COL334 Assignment 1

Aastha Rajani (2021CS10093) Disha Shiraskar (2021CS10578)

August 13, 2023

1 Network Analysis

1.1 Traceroute

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

Tracing route to www.iitd.ac.in [2001:df4:e000:29::212]
over a maximum of 30 hops:

  1     2 ms     2 ms     1 ms  2401:4900:47f3:fe32::b8
  2    22 ms    24 ms    20 ms  2401:4900:47f3:fe32:0:1f:e49c:4540
  3    24 ms    32 ms    23 ms  2401:4900:0:c003::6422
  4    30 ms    26 ms    28 ms  2401:4900:0:c003::6655
  5    31 ms    37 ms    50 ms  2401:4900:0:c003::6664
  6    51 ms    27 ms    29 ms  2404:a800:1a00:801::e5
  7   101 ms    55 ms    53 ms  2404:a800::93
  8    77 ms    67 ms    71 ms  2405:200:1607:600:49:44:220:bc
  9    67 ms    77 ms    66 ms  2405:203:89a::141e
 10    94 ms    79 ms    70 ms  2405:8a00:a:3::2
 11    75 ms    72 ms    74 ms  2405:8a00:a:a::3
 12     *        *        *     Request timed out.
 13    61 ms    61 ms    63 ms  2001:4408:a::1
 14    83 ms    74 ms    60 ms  2405:8a00:a:2::c5
 15   102 ms    56 ms    74 ms  2405:8a00:a:2::c6
 16    67 ms    68 ms    63 ms  2001:df4:e000:108::2
 17    76 ms    61 ms    70 ms  2001:df4:e000:26::24
 18    93 ms    61 ms   101 ms  2001:df4:e000:29::212

Trace complete.
PS C:\Users\disha>
```

Figure 1: Traceroute to www.iitd.ac.in

```
PS C:\Users\disha> tracert -4 www.iitd.ac.in

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

  1     2 ms     1 ms     1 ms  192.168.18.60
  2   110 ms    21 ms   128 ms  192.168.59.1
  3    33 ms    42 ms    27 ms  192.168.27.93
  4    19 ms    40 ms    18 ms  192.168.27.111
  5    27 ms    30 ms    26 ms  nsg-corporate-5.39.185.122.airtel.in [122.185.39.5]
  6    49 ms    34 ms    25 ms  116.119.109.74
  7    23 ms    22 ms    22 ms  49.44.187.164
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10    36 ms    22 ms    23 ms  136.232.148.178
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15    37 ms    64 ms    44 ms  103.27.9.24
 16   169 ms    36 ms    30 ms  103.27.9.24
 17    25 ms    23 ms    23 ms  103.27.9.24
```

Figure 2: Traceroute to www.iitd.ac.in

1.2 Obervations

- The traceroute is using IPv6 addresses for all the hops in the path, starting from our local network (e.g., 2401:4900:47f8:5733::7f). This indicates that the network is configured to prioritize IPv6 communication.
- Forcing Traceroute to Use IPv4: The traceroute output provided is IPv6-based. To force traceroute to use IPv4, we use the -4 option with the traceroute command. For example: traceroute -4 www.google.com.
- The traceroute does show private IP address spaces like 192.168.18.60, 192.168.59.1, 192.168.27.81, and 192.168.27.107 are all private IP addresses from the IPv4 private address ranges.
- Missing Routers: There are some hops that seem to not reply to the traceroute requests. This could indicate that those routers have ICMP (Internet Control Message Protocol) echo requests disabled or are configured to rate-limit or drop these requests. It's common for some routers to prioritize actual data traffic over ICMP requests.
- Varying Latency: The varying "ms" values for each hop indicate the latency or round-trip time between our device and each router or device in the path. Latency can be influenced by factors such as distance, network congestion, and the performance of each intermediate device.
- These private IP addresses indicate that the traceroute is traversing through local network infrastructure before reaching the public internet.

1.3 Ping

```
PS C:\Users\disha>
PS C:\Users\disha> ping -l 1451 www.google.com

Pinging www.google.com [2404:6800:4009:828::2004] with 1451 bytes of data:
Reply from 2404:6800:4009:828::2004: time=56ms
Reply from 2404:6800:4009:828::2004: time=74ms
Reply from 2404:6800:4009:828::2004: time=62ms
Reply from 2404:6800:4009:828::2004: time=69ms

Ping statistics for 2404:6800:4009:828::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 56ms, Maximum = 74ms, Average = 65ms
PS C:\Users\disha>
```

```
PS C:\Users\disha> ping -l 1452 www.google.com

Pinging www.google.com [2404:6800:4009:828::2004] with 1452 bytes of data:
Reply from 2404:6800:4009:828::2004: time=86ms
Reply from 2404:6800:4009:828::2004: time=85ms
Reply from 2404:6800:4009:828::2004: time=282ms
Reply from 2404:6800:4009:828::2004: time=69ms

Ping statistics for 2404:6800:4009:828::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 69ms, Maximum = 282ms, Average = 130ms
PS C:\Users\disha>
```

```
PS C:\Users\disha> ping -l 1453 www.google.com

Pinging www.google.com [2404:6800:4009:828::2004] with 1453 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2404:6800:4009:828::2004:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\disha>
```

Figure 3: Ping to www.google.com

Ping can be used to send data packets with a maximum size of 65,527 bytes. Maximum size of ping packets that we are able to send to www.google.com from our device is 1452 bytes.

2 Replicating Traceroute using Ping

final.py > replicate_tracert

```python
import os
def replicate_tracert(destination):
    for tl in range(1,31):
        result = os.popen("nping --icmp --ttl " + str(tl) +" --count 3 " + destination).read()
        l = result.split("\n")
        if(len(l)<13):
            print(str(tl)+" * * * Request Timed Out")
            continue
        i = 2
        answer = str(tl)+" "
        req_ip = l[2].split(" ")[5]
        while(i<len(l)-5):
            send = l[i].split(" ")
            reci = l[i+1].split(" ")
            st = send[1][1:len(send[1])-2]
            rt = reci[1][1:len(send[1])-2]
            rtt = str(int((float(rt)-float(st))*1000)) + " ms "
            answer += rtt
            i = i+2
        ip = l[3].split(" ")[3][1:]
        answer += " " + ip
        print(answer)
        if(ip==req_ip):
            break
if __name__ == "__main__":
    replicate_tracert("www.example.com")

```

Figure 4: Python Script

This Python code defines a function replicate tracert(destination) that aims to mimic the behavior of the tracert command using the nping tool for sending ICMP echo request packets with gradually increasing TTL values. The function takes a target destination (like a domain name or IP address) as an argument.

For each TTL value from 1 to 30, the code uses the os.popen function to execute the nping command with the specified TTL and a count of 3 packets. It then processes the output to extract the round-trip times (RTTs) of the packets and the responding IP addresses. The extracted RTTs are calculated by subtracting the sending time from the receiving time and converted to milliseconds. The script also checks for "Request Timed Out" messages and handles them appropriately. The loop continues until either it reaches the maximum TTL value or finds the final destination IP matching the last hop's IP. Finally, it prints the gathered information in a format similar to tracert's output.

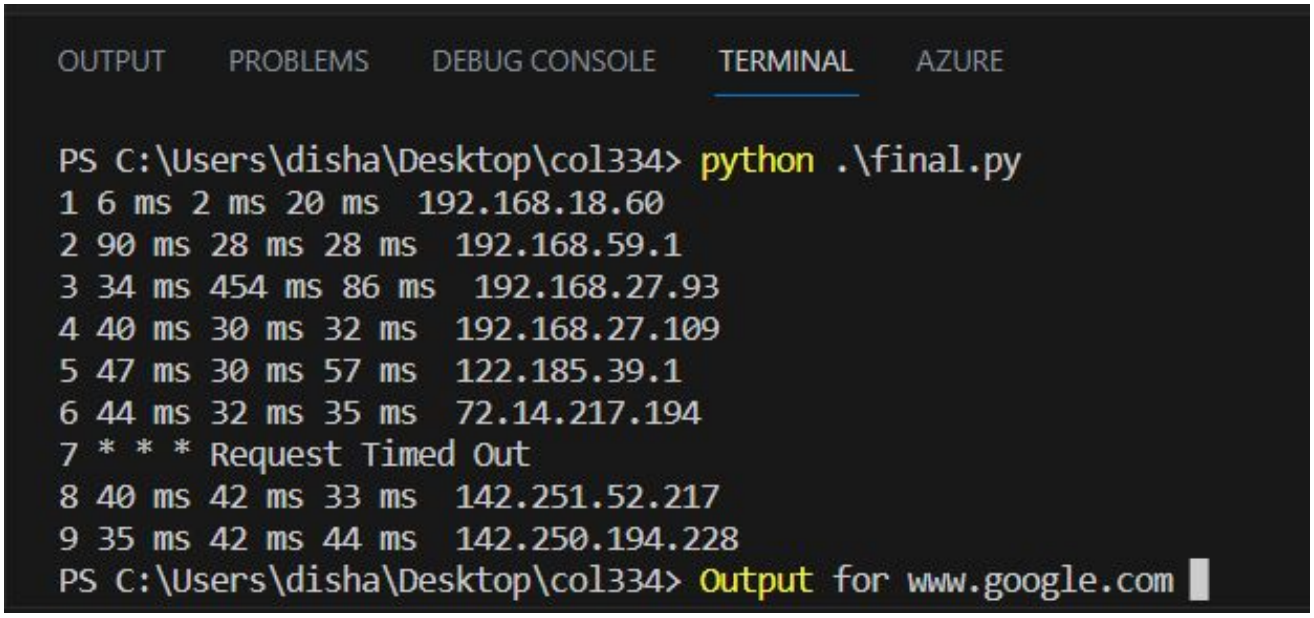


Figure 5: Traceroute to www.google.com

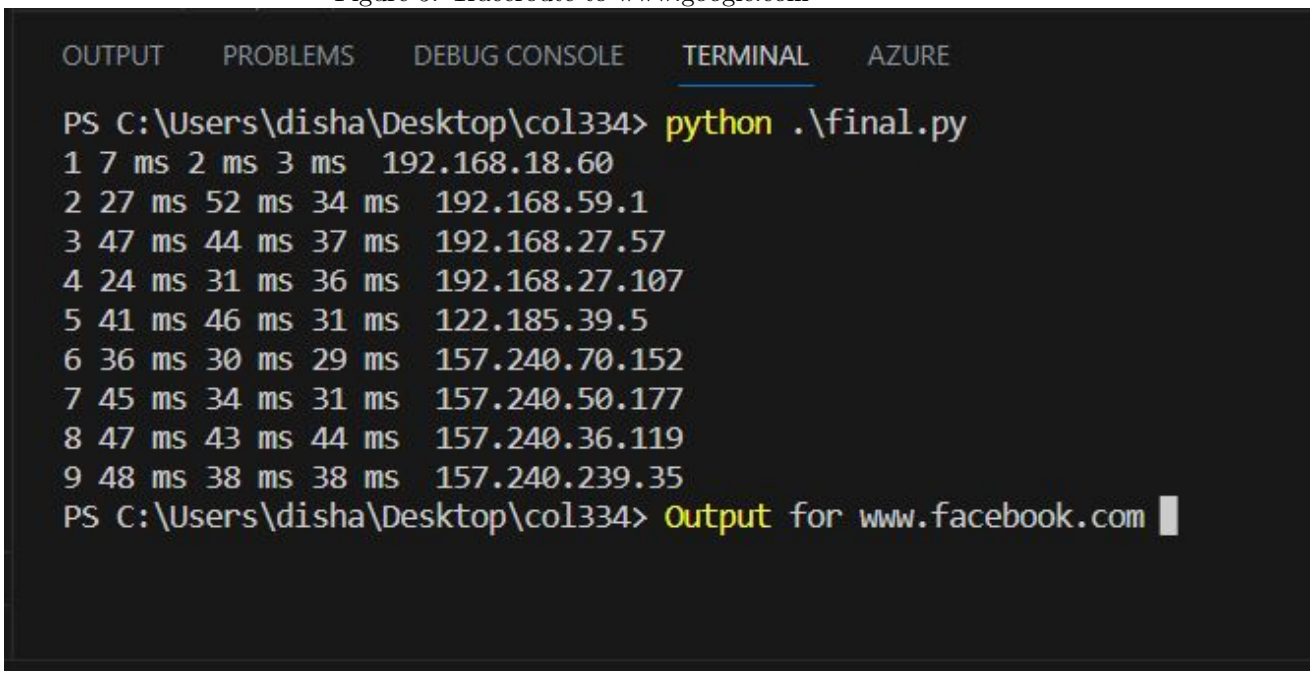


Figure 6: Traceroute to www.facebook.com

3 Internet Architechture

3.1 Traceroute from my device

```
PS C:\Users\disha> tracert -4 www.iitd.ac.in

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

  1     2 ms     1 ms     1 ms  192.168.18.60
  2   110 ms    21 ms   128 ms  192.168.59.1
  3    33 ms    42 ms    27 ms  192.168.27.93
  4    19 ms    40 ms    18 ms  192.168.27.111
  5    27 ms    30 ms    26 ms  nsg-corporate-5.39.185.122.airtel.in [122.185.39.5]
  6    49 ms    34 ms    25 ms  116.119.109.74
  7    23 ms    22 ms    22 ms  49.44.187.164
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10    36 ms    22 ms    23 ms  136.232.148.178
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15    37 ms    64 ms    44 ms  103.27.9.24
 16   169 ms    36 ms    30 ms  103.27.9.24
 17    25 ms    23 ms    23 ms  103.27.9.24
```

Figure 7: Traceroute to www.iitd.ac.in

