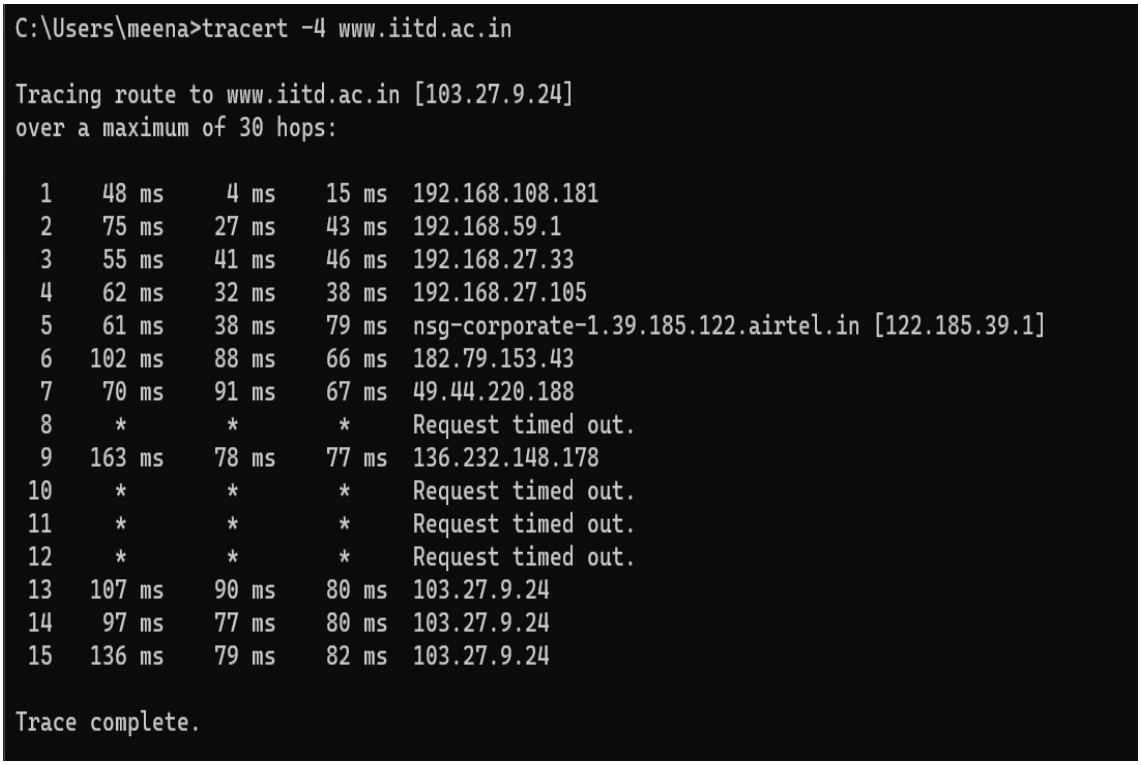
Computer Networks: Assignment 1

Students Priyadarshini Radhakrishnan (2021CS50614), Kartik Meena (2021CS50618)

Network Analysis

- a) Traceroute from mobile hotspot to www.iitd.ac.in via wifi .

