

# COL334 Assignment1

Ankit Mondal\* and Anish Banerjee<sup>†</sup>

August 13, 2023

## §1. Network Analysis

- a. We ran `tracert` on `iitd.ac.in` outside IITD network and got the following output:

```
PS C:\Users\Anish> tracert iitd.ac.in

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

  1    4 ms    3 ms    9 ms dsldevice.lan [192.168.1.1]
  2   87 ms   73 ms   26 ms abts-north-dynamic-255.187.69.182.airtelbroadband.in [182.69.187.255]
  3   34 ms   28 ms   48 ms 125.18.240.153
  4   38 ms   45 ms   38 ms 116.119.106.136
  5   47 ms   53 ms   49 ms 49.44.220.188
  6    *      *      *    Request timed out.
  7    *      *      *    Request timed out.
  8   47 ms   43 ms   47 ms 136.232.148.178
  9    *      *      *    Request timed out.
 10   *      *      *    Request timed out.
 11   *      *      *    Request timed out.
 12   45 ms   59 ms   52 ms 103.27.9.24
 13  187 ms   46 ms   61 ms 103.27.9.24
 14   47 ms   48 ms   49 ms 103.27.9.24

Trace complete.
```

### Observations

As seen above, hops 6 to 11 (except 8) show "Request timed out," which can be indicative of routers along the path that do not respond to the traceroute requests. There is no specific indication of IPv6 usage here; the timeouts could be due to various reasons, including router/firewall configurations.

We also notice that `192.168.1.1` belongs to a private IP space.

Multiple replies from the final destination IP address (`103.27.9.24`) raise some curiosity. This could be due to various configurations, such as load balancers or redundant paths.

- b. We used the `tracert -6` to use IPv6 but always got the output as "Unable to resolve target system name `iitd.ac.in`." Instead, we ran `tracert` and `tracert6` on `google.com` from a different device and got the following outputs:

---

\*2021CS10229

†2021CS10134

```

traceroute to google.com (142.250.194.14), 64 hops max, 52 byte packets
 1  192.168.177.193 (192.168.177.193)  6.868 ms  5.484 ms  6.407 ms
 2  192.168.59.1 (192.168.59.1)  22.799 ms  20.424 ms  27.980 ms
 3  192.168.27.81 (192.168.27.81)  29.813 ms
    192.168.27.93 (192.168.27.93)  23.077 ms
    192.168.27.81 (192.168.27.81)  21.428 ms
 4  192.168.27.109 (192.168.27.109)  36.098 ms
    192.168.27.105 (192.168.27.105)  18.040 ms  28.957 ms
 5  nsg-corporate-1.39.185.122.airtel.in (122.185.39.1)  39.461 ms  66.444 ms  54.972 ms
 6  72.14.217.194 (72.14.217.194)  44.254 ms * *
 7  * * *
 8  * * 142.251.76.196 (142.251.76.196)  66.303 ms
 9  142.251.52.199 (142.251.52.199)  34.779 ms
    74.125.244.196 (74.125.244.196)  21.764 ms *
10  * 108.170.251.97 (108.170.251.97)  54.197 ms
    del12s01-in-f14.1e100.net (142.250.194.14)  28.694 ms

```

```

traceroute6 to google.com (2404:6800:4007:82b::200e) from 2401:4900:47f2:38e0:39b1:d74c:415:5bc2,
64 hops max, 12 byte packets
 1  2401:4900:47f2:38e0::cf  4.692 ms  4.160 ms  8.239 ms
 2  2401:4900:47f2:38e0:0:e:4f83:ae40  19.732 ms  49.145 ms  22.655 ms
 3  2401:4900:0:c003::6402  41.364 ms  24.693 ms  33.984 ms
 4  2401:4900:0:c003::6631  29.735 ms
    2401:4900:0:c003::663d  22.365 ms
    2401:4900:0:c003::6631  37.879 ms
 5  2401:4900:0:c003::6664  24.392 ms
    2401:4900:0:c003::6666  89.694 ms
    2401:4900:0:c003::6662  36.760 ms
 6  2404:a800:1a00:801::e5  30.302 ms  36.528 ms  30.057 ms
 7  2001:4860:1:1::10c4  26.523 ms  36.783 ms  42.481 ms
 8  2404:6800:8107::1  66.432 ms
    2404:6800:8129::1  38.610 ms
    2404:6800:811f::1  87.382 ms
 9  2001:4860:0:1::54e6  23.382 ms
    2001:4860:0:1::539a  26.511 ms
    2001:4860:0:1::306a  64.307 ms
10  2001:4860:0:1a::c  85.624 ms
    2001:4860:0:9e::3  31.224 ms
    2001:4860:0:9e::4  45.091 ms
11  2001:4860::9:4001:67bd  88.336 ms
    2001:4860::9:4001:67bc  74.379 ms  83.693 ms
12  2001:4860:0:1340::1  73.053 ms
    2001:4860::9:4001:b922  69.519 ms
    2001:4860::9:4002:d27c  66.132 ms
13  2001:4860:0:133f::1  66.074 ms
    2001:4860::9:4001:163c  80.668 ms
    2001:4860::9:4001:b922  97.471 ms
14  maa03s46-in-x0e.1e100.net  86.829 ms
    2001:4860:0:1::55ff  106.150 ms
    maa03s46-in-x0e.1e100.net  69.276 ms

```

## Observations

Here, hops 1-4 are private IPs for IPv4. Router 7 did not respond to IPv4 request. We also observe that the number of hops for IPv6 packets are more than that for IPv4 packets. This is because IPv6 packets are routed differently than IPv4 packets.

- c. We observe that the maximum packet size that can be sent is 68 (to google.com)

```

root@IdeapadAB:/mnt/c/Users/Anish# ping -s 68 -c 5 google.com
PING google.com (142.250.194.238) 68(96) bytes of data.
76 bytes from del12s08-in-f14.1e100.net (142.250.194.238): icmp_seq=1 ttl=116 time=7.00 ms
76 bytes from del12s08-in-f14.1e100.net (142.250.194.238): icmp_seq=2 ttl=116 time=6.73 ms
76 bytes from del12s08-in-f14.1e100.net (142.250.194.238): icmp_seq=3 ttl=116 time=7.11 ms
76 bytes from del12s08-in-f14.1e100.net (142.250.194.238): icmp_seq=4 ttl=116 time=6.05 ms
76 bytes from del12s08-in-f14.1e100.net (142.250.194.238): icmp_seq=5 ttl=116 time=7.98 ms

--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 6.052/6.973/7.975/0.621 ms
root@IdeapadAB:/mnt/c/Users/Anish# ping -s 69 -c 5 google.com
PING google.com (142.250.194.238) 69(97) bytes of data.

--- google.com ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4009ms

```

However, the max ping size depends on the site requested for. For example, we saw that for `iitd.ac.in`, it is 1472 bytes. We can run the following python code to find the maximum packet size for a given site. In it, 65007 is the maximum size of the packet that can be sent by ping.

```

#!/usr/bin/python3

import os
site=input("Enter the site: ")
l=1
r=65007
while l<r:
    mid=(l+r)//2
    if os.system("ping -c 1 -s "+str(mid)+" "+site)==0:
        l=mid+1
    else:
        r=mid
print("\n\nMax ping size is: "+str(l-1))

```

## §2. traceroute using python

The code for traceroute can be found in `traceroute.py`.

## §3. Internet Architecture

We ran a traceroute from our own IP address, Buenos Aires and Johannesburg to the 5 different servers.

### 3.1. Local Device, Delhi

#### 3.1.1. www.google.com

```
Ankits-MacBook-Air-6:~ ankitmondal traceroute google.com
traceroute to google.com (142.250.194.238), 64 hops max, 52 byte packets
 1  10.184.0.13 (10.184.0.13)  3.999 ms  3.570 ms  3.506 ms
 2  10.254.175.1 (10.254.175.1)  4.146 ms
    10.254.175.5 (10.254.175.5)  3.675 ms  3.223 ms
 3  10.255.1.34 (10.255.1.34)  3.562 ms  3.512 ms  3.357 ms
 4  10.119.233.65 (10.119.233.65)  3.463 ms  3.959 ms  3.930 ms
 5  * * *
 6  10.119.234.162 (10.119.234.162)  12.045 ms  5.639 ms  5.675 ms
 7  72.14.194.160 (72.14.194.160)  5.484 ms  5.647 ms  6.487 ms
 8  108.170.251.113 (108.170.251.113)  7.106 ms
    108.170.251.97 (108.170.251.97)  6.339 ms  6.480 ms
 9  142.251.52.217 (142.251.52.217)  6.274 ms  6.749 ms  6.689 ms
10  del12s08-in-f14.1e100.net (142.250.194.238)  6.588 ms  6.423 ms  6.608 ms
```

#### 3.1.2. www.uct.ac.za

```
traceroute to cms-vip-prd.uct.ac.za (137.158.159.192), 64 hops max, 52 byte packets
 1  10.184.0.13 (10.184.0.13)  22.724 ms  10.579 ms  12.871 ms
 2  10.254.175.5 (10.254.175.5)  17.468 ms
    10.254.175.1 (10.254.175.1)  14.286 ms  10.934 ms
 3  10.255.1.34 (10.255.1.34)  12.039 ms  5.280 ms  4.924 ms
 4  10.119.233.65 (10.119.233.65)  4.448 ms  10.977 ms  10.331 ms
 5  * * *
 6  10.1.207.65 (10.1.207.65)  30.769 ms  31.445 ms  29.155 ms
 7  10.1.200.137 (10.1.200.137)  28.082 ms  28.558 ms  27.255 ms
 8  10.255.238.122 (10.255.238.122)  32.098 ms
    10.255.238.254 (10.255.238.254)  33.832 ms
    10.255.238.122 (10.255.238.122)  33.503 ms
 9  180.149.48.18 (180.149.48.18)  28.309 ms  28.897 ms  28.542 ms
10  180.149.48.2 (180.149.48.2)  167.262 ms  166.161 ms
    180.149.48.6 (180.149.48.6)  181.931 ms
11  xe-0-0-2-0-600-ams1-ir1.net.tenet.ac.za (155.232.220.18)  199.348 ms  205.185 ms  200.641 ms
12  xe-0-0-1-1-10-mtz1-ir1.net.tenet.ac.za (155.232.1.21)  353.265 ms
    xe-0-0-2-0-600-ams1-ir1.net.tenet.ac.za (155.232.220.18)  218.119 ms  198.841 ms
13  xe-0-0-1-1-10-mtz1-ir1.net.tenet.ac.za (155.232.1.21)  402.440 ms  512.822 ms
    et-1-1-1-0-isd1-pel.net.tenet.ac.za (155.232.1.153)  405.517 ms
14  et-1-1-1-0-isd1-pel.net.tenet.ac.za (155.232.1.153)  411.163 ms
    et-1-1-4-0-cpt3-pel.net.tenet.ac.za (155.232.1.148)  402.903 ms  407.985 ms
15  et-1-1-4-0-cpt3-pel.net.tenet.ac.za (155.232.1.148)  409.552 ms
    et-0-0-1-0-cpt7-pel.net.tenet.ac.za (155.232.64.70)  365.084 ms
    et-1-1-4-0-cpt3-pel.net.tenet.ac.za (155.232.1.148)  400.673 ms
16  154.114.124.1 (154.114.124.1)  553.086 ms
    et-0-0-1-0-cpt7-pel.net.tenet.ac.za (155.232.64.70)  412.126 ms
    154.114.124.1 (154.114.124.1)  406.682 ms
17  * 154.114.124.1 (154.114.124.1)  522.107 ms *
18  * * *
19  * * *
20  * * *
21  * * *
```

```

22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *

