Assignment 1: Getting to Know Network Traffic

Arpit Prasad
COL334: Computer Network

August 21, 2025

1 Measurement Tools

1.1 ping

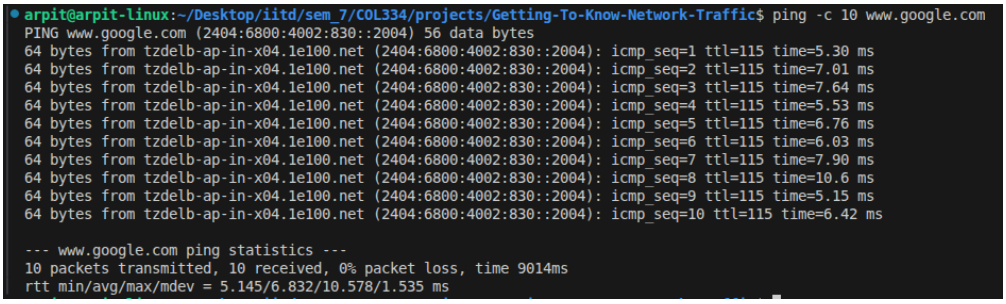

Figure 1: Ten Pings to www.google.com

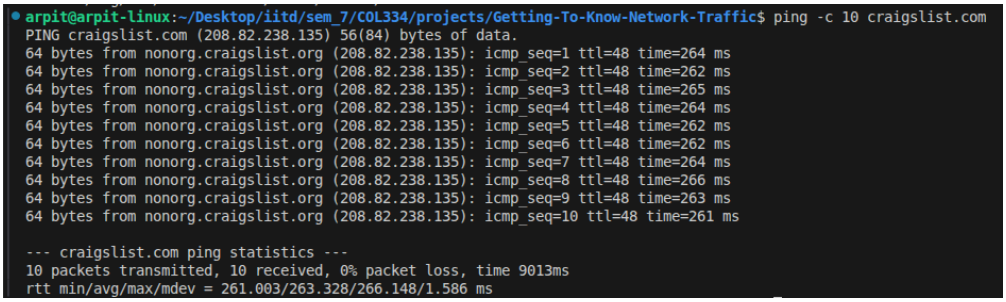

Figure 2: Ten Pings to craigslist.com

1. **Protocols Used**: Ping uses ICMP protocol which is on top of the IP protocol. It uses the Echo Request packet to the destination host and recieves Echo Reply packet from the same. It sits on the third layer of the protocol stack.

2. **Latency**:

(a) **Avg Latency of Craigslist**: 263.328 ms

(b) **Avg Latency of Google**: 6.832 ms

(c) Google's host has **smaller RTT** than Craigslist

(d) **Reason for different latencies of websites**:

i. Google has more number of hosts than Craigslist, which splits newtwork traffic

(e) **Reason for differnt latencies across pings for same website**:

i. Length of Queue for service at destination host is not constant in time and varies according to the number of user who requested for service before, we place any request (queueing of packets, at the host)

ii. Network congestion is not constant, hence each switch in the network may not have same number of packets it has to route across differnt time

iii. Differnt routes may be taken for different pings leading to different distances and hence latencies

