Computer Networks

Kethavath Ajaykumar, 2021CS11211

Voora Akash, 2021CS10104

August 13, 2023

1 Network Analysis

1.1

1.a. We have ran trace route via 4G Network (using 4G networked mobile hotspot acting like a wifi) and Wifi from our laptop as a source and www.google.com as a destination. We have seen different IP address along the route from our personal computer source to destination.We have observed IP address are listed below:

traceroute to www.google.com (142.251.42.68)

1 192.168.113.115
2 * * *
3 192.168.23.225
192.168.23.193
192.168.23.225
4 182.79.112.94
5 182.79.112.89
182.79.112.93
6 72.14.217.194
7 * * *
8 142.251.52.228
9 74.125.243.100
108.170.251.102
10 * * *
11 64.233.174.0
12 * * *
13 142.251.69.103
142.251.69.105
142.251.69.103
14 142.251.42.68

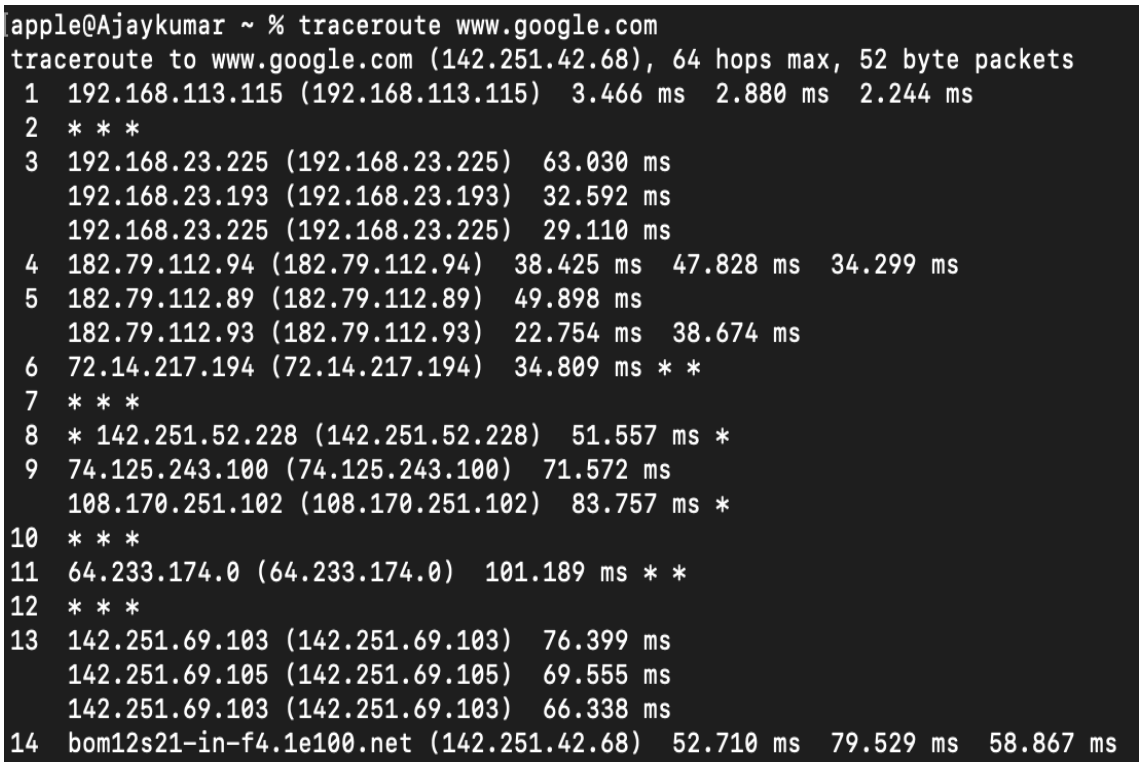

Figure 1: traceroute to google

1.2 Observations:

1. b. 6 columns are observed here for the routers. here is the break down(1-6): 1. 1: This is the first hop in the traceroute, indicating the first router or node in the path to the destination.

2. 192.168.113.115: This is the hostname or domain of the router or node at the current hop. this is to be observed here is, trace route can show domain names that can be of alphabetical letters may or may not include special characters(like ",-,etc.) not always.Domain name and IP address for a few routers are observed to be same. 3. 192.168.113.115: IP address of a respective router along the path from source to destination can be IPV4 or IPV6.

4. 10.791 ms: This is the round-trip time (RTT) in milliseconds for the first packet sent to the router at this hop. It indicates the time it takes for the packet

to travel from the source (your device) to the current hop and back.

5. 5.217 ms: This is the RTT for the second packet. The traceroute usually sends multiple packets to each hop to provide an average RTT.

6. 3.333 ms: This is the RTT for the third packet.

7. Missing routers(*): The asterisks indicate that there was no response from the routers at that hop. This could be due to routers configured not to respond to ping requests or network congestion.

8. There are duplicate entries for IP addresses in hops 3 and 4 (e.g., 192.168.23.225 and 192.168.23.193). This might be an indication of network setup or routing configuration, but it's unusual to see multiple identical entries for the same hop.

9. The final hop (142.251.42.68) is the destination IP address (www.google.com) that you were tracing to is at hop 14.

10. The trace route outputted IP addresses doesn't directly display private IP addresses because these addresses are typically used within local networks and are not visible on the public internet.

11. IP addresses shown are of IPV4 addresses (private computer or laptop) are set by default. But still we can convert these addresses from IPV4 to IPV6 for our convienience using:
traceroute -6 destination (on windows based)
traceroute6 destination (on Linux based) respectively.

12. 64 hops max: This parameter sets the maximum number of hops (routers or nodes) that traceroute will track along the route. If the destination is not reached within 64 hops, the traceroute will stop.

13. 52 byte packets: This parameter specifies the size of the packets sent during the traceroute. In this case, packets of 52 bytes will be sent to each hop in the route.

1.c. The maximum size of ping packets that we are able to send is 255.

