1449 Win=146432 Len=0
 1042 3.619607  151.101.2.132   192.168.0.139   TCP     1474 80 → 63375 [ACK] Seq=80965 Ack=1449 Win=146432 Len=1420 [TCP segment of a reassembled PDU]
 1043 3.619607  151.101.2.132   192.168.0.139   TCP     1474 80 → 63375 [ACK] Seq=82385 Ack=1449 Win=146432 Len=1420 [TCP segment of a reassembled PDU]
 1044 3.619700  192.168.0.139   151.101.2.132   TCP       54 63375 → 80 [ACK] Seq=1449 Ack=83805 Win=262656 Len=0
 1045 3.619861  151.101.2.132   192.168.0.139   TCP     1474 80 → 63375 [PSH, ACK] Seq=83805 Ack=1449 Win=146432 Len=1420 [TCP segment of a reassembled PDU]
 1046 3.620077  151.101.2.132   192.168.0.139   TCP     1474 [TCP Previous segment not captured] 80 → 63375 [ACK] Seq=86645 Ack=1449 Win=146432 Len=1420 [TCP segment of a reassembled PDU]
 1047 3.620124  192.168.0.139   151.101.2.132   TCP       66 63375 → 80 [ACK] Seq=1449 Ack=85225 Win=262656 Len=0 SLE=86645 SRE=88065
 1048 3.620331  151.101.2.132   192.168.0.139   TCP     1474 [TCP Out-Of-Order] 80 → 63375 [ACK] Seq=85225 Ack=1449 Win=146432 Len=1420 [TCP segment of a reassembled PDU]
 1049 3.620331  151.101.2.132   192.168.0.139   TCP     1474 80 → 63375 [PSH, ACK] Seq=88065 Ack=1449 Win=146432 Len=1420 [TCP segment of a reassembled PDU]
 1050 3.620385  192.168.0.139   151.101.2.132   TCP       54 63375 → 80 [ACK] Seq=1449 Ack=88065 Win=262656 Len=0
 1051 3.620403  192.168.0.139   151.101.2.132   TCP       54 63375 → 80 [ACK] Seq=1449 Ack=89485 Win=262656 Len=0
 1052 3.620937  151.101.2.132   192.168.0.139   TCP     1474 [TCP Previous segment not captured] 80 → 63375 [PSH, ACK] Seq=92325 Ack=1449 Win=146432 Len=1420 [TCP segment of a reassembled PDU]
 1053 3.620937  151.101.2.132   192.168.0.139   TCP     1474 [TCP Out-Of-Order] 80 → 63375 [ACK] Seq=90905 Ack=1449 Win=146432 Len=1420 [TCP segment of a reassembled PDU]
 1054 3.621012  192.168.0.139   151.101.2.132   TCP       66 [TCP Dup ACK 1051#1] 63375 → 80 [ACK] Seq=1449 Ack=89485 Win=262656 Len=0 SLE=92325 SRE=93745
 1055 3.621026  192.168.0.139   151.101.2.132   TCP       66 [TCP Dup ACK 1051#2] 63375 → 80 [ACK] Seq=1449 Ack=89485 Win=262656 Len=0 SLE=90905 SRE=93745
 1057 3.621151  151.101.2.132   192.168.0.139   TCP     1474 [TCP Fast Retransmission] 80 → 63375 [ACK] Seq=89485 Ack=1449 Win=146432 Len=1420 [TCP segment of a reassembled PDU]
 1059 3.621258  192.168.0.139   151.101.2.132   TCP       54 63375 → 80 [ACK] Seq=1449 Ack=93745 Win=262656 Len=0
 1061 3.621839  151.101.2.132   192.168.0.139   TCP     1474 [TCP Previous segment not captured] 80 → 63375 [PSH, ACK] Seq=96585 Ack=1449 Win=146432 Len=1420 [TCP segment of a reassembled PDU]