3. using IPv6 for both websites

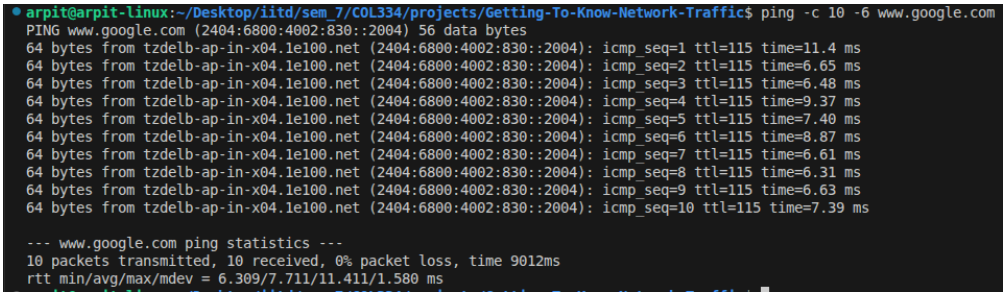

Figure 3: Ten Pings to www.google.com using IPv6

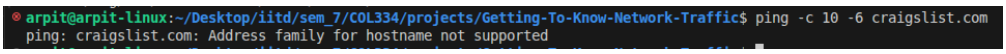

Figure 4: Error when pinging craigslist.com

(a) How to force IPv6: pass a flag -6 to force ping to follow IPv6

(b) Result: IPv6 was supported by Google's host but not by Craigslist's host

(c) Why $ping - 6$ Failed for Craigslist's host: Since IPv6 worked for Google's host, implies that my computer and Google's host both support IPv6. If a failure of Address Family support has occured it must have occured on Craigslist's server. This implies Craigslist's server does not support IPv6 addresses

4. Max size of the packets

Table 1: Max Size of Data Transmitted from Ping, practically obtained by experiment

Host	Max Message Size	ICMP Header Size	Max Total Size
www.google.com	1462 bytes	8 bytes	1470 bytes
craigslist.com	283 bytes	28 bytes	311 bytes

(a) Reason of Limit to Size: The network interfaces have a Maximum Transmission Unit for precautions (not to overload a server or a network device, which would disallow the timely servicing of all packets), that limit the packet size. Hence the bottleneck in the path is the device with the smallest MTU

(b) The packet size may also be limited by the OS

(c) For IPv6 over ethernet networks is limited ideally to 1500 bytes, but Table 1 shows what was practically achieved

(d) The difference between practical and ideal may be caused by a network device through which the packet was routed has smaller MTU.

