Assignment 1

Internet Architecture

Piyush Chauhan	2021CS11010
Shankh Gupta	2021CS50604

A COL334 Homework Assignment

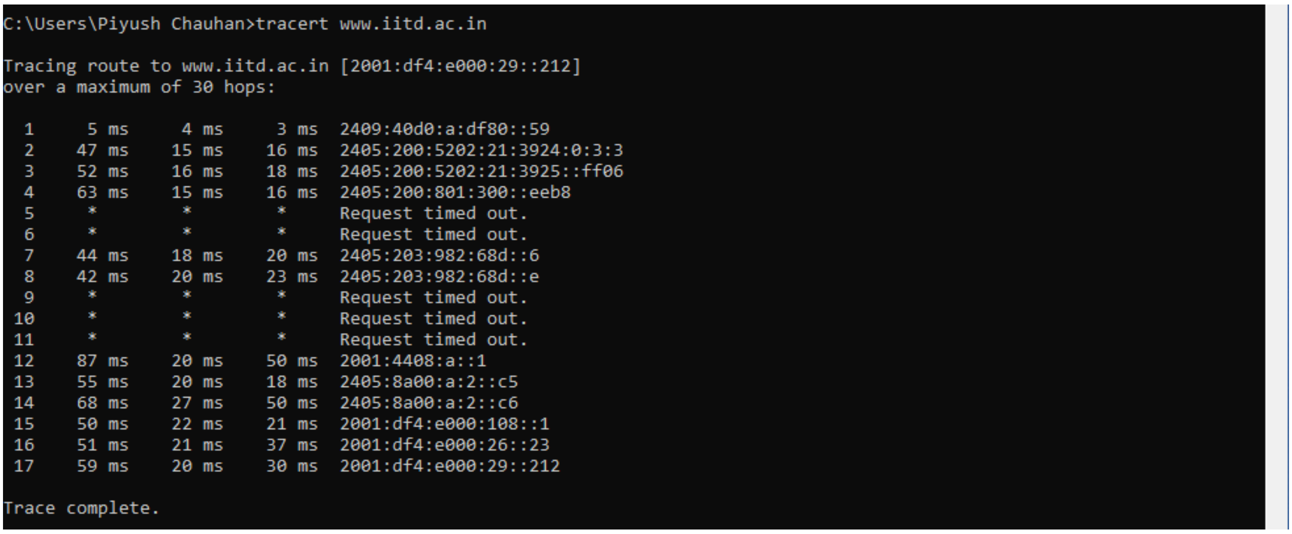
भारतीय प्रौद्योगिकी संस्थान दिल्ली
Indian Institute of Technology Delhi

August 13, 2023

1. Network Analysis

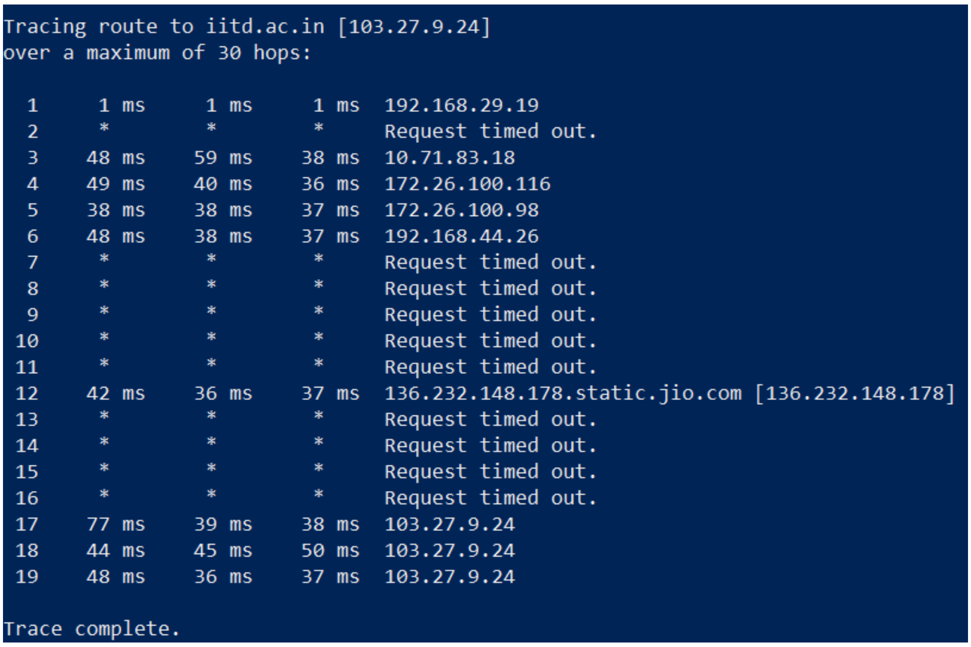
a. Traceroute :

Traceroute for this part was run using Jio 4G network. We ran the tracert for www.iitd.ac.in and www.google.com. Below are the results :



```
C:\Users\Piyush Chauhan>tracert www.iitd.ac.in

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

  1     5 ms     4 ms     3 ms  2409:40d0:a:df80::59
  2    47 ms    15 ms    16 ms  2405:200:5202:21:3924:0:3:3
  3    52 ms    16 ms    18 ms  2405:200:5202:21:3925::ff06
  4    63 ms    15 ms    16 ms  2405:200:801:300::eeb8
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7    44 ms    18 ms    20 ms  2405:203:982:68d::6
  8    42 ms    20 ms    23 ms  2405:203:982:68d::e
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12    87 ms    20 ms    50 ms  2001:4408:a::1
 13    55 ms    20 ms    18 ms  2405:8a00:a:2::c5
 14    68 ms    27 ms    50 ms  2405:8a00:a:2::c6
 15    50 ms    22 ms    21 ms  2001:df4:e000:108::1
 16    51 ms    21 ms    37 ms  2001:df4:e000:26::23
 17    59 ms    20 ms    30 ms  2001:df4:e000:29::212

Trace complete.
```