 1062 3.621882  192.168.0.139   151.101.2.132   TCP       66 [TCP Dup ACK 1059#1] 63375 → 80 [ACK] Seq=1449 Ack=93745 Win=262656 Len=0 SLE=96585 SRE=98005
 1063 3.622049  151.101.2.132   192.168.0.139   TCP     1474 [TCP Out-Of-Order] 80 → 63375 [ACK] Seq=93745 Ack=1449 Win=146432 Len=1420 [TCP segment of a reassembled PDU]
 1064 3.622049  151.101.2.132   192.168.0.139   TCP     1474 [TCP Out-Of-Order] 80 → 63375 [ACK] Seq=95165 Ack=1449 Win=146432 Len=1420 [TCP segment of a reassembled PDU]
 1065 3.622107  192.168.0.139   151.101.2.132   TCP       54 63375 → 80 [ACK] Seq=1449 Ack=98005 Win=262656 Len=0
 1066 3.622835  151.101.2.132   192.168.0.139   TCP     1474 80 → 63375 [ACK] Seq=98005 Ack=1449 Win=146432 Len=1420 [TCP segment of a reassembled PDU]
 1067 3.622835  151.101.2.132   192.168.0.139   HTTP     102 HTTP/1.1 200 OK  (font/woff2)
 1068 3.622918  192.168.0.139   151.101.2.132   TCP       54 63375 → 80 [ACK] Seq=1449 Ack=99473 Win=262656 Len=0
 1070 3.628161  192.168.0.139   151.101.2.132   TCP       54 53664 → 80 [ACK] Seq=1147 Ack=117512 Win=262400 Len=0
 1071 3.628475  192.168.0.139   151.101.2.132   TCP       54 58724 → 80 [ACK] Seq=1218 Ack=114236 Win=261888 Len=0
 1075 3.643121  192.168.0.139   151.101.2.132   TCP       54 61906 → 80 [ACK] Seq=2223 Ack=142030 Win=261632 Len=0
 1962 3.954290  192.168.0.139   151.101.2.132   TCP       55 59679 → 443 [ACK] Seq=1 Ack=1 Win=1025 Len=1 [TCP segment of a reassembled PDU]
 2195 3.992177  151.101.2.132   192.168.0.139   TCP       66 443 → 59679 [ACK] Seq=1 Ack=2 Win=282 Len=0 SLE=1 SRE=2
 2589 4.425618  192.168.0.139   151.101.2.132   HTTP     431 GET /favicons/favicon.ico HTTP/1.1
 2598 4.466616  151.101.2.132   192.168.0.139   TCP       60 80 → 63375 [ACK] Seq=99473 Ack=1826 Win=147456 Len=0
 2599 4.467227  151.101.2.132   192.168.0.139   TCP     1474 80 → 63375 [ACK] Seq=99473 Ack=1826 Win=147456 Len=1420 [TCP segment of a reassembled PDU]
 2600 4.467500  151.101.2.132   192.168.0.139   HTTP     791 HTTP/1.1 200 OK  (PNG)
 2601 4.467600  192.168.0.139   151.101.2.132   TCP       54 63375 → 80 [ACK] Seq=1826 Ack=101630 Win=262656 Len=0
 2602 4.469930  192.168.0.139   151.101.2.132   HTTP     437 GET /favicons/favicon-32x32.png HTTP/1.1
 2605 4.510616  151.101.2.132   192.168.0.139   TCP       60 80 → 63375 [ACK] Seq=101630 Ack=2209 Win=148480 Len=0
 2606 4.511059  151.101.2.132   192.168.0.139   TCP     1474 80 → 63375 [ACK] Seq=101630 Ack=2209 Win=148480 Len=1420 [TCP segment of a reassembled PDU]
 2607 4.511059  151.101.2.132   192.168.0.139   HTTP      84 HTTP/1.1 200 OK  (PNG)
 2608 4.511251  192.168.0.139   151.101.2.132   TCP       54 63375 → 80 [ACK] Seq=2209 Ack=103080 Win=262656 Len=0