(e) To send a larger packet size, the packet must be fragmented

1.2 traceroute

1. IPv4 Address for www.google.com : 172.217.26.36
2. IPv4 Address for craigslist.com : 208.82.238.135

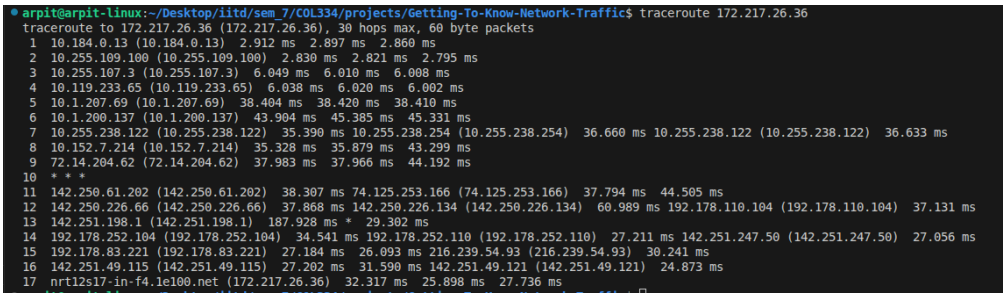

Figure 5: Trace Route of sending packet to www.google.com

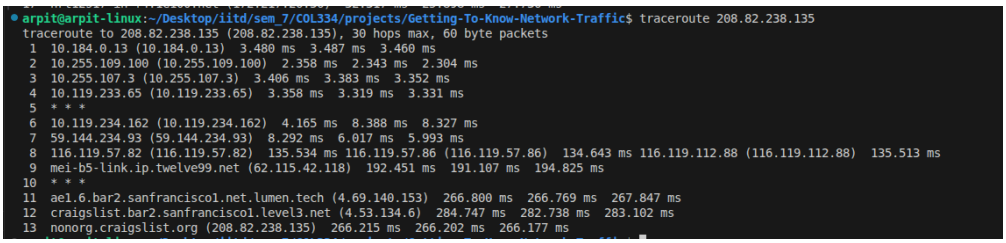

Figure 6: Trace Route of sending packet to craigslist.com

Table 2: Number of Hops for Websites

Host	Number of Hops
www.google.com	17
craigslist.com	13

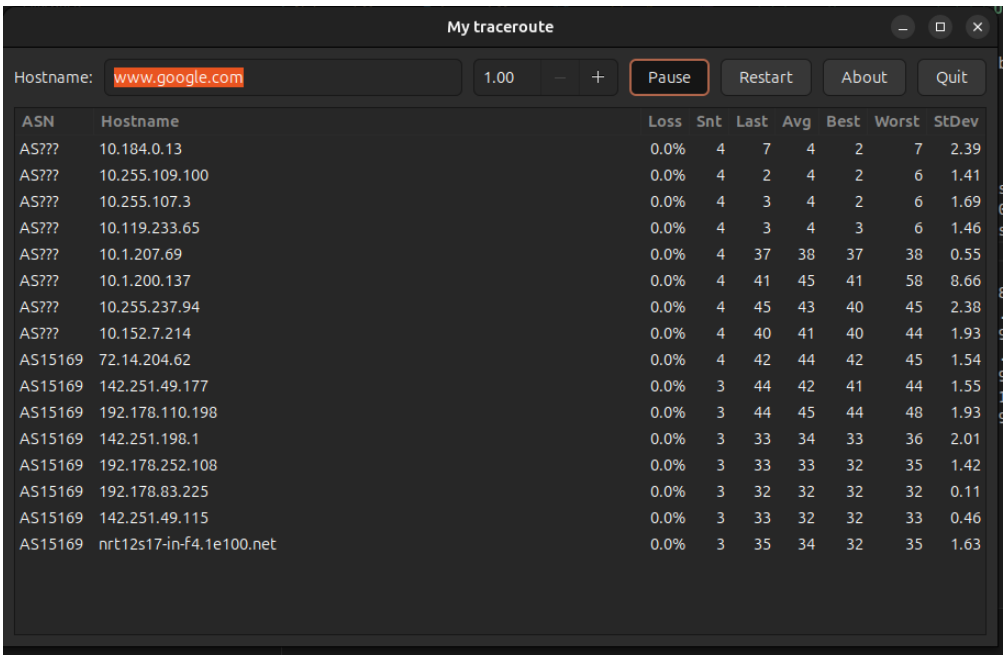

Figure 7: Autonomous System Number for each IP Address in the trace route of www.google.com (produces using mtr)

A Number of Hops:

B Explanation for "*": Some servers do not cater to traceroute packets, for security reasons and traffic control, hence do not send the Time Exceeded packet back to the source and hence, we do not have information about this node. This is represented in the traceroute by "*"

C Multiple IP Addresses for the same Hop Count: *traceroute* sends three packets for each hop. The three packets may opt for independent routes, depending on the congestion of the network. traceroute lists all the unique ip addresses of the nodes encountered by the three packets

D The following table lists the IP Addresses and their correspoding RTTs and Geolocations

(a) For the case of www.google.com, most of the network devices that relay the packet are private and hence no information is obtained about them. However we observe a delta in 9th hop, therefore we can assume that the packet has crossed the country.

