Computer Networks Assignment 1

Ayush Verma

August 30, 2022

Contents

1 Network Tools **1**
1.1 IP Address of my machine . . . 1
1.2 IP Address of different domains . . . 1
1.3 Ping Packets . . . 2
1.4 Traceroute . . . 2
1.4.1 Using Airtel Mobile Hotspot . . . 2

2 Packet Analysis **5**
2.1 DNS Task . . . 5
2.2 Iperf Task . . . 6
2.3 HTTP Task . . . 8
2.4 Ping task . . . 8
2.5 Traceroute Task . . . 10

1 Network Tools

1.1 IP Address of my machine

I used the *ifconfig* command (wlps3s0 interface) to know about the private IP Address of my machine using different providers. I observed that IP address changes on changing the ISP, this happens because the network associated with my device changed upon change of ISP.

IITD WIFI	10.184.41.17
AIRTEL MOBILE HOTSPOT	192.168.131.156

1.2 IP Address of different domains

I used the *nslookup* $<$ *domain name* $>$ to find the IP address of listed domains. I used *cat /etc/resolv.conf* to find the IP address of DNS server.
for changing DNS Server, I did following-

sudo nano /etc/resolv.conf
Added *nameserver* 8.8.8.8 at top and then I used *dig* command to ensure changes made are successful.

DNS Server	HOSTNAME	IP Address
127.0.0.53	www.google.com	142.250.199.164
127.0.0.53	www.facebook.com	157.240.16.35
8.8.8.8	www.google.com	142.250.207.196
8.8.8.8	www.facebook.com	157.240.1.35

```
sam@sam-Lenovo-Y520-15IKBN:~/Documents/Mathematics and Computing/Computer Networks$ nslookup www.google.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.207.196
Name:   www.google.com
Address: 2404:6800:4002:82b::2004

sam@sam-Lenovo-Y520-15IKBN:~/Documents/Mathematics and Computing/Computer Networks$ nslookup www.facebook.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
www.facebook.com        canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 157.240.1.35
Name:   star-mini.c10r.facebook.com
Address: 2a03:2880:f12f:83:face:b00c:0:25de
```

```
sam@sam-Lenovo-Y520-15IKBN:~/Documents/Mathematics and Computing/Computer Networks$ nslookup www.facebook.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.facebook.com        canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 157.240.16.35
Name:   star-mini.c10r.facebook.com
Address: 2a03:2880:f12f:83:face:b00c:0:25de

sam@sam-Lenovo-Y520-15IKBN:~/Documents/Mathematics and Computing/Computer Networks$ nslookup www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.199.164
Name:   www.google.com
Address: 2404:6800:4002:82b::2004
```

It was observed that the IP address changes upon changing the DNS servers. This happens because big host sites like facebook and google have various host servers (in order to reduce congestion on network and respond faster) because of which different DNS servers point to different host servers.

1.3 Ping Packets

I used ping *www.google.com* with default packet size(64 *bytes* , including header bytes) and ttl value(255). Average RTT observed for 11 packets was 41.888.

```
sam@sam-Lenovo-Y520-15IKBN:~/Documents/Mathematics and Computing/Computer Networks$ ping www.google.com
PING www.google.com (172.217.160.228) 56(84) bytes of data.
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=1 ttl=118 time=4.82 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=2 ttl=118 time=6.10 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=3 ttl=118 time=5.19 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=4 ttl=118 time=40.6 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=5 ttl=118 time=5.13 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=6 ttl=118 time=139 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=7 ttl=118 time=154 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=8 ttl=118 time=5.93 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=9 ttl=118 time=22.2 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=10 ttl=118 time=64.1 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=11 ttl=118 time=14.0 ms
^C
--- www.google.com ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10015ms
rtt min/avg/max/mdev = 4.816/41.888/154.009/52.430 ms
```

Then I changed the packet sizes and ttl values.
Command used was $ping \ < domain-name > \ -s \ < packet-size > \ -t \ < ttl-value >$

Packet size(bytes)	TTL	Average RTT(ms) for 11 packets
64	255	41.88
32	255	77.436
32	80	146.934
72	200	177.970