> Frame 39: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface \Device\NPF_{C8C0F5F6-1E9E-4FFC-B26B-8DE9ACA3E2E4}, id 0
> Ethernet II, Src: Dell_10:1e:79 (54:bf:64:10:1e:79), Dst: Tp-LinkT_9d:a3:54 (28:ee:52:9d:a3:54)
> Internet Protocol Version 4, Src: 192.168.0.139, Dst: 151.101.2.132
> Transmission Control Protocol, Src Port: 61906, Dst Port: 80, Seq: 430, Ack: 17332, Len: 332
> Hypertext Transfer Protocol

wireshark_EthernetGNMX70.pcapng          Packets: 2833 · Displayed: 989 (34.9%) · Dropped: 0 (0.0%)          Profile: Default
```

Figure 6: Packets

c.

DNS request time for apache.org = 3.229776
The final content object (HTTP 200 OK response code for a png image) received = 4.511059
The total time taken for downloading the web-page = 1.28 seconds

d.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Links
23:15

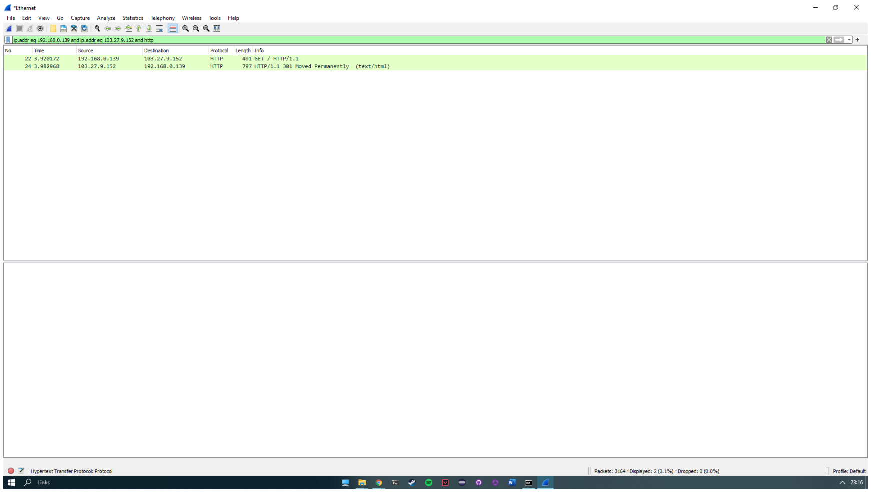
```
ip.addr eq 192.168.0.139 and ip.addr eq 103.27.9.152
```

```
No.  Time      Source         Destination    Protocol Length Info
  19 3.857923  192.168.0.139  103.27.9.152   TCP        66 52139 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  20 3.919803  103.27.9.152   192.168.0.139  TCP        66 80 → 52139 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1380 SACK_PERM=1 WS=32
  21 3.919914  192.168.0.139  103.27.9.152   TCP        54 52139 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
  22 3.920172  192.168.0.139  103.27.9.152   HTTP      491 GET / HTTP/1.1
  23 3.982430  103.27.9.152   192.168.0.139  TCP        60 80 → 52139 [ACK] Seq=1 Ack=438 Win=15680 Len=0
  24 3.982968  103.27.9.152   192.168.0.139  HTTP      797 HTTP/1.1 301 Moved Permanently  (text/html)
  25 3.984979  192.168.0.139  103.27.9.152   TCP        66 60298 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  26 4.023107  192.168.0.139  103.27.9.152   TCP        54 52139 → 80 [ACK] Seq=438 Ack=744 Win=261376 Len=0
  27 4.035940  103.27.9.152   192.168.0.139  TCP        66 443 → 60298 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1380 SACK_PERM=1 WS=32
  28 4.036202  192.168.0.139  103.27.9.152   TCP        54 60298 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
  29 4.036890  192.168.0.139  103.27.9.152   TLSv1.2   571 Client Hello
  30 4.087821  103.27.9.152   192.168.0.139  TCP        60 443 → 60298 [ACK] Seq=1 Ack=518 Win=15680 Len=0
  31 4.088867  103.27.9.152   192.168.0.139  TLSv1.2  1434 Server Hello
  32 4.089198  103.27.9.152   192.168.0.139  TCP      1434 443 → 60298 [ACK] Seq=1381 Ack=518 Win=15680 Len=1380 [TCP segment of a reassembled PDU]
  33 4.089198  103.27.9.152   192.168.0.139  TCP      1390 443 → 60298 [PSH, ACK] Seq=2761 Ack=518 Win=15680 Len=1336 [TCP segment of a reassembled PDU]
  34 4.089443  192.168.0.139  103.27.9.152   TCP        54 60298 → 443 [ACK] Seq=518 Ack=2761 Win=262144 Len=0
  35 4.090691  103.27.9.152   192.168.0.139  TLSv1.2   433 Certificate, Server Key Exchange, Server Hello Done
  36 4.090950  192.168.0.139  103.27.9.152   TCP        54 60298 → 443 [ACK] Seq=518 Ack=4476 Win=262144 Len=0
  37 4.104271  192.168.0.139  103.27.9.152   TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  38 4.155186  103.27.9.152   192.168.0.139  TLSv1.2   328 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
  39 4.155582  192.168.0.139  103.27.9.152   TLSv1.2   717 Application Data
  41 4.245692  103.27.9.152   192.168.0.139  TCP        60 443 → 60298 [ACK] Seq=4750 Ack=1307 Win=17024 Len=0
  42 4.264667  103.27.9.152   192.168.0.139  TLSv1.2  1434 [TCP Previous segment not captured] , Ignored Unknown Record
  43 4.264667  103.27.9.152   192.168.0.139  TLSv1.2  1434 [TCP Previous segment not captured] , Ignored Unknown Record
  44 4.264667  103.27.9.152   192.168.0.139  TCP      1434 [TCP Out-Of-Order] 443 → 60298 [ACK] Seq=6130 Ack=1307 Win=17024 Len=1380
  45 4.264667  103.27.9.152   192.168.0.139  TCP      1434 [TCP Out-Of-Order] 443 → 60298 [ACK] Seq=8890 Ack=1307 Win=17024 Len=1380
  46 4.264667  103.27.9.152   192.168.0.139  TLSv1.2   732 [TCP Previous segment not captured] , Ignored Unknown Record
```