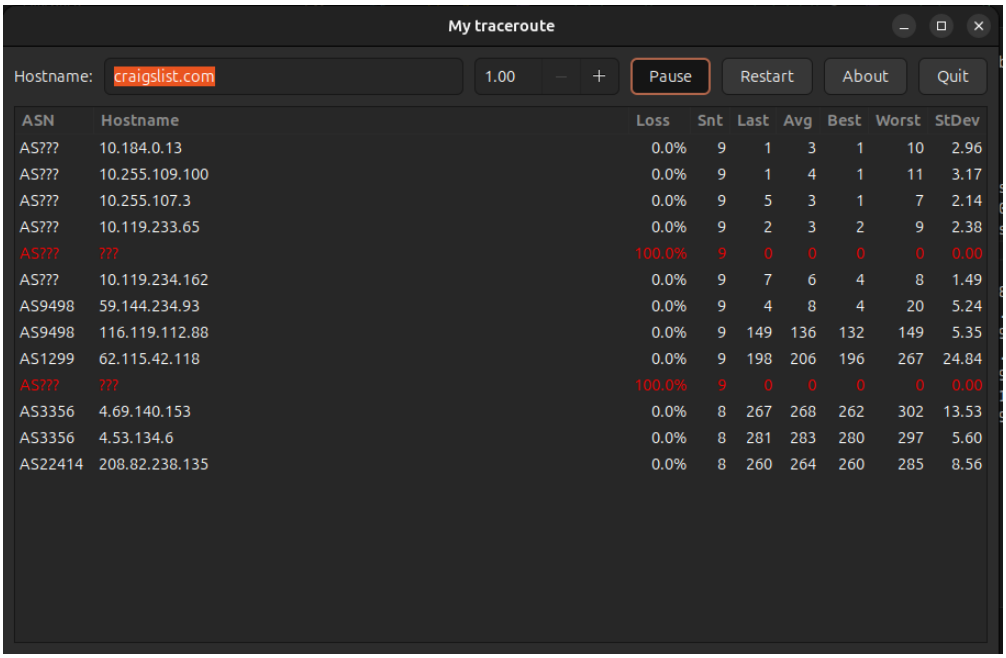

Figure 8: Autonomous System Number for each IP Address in the trace route of craigslist.com (produces using mtr)

Table 3: IP Addresses and their GeoLocations for www.google.com

Sl No	IP Address	DNS	DNS Geolocation	Maxmind Geolocation	RTT (ms)
1	10.194.0.1	NA	NA	NA 6.100	
2	10.254.238.1	NA	NA	NA	6.087
3	10.255.107.3	NA	NA	NA	21.154
4	10.119.233.65	NA	NA	NA	21.147
5	10.1.207.69	NA	NA	NA	37.188
6	10.1.200.137	NA	NA	NA	50.264
7	10.255.237.94	NA	NA	NA	115.352
8	10.152.7.214	NA	NA	NA	215.550
9	72.14.204.62	NA	NA	United States (US), North America	215.512
10	NA	NA	NA	NA	
11	142.250.214.102	NA	NA	United States (US), North America	186.456
12	142.251.77.68	NA	NA	United States (US), North America	151.676
13	142.251.197.253	NA	NA	United States (US), North America	33.512
14	142.251.247.50	NA	NA	United States (US), North America	36.570
15	192.178.83.215	NA	NA	United States (US), North America	59.573
16	142.251.49.115	NA	NA	United States (US), North America	45.122
17	172.217.26.36	nrt12s17-in-f4.1e100.net or nrt12s17-in-f36.1e100.net or tzdelb-ap-in-f4.1e100.net	Narita, Japan, Tanzania	United States (US), North America	48.186

Table 4: IP Addresses and their GeoLocations for craigslist.com

Sl No	IP Address	DNS	DNS Geolocation	Maxmind Geolocation	RTT (ms)
1	10.184.0.13	NA	NA	NA	685.733
2	10.255.109.100	NA	NA	NA	685.597
3	10.255.107.3	NA	NA	NA	685.551
4	10.119.233.65	NA	NA	NA	685.507
5	*	NA	NA	NA	*
6	10.119.234.162	NA	NA	NA	685.376
7	59.144.234.93	NA	NA	Bengaluru, Karnataka, India	5.715
8	116.119.112.88	NA	NA	India	138.551
9	62.115.42.118	mei-b5-link.ip.twelve99.net	Meridian, Mississippi, USA	France	197.050
10	*	NA	NA	NA	*
11	4.69.140.153	ae1.6.bar2.SanFrancisco1.net.lumen.tech	San Francisco, California, United States (US), North America	United States, North America	268.401
12	4.53.134.6	CRAIGSLIST.bar2.SanFrancisco1.Level3.net	San Francisco, California, United States (US), North America	San Francisco, California, United States (US), North America	270.387
13	208.82.238.135	nonorg.craigslist.org	San Francisco, California, United States (US), North America	San Francisco, California, United States (US), North America	259.620

(b) For craigslist.com : The bigger deltas are observed when there is a change in country. For eg., from Table 4, we observe that upto Bangalore the RTT was 5.77 ms but as the relay proceeded to the US, the RTT becomes signficanly higher, 197.05 ms.

Hence the data intuitively makes sense.