```

### 3.1.3. www.iitd.ac.in

```

Ankits-MacBook-Air-6:~ ankitmondal traceroute www.iitd.ac.in
traceroute to www.iitd.ac.in (10.10.211.212), 64 hops max, 52 byte packets
 1  10.184.0.13 (10.184.0.13)  4.675 ms  4.242 ms  3.512 ms
 2  10.254.175.5 (10.254.175.5)  4.012 ms
    10.254.175.1 (10.254.175.1)  4.016 ms  4.356 ms
 3  10.254.236.6 (10.254.236.6)  3.285 ms
    10.254.236.26 (10.254.236.26)  3.920 ms
    10.254.236.2 (10.254.236.2)  5.730 ms
 4  www.iitd.ac.in (10.10.211.212)  3.830 ms  4.643 ms  5.628 ms

```

### 3.1.4. www.utah.edu

```

Ankits-MacBook-Air-6:~ ankitmondal traceroute www.utah.edu
traceroute to www.utah.edu (155.98.186.21), 64 hops max, 52 byte packets
 1  10.184.0.13 (10.184.0.13)  5.480 ms  3.898 ms  3.338 ms
 2  10.254.175.1 (10.254.175.1)  3.602 ms
    10.254.175.5 (10.254.175.5)  3.922 ms  3.769 ms
 3  10.255.1.34 (10.255.1.34)  5.116 ms  5.269 ms  5.756 ms
 4  10.119.233.65 (10.119.233.65)  64.339 ms  67.830 ms  65.010 ms
 5  10.1.207.69 (10.1.207.69)  80.742 ms  86.632 ms  93.759 ms
 6  10.1.200.137 (10.1.200.137)  84.119 ms  85.695 ms  70.847 ms
 7  10.255.238.254 (10.255.238.254)  80.166 ms
    10.255.238.122 (10.255.238.122)  78.281 ms
    10.255.238.254 (10.255.238.254)  86.918 ms
 8  180.149.48.18 (180.149.48.18)  71.995 ms  60.372 ms  58.199 ms
 9  180.149.48.6 (180.149.48.6)  244.512 ms  207.941 ms  197.721 ms
10  180.149.48.20 (180.149.48.20)  182.712 ms
    180.149.48.13 (180.149.48.13)  337.379 ms
    180.149.48.20 (180.149.48.20)  173.159 ms
11  fourhundredge-0-0-0-2.4079.core1.ashb.net.internet2.edu (163.253.1.116)  340.584 ms
    180.149.48.13 (180.149.48.13)  270.570 ms
    fourhundredge-0-0-0-2.4079.core1.ashb.net.internet2.edu (163.253.1.116)  314.143 ms
12  fourhundredge-0-0-0-16.4079.core2.ashb.net.internet2.edu (163.253.1.3)  312.121 ms
    fourhundredge-0-0-0-2.4079.core1.ashb.net.internet2.edu (163.253.1.116)  417.111 ms
    fourhundredge-0-0-0-16.4079.core2.ashb.net.internet2.edu (163.253.1.3)  416.768 ms
13  fourhundredge-0-0-0-16.4079.core2.ashb.net.internet2.edu (163.253.1.3)  313.367 ms
    fourhundredge-0-0-0-1.4079.core2.clev.net.internet2.edu (163.253.1.139)  319.440 ms  418.102 ms
14  fourhundredge-0-0-0-1.4079.core2.clev.net.internet2.edu (163.253.1.139)  417.208 ms
    fourhundredge-0-0-0-2.4079.core2.eqch.net.internet2.edu (163.253.2.17)  416.394 ms
    fourhundredge-0-0-0-1.4079.core2.clev.net.internet2.edu (163.253.1.139)  319.361 ms
15  fourhundredge-0-0-0-2.4079.core2.eqch.net.internet2.edu (163.253.2.17)  410.326 ms
    fourhundredge-0-0-0-2.4079.core2.chic.net.internet2.edu (163.253.2.18)  416.659 ms
    fourhundredge-0-0-0-2.4079.core2.eqch.net.internet2.edu (163.253.2.17)  417.562 ms

```

```

16 fourhundredge-0-0-0-2.4079.core2.chic.net.internet2.edu (163.253.2.18) 415.580 ms 417.440 ms
   fourhundredge-0-0-0-1.4079.core1.kans.net.internet2.edu (163.253.1.245) 418.242 ms
17 fourhundredge-0-0-0-1.4079.core1.kans.net.internet2.edu (163.253.1.245) 418.728 ms
   fourhundredge-0-0-0-1.4079.core1.denv.net.internet2.edu (163.253.1.242) 416.527 ms 417.077 ms
18 fourhundredge-0-0-0-1.4079.core1.denv.net.internet2.edu (163.253.1.242) 416.455 ms
   fourhundredge-0-0-0-3.4079.core1.salt.net.internet2.edu (163.253.1.171) 418.388 ms
   fourhundredge-0-0-0-1.4079.core1.denv.net.internet2.edu (163.253.1.242) 314.445 ms
19 fourhundredge-0-0-0-3.4079.core1.salt.net.internet2.edu (163.253.1.171) 315.540 ms
   fourhundredge-0-0-0-1.4079.core1.lasv.net.internet2.edu (163.253.1.152) 411.072 ms
   fourhundredge-0-0-0-3.4079.core1.salt.net.internet2.edu (163.253.1.171) 417.062 ms
20 163.253.5.7 (163.253.5.7) 319.476 ms 319.171 ms
   fourhundredge-0-0-0-1.4079.core1.lasv.net.internet2.edu (163.253.1.152) 410.432 ms
21 tdc-beibr-b-170-int.uen.net (140.197.249.81) 415.347 ms 322.845 ms 404.272 ms
22 tdc-beibr-b-170-int.uen.net (140.197.249.81) 363.062 ms
   ddc-pep-c-123-int.uen.net (140.197.251.32) 318.119 ms
   tdc-beibr-b-170-int.uen.net (140.197.249.81) 322.820 ms
23 ddc-pep-c-123-int.uen.net (140.197.251.32) 346.374 ms
   ddc-pep-b-129-int.uen.net (140.197.253.97) 416.809 ms
   ddc-pep-c-123-int.uen.net (140.197.251.32) 411.102 ms
24 ddc-pep-b-129-int.uen.net (140.197.253.97) 416.736 ms
   ebc-pep-b-179-int.uen.net (140.197.252.76) 416.798 ms
   ddc-pep-b-129-int.uen.net (140.197.253.97) 412.609 ms
25 ebc-pep-a-178-int.uen.net (140.197.252.84) 416.708 ms 411.943 ms
   ebc-pep-b-179-int.uen.net (140.197.252.76) 419.376 ms
26 * ebc-pep-a-178-int.uen.net (140.197.252.84) 319.891 ms *
27 * 199.104.93.22 (199.104.93.22) 337.648 ms *
28 199.104.93.22 (199.104.93.22) 321.654 ms
   199.104.93.29 (199.104.93.29) 343.305 ms
   199.104.93.22 (199.104.93.22) 345.169 ms
29 155.99.130.57 (155.99.130.57) 416.730 ms
   199.104.93.29 (199.104.93.29) 416.822 ms 416.541 ms
30 155.99.130.103 (155.99.130.103) 414.959 ms
   155.99.130.57 (155.99.130.57) 313.681 ms
   155.99.130.107 (155.99.130.107) 416.673 ms
31 172.31.241.255 (172.31.241.255) 416.605 ms
   155.99.130.101 (155.99.130.101) 412.722 ms
   172.31.241.255 (172.31.241.255) 416.726 ms
32 172.31.241.255 (172.31.241.255) 416.528 ms *
   172.31.241.251 (172.31.241.251) 423.757 ms
33 172.31.241.25 (172.31.241.25) 413.229 ms 404.049 ms
   172.31.241.22 (172.31.241.22) 425.597 ms
34 www.utah.edu (155.98.186.21) 412.101 ms * *

```

### 3.1.5. www.facebook.com

```
Ankits-MacBook-Air-6:~ ankitmondal traceroute facebook.com
traceroute to facebook.com (157.240.16.35), 64 hops max, 52 byte packets
 1  10.184.0.13 (10.184.0.13)  4.151 ms  3.441 ms  3.988 ms
 2  10.254.175.5 (10.254.175.5)  3.479 ms
    10.254.175.1 (10.254.175.1)  3.745 ms  3.525 ms
 3  10.255.1.34 (10.255.1.34)  3.845 ms  3.429 ms  6.735 ms
 4  10.119.233.65 (10.119.233.65)  13.776 ms  5.528 ms  4.366 ms
 5  10.1.207.69 (10.1.207.69)  29.882 ms  30.418 ms  31.270 ms
 6  * * *
 7  10.255.238.122 (10.255.238.122)  39.404 ms
    10.255.238.254 (10.255.238.254)  34.321 ms
    10.255.238.122 (10.255.238.122)  32.331 ms
 8  10.152.7.214 (10.152.7.214)  35.129 ms  33.873 ms  35.280 ms
 9  10.152.7.233 (10.152.7.233)  29.310 ms
    ae1.pr01.bom1.tfbnw.net (157.240.68.238)  53.885 ms  35.890 ms
10  po101.psw01.bom1.tfbnw.net (31.13.29.205)  38.635 ms
    po101.psw02.bom1.tfbnw.net (157.240.33.239)  35.706 ms
    ae2.pr02.bom1.tfbnw.net (157.240.66.204)  30.943 ms
11  po101.psw04.bom1.tfbnw.net (157.240.44.31)  29.498 ms *
    po102.psw02.bom1.tfbnw.net (157.240.35.63)  39.553 ms
12  157.240.38.65 (157.240.38.65)  30.149 ms
    173.252.67.185 (173.252.67.185)  35.504 ms
    edge-star-mini-shv-01-bom1.facebook.com (157.240.16.35)  31.092 ms
```