```
PS C:\Program Files (x86)\Nmap> tracert -4 www.google.com

Tracing route to www.google.com [142.250.194.228]
over a maximum of 30 hops:

  1     1 ms     1 ms     2 ms  192.168.18.60
  2    31 ms    25 ms    36 ms  192.168.59.1
  3    40 ms    28 ms    25 ms  192.168.27.93
  4    37 ms    27 ms    33 ms  192.168.27.109
  5    54 ms    27 ms    30 ms  nsg-corporate-1.39.185.122.airtel.in [122.185.39.1]
  6    36 ms    25 ms    35 ms  72.14.217.194
  7    79 ms    22 ms    35 ms  108.170.237.85
  8    42 ms    30 ms    40 ms  142.251.52.217
  9    45 ms    32 ms    48 ms  del12s08-in-f4.1e100.net [142.250.194.228]

Trace complete.
PS C:\Program Files (x86)\Nmap>
```

Figure 8: Traceroute to www.google.com

```
PS C:\Users\disha> tracert -4 www.facebook.com

Tracing route to star-mini.c10r.facebook.com [157.240.239.35]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  192.168.18.60
  2    17 ms    16 ms    32 ms  192.168.59.1
  3    80 ms    53 ms    22 ms  192.168.27.57
  4    25 ms    21 ms    44 ms  192.168.27.107
  5    37 ms    17 ms    29 ms  nsg-corporate-5.39.185.122.airtel.in [122.185.39.5]
  6    37 ms    29 ms    20 ms  ae20.pr03.del1.tfbnw.net [157.240.70.152]
  7    49 ms    19 ms    58 ms  po103.psw04.del1.tfbnw.net [157.240.50.177]
  8    72 ms    41 ms    55 ms  157.240.36.119
  9    43 ms    75 ms    59 ms  edge-star-mini-shv-02-del1.facebook.com [157.240.239.35]

Trace complete.
PS C:\Users\disha>
```

Figure 9: Traceroute to www.facebook.com

```
PS C:\Program Files (x86)\Nmap> tracert www.utah.edu

Tracing route to www.utah.edu [155.98.186.21]
over a maximum of 30 hops:

  1     2 ms     2 ms     1 ms  192.168.18.60
  2    41 ms    31 ms    25 ms  192.168.59.1
  3    31 ms    28 ms    27 ms  192.168.27.93
  4    35 ms    36 ms    16 ms  192.168.27.109
  5    32 ms    27 ms    27 ms  nsg-corporate-1.39.185.122.airtel.in [122.185.39.1]
  6   177 ms   187 ms   173 ms  182.79.201.122
  7     *        *        *     Request timed out.
  8   193 ms   225 ms   186 ms  be2779.ccr41.par01.atlas.cogentco.com [154.54.72.109]
  9   217 ms   423 ms   318 ms  be12497.ccr41.lon13.atlas.cogentco.com [154.54.56.129]
 10   588 ms   310 ms   321 ms  be2099.ccr31.bos01.atlas.cogentco.com [154.54.82.34]
 11   307 ms   311 ms   320 ms  be3599.ccr21.alb02.atlas.cogentco.com [66.28.4.237]
 12   303 ms   305 ms   318 ms  be2878.ccr21.cle04.atlas.cogentco.com [154.54.26.129]
 13   304 ms   515 ms   318 ms  be2717.ccr41.ord01.atlas.cogentco.com [154.54.6.221]
 14   343 ms   344 ms   314 ms  be2831.ccr21.mci01.atlas.cogentco.com [154.54.42.165]
 15   327 ms   302 ms   308 ms  be3035.ccr21.den01.atlas.cogentco.com [154.54.5.89]
 16   331 ms   309 ms   557 ms  be3037.ccr21.slc01.atlas.cogentco.com [154.54.41.145]
 17   391 ms   325 ms   314 ms  be2685.rcr01.b020767-1.slc01.atlas.cogentco.com [154.54.41.118]
 18   339 ms   331 ms   325 ms  38.142.233.58
 19     *        *        *     Request timed out.
 20   403 ms   315 ms   315 ms  ebc-pep-a-178-int.uen.net [140.197.253.23]
 21     *      524 ms     *     140.197.253.139
 22   308 ms   298 ms   297 ms  199.104.93.22
 23   310 ms   298 ms   297 ms  199.104.93.29
 24   308 ms   307 ms   303 ms  155.99.130.57
 25   296 ms   294 ms   299 ms  155.99.130.101
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29   311 ms   298 ms   308 ms  uhome.web.utah.edu [155.98.186.21]

Trace complete.
PS C:\Program Files (x86)\Nmap>
```

Figure 10: Traceroute to www.utah.edu

```
PS C:\Program Files (x86)\Nmap> tracert www.uct.ac.za

Tracing route to cms-vip-prd.uct.ac.za [137.158.159.192]
over a maximum of 30 hops:

  1     1 ms     1 ms    <1 ms  192.168.18.60
  2    38 ms    29 ms    24 ms  192.168.59.1
  3    51 ms    17 ms    17 ms  192.168.27.57
  4    41 ms    30 ms    35 ms  192.168.27.107
  5    81 ms    27 ms   132 ms  nsg-corporate-5.39.185.122.airtel.in [122.185.39.5]
  6   212 ms   216 ms   217 ms  116.119.121.16
  7   214 ms   218 ms   216 ms  80.249.213.145
  8   280 ms   210 ms   224 ms  lt-1-1-0-0-ams1-ir1.net.tenet.ac.za [155.232.216.6]
  9   347 ms   359 ms   418 ms  ae0-306-mtz1-ir1.net.tenet.ac.za [155.232.1.86]
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12   387 ms   359 ms   374 ms  et-0-0-1-0-cpt7-pe1.net.tenet.ac.za [155.232.64.70]
 13   397 ms   488 ms   460 ms  154.114.124.1
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *     General failure.

Trace complete.
PS C:\Program Files (x86)\Nmap>
```

Figure 11: Traceroute to www.uct.ac.za

3.2 Traceroute from US

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  core-ns-router (128.112.128.2)  0.861 ms  0.657 ms  0.596 ms
 2  rtr-core-east-router.princeton.edu (128.112.12.225)  0.738 ms  0.738 ms  0.550 ms
 3  fw-border-87-router.princeton.edu (128.112.12.10)  0.958 ms  0.925 ms  0.930 ms
 4  rtr-border-87-router.princeton.edu (204.153.48.1)  2.664 ms  1.458 ms  1.413 ms
 5  172-96-130.unassigned.userdns.com (172.96.130.53)  5.116 ms  3.798 ms  4.087 ms
 6  172-96-130.unassigned.userdns.com (172.96.130.77)  5.732 ms  5.724 ms 172-96-130.unassigned.userdns.com (172.96.130.61)  6.145 ms
 7  bundle-ether240.200.core1.newy32aoa.net.internet2.edu (163.253.5.38)  7.540 ms  6.283 ms  6.125 ms
 8  180.149.48.12 (180.149.48.12)  85.873 ms  86.416 ms  85.213 ms
 9  180.149.48.21 (180.149.48.21)  85.464 ms 180.149.48.1 (180.149.48.1)  228.135 ms  227.988 ms
10  180.149.48.17 (180.149.48.17)  227.388 ms 180.149.48.5 (180.149.48.5)  227.563 ms 180.149.48.17 (180.149.48.17)  229.601 ms
11  180.149.48.17 (180.149.48.17)  227.978 ms  227.774 ms *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Done.

Figure 12: Traceroute to www.iitd.ac.in

Traceroute

tracing path from `www.net.princeton.edu` to `142.251.40.132` ...

```
traceroute to 142.251.40.132 (142.251.40.132), 30 hops max, 40 byte packets
 1  core-ns-router (128.112.128.2)  1.138 ms  0.855 ms  0.570 ms
 2  rtr-core-east-router.princeton.edu (128.112.12.225)  0.910 ms  0.698 ms  0.558 ms
 3  fw-border-87-router.princeton.edu (128.112.12.10)  0.986 ms  0.900 ms  0.943 ms
 4  rtr-border-87-router.princeton.edu (204.153.48.1)  1.329 ms  1.544 ms  1.511 ms
 5  172-96-130.unassigned.userdns.com (172.96.130.53)  5.038 ms  5.718 ms  4.157 ms
 6  172-96-130.unassigned.userdns.com (172.96.130.77)  4.245 ms  5.471 ms 172-96-130.unassigned.userdns.com (172.96.130.61)  6.158 ms
 7  bundle-ether240.202.core1.newy32aoa.net.internet2.edu (198.71.47.232)  5.102 ms  5.901 ms  6.051 ms
 8  fourhundredge-0-0-0-48.4079.agg2.newy2.net.internet2.edu (163.253.2.149)  6.154 ms fourhundredge-0-0-0-48.4079.agg1.newy2.net.internet2.ed
 9  162.252.69.197 (162.252.69.197)  4.169 ms  4.751 ms 162.252.69.135 (162.252.69.135)  6.649 ms
10  * * *
11  108.170.248.33 (108.170.248.33)  5.884 ms 142.251.65.114 (142.251.65.114)  4.048 ms 142.251.60.180 (142.251.60.180)  4.534 ms
12  216.239.43.155 (216.239.43.155)  4.969 ms 108.170.248.35 (108.170.248.35)  5.103 ms 108.170.248.52 (108.170.248.52)  4.526 ms
13  142.251.49.87 (142.251.49.87)  4.224 ms 142.251.68.253 (142.251.68.253)  6.137 ms lga25s80-in-f4.1e100.net (142.251.40.132)  4.217 ms
```

Done.

Figure 13: Traceroute to www.google.com

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  core-ns-router (128.112.128.2)  1.134 ms  0.911 ms  0.601 ms
 2  rtr-core-east-router.princeton.edu (128.112.12.225)  0.667 ms  0.560 ms  0.548 ms
 3  fw-border-87-router.princeton.edu (128.112.12.10)  0.968 ms  0.908 ms  0.904 ms
 4  rtr-border-87-router.princeton.edu (204.153.48.1)  1.314 ms  31.163 ms  1.572 ms
 5  172-96-130.unassigned.userdns.com (172.96.130.53)  5.850 ms  5.837 ms  3.985 ms
 6  172-96-130.unassigned.userdns.com (172.96.130.77)  6.349 ms  5.766 ms 172-96-130.unassigned.userdns.com (172.96.130.61)  6.061 ms
 7  bundle-ether240.202.core1.newy32aoa.net.internet2.edu (198.71.47.232)  6.726 ms  5.416 ms  6.139 ms
 8  fourhundredge-0-0-0-48.4079.agg1.newy2.net.internet2.edu (163.253.2.123)  7.555 ms fourhundredge-0-0-0-48.4079.agg2.newy2.net.inter
 9  162.252.69.205 (162.252.69.205)  4.258 ms 162.252.69.207 (162.252.69.207)  4.771 ms  4.879 ms
10  po203.asw02.lga1.tfbnw.net (157.240.103.118)  3.769 ms  3.663 ms po203.asw04.lga1.tfbnw.net (157.240.103.122)  4.196 ms
11  po269.psw03.lga3.tfbnw.net (157.240.104.131)  4.449 ms po298.psw02.lga3.tfbnw.net (157.240.104.165)  3.979 ms po205.psw03.lga3.tfbn
12  157.240.38.239 (157.240.38.239)  4.623 ms 173.252.67.161 (173.252.67.161)  4.639 ms 173.252.67.85 (173.252.67.85)  7.425 ms
13  edge-star-mini-shv-01-lga3.facebook.com (31.13.71.36)  3.952 ms  4.410 ms  4.342 ms
```

Done.