2

Code in the Python file

Source	Destination	Number of hops	latency(ms)
Germany	University of Utah	Unable to reach destination(atleast 30 hops)	146.3
Germany	CapeTown University	Unable to reach destination(atleast 30 hops)	210.03
Germany	IIT Delhi	18 hops	149.3
Germany	Google	10 hops	3.25
Germany	Facebook	11 hops	9.13
USA	Unviersity of Utah	30 hops	64.1
USA	CapeTown University	30 hops	191.8
USA	IIT Delhi	30 hops	227.3
USA	Google	13 hops	4.1
USA	Facebook	13 hops	3.7
Own device	University of Utah	Unable to reach destination(atleast 38 hops)	375.9
Own device	CapeTown University	Unable to reach destination(atleast 23 hops)	385.4
Own device	IIT Delhi	4 hops	4.02
Own device	Google	11 hops	8.5
Own device	Facebook	13 hops	41.9

Table 1: Displaying number of hops took to reach from Source to Destination

3

3.a Below shown table is the number of hops took to reach from the source to Destination. here Germany mean the source is from http://www.han.de/cgi-bin/nph-trace.cgi to the respected mentioned destination. USA mean the source from http://www.net.princeton.edu/traceroute.html to the respective destination. the respective hops from source to destinations are shown in the table and the below images as well.

traceroute to www.utah.edu

```
traceroute to www.utah.edu (155.98.186.21), 30 hops max, 60 byte packets
 1  vsn0057.vs.mass.systems (10.92.36.120)  0.029 ms  0.013 ms  0.014 ms
 2  ae3-u100.sxb1-cr-nunki.bb.gdinf.net (87.230.112.2)  0.287 ms  0.364 ms  0.339 ms
 3  ae1.sxb1-ibr-altair.bb.gdinf.net (87.230.112.14)  5.258 ms  5.283 ms  5.209 ms
 4  217.243.179.244 (217.243.179.244)  3.970 ms  4.044 ms  4.103 ms
 5  f-ed13-i.F.DE.NET.DTAG.DE (217.5.70.42)  4.528 ms f-ed13-i.F.DE.NET.DTAG.DE (217.5.109.58)  4.569 ms f-ed13-i.F.DE.NET.DTAG.DE (217.5.109.54)  4.654 ms
 6  80.150.170.214 (80.150.170.214)  13.430 ms  13.484 ms  13.446 ms
 7  * * *
 8  ae2.cs1.ams17.nl.eth.zayo.com (64.125.29.59)  133.557 ms * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * ae5.cs1.den5.us.eth.zayo.com (64.125.29.19)  133.824 ms
15  * * *
16  ae4.mpr1.las5.us.zip.zayo.com (64.125.26.241)  133.480 ms  133.410 ms  133.553 ms
17  ae7.mcs1.las2.us.zip.zayo.com (64.125.21.202)  133.501 ms  133.434 ms  133.341 ms
18  209.66.120.14.IDIA-249109-ZYO.zip.zayo.com (209.66.120.14)  137.634 ms  137.575 ms  137.475 ms
19  ddc-pep-c-123-int.uen.net (140.197.251.32)  144.826 ms  144.805 ms  144.805 ms
20  ddc-pep-b-129-int.uen.net (140.197.253.97)  144.731 ms  144.397 ms  144.353 ms
21  ebc-pep-b-179-int.uen.net (140.197.252.76)  144.599 ms  144.580 ms  144.726 ms
22  ebc-pep-a-178-int.uen.net (140.197.252.84)  144.653 ms  144.701 ms  144.760 ms
23  * * *
24  199.104.93.22 (199.104.93.22)  144.644 ms  144.951 ms  144.605 ms
25  199.104.93.33 (199.104.93.33)  145.532 ms  146.103 ms  145.804 ms
26  155.99.130.67 (155.99.130.67)  145.685 ms  146.443 ms 155.99.130.65 (155.99.130.65)  145.482 ms
27  155.99.130.103 (155.99.130.103)  146.133 ms 155.99.130.101 (155.99.130.101)  146.803 ms 155.99.130.105 (155.99.130.105)  146.311 ms
28  * * *
29  * * *
30  * * *
```

Figure 2: traceroute from Germany to Utah

traceroute to www.uct.ac.za

```
traceroute to www.uct.ac.za (137.158.159.192), 30 hops max, 60 byte packets
 1  vsn0057.vs.mass.systems (10.92.36.120)  0.047 ms  0.014 ms  0.013 ms
 2  ae3-u100.sxb1-cr-nunki.bb.gdinf.net (87.230.112.2)  0.442 ms  0.396 ms  0.367 ms
 3  ae1.sxb1-ibr-altair.bb.gdinf.net (87.230.112.14)  0.800 ms  0.820 ms  0.736 ms
 4  ffm-bl6-link.ip.twelve99.net (62.115.144.8)  2.931 ms  2.964 ms  2.930 ms
 5  ffm-bb1-link.ip.twelve99.net (62.115.132.226)  3.703 ms  3.668 ms *
 6  ffm-bl1-link.ip.twelve99.net (62.115.124.119)  3.300 ms ffm-bl1-link.ip.twelve99.net (62.115.124.117)  3.390 ms ffm-bl1-link.ip.twelve99.net (62.115.124.119)  3.437 ms
 7  * * *
 8  be2845.ccr41.fra03.atlas.cogentco.com (154.54.56.189)  41.971 ms be2846.ccr42.fra03.atlas.cogentco.com (154.54.37.29)  4.041 ms be2845.ccr41.fra03.atlas.cogentco.com (154.54.56.189)  41.387 ms
 9  be2814.ccr42.ams03.atlas.cogentco.com (130.117.0.141)  10.497 ms be2813.ccr41.ams03.atlas.cogentco.com (130.117.0.121)  10.226 ms be2814.ccr42.ams03.atlas.cogentco.com (130.117.0.141)  10.495 ms
10  be3458.ccr21.ams04.atlas.cogentco.com (154.54.39.186)  10.684 ms  10.473 ms be3457.ccr21.ams04.atlas.cogentco.com (130.117.1.10)  10.658 ms
11  * * *
12  ae0-306-mtz1-ir1.net.tenet.ac.za (155.232.1.86)  185.286 ms  185.226 ms  185.186 ms
13  et-1-1-1-0-isd1-pe1.net.tenet.ac.za (155.232.1.153)  194.266 ms  194.228 ms  194.217 ms
14  et-1-1-4-0-cpt3-pe1.net.tenet.ac.za (155.232.1.148)  209.900 ms  209.932 ms  210.127 ms
15  et-0-0-1-0-cpt7-pe1.net.tenet.ac.za (155.232.64.70)  226.027 ms  209.764 ms  209.729 ms
16  154.114.124.1 (154.114.124.1)  210.019 ms  210.226 ms  210.030 ms
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Figure 3: traceroute from Germany to Uct

traceroute6 to www.iitd.ac.in