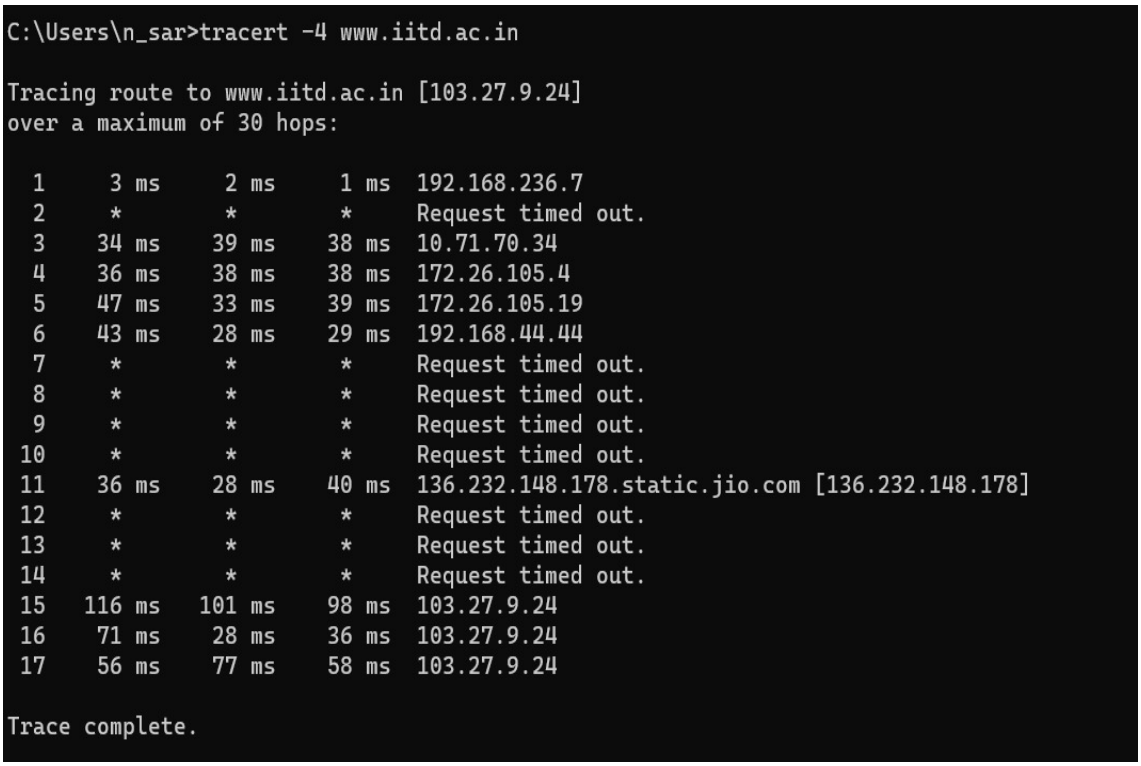


```
C:\Users\meena>tracert -4 www.iitd.ac.in

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

  1    48 ms     4 ms    15 ms  192.168.108.181
  2    75 ms    27 ms    43 ms  192.168.59.1
  3    55 ms    41 ms    46 ms  192.168.27.33
  4    62 ms    32 ms    38 ms  192.168.27.105
  5    61 ms    38 ms    79 ms  nsg-corporate-1.39.185.122.airtel.in [122.185.39.1]
  6   102 ms    88 ms    66 ms  182.79.153.43
  7    70 ms    91 ms    67 ms  49.44.220.188
  8     *        *        *     Request timed out.
  9   163 ms    78 ms    77 ms  136.232.148.178
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13   107 ms    90 ms    80 ms  103.27.9.24
 14    97 ms    77 ms    80 ms  103.27.9.24
 15   136 ms    79 ms    82 ms  103.27.9.24

Trace complete.
```



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

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

  1     3 ms     2 ms     1 ms  192.168.236.7
  2     *        *        *     Request timed out.
  3    34 ms    39 ms    38 ms  10.71.70.34
  4    36 ms    38 ms    38 ms  172.26.105.4
  5    47 ms    33 ms    39 ms  172.26.105.19
  6    43 ms    28 ms    29 ms  192.168.44.44
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11    36 ms    28 ms    40 ms  136.232.148.178.static.jio.com [136.232.148.178]
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15   116 ms   101 ms    98 ms  103.27.9.24
 16    71 ms    28 ms    36 ms  103.27.9.24
 17    56 ms    77 ms    58 ms  103.27.9.24

Trace complete.
```

- b) Curious things noted during the traceroute
  - Initially for both the partners client's default IP was IPv6 address.
  - Traceroute by default send three packets in every hop.
  - We can use the command tracert with option -4 to force the traceroute to give all the addresses in IPv4 on windows.