Figure 1: Traceroute for `www.iitd.ac.in` with ipv6 addresses

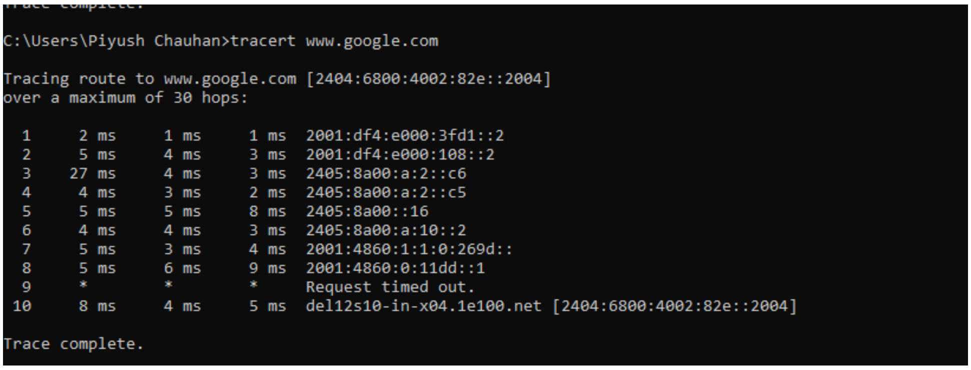


```
Tracing route to iitd.ac.in [103.27.9.24]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.29.19
  2     *        *        *     Request timed out.
  3    48 ms    59 ms    38 ms  10.71.83.18
  4    49 ms    40 ms    36 ms  172.26.100.116
  5    38 ms    38 ms    37 ms  172.26.100.98
  6    48 ms    38 ms    37 ms  192.168.44.26
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12    42 ms    36 ms    37 ms  136.232.148.178.static.jio.com [136.232.148.178]
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17    77 ms    39 ms    38 ms  103.27.9.24
 18    44 ms    45 ms    50 ms  103.27.9.24
 19    48 ms    36 ms    37 ms  103.27.9.24

Trace complete.
```

Figure 2: Traceroute for `www.iitd.ac.in` with ipv4 addresses

b. Observations :

- The first hop **(192.168.29.19)** is within our local network, indicating our local router (Default Gateway).
- The routers from 2 to 6 in figure 2 also belong to the local network. Then the IP address **(136.232.148.178)**



```
Trace complete.

C:\Users\Piyush Chauhan>tracert www.google.com

Tracing route to www.google.com [2404:6800:4002:82e::2004]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  2001:df4:e000:3fd1::2
  2     5 ms     4 ms     3 ms  2001:df4:e000:108::2
  3    27 ms     4 ms     3 ms  2405:8a00:a:2::c6
  4     4 ms     3 ms     2 ms  2405:8a00:a:2::c5
  5     5 ms     5 ms     8 ms  2405:8a00::16
  6     4 ms     4 ms     3 ms  2405:8a00:a:10::2
  7     5 ms     3 ms     4 ms  2001:4860:1:1:0:269d::
  8     5 ms     6 ms     9 ms  2001:4860:0:11dd::1
  9     *        *        *     Request timed out.
 10     8 ms     4 ms     5 ms  del12s10-in-x04.1e100.net [2404:6800:4002:82e::2004]

Trace complete.
```

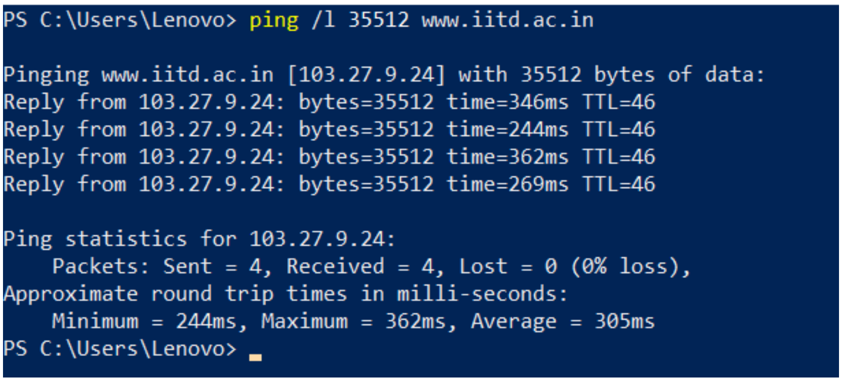
Figure 3: Traceroute for `www.google.com`

belongs to the Tier-2 network (AS NAME : RELIANCEJIO-IN Reliance Jio Infocomm Limited, IN) and lastly the last three IP address lie in the IITD network (AS NAME : IITDEL-AS-IN Indian Institute of Technology Delhi, IN).

- The path includes a mix of private and public IP addresses, suggesting a combination of internal network and ISP routing.
- While doing the traceroute for `www.iitd.ac.in` there were many Ip addresses in the private ip range, viz. 192.168.197.135, 10.71.80.18, 172.26.100.116, 172.26.100.98 and 192.168.44.22
- Many of the requests for were either blocked by the ISP or the routers did not respond to the ICMP requests (due to network security measures or router configurations) during traceroute of `www.iitd.ac.in` (as shown by * in the images) and displayed ”Request Timed Out”. When we did the traceroute on IITD wifi, there were no requests blocks and the trace completed in just 4 hops compared to hops with Jio 4G Network.

c. Size limit for Ping :