```
traceroute to www.iitd.ac.in (2001:df4:e000:29::212) from 2a01:488:66:1000:5c33:9112:0:1, 30 hops max, 24 byte packets
 1  2a01:488:66::a5c:2478 (2a01:488:66::a5c:2478)  0.129 ms  0.171 ms  0.079 ms
 2  ae3-u100.cr-nunki.sxb1.bb.godaddy.com (2a01:488:bb::42)  0.372 ms  0.266 ms  0.243 ms
 3  ae1.sxb1-ibr-altair.bb.gdinf.net (2a01:488:bb00:105::2)  0.597 ms  0.774 ms  1.354 ms
 4  ae0.sxb1-ibr-tarazed.bb.gdinf.net (2a01:488:bb00:107::3)  1.91 ms  5.008 ms  1.806 ms
 5  ae7.fra10-cr-antares.bb.gdinf.net (2a01:488:bb03:101::2)  3.437 ms  3.712 ms  3.632 ms
 6  ae2.fra11-cr-polaris.bb.gdinf.net (2a01:488:bb03:100::2)  3.484 ms  3.548 ms  3.346 ms
 7  jio.com (2001:7f8::fa31:0:1)  4.011 ms *  3.861 ms
 8  * * *
 9  2405:203:89a::141e (2405:203:89a::141e)  134.455 ms  134.438 ms  134.326 ms
10  2405:8a00:a:3::2 (2405:8a00:a:3::2)  133.211 ms  133.454 ms  133.237 ms
11  2405:8a00:a:a::3 (2405:8a00:a:a::3)  144.523 ms  144.554 ms  144.524 ms
12  * * *
13  2001:4408:a::1 (2001:4408:a::1)  150.418 ms  150.417 ms  150.36 ms
14  2405:8a00:a:2::c5 (2405:8a00:a:2::c5)  153.437 ms  150.688 ms  150.696 ms
15  2405:8a00:a:2::c6 (2405:8a00:a:2::c6)  153.386 ms  153.393 ms  153.322 ms
16  2001:df4:e000:108::2 (2001:df4:e000:108::2)  147.667 ms  147.571 ms  147.165 ms
17  2001:df4:e000:26::24 (2001:df4:e000:26::24)  150.601 ms  150.721 ms  150.513 ms
18  2001:df4:e000:29::212 (2001:df4:e000:29::212)  149.379 ms  149.433 ms  149.306 ms
```

Figure 4: traceroute from Germany to IIT Delhi(IPV6)

traceroute to www.google.com

```
traceroute to www.google.com (142.250.184.196), 30 hops max, 60 byte packets
 1  vsn0057.vs.mass.systems (10.92.36.120)  0.029 ms  0.014 ms  0.012 ms
 2  ae3-u100.sxb1-cr-nunki.bb.gdinf.net (87.230.112.2)  0.352 ms  0.337 ms  0.286 ms
 3  ae1.sxb1-ibr-altair.bb.gdinf.net (87.230.112.14)  0.496 ms  0.511 ms  0.538 ms
 4  ffm-b16-link.ip.twelve99.net (62.115.144.8)  3.007 ms  2.982 ms  2.953 ms
 5  * ffm-bb1-link.ip.twelve99.net (62.115.132.226)  3.371 ms  3.414 ms
 6  ffm-b11-link.ip.twelve99.net (62.115.124.119)  3.181 ms  3.338 ms ffm-b11-link.ip.twelve99.net (62.115.124.117)  3.263 ms
 7  google-ic-319726.ip.twelve99-cust.net (62.115.151.25)  3.261 ms google-ic-319727.ip.twelve99-cust.net (62.115.151.27)  3.552 ms  3.526 ms
 8  * * *
 9  192.178.74.162 (192.178.74.162)  3.545 ms 108.170.252.65 (108.170.252.65)  4.596 ms 142.250.214.202 (142.250.214.202)  5.202 ms
10  108.170.251.209 (108.170.251.209)  4.054 ms 142.251.64.187 (142.251.64.187)  3.440 ms 108.170.252.82 (108.170.252.82)  3.513 ms
11  * fra24s11-in-f4.1e100.net (142.250.184.196)  3.247 ms  3.252 ms
```

Figure 5: traceroute from Germany to Google

traceroute to www.facebook.com

```
traceroute to www.facebook.com (157.240.210.35), 30 hops max, 60 byte packets
 1  vsn0057.vs.mass.systems (10.92.36.120)  0.028 ms  0.015 ms  0.010 ms
 2  ae3-u100.sxb1-cr-nunki.bb.gdinf.net (87.230.112.2)  0.542 ms  0.353 ms  0.337 ms
 3  ae1.sxb1-ibr-altair.bb.gdinf.net (87.230.112.14)  0.761 ms  0.738 ms  0.710 ms
 4  ae0.sxb1-ibr-tarazed.bb.gdinf.net (87.230.112.19)  0.679 ms  0.662 ms  0.636 ms
 5  ae7.fra10-cr-antares.bb.gdinf.net (87.230.115.2)  3.805 ms  3.825 ms  3.801 ms
 6  ae2.fra1-cr-polaris.bb.gdinf.net (87.230.115.0)  3.430 ms  3.617 ms  3.579 ms
 7  ae1.pr02.ham3.tfbnw.net (185.1.210.174)  9.140 ms  9.811 ms  9.808 ms
 8  po202.asw02.ham3.tfbnw.net (157.240.111.196)  9.226 ms po202.asw01.ham3.tfbnw.net (157.240.111.194)  9.380 ms  9.374 ms
 9  psw02.ham3.tfbnw.net (129.134.58.116)  9.248 ms psw03.ham3.tfbnw.net (129.134.58.115)  9.224 ms psw01.ham3.tfbnw.net (129.134.58.117)  9.224 ms
10  157.240.38.71 (157.240.38.71)  9.324 ms 157.240.38.169 (157.240.38.169)  9.189 ms 173.252.67.165 (173.252.67.165)  9.215 ms
11  edge-star-mini-shv-01-ham3.facebook.com (157.240.210.35)  9.307 ms  9.146 ms  9.138 ms
```

Figure 6: traceroute from Germany to Facebook

Traceroute

tracing path from www.net.princeton.edu to 155.98.186.21 ...

```
traceroute to 155.98.186.21 (155.98.186.21), 30 hops max, 40 byte packets
 1  128.112.128.2  1.001 ms  0.790 ms  0.753 ms
 2  128.112.12.229  0.742 ms  0.569 ms  0.734 ms
 3  128.112.12.14  1.091 ms  1.043 ms  1.135 ms
 4  204.153.48.253  1.263 ms  1.379 ms  1.689 ms
 5  172.96.130.49  4.339 ms  3.953 ms  3.937 ms
 6  172.96.130.76  5.491 ms  5.978 ms 172.96.130.60  6.042 ms
 7  163.253.5.8  5.085 ms  6.045 ms  6.022 ms
 8  163.253.1.136  63.700 ms  63.350 ms  61.768 ms
 9  163.253.1.139  62.084 ms  63.635 ms  63.119 ms
10  163.253.2.17  63.265 ms  63.487 ms  63.332 ms
11  163.253.2.18  63.250 ms  62.922 ms  62.777 ms
12  163.253.1.245  64.246 ms  63.623 ms  63.564 ms
13  163.253.1.242  63.570 ms  63.474 ms  63.117 ms
14  163.253.1.171  63.287 ms  62.156 ms  63.240 ms
15  163.253.1.152  62.891 ms  63.220 ms  63.699 ms
16  163.253.5.7  63.844 ms  64.283 ms  64.376 ms
17  140.197.249.81  62.072 ms  62.154 ms  62.737 ms
18  140.197.251.32  63.364 ms  62.686 ms  62.567 ms
19  140.197.253.97  63.057 ms  63.220 ms  62.443 ms
20  140.197.252.76  62.409 ms  62.432 ms  63.061 ms
21  140.197.252.84  63.177 ms  62.595 ms  62.682 ms
22  * * *
23  199.104.93.22  62.650 ms  63.286 ms  63.092 ms
24  199.104.93.33  64.320 ms  64.019 ms  64.133 ms
25  155.99.130.65  63.821 ms  63.794 ms 155.99.130.67  63.449 ms
26  155.99.130.107  64.450 ms  65.173 ms 155.99.130.105  64.422 ms
27  * * *
28  * * *
29  * * *
30  155.98.186.21  64.940 ms  64.792 ms  64.166 ms
```

Done.

Figure 7: traceroute from Germany to Utah

Traceroute

tracing path from www.net.princeton.edu to 137.158.159.192 ...