  - As the laptop was connected to a cellular network hotspot (Airtel 4G Network), its IP address was also present in the hops during the traceroute. This means my packet is also going through the router of Airtel Network.
  - Private IP addresses like 192.168.108.181, 192.168.59.1, 198.168.27.33 , 192.168.44.44 ,172.26.105.4, 172.26.105.19 were noted during the traceroute.
  - Also, some routers along the path did not seem to reply to the traceroute requests, as the request sent to them was timed out because Time To Live for the packet got expired.
- c) The maximum size of the packets we were able to send using ping is between 0-35300 bytes for www.iitd.ac.in. The link layers determine the maximum permitted size of the packets.

Traceroute Using Nping

- **Choice of Tool**: The tool used is **nping**. It is configured to send a single echo request and to utilize the TTL value provided by the user.
- **Design Decision**: We chose to send only one packet in the nping command instead of three packets as in traceroute because nping doesn't give individual Round Trip Time.
- **TTL Expiry Handling**:
  - When TTL is expired in transit, the packet is discarded by a router along the path.
  - Upon TTL expiry, the IP address of the router where the packet is dropped and the round trip time is displayed.
- **Handling Missing Echo Replies**:
  - In some cases, the routers might not send an Echo Reply, as the time limit would have exceeded so, "Request timed out" would be displayed.
- **Successful Packet Reach**:
  - When the Echo Request packet reaches the destination router and an Echo Reply is received, the traceroute functionality is completed.
  - Upon successful completion, the output displays the IP addresses of all transit routers, their corresponding RTT values, and a final "Trace Complete" message.

Internet architecture

- **AS Number for the IP addressess**

AS	AS Number	IP address
UTAH	17055	155.98.186.21
UCT	36982	137.158.159.192
Indian Institute of Technology	132780	103.27.9.24
Google	15169	142.250.207.196
Facebook	32934	157.240.16.35

  - In the traceroute to www.utah.edu from New York some Autonomous System like west-net-west, INTERNET2-RESEARCH-EDU, NKN-CORE-NW NKN Core Network, are encountered.
  - In the traceroute to www.uct.ac.za the last known router is TENET-1, ZA(154.114.124.1).

- In the traceroute to www.iitd.ac.in from mobile hotspot there are some AS like Reliance Jio Infocomm Limited . IN, BBIL-AP BHARTI Airtel Ltd., IN.

- **A) Table for the Number of Hopes from Different Sources to the Destination**

  - Traceroute Source is Equinix New York(NY9) IP address of the source 216.218.252.22

Destination	Number of Hopes	IP address
www.utha.edu	15	155.98.186.21
www.uct.ac.za	30	137.158.159.192
www.iitd.ac.in	17	103.27.9.24
www.google.com	11	142.250.207.196
www.facebook.com	8	157.240.16.35

  - Traceroute Source is Equinix Osaka (OS1) IP address of the source (216.218.252.58), Japan

Destination	Number of Hopes	IP address
www.utha.edu	16	155.98.186.21
www.uct.ac.za	30	137.158.159.192
www.iitd.ac.in	18	103.27.9.24
www.google.com	10	142.250.207.196
www.facebook.com	10	157.240.16.35

  - Traceroute form my Mobile Network via Wifi

Destination	Number of Hopes	IP address
www.utha.edu	29	155.98.186.21
www.uct.ac.za	30	137.158.159.192
www.iitd.ac.in	17	103.27.9.24
www.google.com	9	142.250.195.4
www.facebook.com	9	157.240.198.35

    * Special Note for the traceroute of www.uct.ac.za
      In this case, the destination did not reply, and traceroute kept incrementing the TTL, the last known router is 154.114.124.1. for all the traceroutes from different sources.

  - **Some Key points observed during the traceroute.**

    * **Effect of Geographical distance of the source from the destination on Hops**: If the traceroute sources and destinations are geographically close, it might generally result in fewer hops. This is because there are likely to be fewer network nodes and routers in between, as there will be less number of routers, gateway, and subnets to pass. However, other factors such as network coverage, traffic, and routing policies can also influence the number of hops. For example, the University of Utah is closer to New York in comparison to Osaka Japan, so traceroute from New York took fewer hops.