E Three Tier Architecture:

(a) craigslist.com : Here we observe the three tier architecture clearly. Since first the packet travels from Delhi to Bangalore (which is a 2nd tier ISP transfer), then the exchange is observed from Bangalore to France and France to San Fransico which are a 1st Tier ISP Transfer. Finally 2nd and 3rd tier transfers occur for the packet to reach craigslist.com server

(b) www.google.com : Here, we do not observe the three tier architecture clearly. Most of the transfers are through private ip addresses. From RTTs we can conclude some of these transfers are in India and the rest directly in the US. This also occurs when a collection of network devices are considered as private network and do not disclose thier actual IP Address. Google might use these private networks for data transfers, for security reasons, such as avoiding data leaks. TODO

2 Network Traffic Collection and Analysis

2.1 Traffic Capture

A Time taken for the DNS request-response to comlete: Query Time = 0.5815 and Response Time is 0.6966, time taken is **0.115**

B HTTP

(a) Number of HTTP Requests = 364 (fitler used: *http.request*)

(b) How webpages are structured: The webpage is very modular. All images are loaded one by one on the website indicating completion of download.

(c) How browsers render complex pages with multiple images and files: They render the images one at a time, since from the packet information it can be observed different times of completion of the downloads

C TCP Connection

(a) Number of TCP Connections = 31 (filter used: $tcp.flags.syn == 1 and tcp.flags.ack == 0$)

(b) Number of HTTP Conbnections==Number of TCP Connections: No, they are generally not equal, however they are related. In one TCP Connection multiple HTTP requests can be made.

(c) Content Object Fetch over same TCP Connection: Yes, some contents get fetched over the same TCP Connection. This can be supported from the fact that HTTP transfer are made with HTTP/1.1, which implies sustained TCP Connection for multiple HTTP transfers. This was verified using the filter $tcp.flags.syn == 1 and tcp.flags.ack == 0$ and the we checked the upstream flow. This showed multiple HTTP/1.1 transfers in one TCP Connection

D HTTPs packet trace

(a) http traffic there? No, there is no HTTP Traffic

(b) content transfer of HTTP and JavaScript files? and why?: There is no content tranfer of HTTP and JavaScript. HTTPs is secured data transfer, therefor the file content is encrypted and hence not visible without the key to the file. This is the reason why wireshark does not show this content

(c) dns traffic: Yes, DNS Traffic is present. DNS is required for look ups to convert web addresses to their correspoding IP Addresses.

(d) number of tcp connections logged = 25

(e) Number of HTTP Conbnectinos==Number of TCP Connections: They are not equal in this case. However the HTTPS case has smaller number of TCP Connections. A potential reason is multiplexing, allowing many HTTPS request to be sent simultaneously.

2.2 Performance Analysis

E HTTP vs HTTPs

(a) comparision of time taken for downloads: HTPP::17.132s and HTTPs::1.614 (93% faster than HTTP)

(b) Observation from the plots:

i. The download plot for https.pcap has significant throughput for download in comparision to that for http.pcap. Since the amount of data downloaded is the same, hence if the time of download reduces, this implies throughput increases.

ii. This can also be referred from the RTT plot. Since RTT is very small for most of the times that are plotted, we can infer the small download time in the case of htpps.pcap and larger download time in the case of http.pcap