Using ping, we were able to send packets of size not more than **35512 bytes**. This upper limit was tested for `www.iitd.ac.in` using Jio 4G network. Even on increasing the timeout period, we weren’t able to send packets bigger than 35512 bytes. However this max size is not the same for every website; for instance the max packet size that we could send using ping for www.google.com was **1472 bytes** only. Also using IITD WiFi, we were able to send the maxsize of 65500 bytes packet (which is the upper limit of packet size for ping) to `www.iitd.ac.in`.



```
PS C:\Users\Lenovo> ping /l 35512 www.iitd.ac.in

Pinging www.iitd.ac.in [103.27.9.24] with 35512 bytes of data:
Reply from 103.27.9.24: bytes=35512 time=346ms TTL=46
Reply from 103.27.9.24: bytes=35512 time=244ms TTL=46
Reply from 103.27.9.24: bytes=35512 time=362ms TTL=46
Reply from 103.27.9.24: bytes=35512 time=269ms TTL=46

Ping statistics for 103.27.9.24:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 244ms, Maximum = 362ms, Average = 305ms
PS C:\Users\Lenovo> _
```

Figure 4: max packet size for ping

2. Traceroute using Ping

We have written a python script to replicate traceroute functionality using Ping. To do this, we set a max limit on TTL as 30 hops and iterated over the TTL counter from 1 to the max no. of hops, terminating either if TTL == max_ttl or IP address in the output matches the destination address given in the input.

```python
# the ip address/website will be given as in input to the script
# the output should be the same as traceroute
import subprocess

def traceroute(destination):
    #Set Default ttl to be 30. this corresponds to number of hops in traceroute
    max_ttl = 30  # Maximum TTL value == Maximum number of hops
    #increast the TTL by 1
    for ttl in range(1, max_ttl + 1,1):

        command = ["ping","-n/",str(1), "/i", str(ttl), destination]
        result = subprocess.run(command, stdout=subprocess.PIPE, stderr=subprocess.PIPE, text=True)
        lines = result.stdout.strip().split('\n')
        loss = lines[4].split()[9]
        #if packet is lost, print *
        if loss=="1" :
            print(f"{ttl}: * ")
        else:
            lines = result.stdout.strip().split('\n')
            #get the IP address reached
            ip_address = lines[1].split()[2][0:-1]
            print(f"{ttl}: {ip_address}")
            #if IP address reached is destination, terminate.
            if ip_address == destination:
                timetaken = lines[1].split()[4]
                print(timetaken)
                break

if __name__ == "__main__":
    #Get the destination IP using ping command with default TTL.
    destination = input("Enter the IP address or website: ")
    command = ["ping","/n",str(1),destination]
    result = subprocess.run(command, stdout=subprocess.PIPE, stderr=subprocess.PIPE, text=True)
    lines = result.stdout.strip().split('\n')
    DesinationtIP = lines[1].split()[2][0:-1]
    #Call the reaceroute funtion with destination IP.
    traceroute(DesinationtIP)
```

3. Internet Architecture

AS-IP Lookup

`www.utah.edu`		
IP Address	AS Number	AS Name
10.184.32.13	None	local network
10.254.175.5	None	local network
10.255.1.34	None	local network
10.119.233.65	None	local network
*	None	local network
10.1.207.65	None	local network
10.1.200.137	None	local network
10.255.238.122	None	local network
180.149.48.18	55824	NKN-CORE-NW NKN Core Network, IN
180.149.48.2	55824	NKN-CORE-NW NKN Core Network, IN
180.149.48.13	55824	NKN-CORE-NW NKN Core Network, IN
163.253.1.116	11537	INTERNET2-RESEARCH-EDU, US
163.253.1.3	11537	INTERNET2-RESEARCH-EDU, US
163.253.1.139	11537	INTERNET2-RESEARCH-EDU, US
163.253.2.17	11537	INTERNET2-RESEARCH-EDU, US
163.253.2.18	11537	INTERNET2-RESEARCH-EDU, US
163.253.1.245	11537	INTERNET2-RESEARCH-EDU, US
163.253.1.242	11537	INTERNET2-RESEARCH-EDU, US
163.253.1.171	11537	INTERNET2-RESEARCH-EDU, US
163.253.1.152	11537	INTERNET2-RESEARCH-EDU, US
163.253.5.7	11537	INTERNET2-RESEARCH-EDU, US
140.197.249.81	210	WEST-NET-WEST, US
140.197.251.32	210	WEST-NET-WEST, US
140.197.253.97	210	WEST-NET-WEST, US
140.197.252.76	210	WEST-NET-WEST, US
140.197.252.84	210	WEST-NET-WEST, US
140.197.253.139	210	WEST-NET-WEST, US
199.104.93.22	17055	UTAH
199.104.93.29	17055	UTAH
155.99.130.59	17055	UTAH
155.99.130.107	17055	UTAH
172.31.241.255	None	local network
172.31.241.22	None	local network
172.31.241.29	None	local network
155.98.186.21	17055	UTAH

www.uct.ac.za		
IP Address	AS Number	AS Name
10.184.0.13	–	local router
10.254.175.1	–	local router
10.255.1.34	–	local router
10.119.233.65	–	local router
10.1.207.69	–	local router
10.1.200.137	–	local router
10.255.238.254	–	local router
180.149.48.18	55824	NKN-CORE-NW NKN Core Network, IN
180.149.48.6	55824	NKN-CORE-NW NKN Core Network, IN
180.149.48.20	55824	NKN-CORE-NW NKN Core Network, IN
155.232.220.18	2018	TENET-1,ZA
155.232.1.21	2018	TENET-1,ZA
155.232.1.153	2018	TENET-1,ZA
155.232.1.148	2018	TENET-1,ZA
155.232.64.70	2018	TENET-1,ZA
154.114.124.1	2018	TENET-1,ZA

www.iitd.ac.in		
IP Address	AS Number	AS Name
10.184.0.13	–	local router
10.254.175.5	–	local router
10.254.236.6	–	local router
10.10.211.212	–	local router

www.google.com		
IP Address	AS Number	AS Name
10.184.0.13	–	local router
10.254.175.1	–	local router
10.255.1.34	–	local router
10.119.233.65	–	local router
10.119.234.162	–	local router
72.14.194.160	15169	TELCOMDATA Google PNI, KG(Kyrgyzstan)
108.170.251.97	15169	TELCOMDATA Google PNI, KG(Kyrgyzstan)
142.251.76.169	15169	TELCOMDATA Google PNI, KG(Kyrgyzstan)
142.250.207.196	15169	TELCOMDATA Google PNI, KG(Kyrgyzstan)

www.facebook.com		
IP Address	AS Number	AS Name
10.184.0.13	–	local router
10.254.175.1	–	local router
10.255.1.34	–	local router
10.119.233.65	–	local router
10.255.238.254	–	local router
10.152.7.214	–	local router
10.152.7.233	32934	local router
157.240.66.204	32934	FACEBOOK, US
157.240.44.27	32934	FACEBOOK, US
173.252.67.147	32934	FACEBOOK, US
157.240.16.35	32934	FACEBOOK, US

PART A.