Figure 14: Traceroute to www.facebook.com

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  core-ns-router (128.112.128.2)  1.226 ms  0.963 ms  0.629 ms
 2  rtr-core-west-router.princeton.edu (128.112.12.229)  0.619 ms  0.574 ms  0.523 ms
 3  fw-border-hpcrc-router.princeton.edu (128.112.12.14)  1.149 ms  1.032 ms  1.071 ms
 4  rtr-border-hpcrc-router.princeton.edu (204.153.48.253)  1.610 ms  1.474 ms  1.470 ms
 5  172-96-130.unassigned.userdns.com (172.96.130.49)  4.048 ms  4.173 ms *
 6  172-96-130.unassigned.userdns.com (172.96.130.76)  6.158 ms  6.471 ms 172-96-130.unassigned.userdns.com (172.96.130.60)  5.960 ms
 7  bundle-ether1.102.core1.phil.net.internet2.edu (163.253.5.8)  6.583 ms  5.882 ms  6.160 ms
 8  fourhundredge-0-0-0-2.4079.core2.ashb.net.internet2.edu (163.253.1.136)  63.003 ms  63.494 ms  63.456 ms
 9  fourhundredge-0-0-0-1.4079.core2.clev.net.internet2.edu (163.253.1.139)  61.942 ms  64.612 ms  63.215 ms
10  fourhundredge-0-0-0-2.4079.core2.eqch.net.internet2.edu (163.253.2.17)  63.533 ms  62.682 ms  63.059 ms
11  fourhundredge-0-0-0-2.4079.core2.chic.net.internet2.edu (163.253.2.18)  64.438 ms  63.928 ms  63.164 ms
12  fourhundredge-0-0-0-1.4079.core1.kans.net.internet2.edu (163.253.1.245)  63.278 ms  65.293 ms  62.689 ms
13  fourhundredge-0-0-0-1.4079.core1.denv.net.internet2.edu (163.253.1.242)  63.241 ms  62.650 ms  63.008 ms
14  fourhundredge-0-0-0-3.4079.core1.salt.net.internet2.edu (163.253.1.171)  63.718 ms  63.002 ms  62.663 ms
15  fourhundredge-0-0-0-1.4079.core1.lasv.net.internet2.edu (163.253.1.152)  63.966 ms  63.385 ms  62.691 ms
16  163.253.5.7 (163.253.5.7)  63.847 ms  64.500 ms  64.526 ms
17  tdc-beibr-b-170-int.uen.net (140.197.249.81)  62.102 ms  62.265 ms  62.853 ms
18  ddc-pep-c-123-int.uen.net (140.197.251.32)  63.043 ms  62.687 ms  62.564 ms
19  ddc-pep-b-129-int.uen.net (140.197.253.97)  62.876 ms  62.886 ms  62.281 ms
20  ebc-pep-b-179-int.uen.net (140.197.252.76)  62.463 ms  62.373 ms  63.063 ms
21  ebc-pep-a-178-int.uen.net (140.197.252.84)  63.320 ms  62.875 ms  62.495 ms
22  * * *
23  199.104.93.22 (199.104.93.22)  64.606 ms  63.077 ms  63.363 ms
24  199.104.93.33 (199.104.93.33)  63.826 ms  63.217 ms  64.365 ms
25  155.99.130.65 (155.99.130.65)  63.626 ms  63.362 ms  63.133 ms
26  155.99.130.101 (155.99.130.101)  64.661 ms 155.99.130.105 (155.99.130.105)  65.617 ms 155.99.130.107 (155.99.130.107)  63.905 ms
27  * * *
28  * * *
29  * * *
30  www.utah.edu (155.98.186.21)  64.688 ms  64.670 ms  63.998 ms
```

Done.

Figure 15: Traceroute to www.utah.edu

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  core-ns-router (128.112.128.2)  1.275 ms  0.969 ms  0.788 ms
 2  rtr-core-east-router.princeton.edu (128.112.12.225)  1.017 ms  0.771 ms  0.719 ms
 3  fw-border-87-router.princeton.edu (128.112.12.10)  1.054 ms  1.013 ms  0.924 ms
 4  rtr-border-87-router.princeton.edu (204.153.48.1)  1.517 ms  1.197 ms  1.446 ms
 5  172-96-130.unassigned.userdns.com (172.96.130.53)  4.838 ms  4.220 ms  3.990 ms
 6  bundle-ether1.102.core1.phil.net.internet2.edu (163.253.5.8)  4.847 ms  5.931 ms  4.172 ms
 7  fourhundredge-0-0-0-2.4079.core2.ashb.net.internet2.edu (163.253.1.136)  27.633 ms  26.290 ms  26.733 ms
 8  fourhundredge-0-0-0-1.4079.core2.atla.net.internet2.edu (163.253.1.135)  27.025 ms  28.409 ms  28.586 ms
 9  fourhundredge-0-0-0-21.4079.core1.atla.net.internet2.edu (163.253.1.100)  27.404 ms  26.170 ms  26.425 ms
10  fourhundredge-0-0-0-1.4079.core1.jack.net.internet2.edu (163.253.2.33)  26.207 ms  26.778 ms  26.545 ms
11  et-0-1-4-1972-cpt3-pe1.net.tenet.ac.za (155.232.71.2)  191.368 ms  191.782 ms et-0-1-4-1973-cpt3-pe1.net.tenet.ac.za (155.232.71.4)  191.394 ms
12  lt-1-1-0-2-cpt3-pe1.net.tenet.ac.za (155.232.64.34)  194.181 ms lt-1-0-0-2-cpt3-pe1.net.tenet.ac.za (155.232.64.36)  192.719 ms lt-1-1-0-2-cpt3-
13  et-0-0-1-0-cpt7-pe1.net.tenet.ac.za (155.232.64.70)  191.495 ms  191.620 ms  191.416 ms
14  154.114.124.1 (154.114.124.1)  191.849 ms  191.856 ms  191.902 ms
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Done.

Figure 16: Traceroute to www.uct.ac.za

3.3 Traceroute from Gemany

traceroute to www.iitd.ac.in

```
traceroute to www.iitd.ac.in (103.27.9.24), 30 hops max, 60 byte packets
 1  vsn0057.vs.mass.systems (10.92.36.120)  0.026 ms  0.011 ms  0.011 ms
 2  ae3-u100.sxb1-cr-nunki.bb.gdinf.net (87.230.112.2)  1.327 ms  0.269 ms  1.275 ms
 3  ae1.sxb1-ibr-altair.bb.gdinf.net (87.230.112.14)  9.923 ms  9.904 ms  9.879 ms
 4  ae0.sxb1-ibr-tarazed.bb.gdinf.net (87.230.112.19)  0.654 ms  0.635 ms  0.611 ms
 5  ae7.fra10-cr-antares.bb.gdinf.net (87.230.115.2)  3.483 ms  3.461 ms  3.437 ms
 6  ae2.fra1-cr-polaris.bb.gdinf.net (87.230.115.0)  3.565 ms  3.596 ms  3.516 ms
 7  jio.com (80.81.195.32)  3.700 ms  3.623 ms  4.040 ms
 8  103.198.140.84 (103.198.140.84)  117.343 ms  117.806 ms 103.198.140.212 (103.198.140.212)  117.128 ms
 9  103.198.140.84 (103.198.140.84)  116.981 ms 103.198.140.78 (103.198.140.78)  119.012 ms  120.526 ms
10  49.44.220.242 (49.44.220.242)  116.319 ms * 103.198.140.212 (103.198.140.212)  115.293 ms
11  * 49.44.220.242 (49.44.220.242)  117.765 ms *
12  * * *
13  * * *
14  * 136.232.148.178 (136.232.148.178)  154.285 ms  143.281 ms
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Figure 17: Traceroute to www.iitd.ac.in

traceroute to www.google.com

```
traceroute to www.google.com (142.250.186.100), 30 hops max, 60 byte packets
 1  vsn0057.vs.mass.systems (10.92.36.120)  0.037 ms  0.018 ms  0.013 ms
 2  ae3-u100.sxb1-cr-nunki.bb.gdinf.net (87.230.112.2)  0.366 ms  0.353 ms  0.315 ms
 3  ae1.sxb1-ibr-altair.bb.gdinf.net (87.230.112.14)  0.465 ms  0.458 ms  0.469 ms
 4  ffm-b16-link.ip.twelve99.net (62.115.144.8)  2.958 ms  2.963 ms  3.034 ms
 5  * * ffm-bb1-link.ip.twelve99.net (62.115.132.226)  3.337 ms
 6  ffm-b11-link.ip.twelve99.net (62.115.124.119)  3.394 ms *  3.312 ms
 7  google-ic-319726.ip.twelve99-cust.net (62.115.151.25)  3.301 ms google-ic-319727.ip.twelve99-cust.net (62.115.151.27)  3.592 ms
 8  * * *
 9  142.251.64.180 (142.251.64.180)  3.655 ms 142.250.236.56 (142.250.236.56)  3.490 ms 172.253.64.118 (172.253.64.118)  3.648 ms
10  108.170.252.82 (108.170.252.82)  3.424 ms 108.170.252.83 (108.170.252.83)  4.086 ms 108.170.251.209 (108.170.251.209)  4.100 ms
11  fra24s06-in-f4.1e100.net (142.250.186.100)  3.476 ms 216.239.40.147 (216.239.40.147)  5.331 ms fra24s06-in-f4.1e100.net (142.25
```

Figure 18: Traceroute to www.google.com

traceroute to www.facebook.com

```
traceroute to www.facebook.com (157.240.223.35), 30 hops max, 60 byte packets
 1  vsn0057.vs.mass.systems (10.92.36.120)  0.040 ms  0.017 ms  0.014 ms
 2  ae3-u100.sxb1-cr-nunki.bb.gdinf.net (87.230.112.2)  0.304 ms  0.395 ms  0.367 ms
 3  ae1.sxb1-ibr-altair.bb.gdinf.net (87.230.112.14)  0.727 ms  0.699 ms  0.671 ms
 4  ae0.sxb1-ibr-tarazed.bb.gdinf.net (87.230.112.19)  0.894 ms  0.870 ms  0.842 ms
 5  ae7.fra10-cr-antares.bb.gdinf.net (87.230.115.2)  3.486 ms  3.466 ms  3.432 ms
 6  ae2.fra1-cr-polaris.bb.gdinf.net (87.230.115.0)  3.675 ms  3.411 ms  3.363 ms
 7  ae1.pr02.muc2.tfbnw.net (185.1.208.198)  27.545 ms  27.524 ms  26.287 ms
 8  po202.asw01.muc2.tfbnw.net (129.134.75.52)  8.465 ms po202.asw03.muc2.tfbnw.net (129.134.75.88)  8.342 ms po202.asw04.muc2.t
 9  po211.psw03.muc2.tfbnw.net (129.134.75.61)  8.366 ms po213.psw03.muc2.tfbnw.net (129.134.74.221)  8.512 ms po242.psw01.muc2.
10  173.252.67.63 (173.252.67.63)  8.459 ms 173.252.67.113 (173.252.67.113)  8.331 ms 173.252.67.169 (173.252.67.169)  8.317 ms
11  edge-star-mini-shv-01-muc2.facebook.com (157.240.223.35)  8.237 ms  8.374 ms  8.390 ms
```