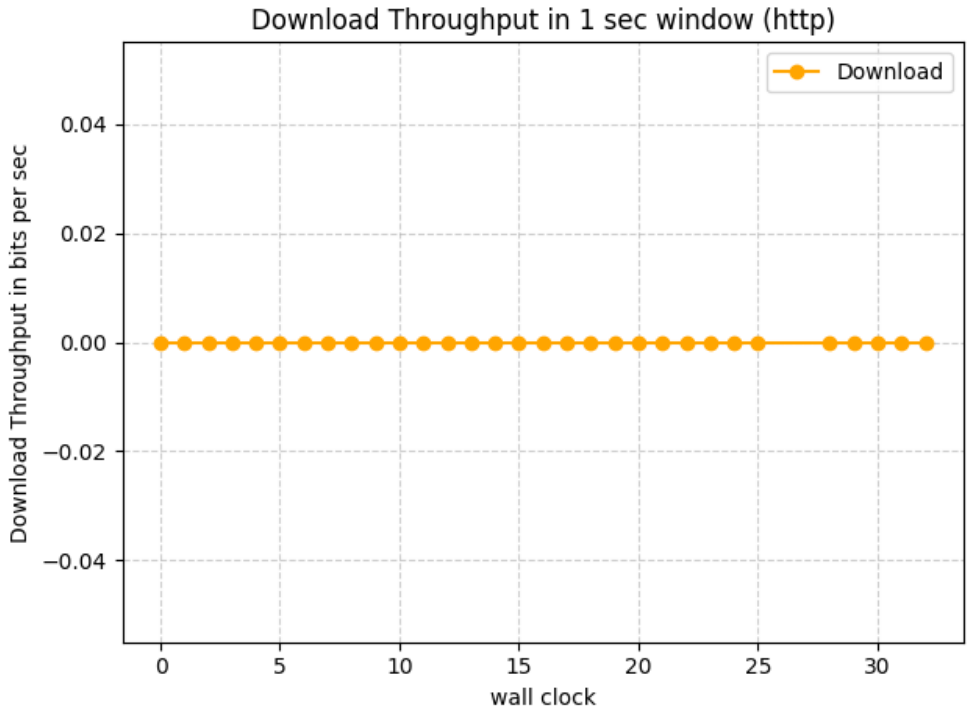

Figure 9: Download Throughput using http.pcap

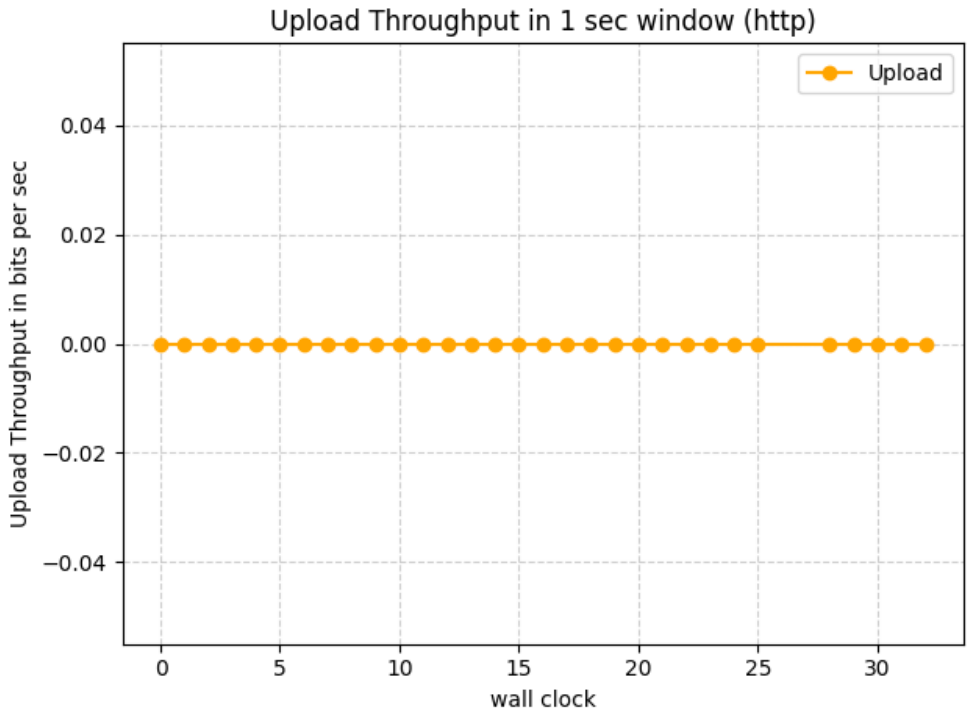

Figure 10: Upload Throughput using http.pcap