NUMBER OF HOPS (hurricane electric)			
Web Servers	SOURCE 1	SOURCE 2	Personal Computer
www.utah.edu	19	19	33 / 30
www.uct.ac.za	15	Doesn't Terminate (last IP : 154.114.124.1)	Stuck at IP(154.114.124.1) Tried 200 hops / -
www.iitd.ac.in	6	19	4 / 17
www.google.com	13	6	10 / 7
www.facebook.com	14	13	13 / 10

SRC1 : Equinix LS1 Portugal.
SRC2 : Bogota Server, Colombia (Equinix BG1).
Personal Computer : First value is using IITD Wifi / Second Value is through mobile hotspot.

If the traceroute source and destination are geographically closer to each other then it result in few hops. For this test, the device was connected to IITD WiFi, and we found that accessing the IITD website results in only 4 hops which are much less as compared to other two sources. We also found that google has a data centre in Chile which is close to Columbia and thus the South American server responded to www.google.com with less hops. Also, Facebook does not have its server in South America and Portugal, thus it took roughly similar hops from both servers to respond.

PART B.

Latencies (in ms)			
Web Servers	SOURCE 1	SOURCE 2	Personal Computer
`www.utah.edu`	138	122.67	422
`www.uct.ac.za`	211	372	inf(390)
`www.iitd.ac.in`	226	336	2
`www.google.com`	104	64	9
`www.facebook.com`	156	142	39

SRC1 : Equinix LS1(Portugal).
SRC2 : Bogota Server, Colombia (Equinix BG1).
Personal Computer : Using IITD WiFi

We found **latency to be directly proportional to the number of hops**. This is visible when we compare server 1 with 2 .
For google.com server 2 took 6 hops with 64ms while server 1 took 104ms for 13 hops thus, latency increased.Also, both the server took similar hops to access Facebook.com and thus had similar latency. Hence, we can conclude that latency increases with number of hops.

PART C.

`www.utah.edu`, `www.uct.ac.za` and `www.iitd.ac.in` all resolve to the same destination server irrespective of the source server because they are hosted on a single server.
Below are the details of server where they are hosted.
`www.utah.edu` : **155.98.186.21**
`www.uct.ac.za` : **137.158.159.192**
`www.iitd.ac.in` : **10.10.211.212**

This is because they are university website and thus are local to their region. They are mostly used by students studying in their own university and thus do not require to host the website to multiple servers all over the world.

While google and Facebook are used by millions of users all over the global. To make faster access to their website, they have hosted their website on multiple server all over the globe. So when we try to access them, The nearest server send response. In this case, the nearest server is (IITD WiFi) running a nslookup gives :

`www.google.com` : **146.112.61.110 (2001:df4:e000:29::104)**
`www.facebook.com` : **146.112.61.110(2001:df4:e000:29::104)**

Surprisingly they were both found on the same IP address. If we change the server to some other location, say LONDON we get
Receiver serve : **Equinix london (LD8)**
`www.google.com` : **2607:f8b0:4008:806::200e**
`www.facebook.com` : **2a03:2880:f131:83:face:b00c::25de**
This shows that bigger and popular website host themselves on different servers to divider the traffic and decrease latency.

PART D.

The paths will appear different for different IP addresses for same web server as they would be connected differently to different routers. The main reasons for different routes are :

- **Load balancing** : the servers are connected differently to different routers to balance the load on them
- **Routing policies**
- **Network congestion**: this allow dynamic adjustment or path from source to server.

The paths can be longer or shorter due to the reasons mentioned above. Length of path doesn't not depend on efficiency and speed of connection. A packet, because of network congestion on shorter path might dynamically change its route to longer path increasing the number of hops and latency.
In an ideal situation, the servers which are remote and far from source geographical location tend to have longer paths because of multiple router(and thus more hops) in between them.

PART E.

For `www.google.com` we find many different IP addresses , some of them are :

- **8.8.4.4** (California, US)
- **34.97.77.117** (Osaka, Japan)

For `facebook.com` we have :

- **185.89.218.12** (Dublin, Ireland)
- **192.33.4.12** (California, US)

On running the tracert to these servers the hops and latency were :

Website	HOPS	LATENCY (in ms)
GOOGLE 1	11	14
GOOGLE 2	9	140
FACEBOOK 1	16	100
FACEBOOK 2	17	253

On exploring GOOGLE official server information website we found that google has a wide network of servers, majorly in US and Europe , Some centres are in Singapore and Taiwan and Japan which covers the Asia region. Many countries like middle East Continents(Oman, Turkey) does not have google server does not have Google servers.

Same is the case with Facebook, which are located in US, UK, Singapore and Sweden. India , Brazil, Russia, Australia, China, Japan , Saudi Arabia does not have Facebook servers.

As these countries does not have serves for respective websites, their local ISPs are not directly connected to the servers.