## 3.2. Buenos Aires, Argentina

### 3.2.1. www.utah.edu

```
traceroute to www.utah.edu (155.98.186.21), 30 hops max, 60 byte packets
 1  * *
 2  be2982.ccr41.mia03.atlas.cogentco.com (154.54.40.57)  141.964 ms  141.989 ms
 3  be3087.ccr22.mia01.atlas.cogentco.com (154.54.88.233)  142.235 ms  142.303 ms
 4  be3569.ccr41.iah01.atlas.cogentco.com (154.54.82.241)  168.591 ms be3570.ccr42.iah01.atlas.cogent
168.661 ms
 5  be2441.ccr31.dfw01.atlas.cogentco.com (154.54.41.66)  173.936 ms be2443.ccr32.dfw01.atlas.cogentc
173.817 ms
 6  be2432.ccr21.mci01.atlas.cogentco.com (154.54.3.134)  183.750 ms  183.779 ms
 7  be3036.ccr22.den01.atlas.cogentco.com (154.54.31.89)  195.119 ms be3035.ccr21.den01.atlas.cogentc
195.010 ms
 8  be3038.ccr32.slc01.atlas.cogentco.com (154.54.42.97)  205.222 ms be3037.ccr21.slc01.atlas.cogentc
205.428 ms
 9  be2685.rcr01.b020767-1.slc01.atlas.cogentco.com (154.54.41.118)  206.426 ms be2686.rcr01.b020767-
206.182 ms
10  38.142.233.58 (38.142.233.58)  206.340 ms  206.447 ms
11  lv3-beibr-a-184-int.uen.net (140.197.249.117)  206.151 ms  206.117 ms
12  ebc-pep-a-178-int.uen.net (140.197.253.23)  206.245 ms  206.264 ms
13  * *
14  199.104.93.22 (199.104.93.22)  206.421 ms  206.271 ms
15  199.104.93.29 (199.104.93.29)  207.058 ms  207.481 ms
16  155.99.130.59 (155.99.130.59)  207.155 ms  206.787 ms
17  155.99.130.105 (155.99.130.105)  208.150 ms  207.853 ms
18  172.31.241.251 (172.31.241.251)  207.861 ms 172.31.241.249 (172.31.241.249)  207.081 ms
19  172.31.241.18 (172.31.241.18)  207.445 ms  207.117 ms
20  172.31.241.29 (172.31.241.29)  209.347 ms  208.680 ms
21  uhome.web.utah.edu (155.98.186.21)  208.396 ms  208.195 ms
```

### 3.2.2. www.uct.ac.za

```
traceroute to www.uct.ac.za (137.158.159.192), 30 hops max, 60 byte packets
 1 * *
 2 be2982.ccr41.mia03.atlas.cogentco.com (154.54.40.57) 142.191 ms 142.206 ms
 3 ntt.mia03.atlas.cogentco.com (154.54.9.42) 141.607 ms 141.613 ms
 4 ae-3.r22.miamfl02.us.bb.gin.ntt.net (129.250.7.45) 141.808 ms 141.823 ms
 5 ae-0.a02.miamfl02.us.bb.gin.ntt.net (129.250.2.4) 141.600 ms ae-1.a02.miamfl02.us.bb.gin.ntt.net
141.759 ms
 6 ce-2-0-2.a02.miamfl02.us.ce.gin.ntt.net (129.250.200.114) 141.791 ms 141.766 ms
 7 30.8.39.170.ampath.net (170.39.8.30) 141.655 ms 141.714 ms
 8 * *
 9 et-0-0-1-0-cpt7-pe1.net.tenet.ac.za (155.232.64.70) 373.454 ms 373.416 ms
10 154.114.124.1 (154.114.124.1) 373.478 ms 373.495 ms
11 * *
12 * *
13 * *
14 * *
15 * *
16 * *
17 * *
18 * *
19 * *
20 * *
21 * *
22 * *
23 * *
24 * *
25 * *
26 * *
27 * *
28 * *
29 * *
30 * *
```

### 3.2.3. www.iitd.ac.in

```
traceroute to iitd.ac.in (103.27.9.24), 30 hops max, 40 byte packets
 1 1.ip-176-103-190.ar.ipxon.net (190.103.176.1) 0.106 ms * 0.098 ms
 2 Internal (Internal) 0.264 ms 0.263 ms 0.260 ms
 3 ae30-75.edge2.BuenosAires1.Level3.net (67.73.142.21) 0.790 ms 0.896 ms 0.803 ms
 4 * * *
 5 4.7.26.62 (4.7.26.62) 245.013 ms 245.016 ms 245.030 ms
 6 49.45.4.87 (49.45.4.87) 358.610 ms 358.603 ms 358.587 ms
 7 49.45.4.102 (49.45.4.102) 348.422 ms 348.424 ms 348.416 ms
 8 49.44.220.8 (49.44.220.8) 352.905 ms 352.905 ms 352.896 ms
 9 * * *
10 * * *
11 136.232.148.178 (136.232.148.178) 389.623 ms 389.614 ms 389.606 ms
12 * * *
13 * * *
14 * * *
15 * * *
16 103.27.9.24 (103.27.9.24) 376.482 ms 376.495 ms 376.572 ms
17 103.27.9.24 (103.27.9.24) 376.449 ms 376.453 ms 376.450 ms
18 103.27.9.24 (103.27.9.24) 376.084 ms 376.096 ms 376.107 ms
```



### 3.2.4. www.google.com

```
traceroute to google.com (142.250.179.174), 30 hops max, 60 byte packets
1  * *
2  be2982.ccr41.mia03.atlas.cogentco.com (154.54.40.57) 142.408 ms 142.458 ms
3  tata.mia03.atlas.cogentco.com (154.54.9.46) 141.594 ms 141.593 ms
4  74.125.146.6 (74.125.146.6) 144.225 ms 141.647 ms
5  108.170.253.18 (108.170.253.18) 142.634 ms 108.170.249.30 (108.170.249.30) 142.640 ms
6  142.250.211.238 (142.250.211.238) 143.012 ms 142.981 ms
7  142.250.61.154 (142.250.61.154) 184.630 ms 142.250.225.22 (142.250.225.22) 225.047 ms
8  216.239.58.153 (216.239.58.153) 183.116 ms 142.250.213.67 (142.250.213.67) 169.519 ms
9  142.250.59.185 (142.250.59.185) 274.210 ms 274.211 ms
10 142.251.232.218 (142.251.232.218) 254.561 ms 253.827 ms
11 142.251.237.170 (142.251.237.170) 253.324 ms 142.251.236.84 (142.251.236.84) 253.641 ms
12 108.170.241.161 (108.170.241.161) 254.483 ms 253.977 ms
13 142.251.48.177 (142.251.48.177) 252.860 ms 142.251.48.175 (142.251.48.175) 253.098 ms
14 ams15s41-in-f14.1e100.net (142.250.179.174) 252.669 ms 253.135 ms
```

### 3.2.5. www.facebook.com

```
traceroute to facebook.com (157.240.12.35), 30 hops max, 60 byte packets
1  * *
2  be2982.ccr41.mia03.atlas.cogentco.com (154.54.40.57) 142.038 ms 142.097 ms
3  38.104.95.114 (38.104.95.114) 141.847 ms 38.104.95.122 (38.104.95.122) 142.233 ms
4  po203.asw03.mia1.tfbnw.net (129.134.64.160) 141.616 ms po203.asw01.mia1.tfbnw.net (129.134.64.15)
141.634 ms
5  ae104.ar01.mia1.tfbnw.net (129.134.64.106) 142.226 ms ae104.ar03.mia1.tfbnw.net (129.134.64.122)
142.011 ms
6  * *
7  * *
8  ae26.bb01.gru1.tfbnw.net (129.134.34.98) 246.405 ms ae2.ar01.gru2.tfbnw.net (129.134.50.215)
246.669 ms
9  ae1.ar01.gru1.tfbnw.net (204.15.20.145) 245.920 ms po221.asw02.gru2.tfbnw.net (31.13.31.201)
245.623 ms
10 po221.asw02.gru1.tfbnw.net (157.240.53.11) 245.596 ms po282.psw03.gru2.tfbnw.net (147.75.214.173)
245.865 ms
11 157.240.39.47 (157.240.39.47) 245.564 ms 157.240.36.75 (157.240.36.75) 246.065 ms
12 157.240.39.199 (157.240.39.199) 246.075 ms edge-star-mini-shv-02-gru2.facebook.com (157.240.12.3)
245.745 ms
```

## 3.3. Johannesburg, South Africa

### 3.3.1. www.utah.edu

```
traceroute to www.utah.edu (155.98.186.21), 30 hops max, 60 byte packets
1  gi0-0-0-17.20.agr11.jnb01.atlas.cogentco.com (206.185.255.1) 1.012 ms 0.935 ms
2  be2355.ccr51.jnb01.atlas.cogentco.com (154.54.43.37) 0.843 ms 0.888 ms
3  be2385.ccr21.lon01.atlas.cogentco.com (154.54.40.93) 195.961 ms 193.712 ms
4  be2871.ccr42.lon13.atlas.cogentco.com (154.54.58.185) 193.760 ms be2868.ccr41.lon13.atlas.cogent
193.616 ms
5  be2101.ccr32.bos01.atlas.cogentco.com (154.54.82.38) 256.072 ms 256.079 ms
6  be3600.ccr22.alb02.atlas.cogentco.com (154.54.0.221) 259.695 ms 259.620 ms
7  be2878.ccr21.cle04.atlas.cogentco.com (154.54.26.129) 270.013 ms be2879.ccr22.cle04.atlas.cogent
270.017 ms
8  be2718.ccr42.ord01.atlas.cogentco.com (154.54.7.129) 278.858 ms be2717.ccr41.ord01.atlas.cogentc
277.041 ms
```

```

 9  be2832.ccr22.mci01.atlas.cogentco.com (154.54.44.169)  288.298 ms be2831.ccr21.mci01.atlas.cogent
290.698 ms
10  be3035.ccr21.den01.atlas.cogentco.com (154.54.5.89)  299.620 ms be3036.ccr22.den01.atlas.cogentco
303.746 ms
11  be3038.ccr32.slc01.atlas.cogentco.com (154.54.42.97)  309.901 ms be3037.ccr21.slc01.atlas.cogentc
311.669 ms
12  be2685.rcr01.b020767-1.slc01.atlas.cogentco.com (154.54.41.118)  312.768 ms  314.768 ms
13  * 38.142.233.58 (38.142.233.58)  316.241 ms
14  lv3-beibr-a-184-int.uen.net (140.197.249.117)  313.536 ms  313.491 ms
15  ebc-pep-a-178-int.uen.net (140.197.253.23)  315.952 ms  316.280 ms
16  * *
17  * 199.104.93.22 (199.104.93.22)  314.488 ms
18  * 199.104.93.33 (199.104.93.33)  316.100 ms
19  155.99.130.67 (155.99.130.67)  316.597 ms  315.285 ms
20  155.99.130.103 (155.99.130.103)  315.946 ms  155.99.130.107 (155.99.130.107)  315.888 ms
21  * 172.31.241.255 (172.31.241.255)  317.363 ms
22  172.31.241.22 (172.31.241.22)  312.997 ms  172.31.241.18 (172.31.241.18)  317.951 ms
23  172.31.241.29 (172.31.241.29)  321.137 ms  313.012 ms
24  * uhome.web.utah.edu (155.98.186.21)  317.384 ms