    * Globally dispersed networks and data centres are present in Google and Facebook. Across many traceroute providers, Google and Facebook display a significant consistency in the number of hops(usually fewer hops). This is because of dedicated pathways, good network protocol policies and optimized routing used by their provider, and these features helps them to establish a big network.

- **B) Latencies between the traceroute sources and the web servers**
  Equinix New York(NY9) IP address of the source 216.218.252.22

Destination	Range of Latenices(RTT)
www.utha.edu	51.330ms - 58.733ms
www.uct.ac.za	no packet received
www.iitd.ac.in	221.899ms - 233.809ms
www.google.com	64.457ms - 72.382ms
www.facebook.com	78.332ms - 81.868ms

Source is Equinix Osaka (OS1) IP address of the source (216.218.252.58)

Destination	Range of Latenices(RTT)
www.utha.edu	111.609ms - 113.331ms
www.uct.ac.za	no packet received
www.iitd.ac.in	256.293ms - 256.563ms
www.google.com	112.806ms - 113.006ms
www.facebook.com	140.041ms - 142.211ms

Source is cellular mobile network via wifi

Destination	Range(RTT)
www.utha.edu	306 ms - 359ms
www.uct.ac.za	no packet received
www.iitd.ac.in	69ms - 94ms
www.google.com	62ms - 79ms
www.facebook.com	30ms - 53ms

  - Yes, the latency in a traceroute can related to the number of hops, and it generally increases as the number of hops increases. This phenomenon is due to the delays introduced at each intermediate network device (router or gateway) that the packets pass through which increases the number of hops For example in the Traceroute to www.utah.com maximum hops are taken by cellular connection mobile so RTT is also maximum for this .
    Here are some of the reasons for the delays:-
    * Network Congestion and Queueing of packets
    * which Routing Protocol is used
    * time taken by the network device to process the packets
    * Load Balancing at a particular server.
    * Network topology.

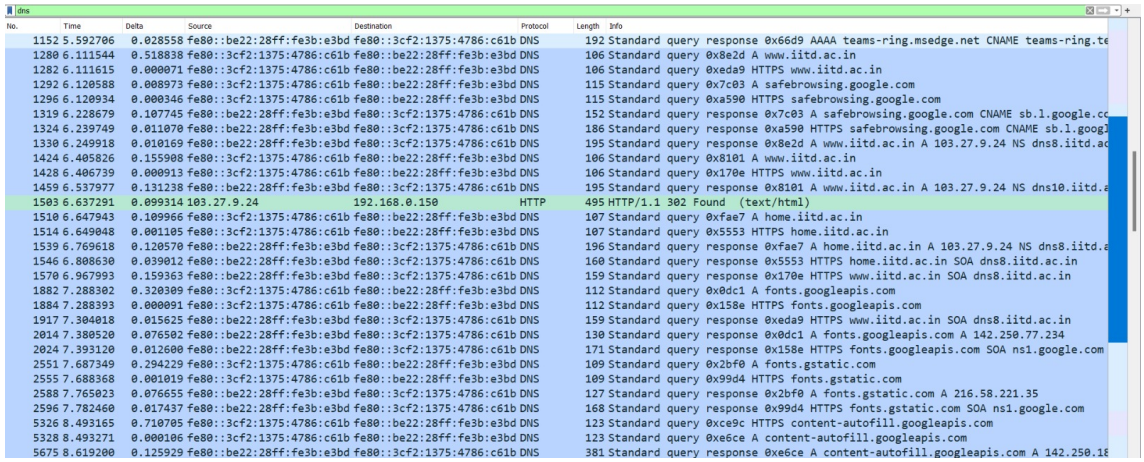
- **C)** Destination www.utah.edu, www.uct.ac.za, www.iitd.ac.in are resolved to the same IP address in traceroute from different sources
  Destinations like www.google.com and www.facebook.com shows different IP addresses when queried from different sources.