Figure 19: Traceroute to www.facebook.com

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)  0.032 ms  0.012 ms  0.010 ms
 2  ae3-u100.sxb1-cr-nunki.bb.gdinf.net (87.230.112.2)  0.384 ms  0.353 ms  0.365 ms
 3  ae1.sxb1-ibr-altair.bb.gdinf.net (87.230.112.14)  0.530 ms  0.499 ms  0.468 ms
 4  217.243.179.244 (217.243.179.244)  4.135 ms  4.210 ms  4.258 ms
 5  f-ed13-i.F.DE.NET.DTAG.DE (217.5.109.58)  4.692 ms f-ed13-i.F.DE.NET.DTAG.DE (217.0.203.14)  5.230 ms f-ed13-i.F.
 6  80.150.170.214 (80.150.170.214)  13.456 ms  13.404 ms  13.469 ms
 7  ae12.cs1.fra6.de.eth.zayo.com (64.125.26.172)  133.858 ms *  133.802 ms
 8  ae2.cs1.ams17.nl.eth.zayo.com (64.125.29.59)  134.548 ms  133.847 ms  133.918 ms
 9  * * *
10  * * *
11  * * *
12  ae5.cs1.lga5.us.eth.zayo.com (64.125.29.126)  133.583 ms  138.269 ms  138.237 ms
13  * * *
14  * * ae5.cs1.den5.us.eth.zayo.com (64.125.29.19)  133.501 ms
15  * * *
16  ae4.mpr1.las5.us.zip.zayo.com (64.125.26.241)  133.379 ms  133.394 ms  133.554 ms
17  ae7.mcs1.las2.us.zip.zayo.com (64.125.21.202)  136.701 ms  133.239 ms  133.604 ms
18  209.66.120.14.IDIA-249109-ZYO.zip.zayo.com (209.66.120.14)  137.557 ms  137.486 ms  137.567 ms
19  ddc-pep-c-123-int.uen.net (140.197.251.32)  145.011 ms  145.080 ms  144.821 ms
20  ddc-pep-b-129-int.uen.net (140.197.253.97)  144.900 ms  144.809 ms  145.272 ms
21  ebc-pep-b-179-int.uen.net (140.197.252.76)  145.141 ms  145.119 ms  145.091 ms
22  ebc-pep-a-178-int.uen.net (140.197.252.84)  145.298 ms  145.262 ms  145.246 ms
23  * * *
24  199.104.93.22 (199.104.93.22)  144.815 ms  144.444 ms  144.867 ms
25  199.104.93.33 (199.104.93.33)  146.277 ms  146.141 ms  145.749 ms
26  155.99.130.67 (155.99.130.67)  145.812 ms  145.891 ms 155.99.130.65 (155.99.130.65)  145.697 ms
27  155.99.130.107 (155.99.130.107)  145.264 ms 155.99.130.103 (155.99.130.103)  146.139 ms  146.426 ms
28  * * *
29  * * *
30  * * *
```

Figure 20: Traceroute to www.utah.edu

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)  0.031 ms  0.012 ms  0.011 ms
 2  ae3-u100.sxb1-cr-nunki.bb.gdinf.net (87.230.112.2)  0.361 ms *  0.305 ms
 3  ae1.sxb1-ibr-altair.bb.gdinf.net (87.230.112.14)  0.596 ms  0.562 ms  0.533 ms
 4  ffm-b16-link.ip.twelve99.net (62.115.144.8)  2.898 ms  2.872 ms  2.872 ms
 5  * * *
 6  ffm-b11-link.ip.twelve99.net (62.115.124.117)  3.383 ms ffm-b11-link.ip.twelve99.net (62.115.124.119)  3.343 ms  3.357 ms
 7  * * *
 8  be2845.ccr41.fra03.atlas.cogentco.com (154.54.56.189)  4.536 ms  3.519 ms  4.893 ms
 9  * be2813.ccr41.ams03.atlas.cogentco.com (130.117.0.121)  10.542 ms be2814.ccr42.ams03.atlas.cogentco.com (130.117.0.141)
10  be3457.ccr21.ams04.atlas.cogentco.com (130.117.1.10)  11.027 ms  10.732 ms be3458.ccr21.ams04.atlas.cogentco.com (154.54.
11  * * *
12  ae0-306-mtz1-ir1.net.tenet.ac.za (155.232.1.86)  185.232 ms  185.099 ms  185.067 ms
13  et-1-1-1-0-isd1-pe1.net.tenet.ac.za (155.232.1.153)  194.062 ms  194.207 ms  194.006 ms
14  et-1-1-4-0-cpt3-pe1.net.tenet.ac.za (155.232.1.148)  210.450 ms  210.418 ms  210.390 ms
15  et-0-0-1-0-cpt7-pe1.net.tenet.ac.za (155.232.64.70)  209.616 ms  209.661 ms  209.625 ms
16  154.114.124.1 (154.114.124.1)  210.047 ms  210.082 ms  210.076 ms
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Figure 21: Traceroute to www.uct.ac.za

3.4 AS-IP Lookup

Autonomous System Lookup (AS / ASN / IP) | HackerTarget.com

IP Address	AS #	AS Name	AS Range
192.168.18.60	None		None
192.168.59.1	None		None
192.168.27.93	None		None
192.168.27.111	None		None
122.185.39.5	9498	BBIL-AP BHARTI Airtel Ltd., IN	122.185.0.0/18
74.125.244.205	15169	GOOGLE	74.125.0.0/16
72.14.239.59	15169	GOOGLE	72.14.192.0/18
74.125.242.129	15169	GOOGLE	74.125.0.0/16
142.251.60.187	15169	GOOGLE	142.251.60.0/24
142.250.205.228	15169	GOOGLE	142.250.205.0/24

Figure 22: ASN Lookup 1

When my device made a traceroute to google.com, the first hops were within private networks (probably within my local network or my Internet Service Provider's internal network). Then, it reached an IP (122.185.39.5) managed by BHARTI Airtel, which might be our Internet Service

Provider or an intermediate network provider. Finally, the remaining hops are all within Google's network infrastructure, ultimately reaching the destination (google.com).

Autonomous System Lookup (AS / ASN / IP) | HackerTarget.com

IP Address	AS #	AS Name	AS Range
192.168.18.60	None		None
192.168.27.93	None		None
192.168.27.109	None		None
122.185.39.1	9498	BBIL-AP BHARTI Airtel Ltd., IN	122.185.0.0/18
182.79.201.122	9498	BBIL-AP BHARTI Airtel Ltd., IN	182.79.201.0/24
154.54.72.109	174	COGENT-174	154.48.0.0/12
154.54.56.129	174	COGENT-174	154.48.0.0/12
154.54.82.34	174	COGENT-174	154.48.0.0/12
66.28.4.237	174	COGENT-174	66.28.0.0/16
154.54.26.129	174	COGENT-174	154.48.0.0/12
154.54.42.165	174	COGENT-174	154.48.0.0/12
154.54.5.89	174	COGENT-174	154.48.0.0/12
154.54.41.145	174	COGENT-174	154.48.0.0/12
154.54.41.118	174	COGENT-174	154.48.0.0/12
38.142.233.58	174	COGENT-174	38.0.0.0/8
140.197.253.23	210	WEST-NET-WEST	140.197.0.0/16
140.197.253.139	210	WEST-NET-WEST	140.197.0.0/16
199.104.23.29	32922	ATCCOMMICATIONS	199.104.23.0/24
155.99.130.101	17055	UTAH	155.99.0.0/16
155.98.186.21	17055	UTAH	155.98.0.0/16

Figure 23: ASN Lookup 2

The private IP addresses like 192.168.18.60, 192.168.27.93, and 192.168.27.109 couldn't be associated with any specific ASN or organization, which is expected as they belong to private address ranges not meant for public routing. IP addresses like 122.185.39.1 and 182.79.201.122 are associated with "BBIL-AP BHARTI Airtel Ltd." with the Autonomous System Number 9498. This suggests that these hops are within the network infrastructure of Airtel, an ISP. IP addresses like 154.54.72.109, 154.54.56.129, and others are associated with "COGENT-174" with the ASN 174. This indicates that these hops are part of the COGENT-174 network, which is a large global Tier 1 Internet service provider. Similarly, other IP addresses are associated with different ASNs and organizations, such as "WEST-NET-WEST," "ATCCOMMICATIONS," and "UTAH," indicating the presence of these networks in the path of the traced route.

3.5 Analysis and Interpretation

a.

Destination	www.iitd.ac.in	Google	Facebook	www.utah.edu	www.uct.ac.za
Src-Laptop	17	12	9	29	13(last reachable)
Src-Germany	14(last reachable)	11	11	27(last reachable)	16(last reachable)
Src-US	11(last reachable)	13	13	30	14(last reachable)

Geographical Proximity and Number of Hops:

- Src-Laptop: Google (12) and Facebook (9) require fewer hops than www.utah.edu (29). This suggests that geographical distance might affect the number of hops, as www.utah.edu is geographically further away from the laptop's location.
- Src-Germany: Google (11) and Facebook (11) again have fewer hops compared to www.utah.edu (27). It's worth noting that Google and Facebook have the same number of hops from Germany, suggesting the presence of possibly similar or optimized routing.
- Src-US: Hops to Google (13) and Facebook (13) are nearly similar but less than to www.utah.edu (30).

Geographical proximity does seem to play a role in the number of hops, but it's not the only factor. Google and Facebook, for example, seem to require fewer hops than other sites from different sources, which can be attributed to their extensive global network infrastructure, CDNs, and optimized routing mechanisms.

b.

Destination	www.iitd.ac.in	Google	Facebook	www.utah.edu	www.uct.ac.za
Src-Laptop	54.33	41.67 ms	59 ms	305.6 ms	448.33 ms(last reachable)
Src-Germany	148.78 ms(last reachable)	4.08 ms	8.33 ms	146.28(last reachable)	210(last reachable)
Src-US	227.87 ms(last reachable)	4.85 ms	4.23 ms	64.45 ms	199.87 ms(last reachable)

Latency and Number of Hops:

- From Src-Laptop, Google has 12 hops and 41.67 ms, while Facebook has 9 hops and 59 ms. This shows that fewer hops don't always mean lesser latency.
- From Src-Germany, Google (4.08 ms) and Facebook (8.33 ms) have similar latencies and hops. The interesting observation here is the drastically low latencies for Google and Facebook compared to other destinations, suggesting that they might have data centers or servers very close to Germany.
- From Src-US, Google (4.85 ms) and Facebook (4.23 ms) again have very low latencies, suggesting local data centers within the US.

In several cases, more hops equate to more latency. However, as seen from the data, this isn't a strict correlation. While every hop introduces some delay (router processing, queuing, transmission time), other factors heavily influence the latency:

- Network congestion: A network path with few hops but heavy traffic can lead to higher latency.
- Router processing times: Some routers may take longer to process and forward packets.
- Server response time: How quickly the destination server responds to requests.
- Transmission mediums: Data travel faster in optical fibers than other mediums.

Google and Facebook: Across all sources, Google and Facebook generally require fewer or similar hops, indicating their massive infrastructure optimization and global presence. Their vast networks, Content Delivery Networks (CDNs), and multiple data centers worldwide, along with peering agreements with ISPs globally, help optimize routes to reach them efficiently.

c.
Observations:
Google:
Destination server when Source is US : 142.251.40.132,
Destination server when Source is Germany: 142.250.186.100,
Destination server when source is India: 142.250.194.228.

Facebook:
Destination server when Source is US : 31.13.71.36,
Destination server when Source is Germany: 157.240.223.35,
Destination server when source is India: 157.240.23.35.

Other:
Destination server of iitd was 103.27.9.24 irrespective of source,
Destination server of utah was 155.98.186.21 irrespective of source,
Destination server of uct was 137.158.159.192 irrespective of source.

Interpretation:

The iitd, uct, utah web-servers are resolved to the same IP address regardless of the source location because they likely have a single global IP address associated with them. This is often the case with educational institutions and organizations that manage their own network infrastructure.

On the other hand, the destination web-servers for Google and Facebook are resolved to different IP addresses depending on the source location. This is because large content providers like Google and Facebook typically have distributed data centers located in different parts of the world. When you access their services, your request is often directed to a server that is geographically closer to you. This helps to reduce latency and improve the performance of the service.
The practice of having multiple IP addresses for the same domain, depending on the source location, is known as content delivery .

d.

```
PS C:\Users\disha> tracert 142.250.194.228

Tracing route to del12s08-in-f4.1e100.net [142.250.194.228]
over a maximum of 30 hops:

  1    23 ms     1 ms     1 ms  192.168.18.60
  2   215 ms    45 ms    22 ms  192.168.59.1
  3    97 ms    41 ms    32 ms  192.168.27.93
  4    32 ms    19 ms    70 ms  192.168.27.109
  5     *       30 ms    49 ms  nsg-corporate-1.39.185.122.airtel.in [122.185.39.1]
  6    40 ms    55 ms    59 ms  72.14.217.194
  7    64 ms    47 ms    31 ms  108.170.237.85
  8    33 ms    64 ms    23 ms  142.251.52.217
  9    91 ms    29 ms     *     del12s08-in-f4.1e100.net [142.250.194.228]
 10   253 ms    31 ms    41 ms  del12s08-in-f4.1e100.net [142.250.194.228]

Trace complete.
PS C:\Users\disha>
```

Figure 24: Traceroute from Laptop to Google India

```
PS C:\Users\disha> tracert 142.251.40.132

Tracing route to lga25s80-in-f4.1e100.net [142.251.40.132]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  192.168.18.60
  2    73 ms    19 ms    24 ms  192.168.59.1
  3   144 ms   142 ms    40 ms  192.168.27.81
  4    48 ms    33 ms    46 ms  192.168.27.107
  5   165 ms   123 ms    51 ms  nsg-corporate-5.39.185.122.airtel.in [122.185.39.5]
  6   148 ms   145 ms    34 ms  74.125.51.184
  7   139 ms    55 ms    32 ms  142.251.66.173
  8    58 ms    20 ms    62 ms  74.125.244.205
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16   419 ms   302 ms   341 ms  142.251.69.166
 17   382 ms   334 ms   658 ms  108.170.248.1
 18   417 ms   303 ms   354 ms  216.239.43.155
 19   332 ms   319 ms   339 ms  lga25s80-in-f4.1e100.net [142.251.40.132]

Trace complete.
PS C:\Users\disha>
```

Figure 25: Traceroute from Laptop to Google US

```
PS C:\Users\disha> tracert 142.250.186.100

Tracing route to fra24s06-in-f4.1e100.net [142.250.186.100]
over a maximum of 30 hops:

  1     2 ms     2 ms     1 ms  192.168.18.60
  2    49 ms    24 ms    60 ms  192.168.59.1
  3    49 ms    38 ms    27 ms  192.168.27.69
  4    35 ms    22 ms    32 ms  192.168.27.111
  5    68 ms    30 ms    52 ms  nsg-corporate-5.39.185.122.airtel.in [122.185.39.5]
  6    34 ms    25 ms    21 ms  74.125.51.184
  7    23 ms    48 ms    26 ms  142.251.66.171
  8    53 ms    43 ms    28 ms  108.170.251.124
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21   400 ms   382 ms   452 ms  142.251.227.122
 22   417 ms   392 ms   408 ms  108.170.252.1
 23   379 ms   439 ms   636 ms  142.250.214.193
 24   543 ms   378 ms   375 ms  fra24s06-in-f4.1e100.net [142.250.186.100]

Trace complete.
PS C:\Users\disha>
```

Figure 26: Traceroute from Laptop to Google Germany

```
PS C:\Users\disha> tracert 157.240.23.35

Tracing route to edge-star-mini-shv-01-maa2.facebook.com [157.240.23.35]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  192.168.18.60
  2    62 ms    57 ms   113 ms  192.168.59.1
  3   166 ms    30 ms   122 ms  192.168.27.81
  4   152 ms    19 ms    53 ms  192.168.27.107
  5    49 ms    41 ms    24 ms  nsg-corporate-5.39.185.122.airtel.in [122.185.39.5]
  6     *        *        *     Request timed out.
  7    65 ms    54 ms    87 ms  ae20.pr02.maa2.tfbnw.net [157.240.84.206]
  8   104 ms    55 ms    79 ms  po102.psw03.maa2.tfbnw.net [129.134.34.155]
  9    91 ms    57 ms    72 ms  173.252.67.111
 10   118 ms    82 ms    56 ms  edge-star-mini-shv-01-maa2.facebook.com [157.240.23.35]

Trace complete.
PS C:\Users\disha>
```

Figure 27: Traceroute from Laptop to Facebook India

```
PS C:\Users\disha> tracert 31.13.71.36

Tracing route to edge-star-mini-shv-01-lga3.facebook.com [31.13.71.36]over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  192.168.18.60
  2    60 ms    35 ms    50 ms  192.168.59.1
  3    67 ms    52 ms    20 ms  192.168.27.93
  4    57 ms    26 ms   147 ms  192.168.27.109
  5   128 ms    72 ms    40 ms  nsg-corporate-1.39.185.122.airtel.in [122.185.39.1]
  6   329 ms   447 ms   303 ms  182.79.245.6
  7   267 ms   321 ms   243 ms  de-cix.nyc.fb.com [206.82.104.136]
  8   349 ms   257 ms   340 ms  po201.asw01.lga1.tfbnw.net [157.240.103.100]
  9   353 ms   246 ms   266 ms  po207.psw04.lga3.tfbnw.net [157.240.104.43]
 10   397 ms   314 ms   297 ms  173.252.67.181
 11   424 ms   316 ms   376 ms  edge-star-mini-shv-01-lga3.facebook.com [31.13.71.36]

Trace complete.
PS C:\Users\disha>
```

Figure 28: Traceroute from Laptop to Facebook US