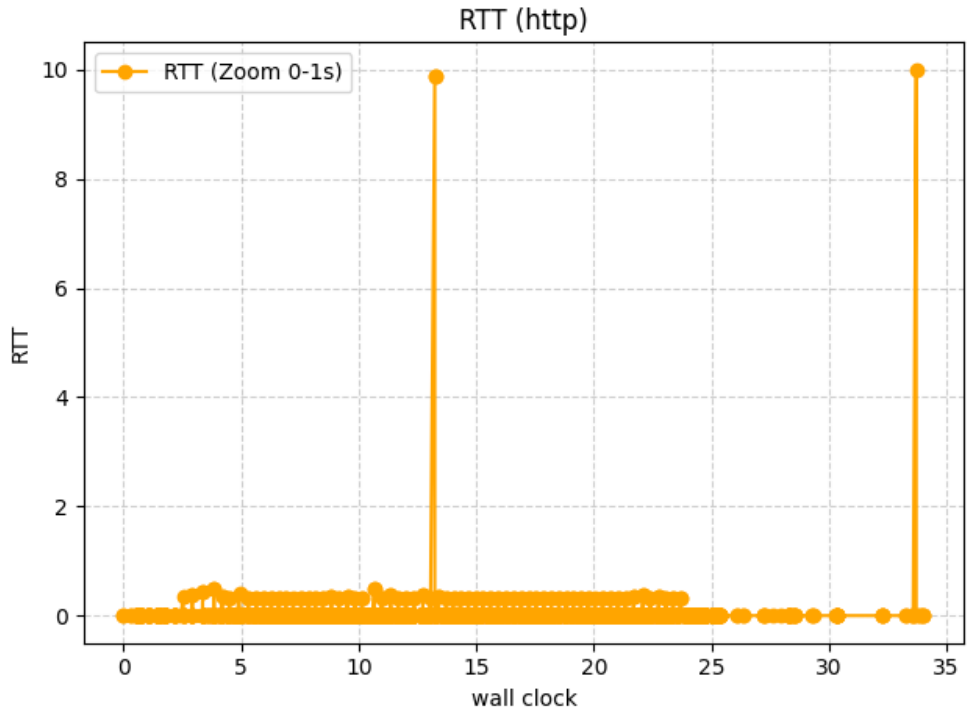

Figure 11: RTT using http.pcap

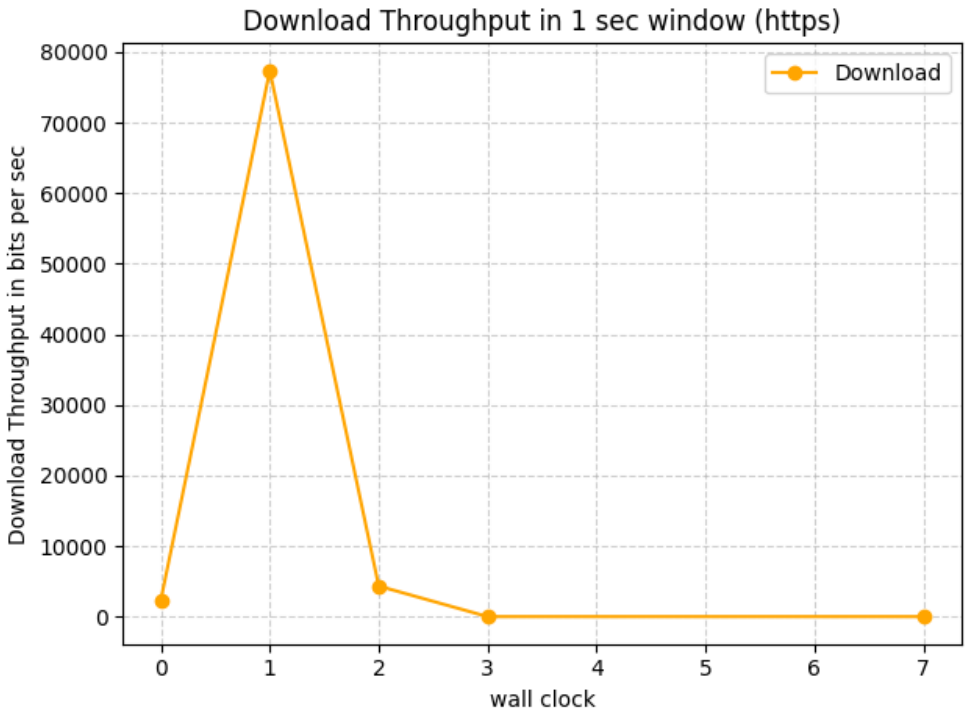

Figure 12: Download Throughput using https.pcap