```
traceroute to 137.158.159.192 (137.158.159.192), 30 hops max, 40 byte packets
 1  128.112.128.2  1.100 ms  0.989 ms  0.783 ms
 2  128.112.12.225  0.789 ms  0.551 ms  0.550 ms
 3  128.112.12.10  0.911 ms  0.897 ms  0.901 ms
 4  204.153.48.1  1.303 ms  2.245 ms  1.220 ms
 5  172.96.130.53  5.545 ms  5.983 ms  6.167 ms
 6  163.253.5.8  4.896 ms  6.031 ms  4.059 ms
 7  163.253.1.136  25.940 ms  26.487 ms  28.547 ms
 8  163.253.1.135  29.156 ms  26.231 ms  28.415 ms
 9  163.253.1.100  26.342 ms  26.484 ms  28.396 ms
10  163.253.2.33  27.219 ms  26.415 ms  26.244 ms
11  155.232.71.4  191.566 ms  191.656 ms 155.232.71.2  193.004 ms
12  155.232.64.36  191.844 ms 155.232.64.34  191.927 ms 155.232.64.144  191.883 ms
13  155.232.64.70  191.563 ms  191.456 ms  191.507 ms
14  154.114.124.1  191.841 ms  191.949 ms  191.829 ms
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Done.

Figure 8: traceroute from USA to Uct

Traceroute

tracing path from www.net.princeton.edu to 103.27.9.24 ...

```
traceroute to 103.27.9.24 (103.27.9.24), 30 hops max, 40 byte packets
 1  128.112.128.2  0.832 ms  0.655 ms  0.957 ms
 2  128.112.12.225  0.662 ms  0.560 ms  0.607 ms
 3  128.112.12.10  1.102 ms  0.887 ms  0.988 ms
 4  204.153.48.1  14.879 ms  7.770 ms  1.370 ms
 5  172.96.130.53  4.617 ms  4.021 ms  4.230 ms
 6  172.96.130.61  6.099 ms  6.064 ms 172.96.130.77  6.190 ms
 7  163.253.5.38  6.800 ms  6.173 ms  6.095 ms
 8  180.149.48.12  85.213 ms  85.185 ms  85.229 ms
 9  180.149.48.1  228.044 ms 180.149.48.21  85.958 ms 180.149.48.1  227.515 ms
10  180.149.48.17  228.479 ms 180.149.48.5  228.298 ms 180.149.48.17  229.027 ms
11  * 180.149.48.17  227.395 ms *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Done.

Figure 9: traceroute from USA to IIT Delhi

traceroute to www.google.com

```
traceroute to www.google.com (142.250.184.196), 30 hops max, 60 byte packets
 1  vsn0057.vs.mass.systems (10.92.36.120)  0.029 ms  0.014 ms  0.012 ms
 2  ae3-u100.sxb1-cr-nunki.bb.gdinf.net (87.230.112.2)  0.352 ms  0.337 ms  0.286 ms
 3  ae1.sxb1-ibr-altair.bb.gdinf.net (87.230.112.14)  0.496 ms  0.511 ms  0.538 ms
 4  ffm-b16-link.ip.twelve99.net (62.115.144.8)  3.007 ms  2.982 ms  2.953 ms
 5  * ffm-bb1-link.ip.twelve99.net (62.115.132.226)  3.371 ms  3.414 ms
 6  ffm-b11-link.ip.twelve99.net (62.115.124.119)  3.181 ms  3.338 ms ffm-b11-link.ip.twelve99.net (62.115.124.117)  3.263 ms
 7  google-ic-319726.ip.twelve99-cust.net (62.115.151.25)  3.261 ms google-ic-319727.ip.twelve99-cust.net (62.115.151.27)  3.552 ms  3.526 ms
 8  * * *
 9  192.178.74.162 (192.178.74.162)  3.545 ms 108.170.252.65 (108.170.252.65)  4.596 ms 142.250.214.202 (142.250.214.202)  5.202 ms
10  108.170.251.209 (108.170.251.209)  4.054 ms 142.251.64.187 (142.251.64.187)  3.440 ms 108.170.252.82 (108.170.252.82)  3.513 ms
11  * fra24s11-in-f4.1e100.net (142.250.184.196)  3.247 ms  3.252 ms
```

Figure 10: traceroute from USA to Google

Traceroute

tracing path from www.net.princeton.edu to 31.13.71.36 ...