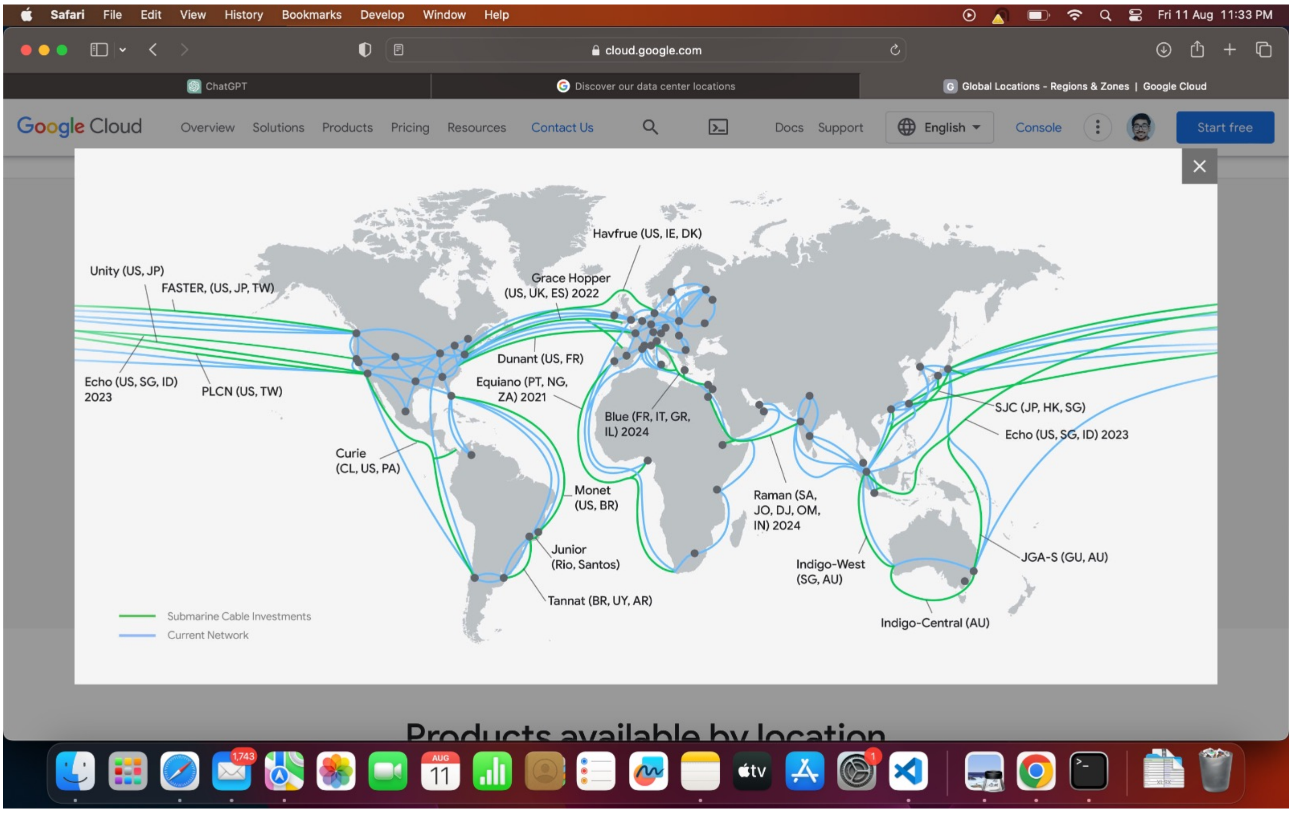
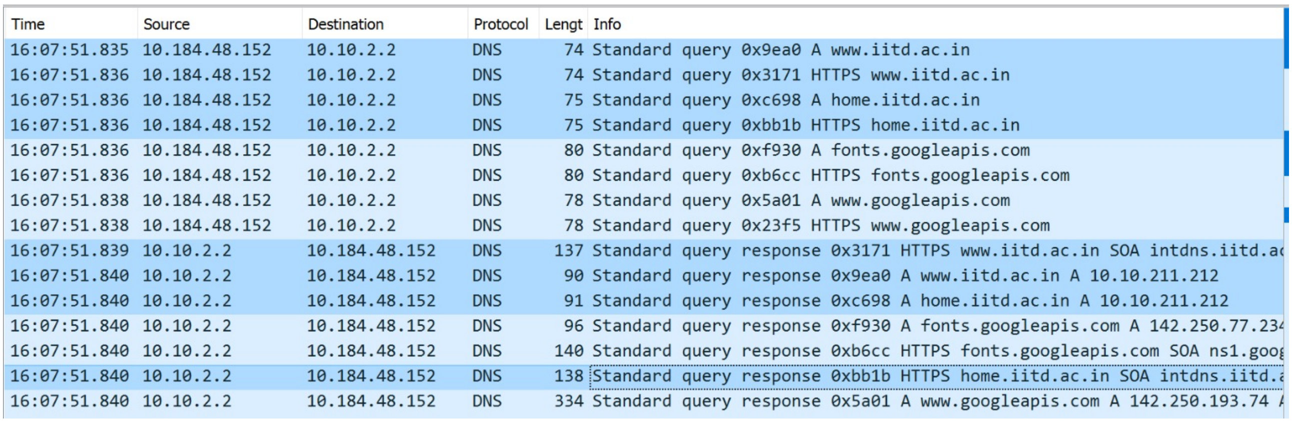


Figure 5: Google Global Locations - Regions and Zones

4. Packet Analysis

a. DNS Queries :

Applying a DNS filter on the packet trace shows some queries for `www.iitd.ac.in` . The time taken to complete the DNS request-response can be obtained by the time difference of the first query (time-stamp : 16:07:51.835) and the response for the last query (time-stamp : 16:07:51.840) which is about **5 milliseconds**. The queries for request and response can be seen (highlighted) in the image below :