```
PS C:\Users\disha> tracert 157.240.223.35

Tracing route to edge-star-mini-shv-01-muc2.facebook.com [157.240.223.35]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.18.60
  2    45 ms    17 ms    18 ms  192.168.59.1
  3   258 ms    31 ms    38 ms  192.168.27.93
  4   153 ms    70 ms    24 ms  192.168.27.111
  5    63 ms   141 ms    42 ms  nsg-corporate-5.39.185.122.airtel.in [122.185.39.5]
  6   167 ms   174 ms     *     116.119.57.80
  7   263 ms   162 ms   140 ms  mei-b5-link.ip.twelve99.net [62.115.42.118]
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10   172 ms   185 ms   172 ms  mcn-b6-link.ip.twelve99.net [62.115.126.185]
 11   219 ms   179 ms   207 ms  facebook-ic-379905.ip.twelve99-cust.net [62.115.11.165]
 12   183 ms   168 ms   186 ms  po201.asw02.muc2.tfbnw.net [129.134.75.50]
 13   179 ms   177 ms   160 ms  po222.psw02.muc2.tfbnw.net [129.134.75.59]
 14   239 ms   188 ms   174 ms  173.252.67.73
 15   191 ms   174 ms   234 ms  edge-star-mini-shv-01-muc2.facebook.com [157.240.223.35]