```
traceroute to 31.13.71.36 (31.13.71.36), 30 hops max, 40 byte packets
 1  128.112.128.2  1.169 ms  0.743 ms  1.069 ms
 2  128.112.12.225  0.787 ms  0.754 ms  0.668 ms
 3  128.112.12.10  0.895 ms  0.878 ms  0.905 ms
 4  204.153.48.1  2.322 ms  1.383 ms  1.298 ms
 5  172.96.130.53  3.308 ms  4.165 ms  3.872 ms
 6  172.96.130.77  6.073 ms 172.96.130.61  5.951 ms  6.263 ms
 7  198.71.47.232  7.510 ms  5.954 ms  6.051 ms
 8  163.253.2.123  7.161 ms 163.253.2.149  6.262 ms  5.973 ms
 9  162.252.69.205  5.094 ms  4.553 ms 162.252.69.207  4.992 ms
10  157.240.103.128  3.641 ms 157.240.103.116  3.645 ms  4.137 ms
11  157.240.107.143  4.535 ms 157.240.107.163  4.036 ms 157.240.107.189  3.823 ms
12  173.252.67.75  4.431 ms 157.240.38.65  4.539 ms 157.240.38.243  3.948 ms
13  31.13.71.36  3.812 ms  4.427 ms  3.704 ms
```

Done.

Figure 11: traceroute from USA to Facebook

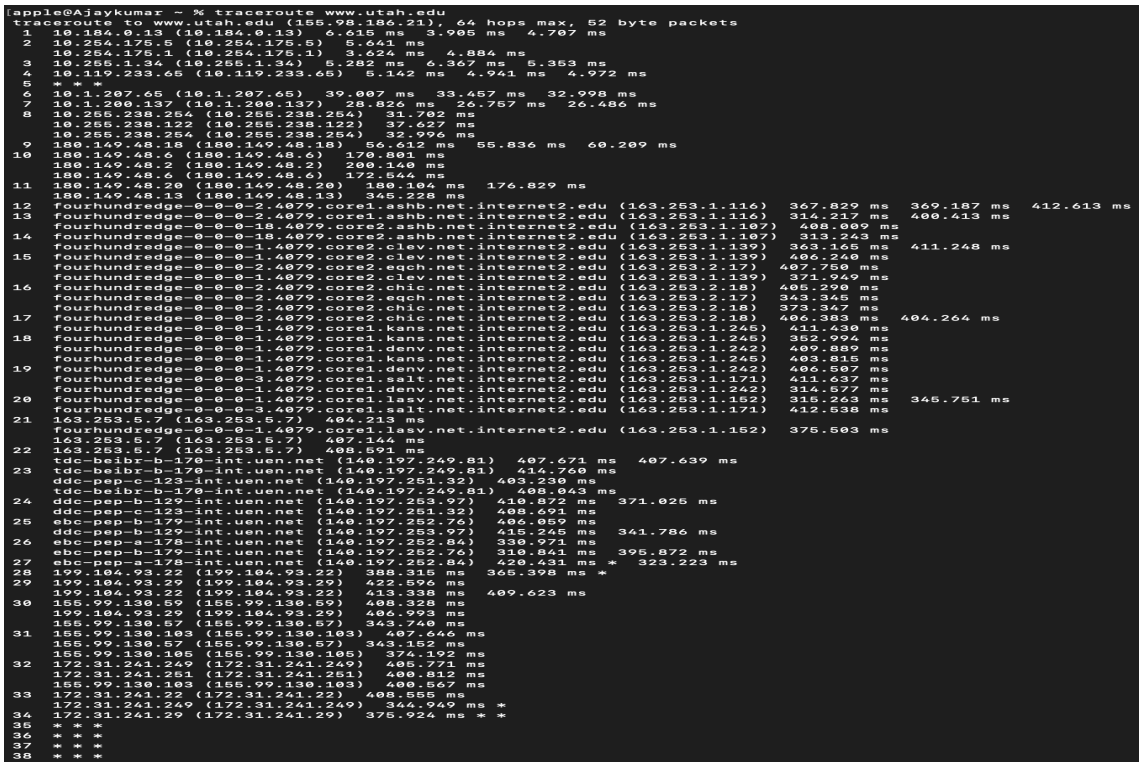

Figure 12: traceroute from my Device to Utah

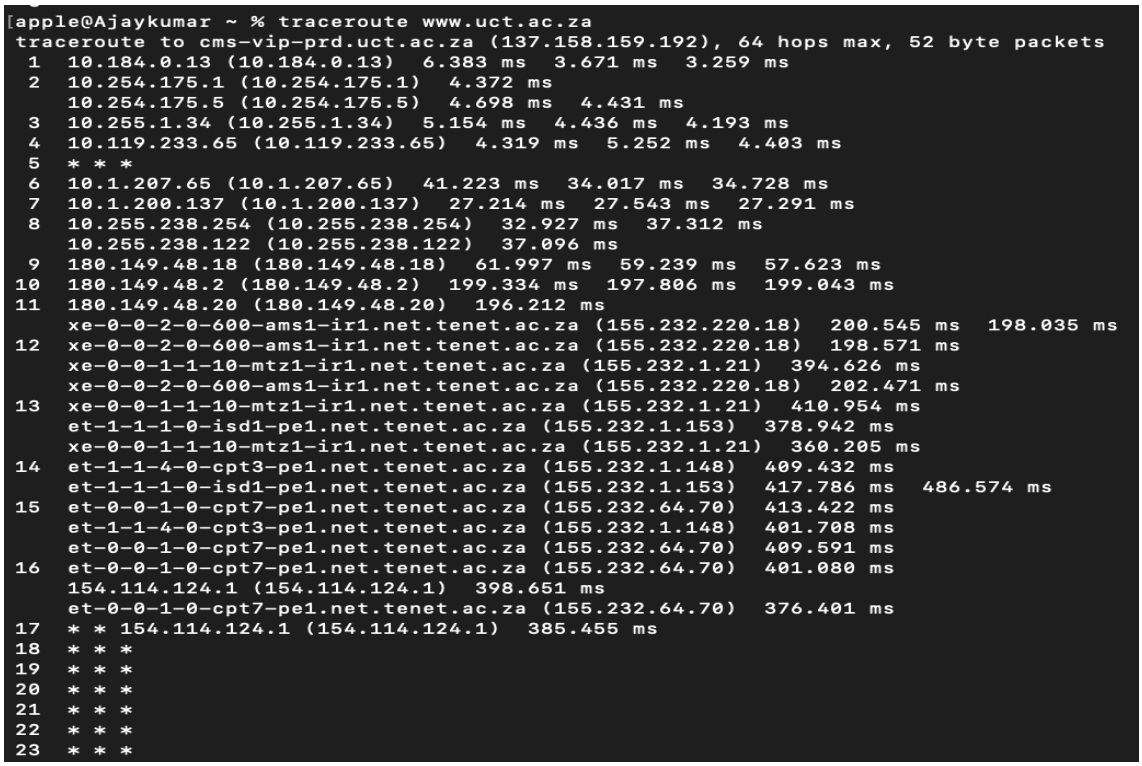

Figure 13: traceroute from my Device to Uct

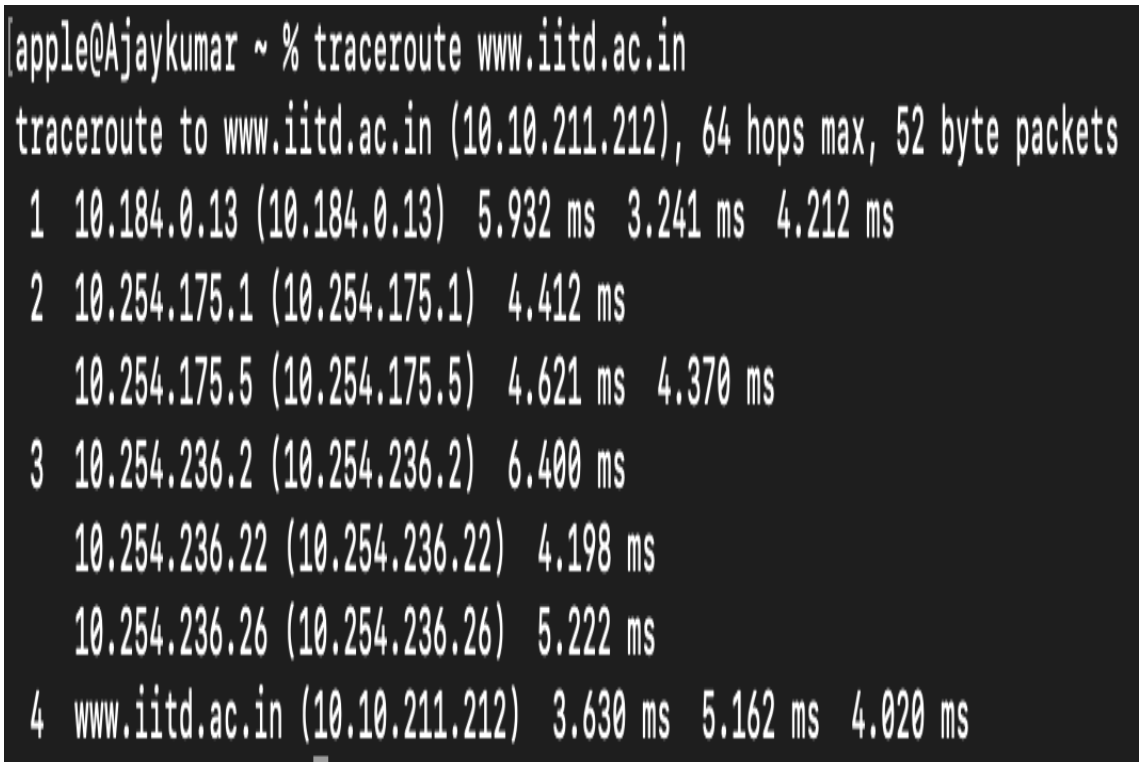

Figure 14: traceroute from my Device to IIT Delhi

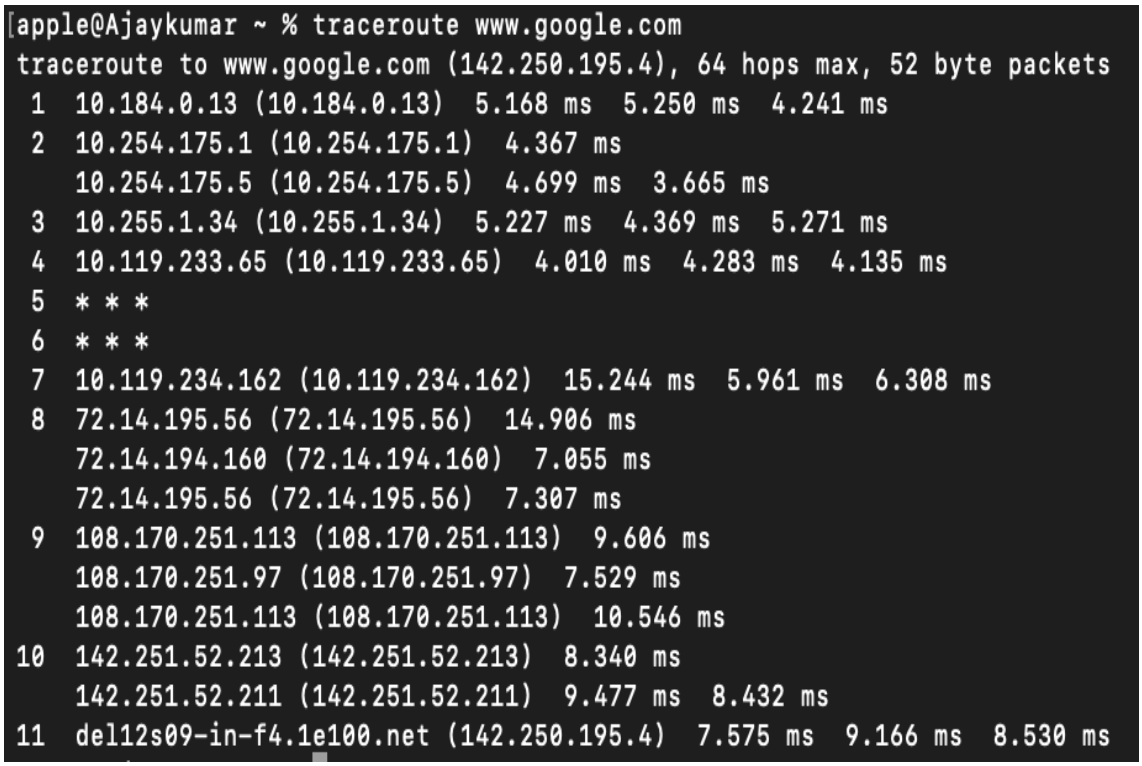

Figure 15: traceroute from my Device to Google

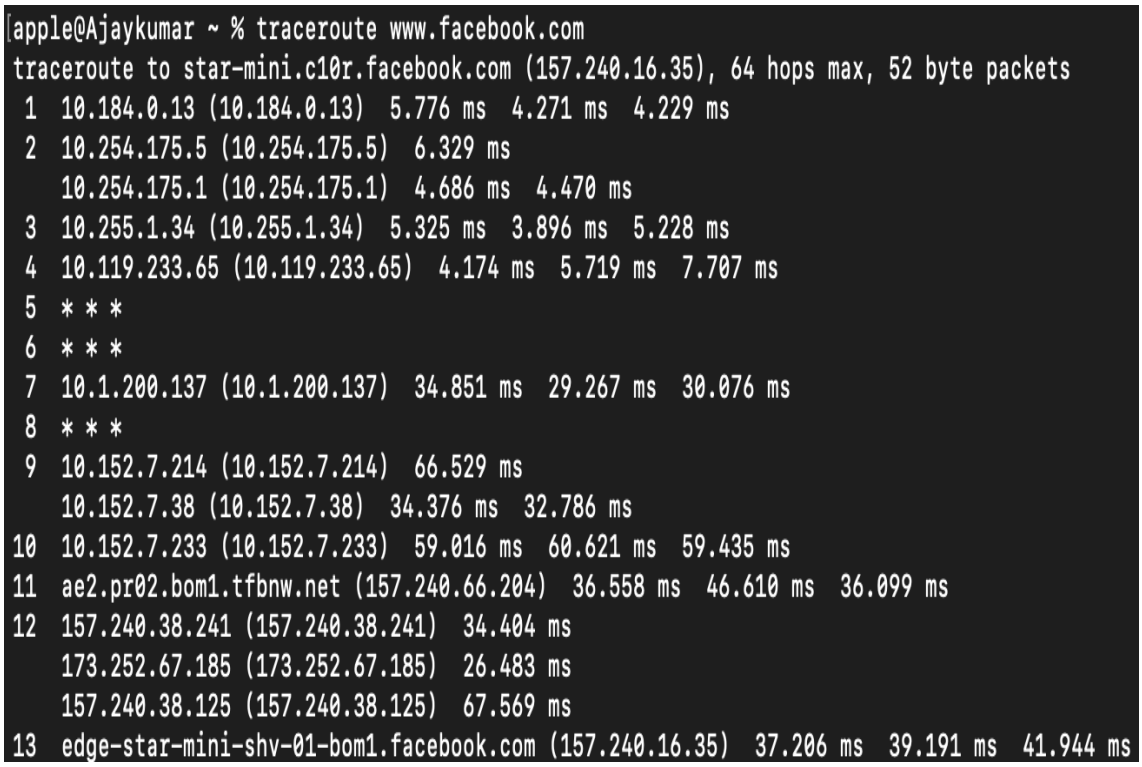

Figure 16: traceroute from my Device to Facebook

If the pair of (traceroute source, destination) are geographically close to each other, does it roughly translate into fewer hops?

Yes, If the pair of Traceroute source and Destination are geograhically close to each other, number of routers in between the respected source to destination will be less than the geographically the router which is far away from a particular. so it translates into fewer hops in the traceroute due to network infrastructure (as per distancing). The data packets can take a more direct route with fewer intermediary routers, resulting in a shorter path and, consequently, fewer hops. (Note: This might not be always true because proximity geography is not the only aspect to observed, it also can depend on various other factors like peering agreements, ISPs balancing, and so on.)

Do Google and Facebook differ from the others in the number of hops required to reach them, irrespective of which traceroute source is used? Why would this be so?

Yes, Google and Facebook will differ from other destinations according to the number of hops required to reach from source to destination. These differences can be observed irrespective of which traceroute source is used.The reasons can be:
1. Network Infrastructure: Global infrastructure locating around the world can result in shorter and more direct paths for data packets, leading to fewer hops.
2. Peering Relationships: Google and Facebook have established peering agreements with many ISPs and networks, allowing them to exchange traffic directly without going through as many intermediary routers. This direct peering can lead to fewer hops and faster connections.
3. Optimized Routing: Large tech companies like Google and Facebook invest in advanced routing technologies to optimize traffic flow. They use tools that dynamically select the best routes based on factors like latency and congestion, leading to efficient paths with fewer hops.
and so on.

3.b. Also report the latencies between the traceroute sources and the webservers. Does the latency seem to be related to the number of hops, being higher when there are more hops? Why is this the case?

Yes, there is a relation (in most of the cases) in between the number of hops and the latency or round trip time in a traceroute. Higher latency tends to be associated with more hops. This is due to the time it takes for data packets to traverse each network node and the nature of network communication too because several factors contribute this like:
1. Processing Delay: Each network device needs time to examine and process the packet header, determine the next hop, and forward the packet. This ddelay accumulates with each hop.
2. Propagation Delay: Data packets travel at the speed of light, but there is a

finite time it takes for the signal to propagate across physical links and cables. As the packet traverses more hops, the cumulative propagation delay increases.
3. Queueing delay: Network devices can introduce delays if they have a large number of packets in their queues awaiting processing or if there is congestion on the network. These delays become more significant with more hops.
4. Transmission delay: The amount of time required to push all the packet's bits into the wire
5. Longer Paths: Longer paths, with more intermediate routers, often involve routing through different geographical locations or across different network providers. These paths can introduce additional latency due to longer physical distances. and so on.
Between every two routers there are these above mentioned delays which cause latency.