1.4 Traceroute

1.4.1 Using Airtel Mobile Hotspot

I used $whois < ip-address >$ to locate the ip address. **www.iitd.ac.in**

```
traceroute to www.iitd.ac.in (103.27.9.24), 30 hops max, 60 byte packets
 1  _gateway (192.168.131.212) 53.645 ms 53.574 ms 53.529 ms
 2  10.50.96.4 (10.50.96.4) 216.414 ms 216.368 ms 217.052 ms
 3  10.50.96.156 (10.50.96.156) 217.008 ms 10.50.96.200 (10.50.96.200) 216.965 ms 10.50.96.156
    (10.50.96.156) 216.922 ms
 4  * * *
 5  10.206.30.1 (10.206.30.1) 216.748 ms * 10.206.30.129 (10.206.30.129) 216.663 ms
 6  dsl-ncr-dynamic-017.24.23.125.airtelbroadband.in (125.23.24.17) 216.621 ms 204.646 ms 204.558 ms
```

```
 7  182.79.141.178 (182.79.141.178) 204.506 ms 182.79.141.180 (182.79.141.180) 183.076 ms
      116.119.61.117 (116.119.61.117) 182.980 ms
 8  49.44.220.188 (49.44.220.188) 184.571 ms 184.520 ms 184.565 ms
 9  * * *
10  136.232.148.254.static.jio.com (136.232.148.254) 184.371 ms 206.061 ms 205.974 ms
11  136.232.148.254.static.jio.com (136.232.148.254) 205.921 ms * 205.824 ms
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

IP Addresses traversed:

1. 192.168.131.212 - this is the private IP address of my smartphone
2. 10.50.96.4 - this is a private IP address on my network
3. hop 4 is blocked.
4. 49.44.220.188 and 136.232.148.254 - this is the IP address of a Reliance server

After hop 11 , there is no connection. This might beacuse IITD have blocked packets.

www.google.com

```
    traceroute to www.google.com (142.250.194.68), 30 hops max, 60 byte packets
 1  _gateway (192.168.131.212) 61.686 ms 61.619 ms 61.573 ms
 2  10.50.96.4 (10.50.96.4) 156.532 ms 156.570 ms 156.692 ms
 3  10.50.96.202 (10.50.96.202) 156.288 ms 10.50.96.154 (10.50.96.154) 156.244 ms 10.50.96.202
      (10.50.96.202) 156.198 ms
 4  * * *
 5  10.206.30.129 (10.206.30.129) 156.025 ms * 10.206.30.1 (10.206.30.1) 155.940 ms
 6  dsl-ncr-dynamic-017.24.23.125.airtelbroadband.in (125.23.24.17) 155.897 ms 85.992 ms 86.662 ms
 7  72.14.217.194 (72.14.217.194) 86.474 ms 25.828 ms 74.125.51.184 (74.125.51.184) 38.202 ms
 8  * * *
 9  216.239.56.252 (216.239.56.252) 93.144 ms 209.85.252.44 (209.85.252.44) 93.096 ms 142.251.52.214
      (142.251.52.214) 93.046 ms
10  142.251.49.121 (142.251.49.121) 92.998 ms 70.346 ms 142.251.49.115 (142.251.49.115) 70.304 ms
11  del12s03-in-f4.1e100.net (142.250.194.68) 70.211 ms 67.229 ms 55.149 ms
```

IP Addresses traversed:

1. 192.168.131.212 - this is the private IP address of my smartphone.
2. hops 2-5 - this is a private IP address on my network.
3. 72.14.217.194,this is the Public IP address of the Bharti Airtel server.
4. hops 7-11, this is the Public IP of Google.

www.facebook.com

```
    traceroute to www.facebook.com (157.240.228.35), 30 hops max, 60 byte packets
 1  _gateway (192.168.131.212) 7.990 ms 8.283 ms 8.357 ms
 2  10.50.96.4 (10.50.96.4) 194.255 ms 194.205 ms 194.214 ms
```