```
> Frame 22: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits) on interface \Device\NPF_{C8C0F5F6-1E9E-4FFC-B26B-8DE9ACA3E2E4}, id 0
> Ethernet II, Src: Dell_10:1e:79 (54:bf:64:10:1e:79), Dst: Tp-LinkT_9d:a3:54 (28:ee:52:9d:a3:54)
> Internet Protocol Version 4, Src: 192.168.0.139, Dst: 103.27.9.152
> Transmission Control Protocol, Src Port: 52139, Dst Port: 80, Seq: 1, Ack: 1, Len: 437
> Hypertext Transfer Protocol
```

```
wireshark_EthernetPBV670.pcapng    Packets: 3164 · Displayed: 1874 (59.2%) · Dropped: 0 (0.0%)    Profile: Default
```

Figure 7: Packets sniffed for cse.iitd.ac.in


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Links
23:16

```
ip.addr eq 192.168.0.139 and ip.addr eq 103.27.9.152 and http
```

```
No.  Time      Source         Destination    Protocol Length Info
  22 3.920172  192.168.0.139  103.27.9.152   HTTP      491 GET / HTTP/1.1
  24 3.982968  103.27.9.152   192.168.0.139  HTTP      797 HTTP/1.1 301 Moved Permanently  (text/html)
```

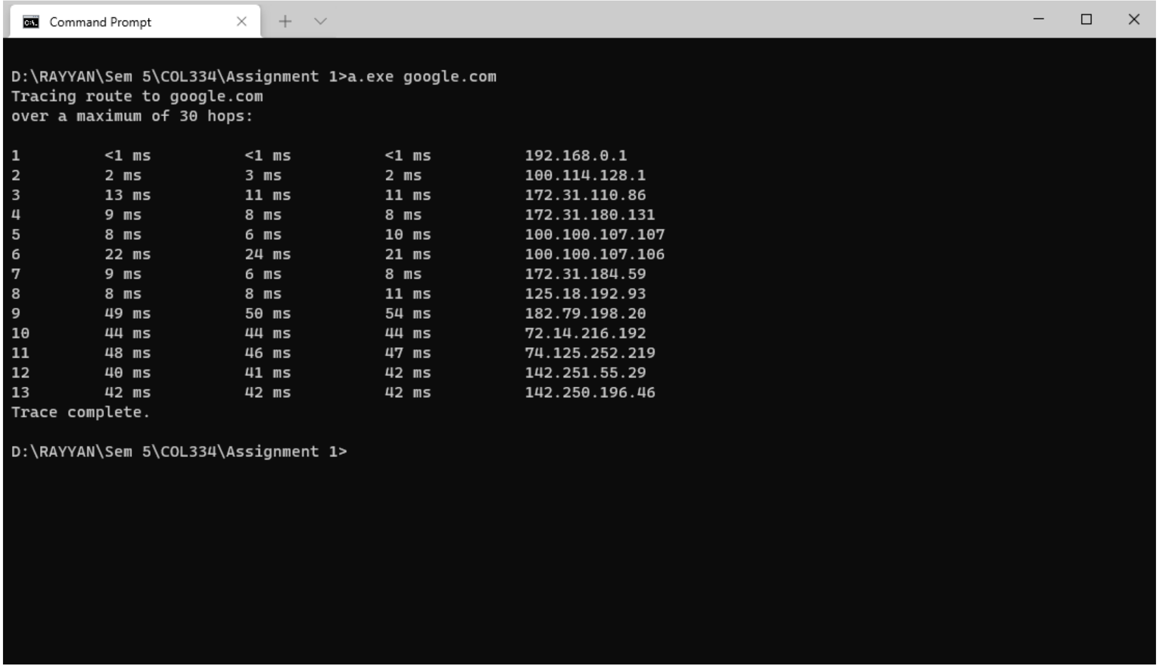
```
Hypertext Transfer Protocol: Protocol    Packets: 3164 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%)    Profile: Default
```

Figure 8: HTTP traffic for cse.iitd.ac.in

We don't find HTTP traffic for cse.iitd.ac.in because it uses the HTTPS protocol instead of HTTP. HTTPS is a secure protocol which uses encryption in order to provide a means of secure communication. The packets sent between the source and the destination are encrypted and as a result the contents of the sniffed packets can't be deciphered. Here, the TLSv1.2 protocol has been used to establish a secure communication channel.

On the other hand, apache.org uses HTTP protocol. Because it is unencrypted, the content of the packets being transmitted is known to anyone who intercepts these packets.

3. Implement Traceroute using Ping