3.c I haven't found any destination web-servers that are resolved to the same IP address with google and facebook on which we have worked on. I think this is because in differnet parts of the world traceroute servers use their nearest location DNS servers, in which DNS servers resolve IP addresses and Google and facebook has large number of data centres with servers across the world. so they could end up showing different IP Addresses. but also found that for any destination web-servers that are resolved to the same IP address with University of Utah and University of Cape Town. This may due to many factors like Geolocation, etc.

3.d Traceroute paths from the same starting point to different IP addresses associated with the same web-server are observed different. The IP addressess which are obtained from other continents their respective paths are longer and cant be reached in 30 hops (webserver used - www.iitd.ac.in), and the IP addressess which is obtained from my mobile-network can be reached in 12 hops.

3.e. Yes i am able to find countries which have high latencies above 200 ms which implies that they do not seem to have their local ISPs directly peered with Google and Facebook namely Nairobi of Africa(approximately 430 ms) and Taipei(approximately 355 ms), etc. because data centres for these countries to achieve lower latencies are far away from them and thus they are having the high latencies when traced via Internet. others like USA, UK they have nearer data centres which have lesser latency and are seemed to be directly peered to the local ISPs.

4

4.a. We have used wireshark and grabbed all packets on the wireless interface on HTTP website http://www.iitd.ac.in from the browser, applied dns filter on

the packet trace, we have observed the DNS queries and responses on wireshark.
Total time for A-type requests and responses is : 0.003628 sec.
Total time for http-type requests and responses is : 0.004049 sec.

We have used wireshark and grabbed all packets on the wireless interface on HTTP website http://act4d.iitd.ac.in from the browser, applied dns filter on the packet trace, we have observed the DNS queries and responses on wireshark. Total time for A-type requests and responses is : 0.003059 sec.
Total time for http-type requests and responses is : 0.003996 sec.

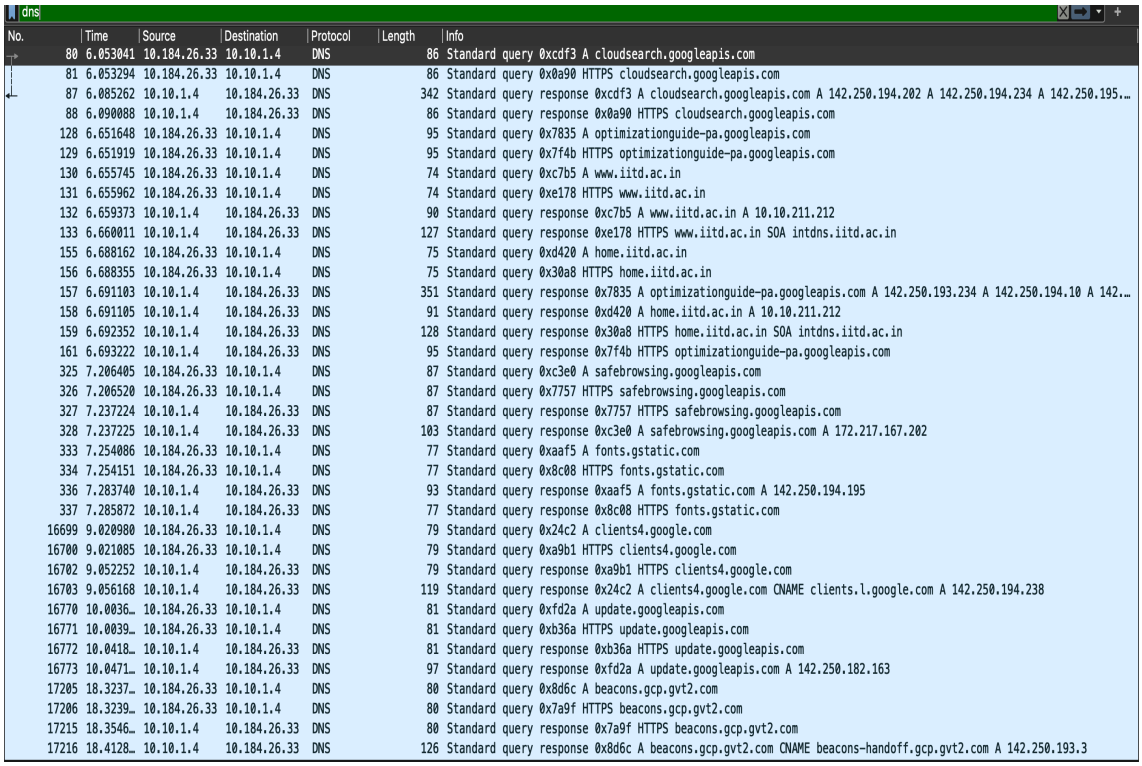

Figure 17: DNS filtered www.iitd.ac.in wireshark

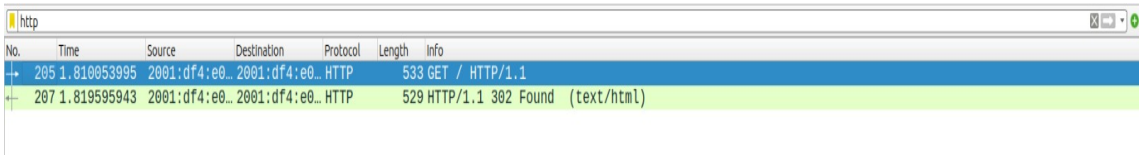

Figure 18: http filtered for http://iitd.ac.in wireshark

4.b. After applying http filter for www.iitd.ac.in, I am getting 1 http request and response as shown in fig.18