```

### 3.3.2. www.uct.ac.za

```

traceroute to www.uct.ac.za (137.158.159.192), 30 hops max, 60 byte packets
 1  gi0-0-0-17.20.agr11.jnb01.atlas.cogentco.com (206.185.255.1)  0.962 ms  0.918 ms
 2  be2355.ccr51.jnb01.atlas.cogentco.com (154.54.43.37)  0.749 ms  0.661 ms
 3  be2385.ccr21.lon01.atlas.cogentco.com (154.54.40.93)  193.635 ms  193.572 ms
 4  be2185.rcr21.b015534-1.lon01.atlas.cogentco.com (154.54.61.61)  196.002 ms  195.926 ms
 5  tenet.demarc.cogentco.com (149.14.146.194)  198.562 ms *
 6  et-1-1-0-0-ams1-iri.net.tenet.ac.za (155.232.1.80)  203.336 ms  203.247 ms
 7  ae0-306-mtz1-iri.net.tenet.ac.za (155.232.1.86)  394.840 ms  394.697 ms
 8  lt-0-0-0-1-mtz1-iri.net.tenet.ac.za (155.232.152.20)  413.789 ms  413.737 ms
 9  lt-1-0-0-0-mtz1-iri.net.tenet.ac.za (155.232.152.23)  375.295 ms  375.201 ms
10  et-1-1-1-0-isd1-pel.net.tenet.ac.za (155.232.1.153)  385.503 ms  385.438 ms
11  et-1-1-4-0-cpt3-pel.net.tenet.ac.za (155.232.1.148)  399.751 ms  399.994 ms
12  et-0-0-1-0-cpt7-pel.net.tenet.ac.za (155.232.64.70)  398.918 ms  398.768 ms
13  154.114.124.1 (154.114.124.1)  399.026 ms  400.762 ms
14  * *
15  * *
16  * *
17  * *
18  * *
19  * *
20  * *
21  * *
22  * *
23  * *
24  * *
25  * *
26  * *
27  * *
28  * *
29  * *
30  * *

```

### 3.3.3. www.iitd.ac.in

```
traceroute to iitd.ac.in (103.27.9.24), 30 hops max, 40 byte packets
 1  1.110.static.rdns.co.za (41.76.110.1)  0.181 ms *  0.733 ms
 2  * * *
 3  41.193.230.5 (41.193.230.5)  1.115 ms  1.152 ms  1.157 ms
 4  41-193-118-45.vox.co.za (41.193.118.45)  1.173 ms  1.914 ms  1.943 ms
 5  196.41.24.122 (196.41.24.122)  178.515 ms  178.570 ms  178.577 ms
 6  ldn-b2-link.ip.twelve99.net (213.248.100.161)  178.650 ms  179.272 ms  179.278 ms
 7  * * *
 8  prs-bb2-link.ip.twelve99.net (62.115.133.239)  185.759 ms  185.104 ms  185.732 ms
 9  mei-b5-link.ip.twelve99.net (62.115.124.57)  240.590 ms  241.707 ms  241.730 ms
10  reliance-ic-361536.ip.twelve99-cust.net (62.115.155.139)  395.344 ms  395.343 ms  395.439 ms
11  103.198.140.214 (103.198.140.214)  392.176 ms  392.163 ms  391.846 ms
12  103.198.140.177 (103.198.140.177)  391.266 ms  391.231 ms  391.237 ms
13  * * *
14  136.232.148.178 (136.232.148.178)  424.906 ms  424.911 ms  424.974 ms
15  * * *
16  * * *
17  * * *
18  * * *
19  103.27.9.24 (103.27.9.24)  428.173 ms  428.191 ms  428.313 ms
20  103.27.9.24 (103.27.9.24)  428.229 ms  428.237 ms  428.239 ms
21  103.27.9.24 (103.27.9.24)  427.742 ms  427.770 ms  427.922 ms
```

### 3.3.4. www.google.com

```
traceroute to www.google.com (172.217.169.36), 30 hops max, 60 byte packets
 1  gi0-0-0-17.20.agr11.jnb01.atlas.cogentco.com (206.185.255.1)  0.915 ms  0.920 ms
 2  be2355.ccr51.jnb01.atlas.cogentco.com (154.54.43.37)  0.760 ms  0.775 ms
 3  be2389.ccr22.lon01.atlas.cogentco.com (154.54.80.201)  193.854 ms be2385.ccr21.lon01.atlas.cogent
195.729 ms
 4  be2869.ccr42.lon13.atlas.cogentco.com (154.54.57.161)  193.933 ms be2870.ccr41.lon13.atlas.cogent
214.296 ms
 5  be2348.rcr21.b023101-0.lon13.atlas.cogentco.com (130.117.51.74)  198.012 ms be2350.rcr21.b023101-
194.056 ms
 6  ae39-xcr1.ltw.cw.net (195.2.26.25)  196.957 ms *
 7  ae8-xcr1.lnt.cw.net (195.2.24.130)  196.961 ms *
 8  google-gw1.lnt.cw.net (195.2.5.10)  196.939 ms  197.481 ms
 9  74.125.242.65 (74.125.242.65)  205.332 ms *
10  172.253.66.87 (172.253.66.87)  200.761 ms 172.253.66.89 (172.253.66.89)  207.074 ms
11  lhr48s08-in-f4.1e100.net (172.217.169.36)  198.192 ms  198.100 ms
```

### 3.3.5. www.facebook.com

```
traceroute to www.facebook.com (157.240.221.35), 30 hops max, 60 byte packets
 1  gi0-0-0-17.20.agr11.jnb01.atlas.cogentco.com (206.185.255.1)  0.848 ms  0.833 ms
 2  be2355.ccr51.jnb01.atlas.cogentco.com (154.54.43.37)  1.043 ms  1.147 ms
 3  be2389.ccr22.lon01.atlas.cogentco.com (154.54.80.201)  194.069 ms  193.812 ms
 4  be2185.rcr21.b015534-1.lon01.atlas.cogentco.com (154.54.61.61)  195.434 ms  193.532 ms
 5  149.14.251.186 (149.14.251.186)  193.681 ms  193.576 ms
 6  po151.asw01.lhr6.tfbnw.net (129.134.44.196)  193.883 ms  po151.asw02.lhr6.tfbnw.net (129.134.44.20
197.696 ms
 7  po221.psw01.lhr8.tfbnw.net (129.134.50.139)  198.827 ms  po241.psw02.lhr8.tfbnw.net (129.134.50.10
199.132 ms
 8  173.252.67.159 (173.252.67.159)  199.616 ms  173.252.67.179 (173.252.67.179)  197.139 ms
 9  edge-star-mini-shv-01-lhr8.facebook.com (157.240.221.35)  194.730 ms  193.402 ms
```

#### a. Hops Analysis

	google.com	facebook.com	utah.edu	iitd.ac.in	uct.ac.za
<b>Laptop</b>	10	12	34	4	-
<b>Buenos Aires</b>	14	12	21	18	-
<b>Johannesburg</b>	11	9	24	21	-

A detailed analysis:-

##### 1. Geographical distance vs number of Hops

Let's use utah.edu as the sample to study the trend. The distance between utah and the 3 traceroute sources vary as follows:

$$\text{Utah-Buenos Aires} < \text{Utah-Delhi} < \text{Utah-Johannesburg}$$

While it does take more hops to go from Delhi to Utah, than from Buenos Aires, it takes less hops to go from Johannesburg to Utah than from Delhi. This shows that there might be some exceptions to the trend that it takes more hops for larger distances.

Similarly for iitd.ac.in, the number of hops needed by local device (laptop) is 4, but Buenos Aires which is farther away from Delhi than Johannesburg takes lesser number of hops than Johannesburg to reach IIT Delhi.

This exception might arise because, the number of hops depends on the geographical distance from source to destination along the path taken by fiber optic cables. If the fiber optic cables do not take the geographically smallest route from source to destination then there might be a difference in the geographical distance vs number of hops trend. For example, if the connection from Delhi to Utah is routed through the Atlantic than the Pacific ocean then the geographical distance becomes larger from India to Utah than Johannesburg to Utah and then it will start following the trend of larger geographical distance implying larger number of hops.

Moreover, this hypothesis can be checked from the fact that the first US based server on the path (163.253.1.116) is actually located in New York which suggests that the path taken is through the Atlantic.

##### 2. Number of hops to Google and Facebook

In general, Google and Facebook seem to take fewer hops than other sites. Also the number of hops needed is almost constant and varies around 9-13. The number of hops required for sites like iitd and utah vary a lot depending on traceroute server and depend on geographical distance as well. This might be because, google and facebook resolve to different IPs from different sources in order to ensure a smooth experience from any country. This results in low variability. On the other hand such a situation is not needed for universities like Utah or IITD as there is only one server for these institutes and they don't need to cater to too many requests from around the world. So the need to optimise hops across the world is not high for these sites.

## b. Latency Analysis

	google.com	Facebook.com	Utah.edu	iitd.ac.in	uct.ac.za
Laptop	14.515	42.32	423.244	16.971	timeout
Buenos Aires	249.360	245.648	208.10	398.504	timeout
Johannesburg	195.502	197.082	316.645	429.453	timeout

In general the latency increases with number of hops, but for similar hop size, there might be some exceptions to the rule. For example latency for facebook in Buenos Aires and Johannesburg is more than that of Local device even though the number of hops is more for local device.