```
D:\RAYYAN\Sem 5\COL334\Assignment 1>a.exe google.com
Tracing route to google.com
over a maximum of 30 hops:

1         <1 ms          <1 ms          <1 ms          192.168.0.1
2         2 ms           3 ms           2 ms           100.114.128.1
3         13 ms          11 ms          11 ms          172.31.110.86
4         9 ms           8 ms           8 ms           172.31.180.131
5         8 ms           6 ms           10 ms          100.100.107.107
6         22 ms          24 ms          21 ms          100.100.107.106
7         9 ms           6 ms           8 ms           172.31.184.59
8         8 ms           8 ms           11 ms          125.18.192.93
9         49 ms          50 ms          54 ms          182.79.198.20
10        44 ms          44 ms          44 ms          72.14.216.192
11        48 ms          46 ms          47 ms          74.125.252.219
12        40 ms          41 ms          42 ms          142.251.55.29
13        42 ms          42 ms          42 ms          142.250.196.46
Trace complete.

D:\RAYYAN\Sem 5\COL334\Assignment 1>
```

Figure 9: Traceroute program output

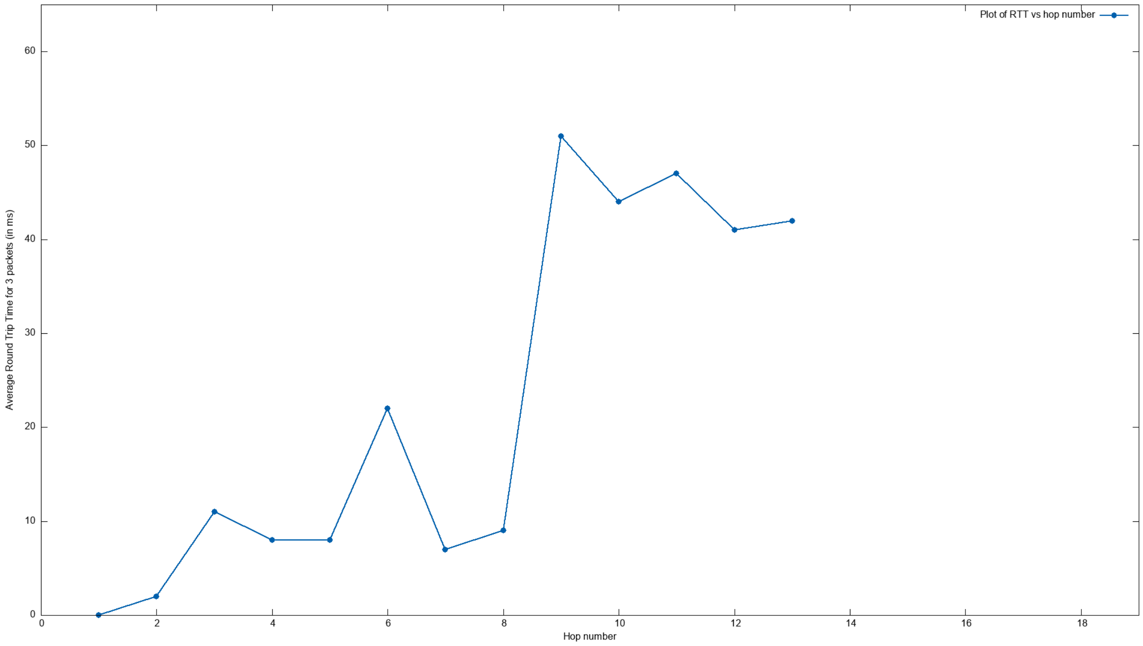


Figure 10: RTT vs hop number plot