```
 3  10.50.96.156 (10.50.96.156) 193.683 ms 193.635 ms 193.584 ms
 4  * * *
 5  10.206.30.129 (10.206.30.129) 193.490 ms 10.206.30.1 (10.206.30.1) 193.342 ms *
 6  dsl-ncr-dynamic-017.24.23.125.airtelbroadband.in (125.23.24.17) 193.342 ms 178.619 ms dsl-ncr-
     dynamic-029.24.23.125.airtelbroadband.in (125.23.24.29) 179.012 ms
 7  * * 182.79.142.216 (182.79.142.216) 219.573 ms
 8  ae5.pr01.tir1.tfbnw.net (157.240.68.40) 219.519 ms 219.991 ms 219.459 ms
 9  po101.psw02.tir2.tfbnw.net (129.134.101.65) 219.117 ms po101.psw01.tir2.tfbnw.net (129.134.101.63)
      219.239 ms po101.psw03.tir2.tfbnw.net (129.134.101.67) 204.407 ms
10  157.240.38.123 (157.240.38.123) 204.298 ms 157.240.38.173 (157.240.38.173) 204.406 ms
    157.240.38.65 (157.240.38.65) 204.635 ms
11  edge-star-mini-shv-01-tir2.facebook.com (157.240.228.35) 194.887 ms 194.387 ms 194.335 ms
```

IP Addresses traversed:

1. 192.168.131.212 - this is the private IP address of my smartphone.
2. hops 2-5 - this is a private IP address on my network.
3. hop 6-7,this is the Public IP address of the Bharti Airtel server.
4. hops 8-11, this is the Public IP of Facebook.

Observation

1. There was no defaulting to IPv6. We Explicitly force IPv6 tracerouting. By default, the program will try to figure out the name given and automatically choose the right protocol. If resolving a host name gives both an IPv4 address and an IPv6 address, traceroute will use the IPv4 address.
2. Upon using traceroute -6 with IITD wifi for www.facebook.com(and www.google.com), it says unreachable, as IIT Delhi routers might not support IPv6.
3. Upon using traceroute -6 Personal Airtel Mobile Hotspot:

   www.google.com