On performing traceroute from other sites with servers from the same cities, we got much less times around 2 ms for google and around 1 ms for facebook. It might be possible that the servers used by cogent co in these cities use some slower connections or have higher traffic due to which the latency is increased.

On the other hand, the latency seems to follow the trend of number of hops for universities like utah and iitd.

## c. Different IP addresses for same site

The IP address of utah.edu and iitd.ac.in seems to remain the same irrespective of the location from where traceroute is requested. On the other hand, the IP address of google and facebook is different for every traceroute location that we chose. One possible reason to explain this can be that sites like google and facebook have to ensure very low latency and high capacity for almost every country. It becomes necessary for them to maintain servers or peering services in almost every country, so the request to google or facebook from every other country seems to be routed to a different IP address corresponding to a different server.

For educational institutions, the requests are mostly from within the country. It is not necessary for them to optimise their performance across nations by maintaining multiple servers across the world. So, they have the same IP for multiple traceroute locations.

For iitd.ac.in, the IP address is 103.27.4.29 when accessed from external networks (like Johannesburg, Buenos Aires, and from Home networks in Delhi) and 10.10.211.212 when accessed from internal networks (like IIT Delhi Wifi). This is because the internal and external networks are different and have different IP addresses. It might be possible that educational institutions like IIT Delhi have different IP addresses for internal and external networks.

## d. Path to different IP addresses

The paths to different IP addresses for the same site gives longer path when request is made to an IP address obtained from a request to a different country.

One possible reason for this can be that networks are optimised to ensure that people always get access to the least latency path. So, the IP address to which the domain name corresponds to in our nation is the least latency IP address (server) available to us.

Path to facebook server in Argentina:-

```
traceroute to 157.240.12.35 (157.240.12.35), 64 hops max, 52 byte packets
 1  10.184.0.13 (10.184.0.13)  4.716 ms  3.439 ms  3.399 ms
 2  10.254.175.5 (10.254.175.5)  3.691 ms
   10.254.175.1 (10.254.175.1)  3.551 ms  4.911 ms
 3  10.255.1.34 (10.255.1.34)  4.078 ms  4.580 ms  3.608 ms
 4  10.119.233.65 (10.119.233.65)  3.430 ms  3.620 ms  3.511 ms
 5  * * *
 6  * * *
 7  10.1.200.137 (10.1.200.137)  70.153 ms  61.226 ms  60.607 ms
 8  * * 10.255.238.254 (10.255.238.254)  64.307 ms
 9  10.152.7.214 (10.152.7.214)  60.612 ms
   10.152.7.38 (10.152.7.38)  33.859 ms  29.950 ms
```

```

10 ae1.pr01.bom1.tfbnw.net (157.240.68.238) 43.677 ms
   ae2.pr02.bom1.tfbnw.net (157.240.66.204) 111.273 ms 33.673 ms
11 ae110.ar04.bom1.tfbnw.net (157.240.53.32) 47.238 ms
   ae1.pr01.bom1.tfbnw.net (157.240.68.238) 61.212 ms
   ae2.pr02.bom1.tfbnw.net (157.240.66.204) 70.719 ms
12 ae101.bb02.bom1.tfbnw.net (31.13.24.28) 31.595 ms
   ae104.bb02.bom1.tfbnw.net (31.13.25.136) 36.856 ms
   ae120.ar03.bom1.tfbnw.net (157.240.52.204) 33.797 ms
13 ae13.bb03.mrs1.tfbnw.net (31.13.24.10) 129.817 ms
   ae103.bb04.bom1.tfbnw.net (204.15.21.6) 129.699 ms
   ae103.bb01.bom1.tfbnw.net (31.13.25.134) 43.936 ms
14 ae151.bb04.mrs1.tfbnw.net (129.134.100.63) 128.767 ms
   ae36.bb03.mrs1.tfbnw.net (74.119.79.134) 120.898 ms
   ae38.bb02.bio1.tfbnw.net (157.240.35.74) 157.822 ms
15 ae202.bb04.vab1.tfbnw.net (129.134.40.17) 289.140 ms
   ae203.bb04.vab1.tfbnw.net (129.134.40.15) 275.552 ms
   ae203.bb02.vab1.tfbnw.net (129.134.40.13) 356.678 ms
16 ae203.bb04.vab1.tfbnw.net (129.134.40.15) 281.882 ms
   ae72.bb02.clt3.tfbnw.net (129.134.49.28) 312.436 ms
   ae203.bb04.vab1.tfbnw.net (129.134.40.15) 275.036 ms
17 ae68.bb04.clt3.tfbnw.net (129.134.103.32) 312.192 ms
   ae0.bb04.jax3.tfbnw.net (129.134.43.239) 353.491 ms 409.257 ms
18 ae0.bb04.jax3.tfbnw.net (129.134.43.239) 425.756 ms 416.653 ms *
19 ae38.bb02.gru2.tfbnw.net (129.134.105.120) 377.806 ms * *
20 ae38.bb02.gru2.tfbnw.net (129.134.105.120) 449.357 ms
   ae26.bb02.gru1.tfbnw.net (129.134.43.176) 417.638 ms *
21 ae1.ar02.gru2.tfbnw.net (129.134.50.239) 452.552 ms
   po211.asw02.gru2.tfbnw.net (31.13.26.37) 475.985 ms
   ae2.ar02.gru1.tfbnw.net (204.15.22.255) 456.700 ms
   ae2.ar02.gru1.tfbnw.net (204.15.22.255) 456.700 ms
22 po231.psw04.gru2.tfbnw.net (129.134.33.103) 374.678 ms
   po284.psw02.gru2.tfbnw.net (129.134.110.253) 365.605 ms
   po211.asw01.gru2.tfbnw.net (31.13.26.35) 370.564 ms
23 po221.asw02.gru1.tfbnw.net (157.240.53.11) 372.071 ms
   po211.asw02.gru1.tfbnw.net (157.240.53.9) 402.270 ms 378.310 ms
24 edge-star-mini-shv-02-gru2.facebook.com (157.240.12.35) 625.707 ms
   157.240.39.51 (157.240.39.51) 381.572 ms
   edge-star-mini-shv-02-gru2.facebook.com (157.240.12.35) 381.528 ms

```

Path to facebook server reached from Johannesburg

```

traceroute to 157.240.221.35 (157.240.221.35), 64 hops max, 52 byte packets
 1 10.184.0.13 (10.184.0.13) 16.150 ms 9.766 ms 3.032 ms
 2 10.254.175.1 (10.254.175.1) 3.990 ms
   10.254.175.5 (10.254.175.5) 17.252 ms 3.784 ms
 3 10.255.1.34 (10.255.1.34) 4.336 ms 3.779 ms 3.978 ms
 4 10.119.233.65 (10.119.233.65) 4.032 ms 3.950 ms 4.568 ms
 5 * * *
 6 * * *
 7 10.1.200.137 (10.1.200.137) 69.485 ms 60.936 ms 62.089 ms
 8 * * 10.255.238.254 (10.255.238.254) 60.728 ms
 9 10.152.7.214 (10.152.7.214) 60.139 ms
   10.152.7.38 (10.152.7.38) 38.051 ms 31.260 ms
10 115.247.69.85 (115.247.69.85) 32.756 ms
   10.152.7.233 (10.152.7.233) 60.649 ms 43.846 ms
11 115.247.69.85 (115.247.69.85) 30.320 ms 28.079 ms 30.105 ms
12 * * *
13 * * *
14 * * *

```

```

15 * * *
16 * po141.asw01.lhr3.tfbnw.net (129.134.45.56) 146.154 ms *
17 po141.asw02.lhr3.tfbnw.net (129.134.45.58) 156.654 ms
   po232.psw02.lhr8.tfbnw.net (129.134.50.85) 144.228 ms
   157.240.38.145 (157.240.38.145) 144.781 ms
18 173.252.67.89 (173.252.67.89) 149.669 ms
   173.252.67.117 (173.252.67.117) 154.259 ms
   157.240.38.235 (157.240.38.235) 155.026 ms
19 edge-star-mini-shv-01-lhr8.facebook.com (157.240.221.35) 155.644 ms 157.143 ms 153.456 ms

```

Clearly both latency and number of hops are much larger than the corresponding values from local device.

	Number of Hops	Latency in ms
IP from local device	11	42.32
IP from Buenos Aires	24	381.528
IP from Johannesburg	19	155.644

### e. Peering with Google and Facebook

For most countries, Google's network seems to be peered to the local ISP. However, on tracerouting for google and facebook from a server in Beijing, no response is received after 20 hops and it seems like the packet is dropped. It is possible that China's local ISPs are not peered with Google's network.

On running traceroute from Luxembourg, we find that the path taken goes through Germany before entering Google's network in Germany. (ae61-101.edge6.Dusseldorf1.Level3.net (62.67.22.45)) This makes sense as Luxembourg is a small nation with a small population which makes it more optimal for it to connect to Germany's ISPs and use Google's network there instead of setting up a peering point for itself.

Similarly on running traceroute to Google from Bahrain (99.83.93.23), we find that the connection jumps from Manama, Bahrain to an Amazon Data center in US but not one of Google.

Similarly for facebook too, Bahrain uses an Amazon Data center to reach US and then changes to Google's network.

On running traceroute from Lagos, the route taken is through the West Indian Ocean Cable Company (154.66.247.85 WIOCC-AS, MU) to the facebook servers in US. The local ISP is not peered to facebook.

The traceroutes have been attached in a separate folder called "Peering Experiments".