  The reason for this can be that some organizations maintain multiple data centres across the world to ensure performance, reliability, and high availability, reduce the load on the server and redundancy across different routes. When users ask queries from different locations they are directed to the nearest location resulting in different IP addresses.

- **D)** For my traceroute to www.google.com and www.facebook.com are giving different IP addresses on the traceroute from the same starting point. The pathways can appear different when traceroutes are run from the same beginning point due to the complexity of routing protocols, network congestion, server load and load balancing. This type of issue generally arises with large web servers.
  IP addresses that are located farther from the source in comparison to closer IP addresses theoretically should take a longer path.

- **E)** Greece, Sweden, and China are some of the countries whose local ISPs are not directly peered with Google and Facebook. Traceroute from this country to Google and Facebook have some other intermediate IP addresses also.

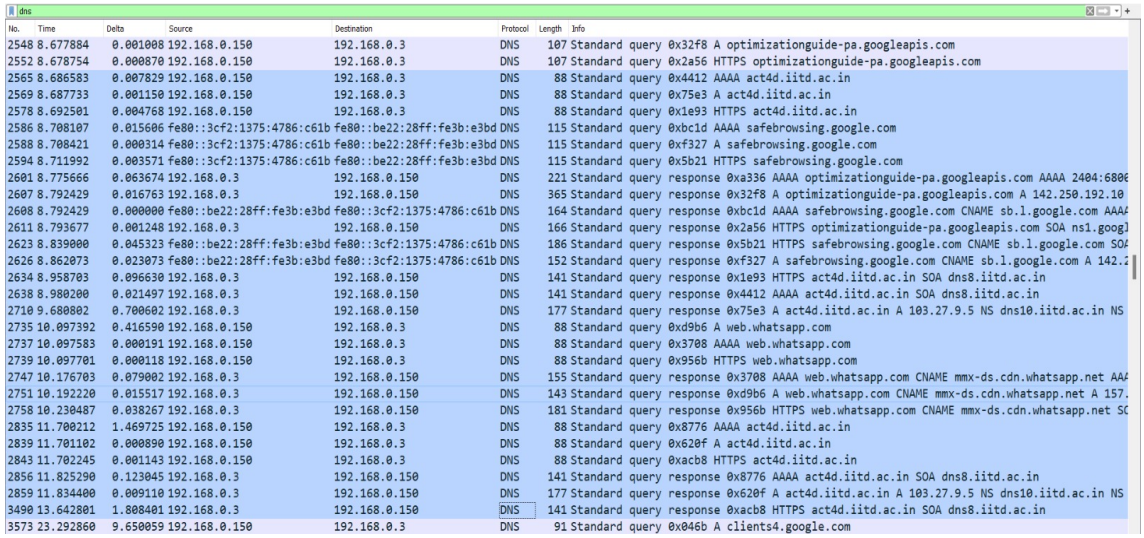
Packet Analysis

- a) **DNS Queries and Responses**:
  - **For www.iitd.ac.in**



*
  - The analysis of the captured packet trace using Wireshark revealed a time difference of 30.6 milliseconds between the initiation of the DNS request and the receipt of the corresponding DNS response.

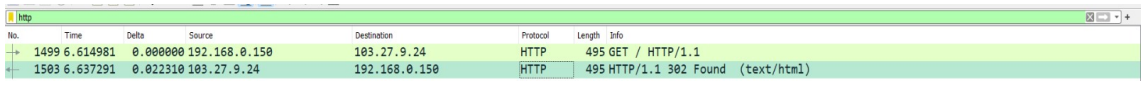
– **For http://act4d.iitd.ac.in**



*
  - The analysis for this website using Wireshark revealed a time difference of approximately 5 milliseconds between the initiation of the DNS request and the receipt of the corresponding DNS response.