```
      traceroute to www.google.com (2404:6800:4007:814::2004), 30 hops max, 80 byte packets
 1  2401:4900:30ca:6ac1:0:31:9876:2740 (2401:4900:30ca:6ac1:0:31:9876:2740) 31.546 ms 43.377 ms
     43.319 ms
 2  * * *
 3  2401:4900:0:c001::105 (2401:4900:0:c001::105) 205.364 ms 205.313 ms 205.262 ms
 4  2401:4900:0:c001::172 (2401:4900:0:c001::172) 205.211 ms 2401:4900:0:c001::17c (2401:4900:0:
     c001::17c) 205.160 ms 2401:4900:0:c001::172 (2401:4900:0:c001::172) 205.108 ms
 5  2401:4900:0:c001::179 (2401:4900:0:c001::179) 205.057 ms 2401:4900:0:c001::69b (2401:4900:0:
     c001::69b) 205.099 ms 2401:4900:0:c001::179 (2401:4900:0:c001::179) 205.047 ms
 6  2404:a800:1a00:500::15 (2404:a800:1a00:500::15) 205.277 ms 2404:a800:1a00:500::d (2404:a800:1
     a00:500::d) 204.647 ms 204.343 ms
 7  2001:4860:1:1::1944 (2001:4860:1:1::1944) 204.663 ms 204.610 ms 2001:4860:1:1::10c4
     (2001:4860:1:1::10c4) 204.173 ms
 8  2404:6800:812e::1 (2404:6800:812e::1) 204.586 ms 2404:6800:8120::1 (2404:6800:8120::1)
     204.533 ms 2404:6800:8095::1 (2404:6800:8095::1) 204.566 ms
 9  2001:4860:0:1::539c (2001:4860:0:1::539c) 204.347 ms 2001:4860:0:1::53a8 (2001:4860:0:1::53a8
     ) 203.974 ms 2001:4860:0:1::1686 (2001:4860:0:1::1686) 204.640 ms
10  2001:4860:0:11dd::2 (2001:4860:0:11dd::2) 204.489 ms 2001:4860:0:1a::3 (2001:4860:0:1a::3)
    204.126 ms 2001:4860:0:1a::2 (2001:4860:0:1a::2) 45.185 ms
11  2001:4860::9:4001:ddce (2001:4860::9:4001:ddce) 206.631 ms 2001:4860::9:4002:d27c
    (2001:4860::9:4002:d27c) 206.752 ms 2001:4860::9:4001:67bc (2001:4860::9:4001:67bc) 206.699
    ms
12  2001:4860::9:4001:163c (2001:4860::9:4001:163c) 206.345 ms 2001:4860::9:4001:67bc
    (2001:4860::9:4001:67bc) 206.648 ms 2001:4860::9:4001:b922 (2001:4860::9:4001:b922) 206.238
    ms
13  2001:4860:0:1::4a23 (2001:4860:0:1::4a23) 206.187 ms 2001:4860::9:4001:163c
    (2001:4860::9:4001:163c) 206.136 ms 2001:4860::9:4001:b923 (2001:4860::9:4001:b923) 206.509
    ms
14  2001:4860:0:1::4a23 (2001:4860:0:1::4a23) 206.035 ms maa03s36-in-x04.1e100.net
    (2404:6800:4007:814::2004) 205.932 ms 2001:4860:0:1::4a25 (2001:4860:0:1::4a25) 205.877 ms
```

2 Packet Analysis

2.1 DNS Task

Steps:

1. I connected Airtel Mobile Hotspot and used the interface wlps3s0
2. I flushed DNS cache using

   ```
   sudo systemd-resolve --flush-caches
   ```

   and verified it by

   ```
   sudo systemd-resolve --statistics
   ```

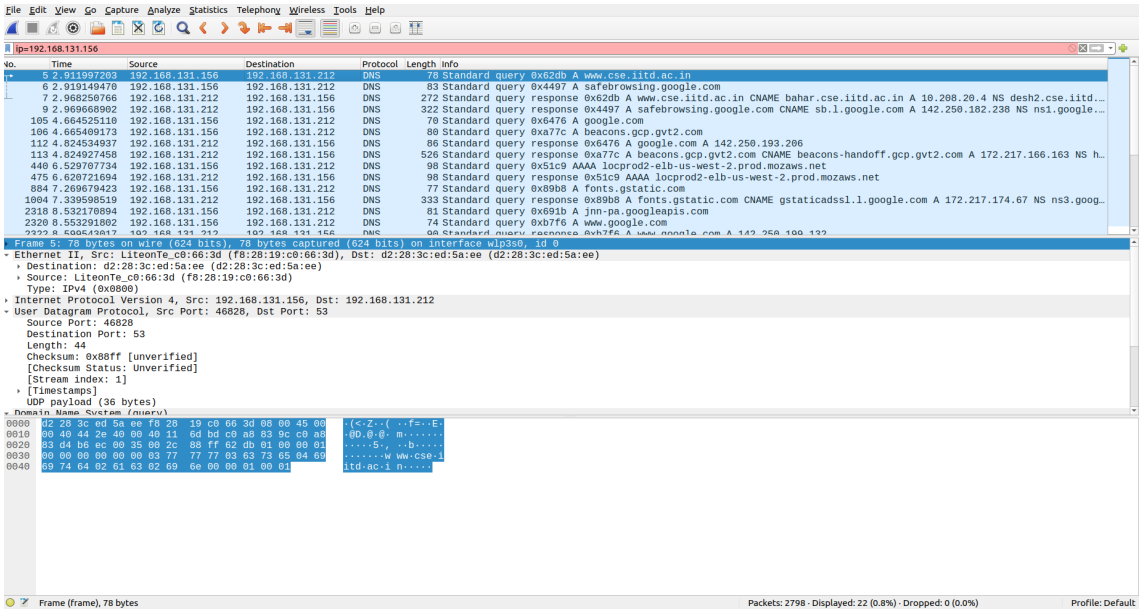
```
sam@sam-Lenovo-Y520-15IKBN:~$ sudo systemd-resolve --flush-caches
[sudo] password for sam:
sam@sam-Lenovo-Y520-15IKBN:~$ sudo systemd-resolve --statistics
DNSSEC supported by current servers: no