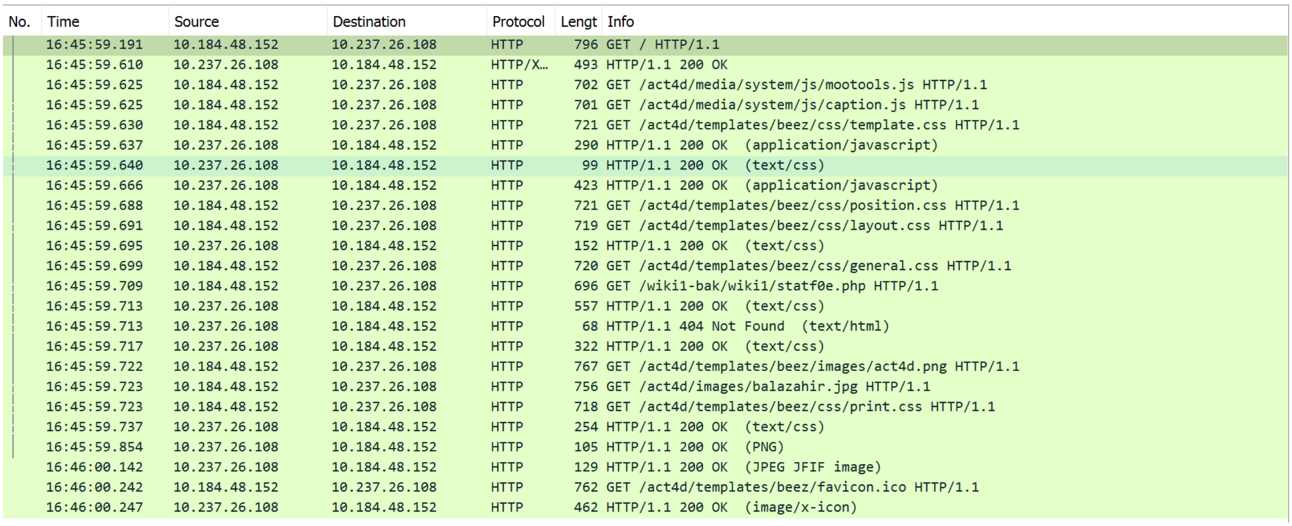


Time	Source	Destination	Protocol	Lengt	Info
16:07:51.835	10.184.48.152	10.10.2.2	DNS	74	Standard query 0x9ea0 A www.iitd.ac.in
16:07:51.836	10.184.48.152	10.10.2.2	DNS	74	Standard query 0x3171 HTTPS www.iitd.ac.in
16:07:51.836	10.184.48.152	10.10.2.2	DNS	75	Standard query 0xc698 A home.iitd.ac.in
16:07:51.836	10.184.48.152	10.10.2.2	DNS	75	Standard query 0xbb1b HTTPS home.iitd.ac.in
16:07:51.836	10.184.48.152	10.10.2.2	DNS	80	Standard query 0xf930 A fonts.googleapis.com
16:07:51.836	10.184.48.152	10.10.2.2	DNS	80	Standard query 0xb6cc HTTPS fonts.googleapis.com
16:07:51.838	10.184.48.152	10.10.2.2	DNS	78	Standard query 0x5a01 A www.googleapis.com
16:07:51.838	10.184.48.152	10.10.2.2	DNS	78	Standard query 0x23f5 HTTPS www.googleapis.com
16:07:51.839	10.10.2.2	10.184.48.152	DNS	137	Standard query response 0x3171 HTTPS www.iitd.ac.in SOA intdns.iitd.ac
16:07:51.840	10.10.2.2	10.184.48.152	DNS	90	Standard query response 0x9ea0 A www.iitd.ac.in A 10.10.211.212
16:07:51.840	10.10.2.2	10.184.48.152	DNS	91	Standard query response 0xc698 A home.iitd.ac.in A 10.10.211.212
16:07:51.840	10.10.2.2	10.184.48.152	DNS	96	Standard query response 0xf930 A fonts.googleapis.com A 142.250.77.23
16:07:51.840	10.10.2.2	10.184.48.152	DNS	140	Standard query response 0xb6cc HTTPS fonts.googleapis.com SOA ns1.goog
16:07:51.840	10.10.2.2	10.184.48.152	DNS	138	Standard query response 0xbb1b HTTPS home.iitd.ac.in SOA intdns.iitd.a
16:07:51.840	10.10.2.2	10.184.48.152	DNS	334	Standard query response 0x5a01 A www.googleapis.com A 142.250.193.74

Figure 6: DNS request-response queries for www.iitd.ac.in

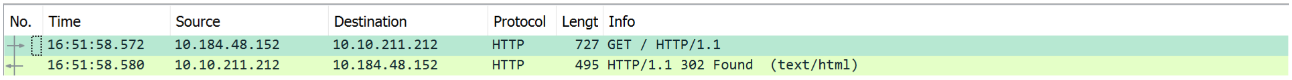
b. HTTP Queries :

We will apply 'http' filter to the packet trace of two web searches, one `act4d.iitd.ac.in`, which is unsecured website and the other `www.iitd.ac.in`, which is a secured website.
For the first one, i.e. `act4d.iitd.ac.in`, we could see a total of 24 HTTP requests were generated as seen in figure 7. All the html content, including the files imported (like javascript and css files) are also visible. We note that Images, GIFs, favicons etc. are transferred at the last and the JS and CSS files are imported first so as that the user can see the main content.
For the second website, i.e. `www.iitd.ac.in`, we could see only 2 http requests as seen in the figure 8.