## ASIP Analysis

IP Address	AS
1 10.184.0.13 (10.184.0.13)	Private IP
2 10.254.175.1 (10.254.175.1)	Private IP
3 10.255.1.34 (10.255.1.34)	Private IP
4 10.119.233.65 (10.119.233.65)	Private IP
5 10.1.207.69 (10.1.207.69)	Private IP
6 10.1.200.137 (10.1.200.137)	Private IP
7 10.255.238.254 (10.255.238.254)	Private IP
8 180.149.48.18 (180.149.48.18)	NKN-CORE-NW NKN Core Network, IN
9 180.149.48.6 (180.149.48.6)	NKN-CORE-NW NKN Core Network, IN
10 180.149.48.20 (180.149.48.20)	NKN-CORE-NW NKN Core Network, IN
11 fourhundredge-0-0-0-2.4079.core1.ashb.net.internet2.edu (163.253.1.116)	INTERNET2-RESEARCH-EDU
12 fourhundredge-0-0-0-16.4079.core2.ashb.net.internet2.edu (163.253.1.3)	INTERNET2-RESEARCH-EDU
13 fourhundredge-0-0-0-16.4079.core2.ashb.net.internet2.edu (163.253.1.3)	INTERNET2-RESEARCH-EDU
14 fourhundredge-0-0-0-1.4079.core2.clev.net.internet2.edu (163.253.1.139)	INTERNET2-RESEARCH-EDU
15 fourhundredge-0-0-0-2.4079.core2.eqch.net.internet2.edu (163.253.2.17)	INTERNET2-RESEARCH-EDU
16 fourhundredge-0-0-0-2.4079.core2.chic.net.internet2.edu (163.253.2.18)	INTERNET2-RESEARCH-EDU
17 fourhundredge-0-0-0-1.4079.core1.kans.net.internet2.edu (163.253.1.245)	INTERNET2-RESEARCH-EDU
18 fourhundredge-0-0-0-1.4079.core1.denv.net.internet2.edu (163.253.1.242)	INTERNET2-RESEARCH-EDU
19 fourhundredge-0-0-0-3.4079.core1.salt.net.internet2.edu (163.253.1.171)	INTERNET2-RESEARCH-EDU
20 163.253.5.7 (163.253.5.7)	INTERNET2-RESEARCH-EDU
21 tdc-beibr-b-170-int.uen.net (140.197.249.81)	WEST-NET-WEST
22 tdc-beibr-b-170-int.uen.net (140.197.249.81)	WEST-NET-WEST
24 ddc-pep-b-129-int.uen.net (140.197.253.97)	WEST-NET-WEST
25 ebc-pep-a-178-int.uen.net (140.197.252.84)	WEST-NET-WEST
26 * ebc-pep-a-178-int.uen.net (140.197.252.84)	WEST-NET-WEST
27 * 199.104.93.22 (199.104.93.22)	UTAH
28 199.104.93.22 (199.104.93.22) 321.654 ms	UTAH
29 155.99.130.57 (155.99.130.57) 416.730 ms	UTAH
30 155.99.130.103 (155.99.130.103) 414.959 ms	UTAH
31 172.31.241.255 (172.31.241.255) 416.605 ms	UTAH
32 172.31.241.255 (172.31.241.255) 416.528 ms	PRIVATE
33 172.31.241.25 (172.31.241.25)	PRIVATE
34 www.utah.edu (155.98.186.21)	UTAH

Table 1: Path from Laptop (Hostel wifi) to utah.edu

IP Adresses	AS
1 10.184.0.13 (10.184.0.13)	Private
2 10.254.175.5 (10.254.175.5)	Private
3 10.255.1.34 (10.255.1.34)	Private
4 10.119.233.65 (10.119.233.65)	Private
5 10.1.207.69 (10.1.207.69)	Private
6 * * *	
7 10.255.238.122 (10.255.238.122)	Private
8 10.152.7.214 (10.152.7.214)	Private
9 10.152.7.233 (10.152.7.233)	Private
10 po101.psw01.bom1.tfbnw.net (31.13.29.205)	Facebook
11 po101.psw04.bom1.tfbnw.net (157.240.44.31)	Facebook
12 157.240.38.65 (157.240.38.65)	Facebook

Table 2: Path from Laptop (Hostel wifi) to facebook



IP Adresses	AS
1 10.184.0.13 (10.184.0.13)	Private
2 10.254.175.5 (10.254.175.5)	Private
3 10.254.236.6 (10.254.236.6)	Private
4 www.iitd.ac.in (10.10.211.212)	Private

Table 3: Path from Laptop (Hostel wifi) to iitd.ac.in

IP Adresses	AS
1 10.184.0.13 (10.184.0.13)	Private
2 10.254.175.1 (10.254.175.1)	Private
3 10.255.1.34 (10.255.1.34)	Private
4 10.119.233.65 (10.119.233.65)	Private
5 * * *	
6 10.119.234.162	Private
7 72.14.194.160	Google
8 108.170.251.113	Google
9 142.251.52.217 (142.251.52.217)	Google
10 del12s08-in-f14.1e100.net (142.250.194.238)	Google

Table 4: Path from Laptop (Hostel wifi) to iitd.ac.in

IP Address	ASN
1 10.184.0.13 (10.184.0.13)	Private
2 10.254.175.5 (10.254.175.5)	Private
3 10.255.1.34 (10.255.1.34)	Private
4 10.119.233.65 (10.119.233.65)	Private
5 * * *	-
6 10.1.207.65 (10.1.207.65)	Private
7 10.1.200.137 (10.1.200.137)	Private
8 10.255.238.122 (10.255.238.122)	Private
9 180.149.48.18 (180.149.48.18)	NKN-CORE-NW
10 180.149.48.2 (180.149.48.2)	NKN-CORE-NW
11 xe-0-0-2-0-600-ams1-ir1.net.tenet.ac.za (155.232.220.18)	TENET-1
12 xe-0-0-1-1-10-mtz1-ir1.net.tenet.ac.za (155.232.1.21)	TENET-1
13 xe-0-0-1-1-10-mtz1-ir1.net.tenet.ac.za (155.232.1.21)	TENET-1
14 et-1-1-1-0-isd1-pe1.net.tenet.ac.za (155.232.1.153)	TENET-1
15 et-1-1-4-0-cpt3-pe1.net.tenet.ac.za (155.232.1.148)	TENET-1
16 154.114.124.1 (154.114.124.1)	TENET-1
17 * 154.114.124.1 (154.114.124.1)	TENET-1
18 * * *	-
19 * * *	-
20 * * *	-

Table 5: Path from Laptop (Hostel wifi) to uct.ac.za

## §4. Packet Analysis

- a. We ran a DNS filter on the output to iitd.ac.in and got the following result(Fig. 1):

Time	Source	Destination	Protocol	Length	Info
47 2.077393	10.184.22.156	10.10.1.4	DNS	95	Standard query 0x3f66 A optimizationguide-pa.googleap
48 2.077588	10.184.22.156	10.10.1.4	DNS	95	Standard query 0xbc2c HTTPS optimizationguide-pa.goog
49 2.080615	10.184.22.156	10.10.1.4	DNS	70	Standard query 0xf27b A iitd.ac.in
50 2.080821	10.184.22.156	10.10.1.4	DNS	70	Standard query 0xb5ee HTTPS iitd.ac.in
53 2.088379	10.10.1.4	10.184.22.156	DNS	123	Standard query response 0xb5ee HTTPS iitd.ac.in SOA in
54 2.088379	10.10.1.4	10.184.22.156	DNS	86	Standard query response 0xf27b A iitd.ac.in A 10.10.2
63 2.111611	10.10.1.4	10.184.22.156	DNS	95	Standard query response 0xbc2c HTTPS optimizationguide
64 2.111611	10.10.1.4	10.184.22.156	DNS	351	Standard query response 0x3f66 A optimizationguide-pa
69 2.116865	10.184.22.156	10.10.1.4	DNS	75	Standard query 0xc58c A home.iitd.ac.in
72 2.117006	10.184.22.156	10.10.1.4	DNS	75	Standard query 0x56cc HTTPS home.iitd.ac.in
75 2.118772	10.10.1.4	10.184.22.156	DNS	91	Standard query response 0xc58c A home.iitd.ac.in A 10
76 2.119241	10.10.1.4	10.184.22.156	DNS	128	Standard query response 0x56cc HTTPS home.iitd.ac.in

Figure 1: IITD DNS

### Observations

There was 1 DNS query and response for iitd.ac.in. The request-response began at 2.080615s and ended at 2.088379s lasting for a total of 7.764ms.

- b. On applying a http filter, only one request is observed as shown in Fig. 2

The figure shows a Wireshark packet capture with a filter applied to 'http'. The packet list shows two packets: a GET request (No. 35) and a 302 Found response (No. 41). The packet details pane shows the structure of the HTTP response, including the status line '302 Found' and the body text 'The document has moved to https://home.iitd.ac.in/'. The packet bytes pane shows the raw data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
35	0.010047	10.184.22.156	10.10.211.212	HTTP	517	GET / HTTP/1.1
41	0.021455	10.10.211.212	10.184.22.156	HTTP	495	HTTP/1.1 302 Found (text/html)

Frame 41: 495 bytes on wire (3960 bits), 495 bytes captured (3960 bits) on interface 0  
Ethernet II, Src: Cisco\_1b:48:73 (5c:3e:06:1b:48:73), Dst: Intel\_82:55:08:00:00:00 (08:00:00:00:00:00)  
Internet Protocol Version 4, Src: 10.10.211.212, Dst: 10.184.22.156  
Transmission Control Protocol, Src Port: 80, Dst Port: 50601, Seq: 302, Len: 495  
Hypertext Transfer Protocol  
Line-based text data: text/html (7 lines)  
!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n<html><head>\n<title>302 Found</title>\n</head><body>\n<h1>Found</h1>\n<p>The document has moved to <a href="https://home.iitd.ac.in/">https://home.iitd.ac.in/</a>.\n</body></html>\n

Figure 2: IITD HTTP

### Observations

Only one request is observed. The request was for <http://www.iitd.ac.in/> and the response was 302 Found indicating that the requested resource has been moved to a different URL. The text data tells us that "The document has moved <https://home.iitd.ac.in/>".

HTTPS traffic is encrypted using SSL/TLS, and the contents of the packets are scrambled and unreadable without the decryption keys. Hence, we are not able to find any html / css / js files for the webpage in the packets.

- c. Next we applied the filter ((ip.src==10.184.22.156 && ip.dst==10.10.211.212) || (ip.src==10.10.211.212 && ip.dst==10.184.22.156)) && tcp to get the TCP packets between the two hosts. The output is shown in Fig. 3

No.	Time	Source	Destination	Protocol	Length	Info
55	2.088924	10.184.22.156	10.10.211.212	TCP	66	51660 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
56	2.089944	10.184.22.156	10.10.211.212	TCP	66	51661 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
57	2.105122	10.10.211.212	10.184.22.156	TCP	66	80 → 51660 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
58	2.105122	10.10.211.212	10.184.22.156	TCP	66	80 → 51661 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
59	2.105226	10.184.22.156	10.10.211.212	TCP	54	51660 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
60	2.105284	10.184.22.156	10.10.211.212	TCP	54	51661 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
61	2.105482	10.184.22.156	10.10.211.212	HTTP	512	GET / HTTP/1.1
62	2.110473	10.10.211.212	10.184.22.156	TCP	54	80 → 51661 [ACK] Seq=1 Ack=459 Win=64128 Len=0
66	2.113536	10.10.211.212	10.184.22.156	HTTP	495	HTTP/1.1 302 Found (text/html)
77	2.119520	10.184.22.156	10.10.211.212	TCP	66	51664 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
82	2.120880	10.10.211.212	10.184.22.156	TCP	66	443 → 51664 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=
83	2.120920	10.184.22.156	10.10.211.212	TCP	54	51664 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
84	2.121163	10.184.22.156	10.10.211.212	TLSv1.3	571	Client Hello
86	2.122698	10.10.211.212	10.184.22.156	TCP	54	443 → 51664 [ACK] Seq=1 Ack=518 Win=64128 Len=0
88	2.129209	10.10.211.212	10.184.22.156	TLSv1.3	3806	Server Hello, Change Cipher Spec, Application Dat
89	2.130200	10.10.211.212	10.184.22.156	TCP	308	443 → 51664 [PSH, ACK] Seq=3753 Ack=518 Win=64128

Figure 3: IITD TCP

## Observations

Total 9 connections were opened. Of these 2 were http and 7 were https, as identified by their port number (80 for http and 443 for https). Thus, for the http request in part (b), we have 2 corresponding tcp connections.