Trace complete.
PS C:\Users\disha>
```

Figure 29: Traceroute from Laptop to Facebook Germany

It's clear that the paths can vary depending on the destination IP address, even for the same web-server. In most cases, the paths with more hops tend to have higher latency, although this is not always a strict rule.

For Google:
The path with the shortest number of hops is from India, with 10 hops and a latency of 108ms. The path with the longest number of hops is from Germany, with 24 hops and a latency of 432ms.

For Facebook:
The paths from both India and the US have the same number of hops (10), but the latency is slightly lower from India (85ms) compared to the US (372ms). The path from Germany has 15 hops and a latency of 199ms.

In general, the paths with more hops are likely to be longer in terms of network distance and might involve more intermediate routers and network nodes. This can result in higher latency due to the increased number of network hops and potential for congestion or delays at various points along the route

e.

core2.tor1.he.net> traceroute 142.251.46.228 source 216.218.252.7

Target	142.251.46.228
Hop Start	1
Hop End	30

Hop	Packet 1	Packet 2	Packet 3	Hostname
1	20.934 ms	20.914 ms	21.932 ms	**as15169.toronto.megaport.com** (206.53.203.9)
2	21.948 ms	21.968 ms	*	**74.125.244.151** (74.125.244.151)
7	60.431 ms	59.538 ms	59.507 ms	**142.250.234.138** (142.250.234.138)
8	59.961 ms	59.971 ms	59.977 ms	**108.170.243.1** (108.170.243.1)
9	58.974 ms	58.983 ms	58.995 ms	**142.251.228.83** (142.251.228.83)
10	59.235 ms	59.560 ms	59.571 ms	**sfo03s27-in-f4.1e100.net** (142.251.46.228)

Entry cached for another 60 seconds. 2023-08-12 11:31:09 UTC

Figure 30: Traceroute from Canada (Toronto) to www.google.com

core2.tor1.he.net> traceroute 157.240.14.35 source 216.218.252.7

Target	157.240.14.35
Hop Start	1
Hop End	30

Hop	Packet 1	Packet 2	Packet 3	Hostname
1	21.131 ms	*	*	**100ge0-76.core3.nyc4.he.net** (184.104.196.177)
2	33.992 ms	34.079 ms	34.105 ms	**nyk-b1-link.ip.twelve99.net** (80.239.161.117)
3	34.527 ms	34.557 ms	34.567 ms	**nyk-bb1-link.ip.twelve99.net** (62.115.135.130)
4	53.829 ms	53.853 ms	53.873 ms	**rest-bb1-link.ip.twelve99.net** (62.115.141.244)
6	71.462 ms	52.599 ms	52.499 ms	**facebook-ic-337758.ip.twelve99-cust.net** (213.248.91.131)
7	45.050 ms	45.078 ms	45.291 ms	**po201.asw02.mia1.tfbnw.net** (129.134.64.142)
8	45.613 ms	45.725 ms	42.665 ms	**psw04.mia3.tfbnw.net** (157.240.58.176)
9	42.650 ms	42.942 ms	42.551 ms	**157.240.39.213** (157.240.39.213)
10	42.710 ms	42.693 ms	42.745 ms	**edge-star-mini-shv-02-mia3.facebook.com** (157.240.14.35)

Entry cached for another 59 seconds. 2023-08-12 11:27:37 UTC

Figure 31: Traceroute from Canada (Toronto) to www.facebook.com

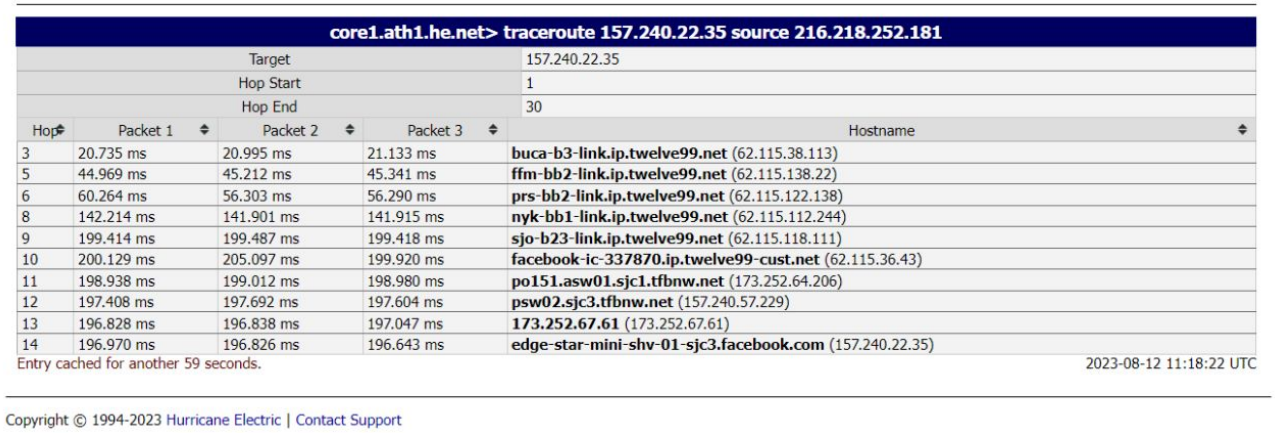
core1.ath1.he.net> traceroute 142.251.46.228 source 216.218.252.181

Target	142.251.46.228
Hop Start	1
Hop End	30

Hop	Packet 1	Packet 2	Packet 3	Hostname
1	12.392 ms	*	*	**100ge0-75.core3.sof1.he.net** (184.105.64.169)
2	13.175 ms	13.442 ms	13.712 ms	**185.1.226.90** (185.1.226.90)
3	20.274 ms	20.288 ms	20.616 ms	**142.251.92.67** (142.251.92.67)
4	44.580 ms	44.620 ms	44.731 ms	**142.251.243.252** (142.251.243.252)
5	49.982 ms	49.999 ms	50.033 ms	**142.251.237.184** (142.251.237.184)
6	55.252 ms	50.472 ms	50.442 ms	**142.251.232.219** (142.251.232.219)
7	116.748 ms	116.770 ms	116.741 ms	**142.251.69.180** (142.251.69.180)
8	132.533 ms	132.520 ms	131.581 ms	**142.251.69.179** (142.251.69.179)
9	150.756 ms	152.656 ms	151.428 ms	**192.178.72.194** (192.178.72.194)
10	178.834 ms	178.866 ms	178.171 ms	**192.178.74.245** (192.178.74.245)
11	178.051 ms	178.114 ms	177.962 ms	**142.251.51.41** (142.251.51.41)
12	178.561 ms	178.573 ms	178.160 ms	**74.125.253.148** (74.125.253.148)
13	179.467 ms	179.767 ms	179.170 ms	**108.170.243.1** (108.170.243.1)
14	177.283 ms	177.464 ms	177.272 ms	**142.251.228.83** (142.251.228.83)
15	177.337 ms	177.263 ms	177.268 ms	**sfo03s27-in-f4.1e100.net** (142.251.46.228)

Entry cached for another 53 seconds. 2023-08-12 11:12:31 UTC

Figure 32: Traceroute from Greece (Koropi) to www.google.com



core1.ath1.he.net> traceroute 157.240.22.35 source 216.218.252.181

Target	157.240.22.35
Hop Start	1
Hop End	30

Hop	Packet 1	Packet 2	Packet 3	Hostname
3	20.735 ms	20.995 ms	21.133 ms	**buca-b3-link.ip.twelve99.net** (62.115.38.113)
5	44.969 ms	45.212 ms	45.341 ms	**ffm-bb2-link.ip.twelve99.net** (62.115.138.22)
6	60.264 ms	56.303 ms	56.290 ms	**prs-bb2-link.ip.twelve99.net** (62.115.122.138)
8	142.214 ms	141.901 ms	141.915 ms	**nyk-bb1-link.ip.twelve99.net** (62.115.112.244)
9	199.414 ms	199.487 ms	199.418 ms	**sjo-b23-link.ip.twelve99.net** (62.115.118.111)
10	200.129 ms	205.097 ms	199.920 ms	**facebook-ic-337870.ip.twelve99-cust.net** (62.115.36.43)
11	198.938 ms	199.012 ms	198.980 ms	**po151.asw01.sjc1.tfbnw.net** (173.252.64.206)
12	197.408 ms	197.692 ms	197.604 ms	**psw02.sjc3.tfbnw.net** (157.240.57.229)
13	196.828 ms	196.838 ms	197.047 ms	**173.252.67.61** (173.252.67.61)
14	196.970 ms	196.826 ms	196.643 ms	**edge-star-mini-shv-01-sjc3.facebook.com** (157.240.22.35)

Entry cached for another 59 seconds. 2023-08-12 11:18:22 UTC

Figure 33: Traceroute from Greece (Koropi) to www.facebook.com

core1.nbo1.he.net> traceroute 142.251.46.228 source 216.218.252.183 numeric

Target	142.251.46.228
Hop Start	1
Hop End	30

Hop	Packet 1	Packet 2	Packet 3	Hostname
1	59 ms	59 ms	61 ms	**port-channel6.core2.jnb1.he.net** (184.104.198.45)
2	60 ms	60 ms	60 ms	**196-60-9-113.ixp.joburg** (196.60.9.113)
3	60 ms	63 ms	60 ms	**74.125.245.209** (74.125.245.209)
4	59 ms	59 ms	66 ms	**74.125.245.210** (74.125.245.210)
5	180 ms	179 ms	*	**192.178.46.189** (192.178.46.189)
6	206 ms	196 ms	*	**216.239.35.201** (216.239.35.201)
7	265 ms	*	265 ms	**142.251.49.44** (142.251.49.44)
8	263 ms	*	267 ms	**142.251.49.27** (142.251.49.27)
9	280 ms	*	278 ms	**142.251.65.5** (142.251.65.5)
10	346 ms	302 ms	303 ms	**192.178.72.206** (192.178.72.206)
11	323 ms	327 ms	323 ms	**192.178.74.247** (192.178.74.247)
12	323 ms	324 ms	323 ms	**142.250.237.173** (142.250.237.173)
13	322 ms	322 ms	322 ms	**142.250.234.138** (142.250.234.138)
14	324 ms	325 ms	325 ms	**108.170.243.1** (108.170.243.1)
15	323 ms	333 ms	323 ms	**142.251.228.83** (142.251.228.83)
16	323 ms	323 ms	323 ms	**sfo03s27-in-f4.1e100.net** (142.251.46.228)

Entry cached for another 60 seconds. 2023-08-13 15:03:28 UTC

Figure 34: Traceroute from Kenya to www.google.com

core1.nbo1.he.net> traceroute 157.240.22.35 source 216.218.252.183 numeric

Target	157.240.22.35
Hop Start	1
Hop End	30

Hop	Packet 1	Packet 2	Packet 3	Hostname
1	149 ms	148 ms	*	**10ge0-7.core3.mrs1.he.net** (184.104.194.77)
2	*	*	*	-
3	159 ms	158 ms	159 ms	**mei-b5-link.ip.twelve99.net** (62.115.165.37)
4	175 ms	174 ms	175 ms	**prs-bb2-link.ip.twelve99.net** (62.115.124.56)
5	*	*	*	-
6	251 ms	251 ms	250 ms	**nyk-bb1-link.ip.twelve99.net** (62.115.112.244)
7	302 ms	301 ms	301 ms	**sjo-b23-link.ip.twelve99.net** (62.115.118.111)
8	*	315 ms	304 ms	**facebook-ic-337870.ip.twelve99-cust.net** (62.115.36.43)
9	302 ms	304 ms	300 ms	**po151.asw04.sjc1.tfbnw.net** (157.240.32.140)
10	306 ms	306 ms	316 ms	**psw03.sjc3.tfbnw.net** (157.240.57.227)
11	314 ms	308 ms	304 ms	**173.252.67.133** (173.252.67.133)
12	299 ms	299 ms	299 ms	**edge-star-mini-shv-01-sjc3.facebook.com** (157.240.22.35)

Entry cached for another 60 seconds. 2023-08-13 15:05:07 UTC

Figure 35: Traceroute from Kenya to www.facebook.com

Google

Country	Hops	Latency
India	9	41 ms
Germany	11	4 ms
US	13	4 ms
Koropi(Greece)	15	177 ms
Toronto(Canada)	10	59 ms
Kenya	16	323 ms

Facebook

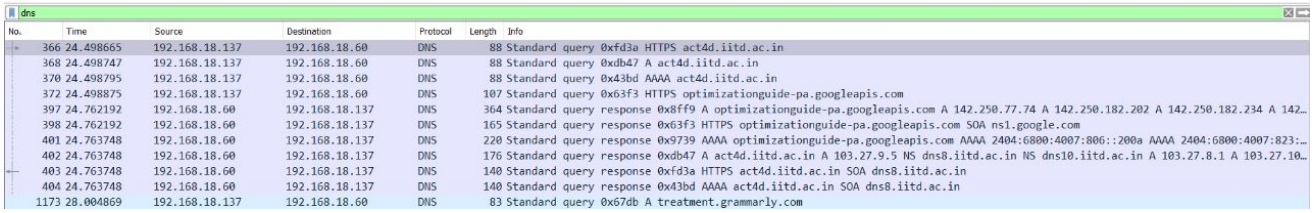
Country	Hops	Latency
India	9	59 ms
Germany	11	8 ms
US	13	4 ms
Koropi(Greece)	14	196 ms
Toronto(Canada)	10	42 ms
Kenya	12	299 ms

From these observations, it's difficult to definitively conclude whether any countries lack direct local ISP peering with Google and Facebook. However, the higher latency and larger number of hops observed in certain countries might suggest that they might not have as optimized routing paths or as direct peering agreements with these services as some other countries do.

Based on the higher latency and larger number of hops observed in traceroutes from Koropi, Greece and Nairobi(Kenya) compared to other countries like India, the US, and Germany, it is possible that Greece, Kenya might not have direct local ISP peering with Google and Facebook. The longer and more convoluted path the traceroute takes could indicate that the routing is not as optimized as in other regions where the latency is lower and the number of hops is fewer.

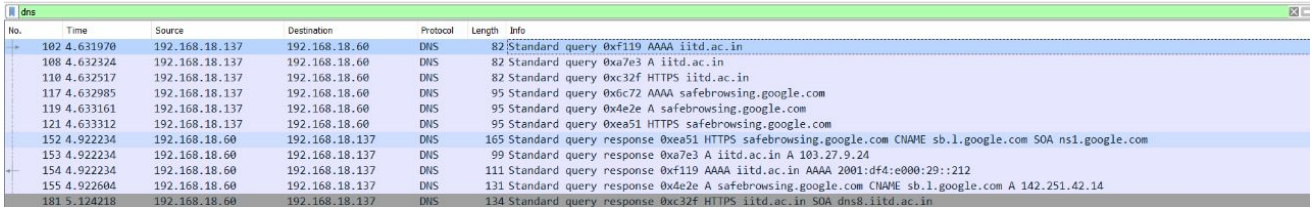
4 Packet Analysis

4.1 DNS Filter



No.	Time	Source	Destination	Protocol	Length	Info
366	24.498665	192.168.18.137	192.168.18.60	DNS	88	Standard query 0xfd3a HTTPS act4d.iitd.ac.in
368	24.498747	192.168.18.137	192.168.18.60	DNS	88	Standard query 0xdb47 A act4d.iitd.ac.in
370	24.498795	192.168.18.137	192.168.18.60	DNS	88	Standard query 0x43bd AAAA act4d.iitd.ac.in
372	24.498875	192.168.18.137	192.168.18.60	DNS	107	Standard query 0x63f3 HTTPS optimizationguide-pa.googleapis.com
397	24.762192	192.168.18.60	192.168.18.137	DNS	364	Standard query response 0x8ff9 A optimizationguide-pa.googleapis.com A 142.250.77.74 A 142.250.182.202 A 142.250.182.234 A 142…
398	24.762192	192.168.18.60	192.168.18.137	DNS	165	Standard query response 0x63f3 HTTPS optimizationguide-pa.googleapis.com SOA ns1.google.com