No.	Time	Source	Destination	Protocol	Lengt	Info
	16:45:59.191	10.184.48.152	10.237.26.108	HTTP	796	GET / HTTP/1.1
	16:45:59.610	10.237.26.108	10.184.48.152	HTTP/X…	493	HTTP/1.1 200 OK
	16:45:59.625	10.184.48.152	10.237.26.108	HTTP	702	GET /act4d/media/system/js/mootools.js HTTP/1.1
	16:45:59.625	10.184.48.152	10.237.26.108	HTTP	701	GET /act4d/media/system/js/caption.js HTTP/1.1
	16:45:59.630	10.184.48.152	10.237.26.108	HTTP	721	GET /act4d/templates/beez/css/template.css HTTP/1.1
	16:45:59.637	10.237.26.108	10.184.48.152	HTTP	290	HTTP/1.1 200 OK (application/javascript)
	16:45:59.640	10.237.26.108	10.184.48.152	HTTP	99	HTTP/1.1 200 OK (text/css)
	16:45:59.666	10.237.26.108	10.184.48.152	HTTP	423	HTTP/1.1 200 OK (application/javascript)
	16:45:59.688	10.184.48.152	10.237.26.108	HTTP	721	GET /act4d/templates/beez/css/position.css HTTP/1.1
	16:45:59.691	10.184.48.152	10.237.26.108	HTTP	719	GET /act4d/templates/beez/css/layout.css HTTP/1.1
	16:45:59.695	10.237.26.108	10.184.48.152	HTTP	152	HTTP/1.1 200 OK (text/css)
	16:45:59.699	10.184.48.152	10.237.26.108	HTTP	720	GET /act4d/templates/beez/css/general.css HTTP/1.1
	16:45:59.709	10.184.48.152	10.237.26.108	HTTP	696	GET /wiki1-bak/wiki1/statf0e.php HTTP/1.1
	16:45:59.713	10.237.26.108	10.184.48.152	HTTP	557	HTTP/1.1 200 OK (text/css)
	16:45:59.713	10.237.26.108	10.184.48.152	HTTP	68	HTTP/1.1 404 Not Found (text/html)
	16:45:59.717	10.237.26.108	10.184.48.152	HTTP	322	HTTP/1.1 200 OK (text/css)
	16:45:59.722	10.184.48.152	10.237.26.108	HTTP	767	GET /act4d/templates/beez/images/act4d.png HTTP/1.1
	16:45:59.723	10.184.48.152	10.237.26.108	HTTP	756	GET /act4d/images/balazahir.jpg HTTP/1.1
	16:45:59.723	10.184.48.152	10.237.26.108	HTTP	718	GET /act4d/templates/beez/css/print.css HTTP/1.1
	16:45:59.737	10.237.26.108	10.184.48.152	HTTP	254	HTTP/1.1 200 OK (text/css)
	16:45:59.854	10.237.26.108	10.184.48.152	HTTP	105	HTTP/1.1 200 OK (PNG)
	16:46:00.142	10.237.26.108	10.184.48.152	HTTP	129	HTTP/1.1 200 OK (JPEG JFIF image)
	16:46:00.242	10.184.48.152	10.237.26.108	HTTP	762	GET /act4d/templates/beez/favicon.ico HTTP/1.1
	16:46:00.247	10.237.26.108	10.184.48.152	HTTP	462	HTTP/1.1 200 OK (image/x-icon)

Figure 7: HTTP requests for `www.act4d.iitd.ac.in`

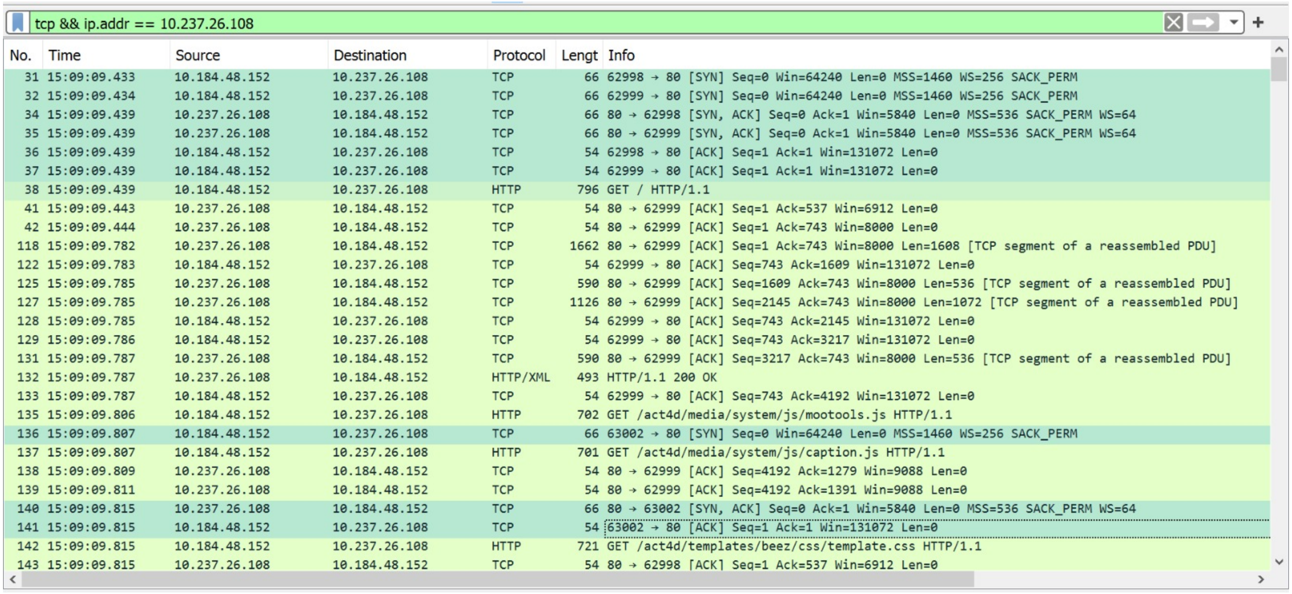


No.	Time	Source	Destination	Protocol	Lengt	Info
	16:51:58.572	10.184.48.152	10.10.211.212	HTTP	727	GET / HTTP/1.1
	16:51:58.580	10.10.211.212	10.184.48.152	HTTP	495	HTTP/1.1 302 Found (text/html)

Figure 8: HTTP requests for `www.iitd.ac.in`

c. TCP Connections :

We will apply a TCP filter for the server `www.act4d.iitd.ac.in`. There were a total of **3 TCP connections** established between ports **(62998 and 80), (62999 and 80) and (63002 and 80)**. As seen in the previous part, there were 24 HTTP requests generated for act4d.iitd.ac.in, so the number of HTTP requests generated is not the same as the number of TCP connections established.
So this means that some of the content objects were fetched over the same connection. For `www.iitd.ac.in` there were a total of 9 TCP connections estabilished (Between ports 4208-80, 4209-443, 4210-80, 4215-443, 4216-443, 4218-443, 4219-443, 4220-443 and 4221-443).