- d. On running a http filter on indianexpress.com, we received the output Fig. 4

No.	Time	Source	Destination	Protocol	Length	Info
29	8.692398	10.184.22.156	104.112.98.185	HTTP	519	GET / HTTP/1.1
33	8.716837	104.112.98.185	10.184.22.156	HTTP	227	HTTP/1.1 301 Moved Permanently
4350	11.502918	10.184.22.156	23.63.111.99	HTTP	452	GET /roots/dstrootcax3.p7c HTTP/1.1
4376	11.518557	23.63.111.99	10.184.22.156	HTTP	324	HTTP/1.1 304 Not Modified
16242	29.880599	10.184.22.156	209.197.3.8	HTTP	336	GET /msdownload/update/v3/static/trusted/en/pinrulesstl.cab?dc1e16f2390b5f13 HTTP/1.1
16252	30.035445	209.197.3.8	10.184.22.156	HTTP	245	HTTP/1.1 304 Not Modified

Figure 4: Indian Express

## Observations

As mentioned above, HTTPS traffic is encrypted using SSL/TLS, and the contents of the packets are unreadable without the decryption keys. Hence, we see a very sparse http traffic and are not able to find any html/css/js files being transferred for the webpage in the packets. Wireshark can capture the encrypted packets, but the payload will appear as encrypted gibberish.

Similarly, we ran the filters for `act4d.iitd.ac.in` and got the outputs **Fig. 5** **Fig. 6** **Fig. 7**:

No.	Time	Source	Destination	Protocol	Length	Info
134	1.341221	10.184.22.156	10.10.1.4	DNS	95	Standard query 0x7127 A optimizationguide-pa.googleapis.co
135	1.341552	10.184.22.156	10.10.1.4	DNS	95	Standard query 0x2254 HTTPS optimizationguide-pa.googleapi
136	1.343979	10.184.22.156	10.10.1.4	DNS	76	Standard query 0x5939 A act4d.iitd.ac.in
137	1.344226	10.184.22.156	10.10.1.4	DNS	76	Standard query 0x2a92 HTTPS act4d.iitd.ac.in
138	1.348164	10.10.1.4	10.184.22.156	DNS	92	Standard query response 0x5939 A act4d.iitd.ac.in A 10.237
139	1.348164	10.10.1.4	10.184.22.156	DNS	129	Standard query response 0x2a92 HTTPS act4d.iitd.ac.in SOA
141	1.350497	10.184.22.156	10.10.1.4	DNS	83	Standard query 0x61ea A safebrowsing.google.com
142	1.350723	10.184.22.156	10.10.1.4	DNS	83	Standard query 0x0658 HTTPS safebrowsing.google.com
151	1.375024	10.10.1.4	10.184.22.156	DNS	351	Standard query response 0x7127 A optimizationguide-pa.goog
152	1.378453	10.10.1.4	10.184.22.156	DNS	95	Standard query response 0x2254 HTTPS optimizationguide-pa.
154	1.380227	10.10.1.4	10.184.22.156	DNS	118	Standard query response 0x61ea A safebrowsing.google.com C
155	1.380989	10.10.1.4	10.184.22.156	DNS	83	Standard query response 0x0658 HTTPS safebrowsing.google.c
212	1.697680	10.184.22.156	10.10.1.4	DNS	80	Standard query 0x64cd A beacons.gcp.gvt2.com
213	1.698423	10.184.22.156	10.10.1.4	DNS	80	Standard query 0xf783 HTTPS beacons.gcp.gvt2.com
224	1.739103	10.10.1.4	10.184.22.156	DNS	80	Standard query response 0xf783 HTTPS beacons.gcp.gvt2.com
232	1.798703	10.10.1.4	10.184.22.156	DNS	126	Standard query response 0x64cd A beacons.gcp.gvt2.com CNAM
817	4.246289	10.184.22.156	10.10.1.4	DNS	80	Standard query 0x4250 A beacons.gcp.gvt2.com
818	4.246683	10.184.22.156	10.10.1.4	DNS	80	Standard query 0xcdb8 HTTPS beacons.gcp.gvt2.com

Figure 5: ACT4D DNS

No.	Time	Source	Destination	Protocol	Length	Info
145	1.351143	10.184.22.156	10.237.26.108	HTTP	976	GET / HTTP/1.1
210	1.691223	10.237.26.108	10.184.22.156	HTTP/XML	574	HTTP/1.1 200 OK
294	2.269555	10.184.22.156	10.237.26.108	HTTP	943	GET /act4d/media/system/js/mootools.js HTTP/1.1
299	2.297890	10.184.22.156	10.237.26.108	HTTP	942	GET /act4d/media/system/js/caption.js HTTP/1.1
322	2.307110	10.237.26.108	10.184.22.156	HTTP	290	HTTP/1.1 200 OK (application/javascript)
326	2.307754	10.184.22.156	10.237.26.108	HTTP	962	GET /act4d/templates/beez/css/template.css HTTP/1.1
327	2.308037	10.184.22.156	10.237.26.108	HTTP	962	GET /act4d/templates/beez/css/position.css HTTP/1.1
328	2.309048	10.184.22.156	10.237.26.108	HTTP	960	GET /act4d/templates/beez/css/layout.css HTTP/1.1
329	2.309806	10.184.22.156	10.237.26.108	HTTP	961	GET /act4d/templates/beez/css/general.css HTTP/1.1
332	2.311261	10.184.22.156	10.237.26.108	HTTP	937	GET /wikii-bak/wikii/statf0e.php HTTP/1.1
357	2.321205	10.237.26.108	10.184.22.156	HTTP	323	HTTP/1.1 200 OK (text/css)
360	2.323863	10.237.26.108	10.184.22.156	HTTP	423	HTTP/1.1 200 OK (application/javascript)
370	2.330932	10.237.26.108	10.184.22.156	HTTP	99	HTTP/1.1 200 OK (text/css)
371	2.330932	10.237.26.108	10.184.22.156	HTTP	153	HTTP/1.1 200 OK (text/css)
373	2.330932	10.237.26.108	10.184.22.156	HTTP	68	HTTP/1.1 404 Not Found (text/html)
378	2.333544	10.237.26.108	10.184.22.156	HTTP	558	HTTP/1.1 200 OK (text/css)
380	2.340298	10.184.22.156	10.237.26.108	HTTP	1008	GET /act4d/templates/beez/images/act4d.png HTTP/1.1
381	2.341510	10.184.22.156	10.237.26.108	HTTP	997	GET /act4d/images/balazahir.jpg HTTP/1.1
383	2.342910	10.184.22.156	10.237.26.108	HTTP	959	GET /act4d/templates/beez/css/print.css HTTP/1.1
408	2.360239	10.237.26.108	10.184.22.156	HTTP	254	HTTP/1.1 200 OK (text/css)
601	2.447541	10.237.26.108	10.184.22.156	HTTP	257	HTTP/1.1 200 OK (PNG)
798	2.597379	10.237.26.108	10.184.22.156	HTTP	585	HTTP/1.1 200 OK (JPEG JFIF image)
800	2.652607	10.184.22.156	10.237.26.108	HTTP	1003	GET /act4d/templates/beez/favicon.ico HTTP/1.1
804	2.657584	10.237.26.108	10.184.22.156	HTTP	462	HTTP/1.1 200 OK (image/x-icon)

Figure 6: ACT4D http

No.	Time	Source	Destination	Protocol	Length	Info
140	1.348556	10.184.22.156	10.237.26.108	TCP	66	59649 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
143	1.350810	10.237.26.108	10.184.22.156	TCP	66	80 → 59649 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=536 SACK_PERM WS=64
144	1.350876	10.184.22.156	10.237.26.108	TCP	54	59649 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
145	1.351143	10.184.22.156	10.237.26.108	HTTP	976	GET / HTTP/1.1
146	1.351905	10.184.22.156	10.237.26.108	TCP	66	59650 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
147	1.353436	10.237.26.108	10.184.22.156	TCP	54	80 → 59649 [ACK] Seq=1 Ack=537 Win=6912 Len=0
148	1.353436	10.237.26.108	10.184.22.156	TCP	54	80 → 59649 [ACK] Seq=1 Ack=923 Win=8000 Len=0
149	1.354123	10.237.26.108	10.184.22.156	TCP	66	80 → 59650 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=536 SACK_PERM WS=64
150	1.354195	10.184.22.156	10.237.26.108	TCP	54	59650 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
202	1.683452	10.237.26.108	10.184.22.156	TCP	1126	80 → 59649 [ACK] Seq=1 Ack=923 Win=8000 Len=1072 [TCP segment of a reassembled F
203	1.683605	10.184.22.156	10.237.26.108	TCP	54	59649 → 80 [ACK] Seq=923 Ack=1073 Win=131072 Len=0
205	1.685538	10.237.26.108	10.184.22.156	TCP	1126	80 → 59649 [ACK] Seq=1073 Ack=923 Win=8000 Len=1072 [TCP segment of a reassembled
206	1.685634	10.184.22.156	10.237.26.108	TCP	54	59649 → 80 [ACK] Seq=923 Ack=2145 Win=131072 Len=0
207	1.688519	10.237.26.108	10.184.22.156	TCP	1662	80 → 59649 [ACK] Seq=2145 Ack=923 Win=8000 Len=1608 [TCP segment of a reassembled
208	1.688688	10.184.22.156	10.237.26.108	TCP	54	59649 → 80 [ACK] Seq=923 Ack=3753 Win=131072 Len=0
210	1.691223	10.237.26.108	10.184.22.156	HTTP/XML	574	HTTP/1.1 200 OK
211	1.691370	10.184.22.156	10.237.26.108	TCP	54	59649 → 80 [ACK] Seq=923 Ack=4273 Win=130560 Len=0
294	2.269555	10.184.22.156	10.237.26.108	HTTP	943	GET /act4d/media/system/js/mootools.js HTTP/1.1
295	2.272164	10.237.26.108	10.184.22.156	TCP	54	80 → 59649 [ACK] Seq=4273 Ack=1459 Win=9088 Len=0
296	2.272671	10.237.26.108	10.184.22.156	TCP	54	80 → 59649 [ACK] Seq=4273 Ack=1812 Win=10176 Len=0
297	2.296379	10.237.26.108	10.184.22.156	TCP	2198	80 → 59649 [ACK] Seq=4273 Ack=1812 Win=10176 Len=2144 [TCP segment of a reassemb
298	2.296829	10.184.22.156	10.237.26.108	TCP	54	59649 → 80 [ACK] Seq=1812 Ack=6417 Win=131072 Len=0
299	2.297890	10.184.22.156	10.237.26.108	HTTP	942	GET /act4d/media/system/js/caption.js HTTP/1.1
300	2.299875	10.237.26.108	10.184.22.156	TCP	2734	80 → 59649 [ACK] Seq=6417 Ack=1812 Win=10176 Len=2680 [TCP segment of a reassemb
301	2.299875	10.237.26.108	10.184.22.156	TCP	54	80 → 59650 [ACK] Seq=1 Ack=537 Win=6912 Len=0
302	2.299969	10.184.22.156	10.237.26.108	TCP	54	59649 → 80 [ACK] Seq=1812 Ack=9097 Win=131072 Len=0
303	2.300447	10.184.22.156	10.237.26.108	TCP	66	59654 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
304	2.301787	10.237.26.108	10.184.22.156	TCP	54	80 → 59650 [ACK] Seq=1 Ack=889 Win=8000 Len=0