After applying http filter for www.act4d.iitd.ac.in, I am getting 11 http requests , requesting the server for html, css, js files required for a webpage and also images.

From this I can unuderstand that http requests are used for requesting the html, css, js, images, etc.. required for a webpage.

4.c. No, they are not same as the number of HTTP requests for content objects that we have found in the previous part. In the previous part we have got 11 https but now here we are able to see 20 TCPs so they are different.

4.d. On doing trace for http://www.indianexpress.com wew came across a few http requests on filtering http in the wireshark. By this we can say that there is a http traffic for http://www.indianexpress.com
yes, we have browsed the entire trace without any filters for http://indianexpress.com and we have seen the HTML file transferred, this means that the network traffic captured is not encrypted and the HTML content is being sent in clear text format.

http

No.	Time	Source	Destination	Protocol	Length	Info
211	4.613485	10.184.26.33	13.126.221.…	HTTP	450	GET / HTTP/1.1
213	4.646425	13.126.221.…	10.184.26.33	HTTP	438	HTTP/1.1 301 Moved Permanently (text/html)
1887	5.813076	10.184.26.33	142.250.192…	HTTP	440	GET /gts1c3/MFAwTjBMMEowSDAHBgUrDgMCGgQUxy55it3%2FYTSzuu1HQri7xsAkB2MEFIp0f6%2BFze6VzT2c0OJGFPNxNR0nAhEAyIknn6…
1888	5.813766	10.184.26.33	142.250.192…	HTTP	432	GET /gts1c3/ME8wTTBLMEkwRzAHBgUrDgMCGgQUxy55it3%2FYTSzuu1HQri7xsAkB2MEFIp0f6%2BFze6VzT2c0OJGFPNxNR0nAhBF7EQ1t3…
1895	5.822340	142.250.192…	10.184.26.33	OCSP	254	Response
1900	5.823177	142.250.192…	10.184.26.33	OCSP	253	Response
3220	6.651388	10.184.26.33	152.195.38.…	HTTP	429	GET /ME8wTTBLMEkwRzAHBgUrDgMCGgQUKx0emMzzdgTWwci9FaIkyAQTADgEFAq8CCkXjKU5bXoOzjPHLrPt%2B8N6AhAKTcD7q1oZF21lH%2…
3266	6.666176	152.195.38.…	10.184.26.33	OCSP	120	Response
4343	7.750705	10.184.26.33	108.158.57.…	HTTP	442	GET /ME8wTTBLMEkwRzAHBgUrDgMCGgQUoXVRBZ0hENIBuQgbczOPHDzHvV8EFIG4DmOKiRIY5fo7O1CVn%2BblkBOFAhAOQhQc4A%2B%2FylA…
4364	7.805119	108.158.57.…	10.184.26.33	OCSP	537	Response
5921	9.611744	10.184.26.33	142.250.192…	HTTP	442	GET /gts1c3/MFAwTjBMMEowSDAHBgUrDgMCGgQUxy55it3%2FYTSzuu1HQri7xsAkB2MEFIp0f6%2BFze6VzT2c0OJGFPNxNR0nAhEAqxsAd1…
5940	9.623798	142.250.192…	10.184.26.33	OCSP	255	Response

Figure 19: http filtered www.indianexpress.com.in wireshark

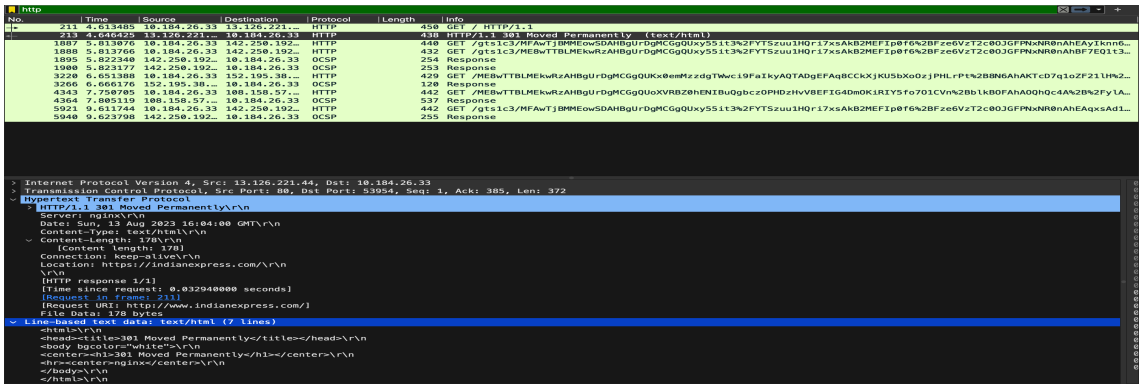

Figure 20: HTML clear text for http://indianexpress.com inn wireshark

Figure 21: http filtered for http://act4d.iitd.ac.in wireshark