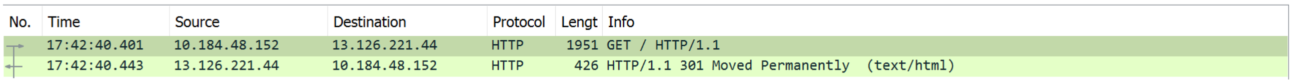
tcp && ip.addr == 10.237.26.108

No.	Time	Source	Destination	Protocol	Lengt	Info
31	15:09:09.433	10.184.48.152	10.237.26.108	TCP	66	62998 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
32	15:09:09.434	10.184.48.152	10.237.26.108	TCP	66	62999 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
34	15:09:09.439	10.237.26.108	10.184.48.152	TCP	66	80 → 62998 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=536 SACK_PERM WS=64
35	15:09:09.439	10.237.26.108	10.184.48.152	TCP	66	80 → 62999 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=536 SACK_PERM WS=64
36	15:09:09.439	10.184.48.152	10.237.26.108	TCP	54	62998 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
37	15:09:09.439	10.184.48.152	10.237.26.108	TCP	54	62999 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
38	15:09:09.439	10.184.48.152	10.237.26.108	HTTP	796	GET / HTTP/1.1
41	15:09:09.443	10.237.26.108	10.184.48.152	TCP	54	80 → 62999 [ACK] Seq=1 Ack=537 Win=6912 Len=0
42	15:09:09.444	10.237.26.108	10.184.48.152	TCP	54	80 → 62999 [ACK] Seq=1 Ack=743 Win=8000 Len=0
118	15:09:09.782	10.237.26.108	10.184.48.152	TCP	1662	80 → 62999 [ACK] Seq=1 Ack=743 Win=8000 Len=1608 [TCP segment of a reassembled PDU]
122	15:09:09.783	10.184.48.152	10.237.26.108	TCP	54	62999 → 80 [ACK] Seq=743 Ack=1609 Win=131072 Len=0
125	15:09:09.785	10.237.26.108	10.184.48.152	TCP	590	80 → 62999 [ACK] Seq=1609 Ack=743 Win=8000 Len=536 [TCP segment of a reassembled PDU]
127	15:09:09.785	10.237.26.108	10.184.48.152	TCP	1126	80 → 62999 [ACK] Seq=2145 Ack=743 Win=8000 Len=1072 [TCP segment of a reassembled PDU]
128	15:09:09.785	10.184.48.152	10.237.26.108	TCP	54	62999 → 80 [ACK] Seq=743 Ack=2145 Win=131072 Len=0
129	15:09:09.786	10.184.48.152	10.237.26.108	TCP	54	62999 → 80 [ACK] Seq=743 Ack=3217 Win=131072 Len=0
131	15:09:09.787	10.237.26.108	10.184.48.152	TCP	590	80 → 62999 [ACK] Seq=3217 Ack=743 Win=8000 Len=536 [TCP segment of a reassembled PDU]
132	15:09:09.787	10.237.26.108	10.184.48.152	HTTP/XML	493	HTTP/1.1 200 OK
133	15:09:09.787	10.184.48.152	10.237.26.108	TCP	54	62999 → 80 [ACK] Seq=743 Ack=4192 Win=131072 Len=0
135	15:09:09.806	10.184.48.152	10.237.26.108	HTTP	702	GET /act4d/media/system/js/mootools.js HTTP/1.1
136	15:09:09.807	10.184.48.152	10.237.26.108	TCP	66	63002 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
137	15:09:09.807	10.184.48.152	10.237.26.108	HTTP	701	GET /act4d/media/system/js/caption.js HTTP/1.1
138	15:09:09.809	10.237.26.108	10.184.48.152	TCP	54	80 → 62999 [ACK] Seq=4192 Ack=1279 Win=9088 Len=0
139	15:09:09.811	10.237.26.108	10.184.48.152	TCP	54	80 → 62999 [ACK] Seq=4192 Ack=1391 Win=9088 Len=0
140	15:09:09.815	10.237.26.108	10.184.48.152	TCP	66	80 → 63002 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=536 SACK_PERM WS=64
141	15:09:09.815	10.184.48.152	10.237.26.108	TCP	54	63002 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
142	15:09:09.815	10.184.48.152	10.237.26.108	HTTP	721	GET /act4d/templates/beez/css/template.css HTTP/1.1
143	15:09:09.815	10.237.26.108	10.184.48.152	TCP	54	80 → 62998 [ACK] Seq=1 Ack=537 Win=6912 Len=0

Figure 9: TCP connections to act4d.iitd.ac.in

d. HTTP Queries for indianexpress.com :

On applying an http filter for the packet trace of `www.indianexpress.com`, we see only 2 http requests generated as was the case with `www.iitd.ac.in` as they are both secured websites. Neither could we see the contents of any HTML or javascript files being transferred. This is because for secured websites (https), the data being transferred is encrypted and the contents cannot be read by someone looking at the network packets. Decrypting would require the knowledge of a public key, which is not available to the general public, and hence we only see encrypted cipher text over the TCP protocol. The HTTP requests can be seen in the image below :



No.	Time	Source	Destination	Protocol	Lengt	Info
	17:42:40.401	10.184.48.152	13.126.221.44	HTTP	1951	GET / HTTP/1.1
	17:42:40.443	13.126.221.44	10.184.48.152	HTTP	426	HTTP/1.1 301 Moved Permanently (text/html)

Figure 10: HTTP requests for indianexpress.com