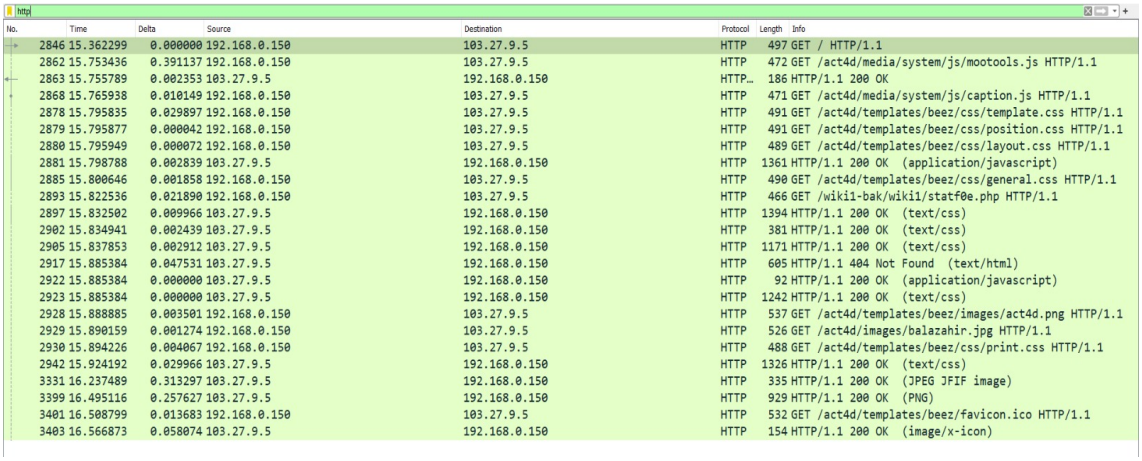
- b) **HTTP Requests in Packet Trace**:

– **For www.iitd.ac.in**



*
  - We can see that there is only one unique HTTP request identified.
  - This underlines the security controls put in place by the website to protect the privacy and accuracy of data transmission.

– **For http://act4d.iitd.ac.in**



No.	Time	Delta	Source	Destination	Protocol	Length	Info
2846	15.362299	0.000000	192.168.0.150	103.27.9.5	HTTP	497	GET / HTTP/1.1
2862	15.753436	0.391137	192.168.0.150	103.27.9.5	HTTP	472	GET /act4d/media/system/js/mootools.js HTTP/1.1
2863	15.755789	0.002353	103.27.9.5	192.168.0.150	HTTP…	186	HTTP/1.1 200 OK
2868	15.765938	0.010149	192.168.0.150	103.27.9.5	HTTP	471	GET /act4d/media/system/js/caption.js HTTP/1.1
2878	15.795835	0.029897	192.168.0.150	103.27.9.5	HTTP	491	GET /act4d/templates/beez/css/template.css HTTP/1.1
2879	15.795877	0.000042	192.168.0.150	103.27.9.5	HTTP	491	GET /act4d/templates/beez/css/position.css HTTP/1.1
2880	15.795949	0.000072	192.168.0.150	103.27.9.5	HTTP	489	GET /act4d/templates/beez/css/layout.css HTTP/1.1
2881	15.798788	0.002839	103.27.9.5	192.168.0.150	HTTP	1361	HTTP/1.1 200 OK (application/javascript)
2885	15.800646	0.001858	192.168.0.150	103.27.9.5	HTTP	490	GET /act4d/templates/beez/css/general.css HTTP/1.1
2893	15.822536	0.021890	192.168.0.150	103.27.9.5	HTTP	466	GET /wiki1-bak/wiki1/statf0e.php HTTP/1.1
2897	15.832502	0.009966	103.27.9.5	192.168.0.150	HTTP	1394	HTTP/1.1 200 OK (text/css)
2902	15.834941	0.002439	103.27.9.5	192.168.0.150	HTTP	381	HTTP/1.1 200 OK (text/css)
2905	15.837853	0.002912	103.27.9.5	192.168.0.150	HTTP	1171	HTTP/1.1 200 OK (text/css)
2917	15.885384	0.047531	103.27.9.5	192.168.0.150	HTTP	605	HTTP/1.1 404 Not Found (text/html)
2922	15.885384	0.000000	103.27.9.5	192.168.0.150	HTTP	92	HTTP/1.1 200 OK (application/javascript)
2923	15.885384	0.000000	103.27.9.5	192.168.0.150	HTTP	1242	HTTP/1.1 200 OK (text/css)
2928	15.888885	0.003501	192.168.0.150	103.27.9.5	HTTP	537	GET /act4d/templates/beez/images/act4d.png HTTP/1.1
2929	15.890159	0.001274	192.168.0.150	103.27.9.5	HTTP	526	GET /act4d/images/balazahir.jpg HTTP/1.1
2930	15.894226	0.004067	192.168.0.150	103.27.9.5	HTTP	488	GET /act4d/templates/beez/css/print.css HTTP/1.1
2942	15.924192	0.029966	103.27.9.5	192.168.0.150	HTTP	1326	HTTP/1.1 200 OK (text/css)
3331	16.237489	0.313297	103.27.9.5	192.168.0.150	HTTP	335	HTTP/1.1 200 OK (JPEG JFIF image)
3399	16.495116	0.257627	103.27.9.5	192.168.0.150	HTTP	929	HTTP/1.1 200 OK (PNG)
3401	16.508799	0.013683	192.168.0.150	103.27.9.5	HTTP	532	GET /act4d/templates/beez/favicon.ico HTTP/1.1
3403	16.566873	0.058074	103.27.9.5	192.168.0.150	HTTP	154	HTTP/1.1 200 OK (image/x-icon)

    - A total of **12** distinct HTTP requests were generated and their corresponding 12 responses were generated.