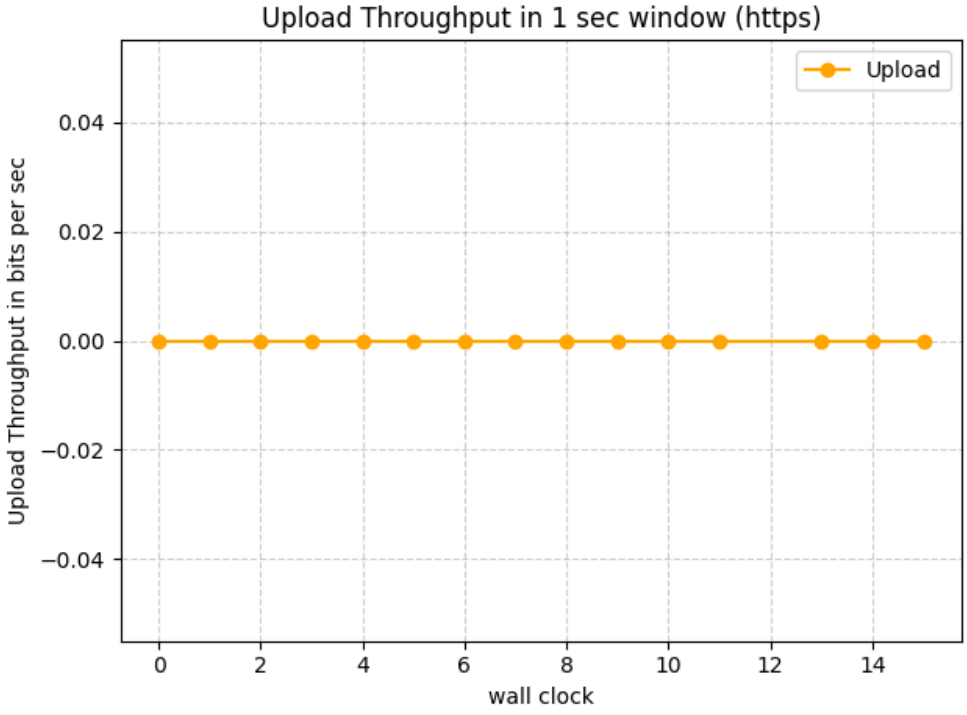

Figure 13: Upload Throughput using https.pcap

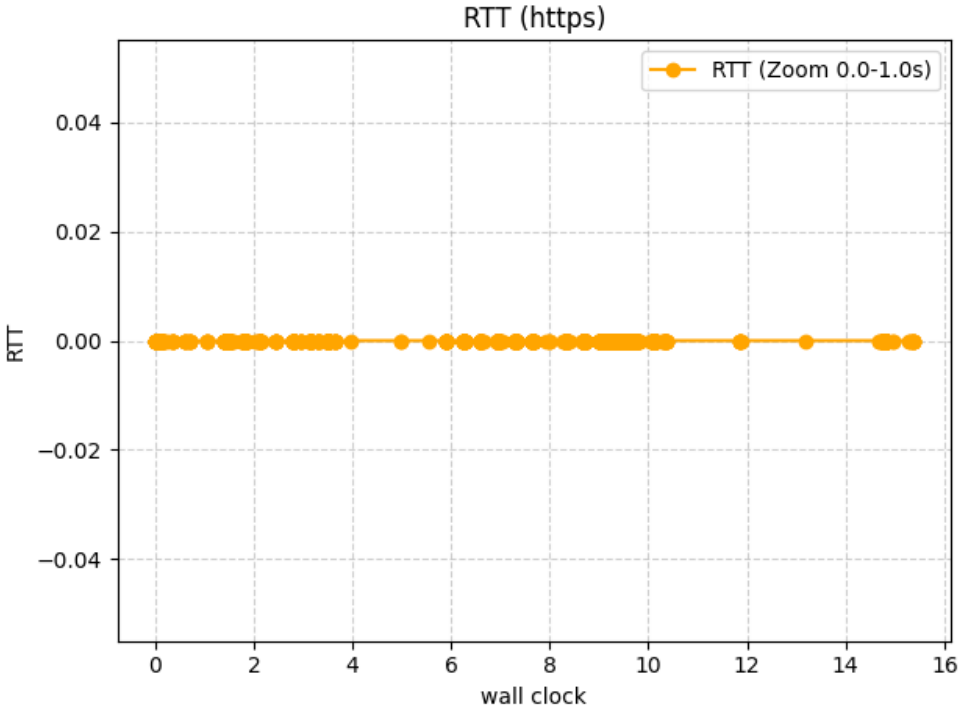

Figure 14: RTT using http.pcap