401	24.763748	192.168.18.60	192.168.18.137	DNS	220	Standard query response 0x9739 AAAA optimizationguide-pa.googleapis.com AAAA 2404:6800:4007:806::200a AAAA 2404:6800:4007:823:…
402	24.763748	192.168.18.60	192.168.18.137	DNS	176	Standard query response 0xdb47 A act4d.iitd.ac.in A 103.27.9.5 NS dns8.iitd.ac.in NS dns10.iitd.ac.in A 103.27.8.1 A 103.27.10…
403	24.763748	192.168.18.60	192.168.18.137	DNS	140	Standard query response 0xfd3a HTTPS act4d.iitd.ac.in SOA dns8.iitd.ac.in
404	24.763748	192.168.18.60	192.168.18.137	DNS	140	Standard query response 0x43bd AAAA act4d.iitd.ac.in SOA dns8.iitd.ac.in
1173	28.004869	192.168.18.137	192.168.18.60	DNS	83	Standard query 0x67db A treatment.grammarly.com

Figure 36: Wireshark DNS Filter for www.act4d.iitd.ac.in



No.	Time	Source	Destination	Protocol	Length	Info
102	4.631970	192.168.18.137	192.168.18.60	DNS	82	Standard query 0xf119 AAAA iitd.ac.in
108	4.632324	192.168.18.137	192.168.18.60	DNS	82	Standard query 0xa7e3 A iitd.ac.in
110	4.632517	192.168.18.137	192.168.18.60	DNS	82	Standard query 0xc32f HTTPS iitd.ac.in
117	4.632985	192.168.18.137	192.168.18.60	DNS	95	Standard query 0x6c72 AAAA safebrowsing.google.com
119	4.633161	192.168.18.137	192.168.18.60	DNS	95	Standard query 0x4e2e A safebrowsing.google.com
121	4.633312	192.168.18.137	192.168.18.60	DNS	95	Standard query 0xea51 HTTPS safebrowsing.google.com
152	4.922234	192.168.18.60	192.168.18.137	DNS	165	Standard query response 0xea51 HTTPS safebrowsing.google.com CNAME sb.l.google.com SOA ns1.google.com
153	4.922234	192.168.18.60	192.168.18.137	DNS	99	Standard query response 0xa7e3 A iitd.ac.in A 103.27.9.24
154	4.922234	192.168.18.60	192.168.18.137	DNS	111	Standard query response 0xf119 AAAA iitd.ac.in AAAA 2001:df4:e000:29::212
155	4.922604	192.168.18.60	192.168.18.137	DNS	131	Standard query response 0x4e2e A safebrowsing.google.com CNAME sb.l.google.com A 142.251.42.14
181	5.124218	192.168.18.60	192.168.18.137	DNS	134	Standard query response 0xc32f HTTPS iitd.ac.in SOA dns8.iitd.ac.in

Figure 37: Wireshark DNS Filter for www.iitd.ac.in

The website "act4.iitd" was analyzed using Wireshark to monitor the sent and received DNS queries. A total of three request/response pairs were observed, as depicted in the provided screenshot.

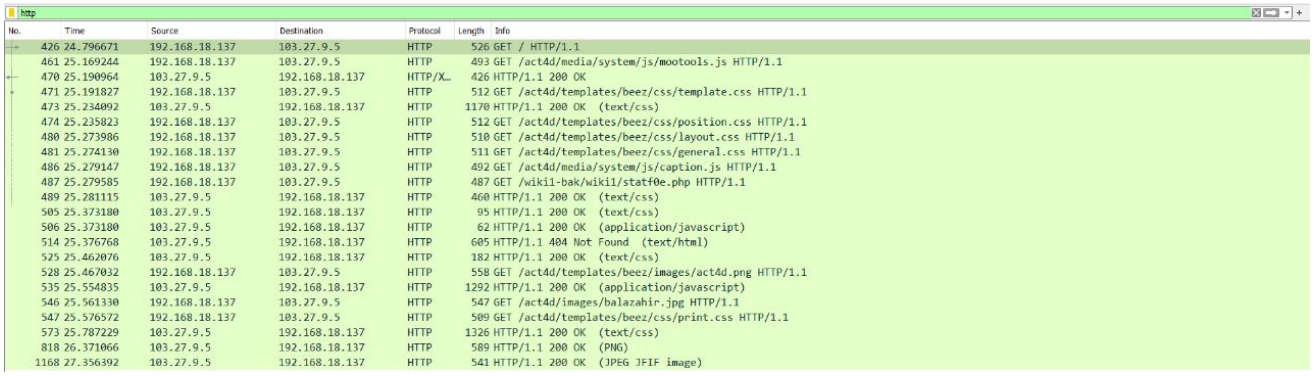
Query type	**Dispatched timestamp**	**Recieved timestamp**	**Time elapsed**
HTTPS	24.49866 ms	24.76374 ms	0.26508 ms
A	24.49874 ms	24.76374 ms	0.265 ms
AAAA	24.49879 ms	24.76374 ms	0.26485 ms

The average query-response time is 0.26497ms.

Query type	**Dispatched timestamp**	**Recieved timestamp**	**Time elapsed**
HTTPS	4.63251 ms	5.12421 ms	0.4917 ms
A	4.63232 ms	4.92223 ms	0.2899 ms
AAAA	4.63197 ms	4.92223 ms	0.29026 ms

The average query-response time is 0.35728 ms.

4.2 HTTP Filter



No.	Time	Source	Destination	Protocol	Length	Info
426	24.796671	192.168.18.137	103.27.9.5	HTTP	526	GET / HTTP/1.1
461	25.169244	192.168.18.137	103.27.9.5	HTTP	493	GET /act4d/media/system/js/mootools.js HTTP/1.1
470	25.190964	103.27.9.5	192.168.18.137	HTTP/X…	426	HTTP/1.1 200 OK
471	25.191827	192.168.18.137	103.27.9.5	HTTP	512	GET /act4d/templates/beez/css/template.css HTTP/1.1
473	25.234092	103.27.9.5	192.168.18.137	HTTP	1170	HTTP/1.1 200 OK (text/css)
474	25.235823	192.168.18.137	103.27.9.5	HTTP	512	GET /act4d/templates/beez/css/position.css HTTP/1.1
480	25.273986	192.168.18.137	103.27.9.5	HTTP	510	GET /act4d/templates/beez/css/layout.css HTTP/1.1
481	25.274130	192.168.18.137	103.27.9.5	HTTP	511	GET /act4d/templates/beez/css/general.css HTTP/1.1
486	25.279147	192.168.18.137	103.27.9.5	HTTP	492	GET /act4d/media/system/js/caption.js HTTP/1.1
487	25.279585	192.168.18.137	103.27.9.5	HTTP	487	GET /wiki1-bak/wiki1/statf0e.php HTTP/1.1
489	25.281115	103.27.9.5	192.168.18.137	HTTP	460	HTTP/1.1 200 OK (text/css)
505	25.373180	103.27.9.5	192.168.18.137	HTTP	95	HTTP/1.1 200 OK (text/css)
506	25.373180	103.27.9.5	192.168.18.137	HTTP	62	HTTP/1.1 200 OK (application/javascript)
514	25.376768	103.27.9.5	192.168.18.137	HTTP	605	HTTP/1.1 404 Not Found (text/html)
525	25.462076	103.27.9.5	192.168.18.137	HTTP	182	HTTP/1.1 200 OK (text/css)
528	25.467032	192.168.18.137	103.27.9.5	HTTP	558	GET /act4d/templates/beez/images/act4d.png HTTP/1.1
535	25.554835	103.27.9.5	192.168.18.137	HTTP	1292	HTTP/1.1 200 OK (application/javascript)
546	25.561330	192.168.18.137	103.27.9.5	HTTP	547	GET /act4d/images/balazahir.jpg HTTP/1.1
547	25.576572	192.168.18.137	103.27.9.5	HTTP	509	GET /act4d/templates/beez/css/print.css HTTP/1.1
573	25.787229	103.27.9.5	192.168.18.137	HTTP	1326	HTTP/1.1 200 OK (text/css)
818	26.371066	103.27.9.5	192.168.18.137	HTTP	589	HTTP/1.1 200 OK (PNG)
1168	27.356392	103.27.9.5	192.168.18.137	HTTP	541	HTTP/1.1 200 OK (JPEG JFIF image)

Figure 38: Wireshark HTTP Filter for www.act4d.iitd.ac.in

From the provided snapshot, it's evident that around 11 distinct requests were initiated, encompassing various resource types such as CSS, HTML, JPG images, and text files. This highlights the multifaceted nature of webpages, which are intricately crafted using a combination of HTML, CSS, JavaScript, among other resources. To effectively render these intricate pages, browsers execute separate HTTP requests for each individual resource. This concurrent retrieval mechanism optimizes loading speeds, ensuring a seamless and efficient user experience.

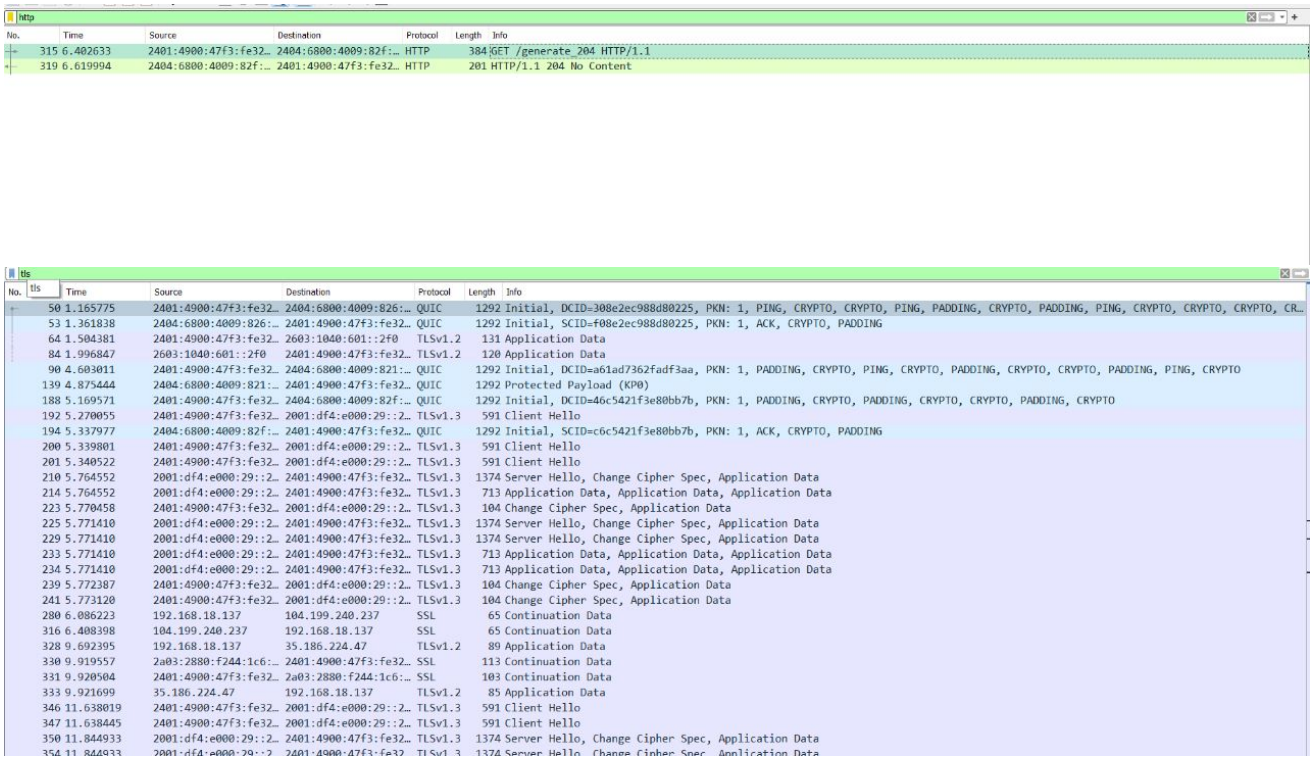
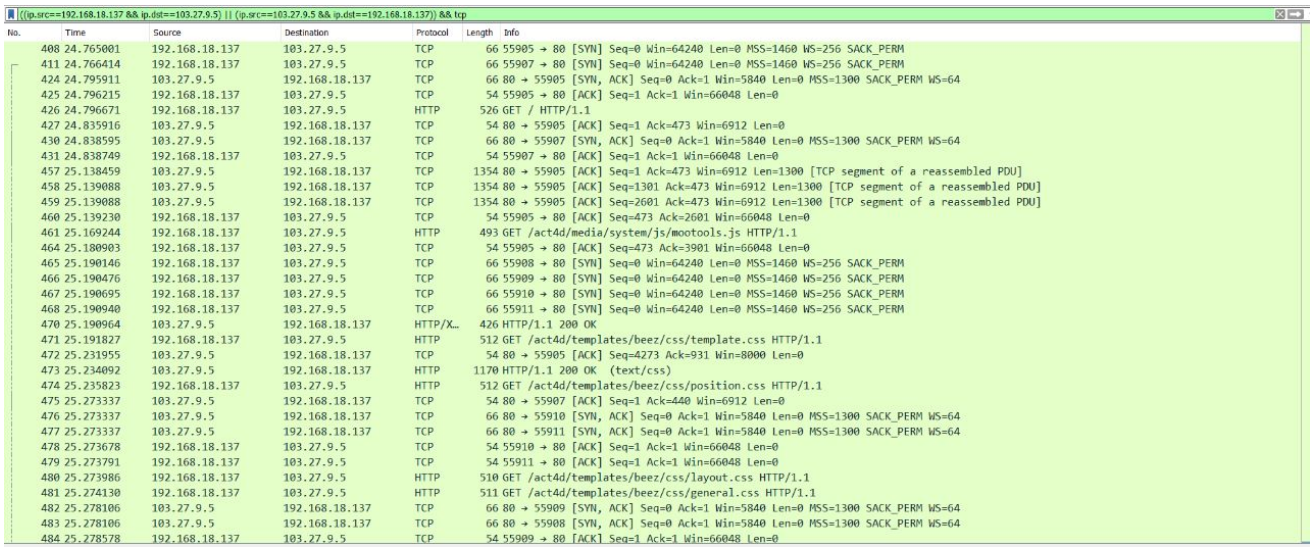


Figure 39: Wireshark HTTP Filter for www.iitd.ac.in

We did not recieve any HTTP traffic for www.iitd.ac.in. This may be because it uses HTTPS instead of HTTP. If we trace a website that uses HTTPS, encrypted TLS traffic can be seen in Wireshark captures. The above screenshot shows TLS traffic for www.iitd.ac.in

4.3 TCP Connections



((ip.src==192.168.18.137 && ip.dst==103.27.9.5) || (ip.src==103.27.9.5 && ip.dst==192.168.18.137)) && tcp

No.	Time	Source	Destination	Protocol	Length	Info
408	24.765001	192.168.18.137	103.27.9.5	TCP	66	55905 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
411	24.766414	192.168.18.137	103.27.9.5	TCP	66	55907 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
424	24.795911	103.27.9.5	192.168.18.137	TCP	66	80 → 55905 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1300 SACK_PERM WS=64
425	24.796215	192.168.18.137	103.27.9.5	TCP	54	55905 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
426	24.796671	192.168.18.137	103.27.9.5	HTTP	526	GET / HTTP/1.1
427	24.835916	103.27.9.5	192.168.18.137	TCP	54	80 → 55905 [ACK] Seq=1 Ack=473 Win=6912 Len=0
430	24.838595	103.27.9.5	192.168.18.137	TCP	66	80 → 55907 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1300 SACK_PERM WS=64
431	24.838749	192.168.18.137	103.27.9.5	TCP	54	55907 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
457	25.138459	103.27.9.5	192.168.18.137	TCP	1354	80 → 55905 [ACK] Seq=1 Ack=473 Win=6912 Len=1300 [TCP segment of a reassembled PDU]
458	25.139088	103.27.9.5	192.168.18.137	TCP	1354	80 → 55905 [ACK] Seq=1301 Ack=473 Win=6912 Len=1300 [TCP segment of a reassembled PDU]
459	25.139088	103.27.9.5	192.168.18.137	TCP	1354	80 → 55905 [ACK] Seq=2601 Ack=473 Win=6912 Len=1300 [TCP segment of a reassembled PDU]
460	25.139230	192.168.18.137	103.27.9.5	TCP	54	55905 → 80 [ACK] Seq=473 Ack=2601 Win=66048 Len=0
461	25.169244	192.168.18.137	103.27.9.5	HTTP	493	GET /act4d/media/system/js/mootools.js HTTP/1.1
464	25.180903	192.168.18.137	103.27.9.5	TCP	54	55905 → 80 [ACK] Seq=473 Ack=3901 Win=66048 Len=0
465	25.190146	192.168.18.137	103.27.9.5	TCP	66	55908 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
466	25.190476	192.168.18.137	103.27.9.5	TCP	66	55909 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
467	25.190695	192.168.18.137	103.27.9.5	TCP	66	55910 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
468	25.190940	192.168.18.137	103.27.9.5	TCP	66	55911 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
470	25.190964	103.27.9.5	192.168.18.137	HTTP/X…	426	HTTP/1.1 200 OK
471	25.191827	192.168.18.137	103.27.9.5	HTTP	512	GET /act4d/templates/beez/css/template.css HTTP/1.1
472	25.231955	103.27.9.5	192.168.18.137	TCP	54	80 → 55905 [ACK] Seq=4273 Ack=931 Win=8000 Len=0
473	25.234092	103.27.9.5	192.168.18.137	HTTP	1170	HTTP/1.1 200 OK (text/css)
474	25.235823	192.168.18.137	103.27.9.5	HTTP	512	GET /act4d/templates/beez/css/position.css HTTP/1.1
475	25.273337	103.27.9.5	192.168.18.137	TCP	54	80 → 55907 [ACK] Seq=1 Ack=440 Win=6912 Len=0
476	25.273337	103.27.9.5	192.168.18.137	TCP	66	80 → 55910 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1300 SACK_PERM WS=64
477	25.273337	103.27.9.5	192.168.18.137	TCP	66	80 → 55911 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1300 SACK_PERM WS=64
478	25.273678	192.168.18.137	103.27.9.5	TCP	54	55910 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
479	25.273791	192.168.18.137	103.27.9.5	TCP	54	55911 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
480	25.273986	192.168.18.137	103.27.9.5	HTTP	510	GET /act4d/templates/beez/css/layout.css HTTP/1.1
481	25.274130	192.168.18.137	103.27.9.5	HTTP	511	GET /act4d/templates/beez/css/general.css HTTP/1.1
482	25.278106	103.27.9.5	192.168.18.137	TCP	66	80 → 55909 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1300 SACK_PERM WS=64
483	25.278106	103.27.9.5	192.168.18.137	TCP	66	80 → 55908 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1300 SACK_PERM WS=64
484	25.278578	192.168.18.137	103.27.9.5	TCP	54	55909 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0

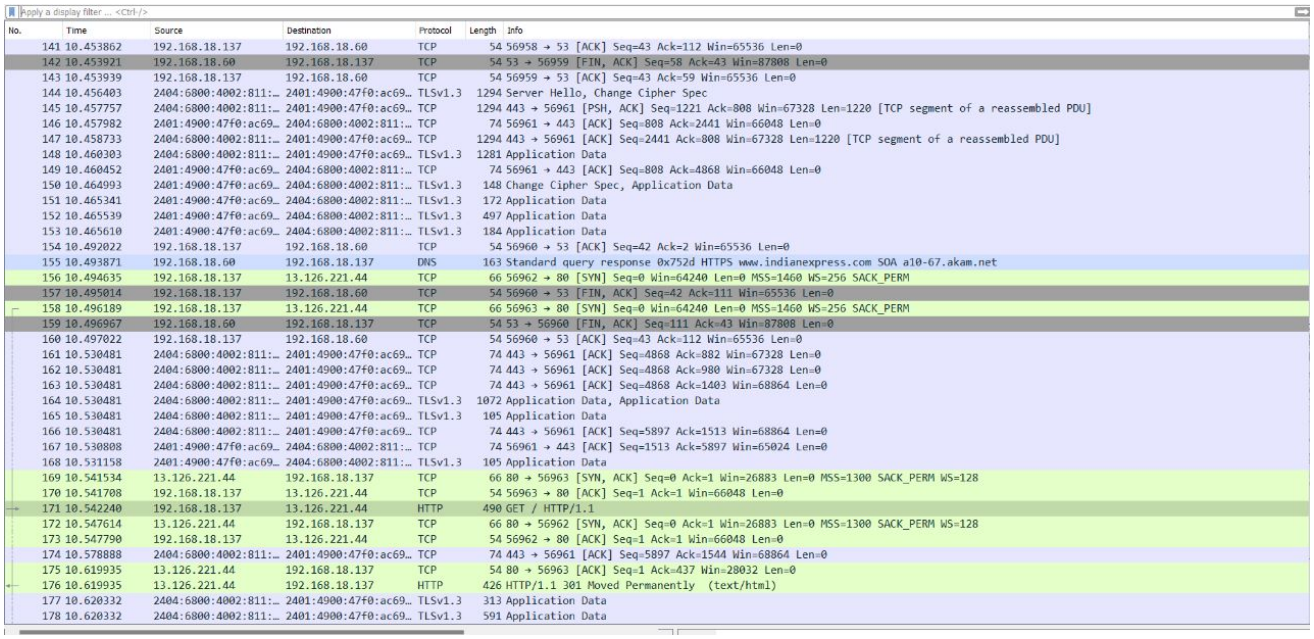