Figure 7: ACT4D TCP (filter ((ip.src==10.184.22.156 && ip.dst==10.237.26.108) || (ip.src==10.237.26.108 && ip.dst==10.184.22.156)) && tcp)

## Observations

- a. There were DNS queries and responses for `act4d.iitd.ac.in`. The request-response began at 1.343979s and ended at 1.348164s lasting for a total of 4.185ms.
- b. A total of 12 http requests were observed. Further, the rough order of requests is as follows:
  - (a) HTML-1
  - (b) JavaScript-2
  - (c) CSS-5
  - (d) PHP-1 (Not found)
  - (e) Images-3

This gives a fair idea about the way a browser loads a webpage. Initially, it prioritizes the loading of the HTML file, which serves as the blueprint for the webpage's structure. Subsequently, it proceeds to fetch JavaScript and CSS files, which respectively provide the interactivity and visual styling essential for the webpage's functionality and aesthetics.

Concluding this sequence, the browser focuses on loading images. These visual elements, while essential for content enhancement, often possess a larger file size. Hence, deferring their loading until the end optimizes the overall loading performance.

In essence, this loading hierarchy ensures an organized and efficient rendering process, enabling the browser to progressively construct a fully-fledged and visually appealing webpage.

- c. Total 6 tcp connections were opened, which is more than the number of http requests. This is because multiple http requests can be served over a single tcp connection. The requests served by the connections are summarized in [Table 6](#).

Source Port	Request Handled
59649	html, monotools.js
59650	caption.js, favicon, balazahir.jpg
59654	layout.css, act4d.png
59655	position.css, print.css
59656	template.css
59657	general.css

Table 6: Ports and Requests

Reusing connections helps to improve performance by saving the time taken to establish a connection. Further, the server can also reuse the same resources for multiple requests, which saves time and bandwidth.

## §5. Appendix: Preparatory Tasks

Here, we provide information about the various tools available for network analysis

### 5.1. ifconfig/ipconfig

This is used to find the following for the network interfaces on the computer:

**IP address** An IP (Internet Protocol) address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves two main purposes: identifying the host or network interface and providing the location of the host in the network. IP addresses can be either IPv4 (32-bit) or IPv6 (128-bit) and are written in a dotted-decimal format (e.g., 172.31.225.222 for IPv4 or fe80::215:5dff:feeb:19f7 for IPv6).

**Gateway** A gateway, often referred to as a default gateway, is a network device (usually a router) that serves as an access point to other networks. It acts as an intermediary between devices within a local network and devices on other networks, including the internet. When a device on a local network wants to communicate with a device on another network, it sends the data to the gateway, which then forwards it to the appropriate destination.

**Network mask** A network mask, also known as a subnet mask, is used in conjunction with an IP address to determine the network portion and the host portion of the address. It is a binary pattern of bits that help divide an IP address into a network address and a host address. The network mask is typically represented in decimal format as four octets (e.g., 255.255.255.0 for IPv4). It is used in the process of subnetting to identify which part of the IP address identifies the network and which part identifies the individual host within that network.

**Hardware address** A hardware address, also known as a MAC (Media Access Control) address, is a unique identifier assigned to a network interface card (NIC) by its manufacturer. It is a 48-bit address expressed in hexadecimal format and is used to identify a specific device on a local network. Each NIC in the world has its own unique MAC address, allowing devices to communicate with each other at the data link layer of the networking model.

**DNS server** A DNS (Domain Name System) server translates human-readable domain names, like `www.google.com`, into IP addresses that machines can understand. When you enter a URL in a web browser or try to access any internet resource, your device sends a DNS query to a DNS server. The DNS server then looks up the corresponding IP address associated with the domain name and returns it to your device, allowing it to establish a connection to the desired resource.

Running `ifconfig` on our system connected to Wifi gives the following output:

```
root@IdeapadAB:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.31.225.222 netmask 255.255.240.0 broadcast 172.31.239.255
    inet6 fe80::215:5dff:feeb:19f7 prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:eb:19:f7 txqueuelen 1000 (Ethernet)
    RX packets 149 bytes 20663 (20.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 13 bytes 1006 (1.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

And on running it on mobile hotspot, we get the following output:

```
root@IdeapadAB:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.31.225.222 netmask 255.255.240.0 broadcast 172.31.239.255
    inet6 fe80::215:5dff:feeb:19f7 prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:eb:19:f7 txqueuelen 1000 (Ethernet)
    RX packets 1035 bytes 154375 (154.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 103 bytes 8962 (8.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

eth0 and lo are two different network interfaces. eth0 is associated with the Ethernet connection and lo is the loopback(localhost) interface.

Here is a description of the various fields in the output:

**flags** A set of flags that indicate the status of the network interface.

**mtu** The Maximum Transmission Unit (MTU) is the size of the largest packet that can be transmitted over the network interface without being fragmented. The MTU is typically measured in bytes and can range from 64 to 65535 bytes.

**inet** The IPv4 address assigned to the network interface.

**netmask** The subnet mask for the IPv4 address. It helps determine the network and host portions of the IP address.

**broadcast** The broadcast address for the network. It is used to send data to all devices on the local network.

**inet6** The IPv6 link-local address with a prefix length of 64 bits. IPv6 addresses are written in hexadecimal format and are longer than IPv4 addresses.

**ether** The unique hardware address (MAC address) of the network interface card.

**txqueuelen** The length of the transmit queue.

**RX packets** The number of received packets.

**TX packets** The number of transmitted packets.

**RX errors** The number of receive errors.

**TX errors** The number of transmit errors.

**dropped** The number of dropped packets due to errors.

**overruns** The number of packets that had data sent beyond their allowed length.

**frame** The number of packets with framing errors.

**collisions** The number of packet collisions (i.e., when two devices transmit data at the same time).

The IP address of the smartphone can be found by "Settings→About phone→Status→IP address"

## 5.2. ping

This is used to discover if a particular IP address is online or not. For example, in the following code we are pinging `www.google.com` with packets of size 10 bytes and varying the TTL. We observe that as the TTL decreases, the packet doesn't reach the destination. This is because the TTL is decremented by 1 at each hop and when it reaches 0, the packet is dropped and an ICMP error message is sent back to the source. The source then knows that the packet didn't reach the destination and hence the destination is not online.

```
root@IdeapadAB:~# ping -c 3 -s 50 -t 10 www.google.com
PING www.google.com (142.250.195.4) 50(78) bytes of data.
58 bytes from del12s09-in-f4.1e100.net (142.250.195.4): icmp_seq=1 ttl=55 time=82.3 ms
58 bytes from del12s09-in-f4.1e100.net (142.250.195.4): icmp_seq=2 ttl=55 time=67.1 ms
58 bytes from del12s09-in-f4.1e100.net (142.250.195.4): icmp_seq=3 ttl=55 time=33.1 ms

--- www.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 33.130/60.834/82.271/20.545 ms
root@IdeapadAB:~# ping -c 3 -s 50 -t 9 www.google.com
PING www.google.com (142.250.195.4) 50(78) bytes of data.
From 142.251.52.213 (142.251.52.213) icmp_seq=1 Time to live exceeded
From 142.251.52.213 (142.251.52.213) icmp_seq=2 Time to live exceeded
From 142.251.52.213 (142.251.52.213) icmp_seq=3 Time to live exceeded

--- www.google.com ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2299ms
pipe 2
```

## 5.3. traceroute

This gives you the sequence of routers that a packet traverses to get to a particular destination.

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

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

 1      3 ms      4 ms      3 ms    192.168.107.98
 2     39 ms     29 ms     21 ms    10.50.97.29
 3     54 ms     46 ms     23 ms    10.50.97.223
 4     58 ms     25 ms     34 ms    10.50.97.77
 5    190 ms     30 ms     46 ms    dsl-ncr-dynamic-017.24.23.125.airtelbroadband.in [125.23.24.17]
 6     63 ms     37 ms     27 ms    116.119.109.76
 7     51 ms     38 ms     26 ms    49.44.187.164
 8      *        *        *      Request timed out.
 9      *        *        *      Request timed out.
10     38 ms     27 ms     27 ms    136.232.148.178
11      *        *        *      Request timed out.
12      *        *        *      Request timed out.
13      *        *        *      Request timed out.
14     53 ms     36 ms     60 ms    103.27.9.24
15     85 ms     35 ms     36 ms    103.27.9.24
16    148 ms    101 ms     86 ms    103.27.9.24

Trace complete.
```

## 5.4. nslookup

This command helps you communicate with DNS servers to get the IP address for a particular hostname.



### **5.5. nmap**

This is a handy network diagnostics tool that you can use to discover which hosts are online in the network, and even try to infer what operating system the hosts might be running.

### **5.6. Wireshark**

This is a very useful tool to sniff packets on the wire (or wireless medium). Sniffed data is parsed by wireshark and presented in an easily readable format with details of the protocols being used at different layers.