    - The provided screenshot shows that the browsing experience follows a recognizable pattern. The client starts the communication by asking for the basic HTML, then particular JavaScript files like "mototools.js" and "caption.js." The process then moves on to fetching several CSS files like "template.css," "position.css," "layout.css," and "general.css."
    - GET request for image and files in HTTP and response to it helps the browser to render complex images and files. If the HTML response contains references to external resources like images, CSS files, or scripts, the browser fetches these resources using separate HTTP requests.
  - Websites are structured using HTML, CSS and JavaScript. The browser first parses the HTML content, after which there are subsequent triggers resources like images, stylesheets, scripts and other assets. This collective effort leads to the comprehensive display of a webpage.

- c) **Investigating TCP Connections**
  - **For www.iitd.ac.in**:
    - A total of **10** distinct TCP connections were identified between the browser and the web server.
    - We identified only one unique HTTP request as the website is highly encrypted.
  - **For http://act4d.iitd.ac.in**:
    - A total of **6** distinct TCP connections were identified between the browser and the web server.
    - The number of HTTP requests is **12** which is greater than the number of TCP connections.
  - Upon applying the network filter, it was observed that several TCP connections were established between the browser and the web server.
  - Comparing the number of TCP connections with the number of HTTP requests, the number of HTTP requests was more than the number of TCP requests. This is because a single TCP connection was used to fetch multiple HTTP requests. This enhances efficiency by minimising the need to create new connections for every resource.
  - Furthermore, it was observed that some content objects were indeed fetched over the same TCP connection. For example, we noticed that some CSS files and images were fetched over a same TCP connection.

- d) On doing the HTTP filter in Wireshark, there was no or very less HTTP traffic coming from www.indianexpress.com. The reason for this could be that HTTP traffic is encrypted, so Wireshark won't be able to decipher the payload of the packets unless we have administrative rights or an SSL encryption key. We won't be able to see the content of HTML and javascript files being transferred as explained above, the content of the packets will be encrypted and we constantly get encryption alerts in the trace. This is a security feature that ensures data privacy during transmission.

225…	290.990…	2001:df4:e0…	2402:6800:7…	HTTP	356	GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?a529bad9e31cdb35 HTTP/1.1
225…	291.001…	2402:6800:7…	2001:df4:e0…	HTTP	329	HTTP/1.1 304 Not Modified