Figure 40: Wireshark TCP Connections

We observed 6 TCP connections being opened and 11 HTTP requests being sent which indicates that multiple HTTP requests can be transmitted over the same TCP connection. In modern web browsers, a single TCP connection is often reused to fetch multiple resources from a single webpage. This technique is known as "persistent connection."

My browser initiated 11 separate requests to fetch various resources required to render the webpage. These requests could be for different types of content objects that constitute the webpage.

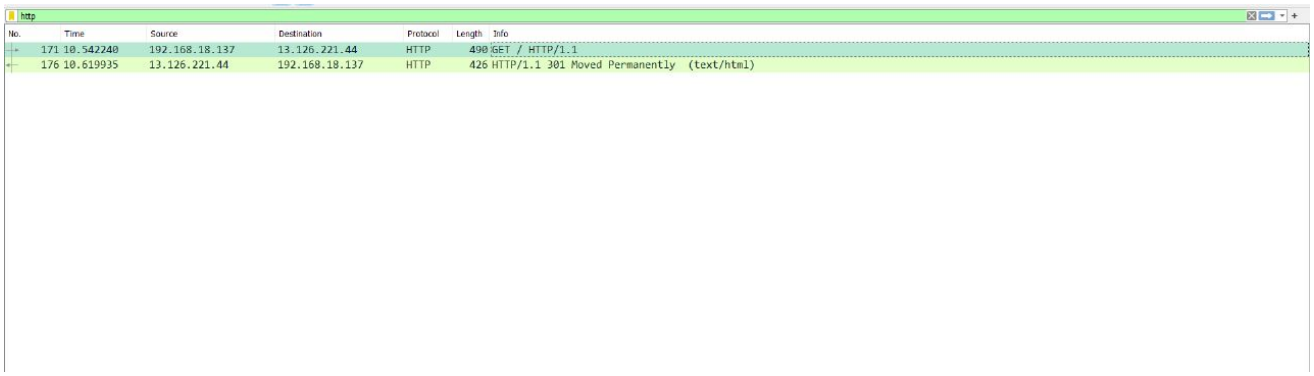
It's common for browsers to fetch multiple content objects over the same established TCP connection to reduce latency and overhead associated with repeatedly opening new connections. This practice is more efficient compared to opening a new TCP connection for each content object. The same TCP connection can serve requests for various resources, optimizing the loading process of a webpage.

4.4 Indian Express



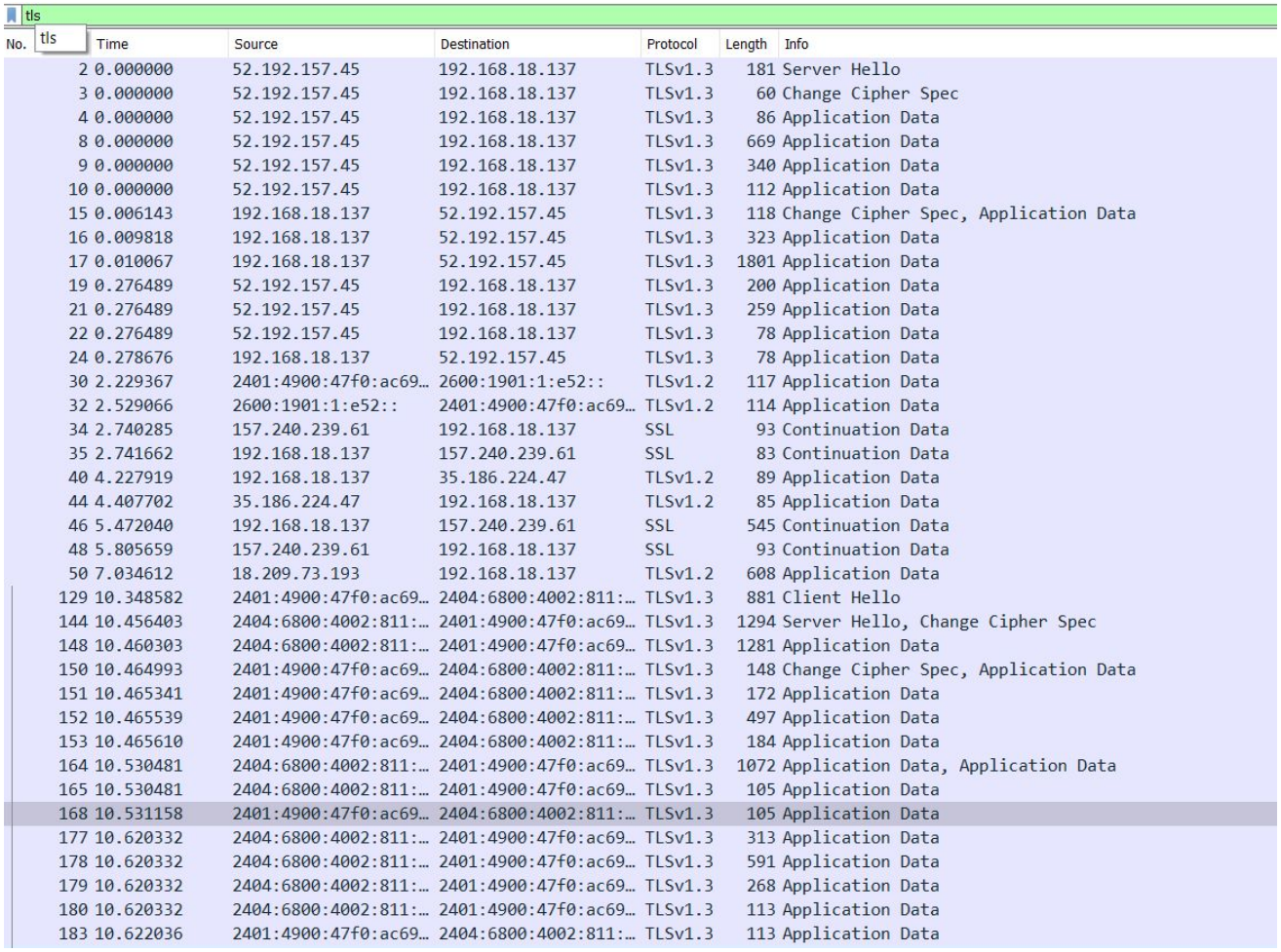
No.	Time	Source	Destination	Protocol	Length	Info
141	10.453862	192.168.18.137	192.168.18.60	TCP	54	56958 → 53 [ACK] Seq=43 Ack=112 Win=65536 Len=0
142	10.453921	192.168.18.60	192.168.18.137	TCP	54	53 → 56959 [FIN, ACK] Seq=58 Ack=43 Win=87808 Len=0
143	10.453939	192.168.18.137	192.168.18.60	TCP	54	56959 → 53 [ACK] Seq=43 Ack=59 Win=65536 Len=0
144	10.456403	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TLSv1.3	1294	Server Hello, Change Cipher Spec
145	10.457757	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TCP	1294	443 → 56961 [PSH, ACK] Seq=1221 Ack=808 Win=67328 Len=1220 [TCP segment of a reassembled PDU]
146	10.457982	2401:4900:47f0:ac69…	2404:6800:4002:811:…	TCP	74	56961 → 443 [ACK] Seq=808 Ack=2441 Win=66048 Len=0
147	10.458733	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TCP	1294	443 → 56961 [ACK] Seq=2441 Ack=808 Win=67328 Len=1220 [TCP segment of a reassembled PDU]
148	10.460303	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TLSv1.3	1281	Application Data
149	10.460452	2401:4900:47f0:ac69…	2404:6800:4002:811:…	TCP	74	56961 → 443 [ACK] Seq=808 Ack=4868 Win=66048 Len=0
150	10.464993	2401:4900:47f0:ac69…	2404:6800:4002:811:…	TLSv1.3	148	Change Cipher Spec, Application Data
151	10.465341	2401:4900:47f0:ac69…	2404:6800:4002:811:…	TLSv1.3	172	Application Data
152	10.465539	2401:4900:47f0:ac69…	2404:6800:4002:811:…	TLSv1.3	497	Application Data
153	10.465610	2401:4900:47f0:ac69…	2404:6800:4002:811:…	TLSv1.3	184	Application Data
154	10.492022	192.168.18.137	192.168.18.60	TCP	54	56960 → 53 [ACK] Seq=42 Ack=2 Win=65536 Len=0
155	10.493871	192.168.18.60	192.168.18.137	DNS	163	Standard query response 0x752d HTTPS www.indianexpress.com SOA a10-67.akam.net
156	10.494635	192.168.18.137	13.126.221.44	TCP	66	56962 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
157	10.495014	192.168.18.137	192.168.18.60	TCP	54	56960 → 53 [FIN, ACK] Seq=42 Ack=111 Win=65536 Len=0
158	10.496189	192.168.18.137	13.126.221.44	TCP	66	56963 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
159	10.496967	192.168.18.60	192.168.18.137	TCP	54	53 → 56960 [FIN, ACK] Seq=111 Ack=43 Win=87808 Len=0
160	10.497022	192.168.18.137	192.168.18.60	TCP	54	56960 → 53 [ACK] Seq=43 Ack=112 Win=65536 Len=0
161	10.530481	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TCP	74	443 → 56961 [ACK] Seq=4868 Ack=882 Win=67328 Len=0
162	10.530481	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TCP	74	443 → 56961 [ACK] Seq=4868 Ack=980 Win=67328 Len=0
163	10.530481	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TCP	74	443 → 56961 [ACK] Seq=4868 Ack=1403 Win=68864 Len=0
164	10.530481	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TLSv1.3	1072	Application Data, Application Data
165	10.530481	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TLSv1.3	105	Application Data
166	10.530481	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TCP	74	443 → 56961 [ACK] Seq=5897 Ack=1513 Win=68864 Len=0
167	10.530808	2401:4900:47f0:ac69…	2404:6800:4002:811:…	TCP	74	56961 → 443 [ACK] Seq=1513 Ack=5897 Win=65024 Len=0
168	10.531158	2401:4900:47f0:ac69…	2404:6800:4002:811:…	TLSv1.3	105	Application Data
169	10.541534	13.126.221.44	192.168.18.137	TCP	66	80 → 56963 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1300 SACK_PERM WS=128
170	10.541708	192.168.18.137	13.126.221.44	TCP	54	56963 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
171	10.542240	192.168.18.137	13.126.221.44	HTTP	490	GET / HTTP/1.1
172	10.547614	13.126.221.44	192.168.18.137	TCP	66	80 → 56962 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1300 SACK_PERM WS=128
173	10.547790	192.168.18.137	13.126.221.44	TCP	54	56962 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
174	10.578888	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TCP	74	443 → 56961 [ACK] Seq=5897 Ack=1544 Win=68864 Len=0
175	10.619935	13.126.221.44	192.168.18.137	TCP	54	80 → 56963 [ACK] Seq=1 Ack=437 Win=28032 Len=0
176	10.619935	13.126.221.44	192.168.18.137	HTTP	426	HTTP/1.1 301 Moved Permanently (text/html)
177	10.620332	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TLSv1.3	313	Application Data
178	10.620332	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TLSv1.3	591	Application Data

Figure 41: Wireshark



No.	Time	Source	Destination	Protocol	Length	Info
171	10.542240	192.168.18.137	13.126.221.44	HTTP	490	GET / HTTP/1.1
176	10.619935	13.126.221.44	192.168.18.137	HTTP	426	HTTP/1.1 301 Moved Permanently (text/html)

Figure 42: Wireshark HTTP Filter



tls

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000000	52.192.157.45	192.168.18.137	TLSv1.3	181	Server Hello
3	0.000000	52.192.157.45	192.168.18.137	TLSv1.3	60	Change Cipher Spec
4	0.000000	52.192.157.45	192.168.18.137	TLSv1.3	86	Application Data
8	0.000000	52.192.157.45	192.168.18.137	TLSv1.3	669	Application Data
9	0.000000	52.192.157.45	192.168.18.137	TLSv1.3	340	Application Data
10	0.000000	52.192.157.45	192.168.18.137	TLSv1.3	112	Application Data
15	0.006143	192.168.18.137	52.192.157.45	TLSv1.3	118	Change Cipher Spec, Application Data
16	0.009818	192.168.18.137	52.192.157.45	TLSv1.3	323	Application Data
17	0.010067	192.168.18.137	52.192.157.45	TLSv1.3	1801	Application Data
19	0.276489	52.192.157.45	192.168.18.137	TLSv1.3	200	Application Data
21	0.276489	52.192.157.45	192.168.18.137	TLSv1.3	259	Application Data
22	0.276489	52.192.157.45	192.168.18.137	TLSv1.3	78	Application Data
24	0.278676	192.168.18.137	52.192.157.45	TLSv1.3	78	Application Data
30	2.229367	2401:4900:47f0:ac69…	2600:1901:1:e52::	TLSv1.2	117	Application Data
32	2.529066	2600:1901:1:e52::	2401:4900:47f0:ac69…	TLSv1.2	114	Application Data
34	2.740285	157.240.239.61	192.168.18.137	SSL	93	Continuation Data
35	2.741662	192.168.18.137	157.240.239.61	SSL	83	Continuation Data
40	4.227919	192.168.18.137	35.186.224.47	TLSv1.2	89	Application Data
44	4.407702	35.186.224.47	192.168.18.137	TLSv1.2	85	Application Data
46	5.472040	192.168.18.137	157.240.239.61	SSL	545	Continuation Data
48	5.805659	157.240.239.61	192.168.18.137	SSL	93	Continuation Data
50	7.034612	18.209.73.193	192.168.18.137	TLSv1.2	608	Application Data
129	10.348582	2401:4900:47f0:ac69…	2404:6800:4002:811:…	TLSv1.3	881	Client Hello
144	10.456403	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TLSv1.3	1294	Server Hello, Change Cipher Spec
148	10.460303	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TLSv1.3	1281	Application Data
150	10.464993	2401:4900:47f0:ac69…	2404:6800:4002:811:…	TLSv1.3	148	Change Cipher Spec, Application Data
151	10.465341	2401:4900:47f0:ac69…	2404:6800:4002:811:…	TLSv1.3	172	Application Data
152	10.465539	2401:4900:47f0:ac69…	2404:6800:4002:811:…	TLSv1.3	497	Application Data
153	10.465610	2401:4900:47f0:ac69…	2404:6800:4002:811:…	TLSv1.3	184	Application Data
164	10.530481	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TLSv1.3	1072	Application Data, Application Data
165	10.530481	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TLSv1.3	105	Application Data
168	10.531158	2401:4900:47f0:ac69…	2404:6800:4002:811:…	TLSv1.3	105	Application Data
177	10.620332	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TLSv1.3	313	Application Data
178	10.620332	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TLSv1.3	591	Application Data
179	10.620332	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TLSv1.3	268	Application Data
180	10.620332	2404:6800:4002:811:…	2401:4900:47f0:ac69…	TLSv1.3	113	Application Data
183	10.622036	2401:4900:47f0:ac69…	2404:6800:4002:811:…	TLSv1.3	113	Application Data

Figure 43: Wireshark TLS Filter

We did not find any HTTP traffic while tracing http://www.indianexpress.com because many modern websites use HTTPS (secure HTTP) for transmitting data. HTTPS traffic is encrypted, and Wireshark cannot decrypt it by default.

HTTPS (Hypertext Transfer Protocol Secure) is the secure version of HTTP. It encrypts the data exchanged between a user's browser and a website's server to ensure the confidentiality and integrity of the information. HTTPS is widely used to protect sensitive data such as login credentials, personal information, and payment details.

If we trace a website that uses HTTPS, encrypted TLS traffic can be seen in Wireshark captures. While Wireshark can provide information about the TLS handshake and the initial connection setup, it cannot easily decode the encrypted content of HTTPS packets without access to the server's private keys. This is done to ensure the security and privacy of user data during transmission.