Transactions
Current Transactions: 0
  Total Transactions: 31996

Cache
  Current Cache Size: 0
          Cache Hits: 219
        Cache Misses: 183

DNSSEC Verdicts
              Secure: 0
            Insecure: 0
               Bogus: 0
       Indeterminate: 0
```

3. I cleared my chrome browser cache.
4. Applied filter for my IP address and then started packet capturing.
5. I immediately visited http://www.cse.iitd.ac.in and as the page shows up, I stopped packet capturing.
6. I located DNS queries and response.



Observation DNS queries and response were sent over UDP. In the Figure above , we can see that query is at No. 5 and response is at No. 7

1. **How many DNS queries are sent from your browser (host machine) to DNS Server(s)?**
   There is one DNS query sent from my browser to DNS server(192.168.131.212).

2. **How many DNS servers are involved?**
   There was only one DNS server involved.

3. **Which DNS Server replies with actual IP Address(es).**
   10.208.20.4 replies with actual IP , none were hidden.

4. **Do all DNS servers respond?**
   All the servers responds

5. **Clearly list the resource records involved in resolving the IP address of the site, mentioning, Name, value, type, TTL appropriately in the complete resolving process of this DNS conversation including query/queries and response/answer(s).**
   Resource record for DNS query :
   {Name : www.cse.iitd,ac,in ,Value : 192.168.131.156,type : A, TTL : 64}

   Resource record for DNS Response :
   {Name : www.cse.iitd,ac,in ,Value : bahar.cse.iitd.ac.in, type : CNAME, TTL : 64}
   {Name : bahar.cse.iitd,ac,in ,Value : 10.208.20.4 type : A, TTL : 64}

2.2 Iperf Task

Steps:

1. I connected Airtel Mobile Hotspot and used the interface wlps3s0.

2. Started packet capturing and then immediately opned the terminal and ran the command :

   ```
   iperf3 -u -t 10 -c ping.online.net -p 5208 -R
   ```

   ```
   sam@sam-Lenovo-Y520-15IKBN:~$ iperf3 -u -t 10 -c ping.online.net -p 5208 -R

   Connecting to host ping.online.net, port 5208
   Reverse mode, remote host ping.online.net is sending
   [  5] local 192.168.131.156 port 46786 connected to 62.210.18.40 port 5208
   [ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
   [  5]   0.00-1.00   sec   116 KBytes   947 Kbits/sec  292311607.118 ms  0/92 (0%)
   [  5]   1.00-2.00   sec   128 KBytes  1.05 Mbits/sec  404505.246 ms  0/102 (0%)
   [  5]   2.00-3.00   sec   141 KBytes  1.15 Mbits/sec  301.075 ms  0/112 (0%)
   [  5]   3.00-4.00   sec   128 KBytes  1.05 Mbits/sec  7.117 ms  0/102 (0%)
   [  5]   4.00-5.00   sec   127 KBytes  1.04 Mbits/sec  7.501 ms  0/101 (0%)
   [  5]   5.00-6.00   sec   128 KBytes  1.05 Mbits/sec  2.723 ms  0/102 (0%)
   [  5]   6.00-7.00   sec   128 KBytes  1.05 Mbits/sec  9.003 ms  0/102 (0%)
   [  5]   7.00-8.00   sec   128 KBytes  1.05 Mbits/sec  8.288 ms  0/102 (0%)
   [  5]   8.00-9.00   sec   114 KBytes   937 Kbits/sec  6.658 ms  0/91 (0%)
   [  5]   9.00-10.00  sec   128 KBytes  1.05 Mbits/sec  7.387 ms  0/102 (0%)
   - - - - - - - - - - - - - - - - - - - - - - - - -
   [ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
   [  5]   0.00-10.00  sec  1.29 MBytes  1.08 Mbits/sec  0.000 ms  0/1008 (0%)  sender
   [  5]   0.00-10.00  sec  1.24 MBytes  1.04 Mbits/sec  7.387 ms  0/1008 (0%)  receiver

   iperf Done.
   ```

   We can observe that IP for the iperf client is 62.210.18.40.

3. I immediately stopped the capturing once the iperf is done.

4. filters applied were –

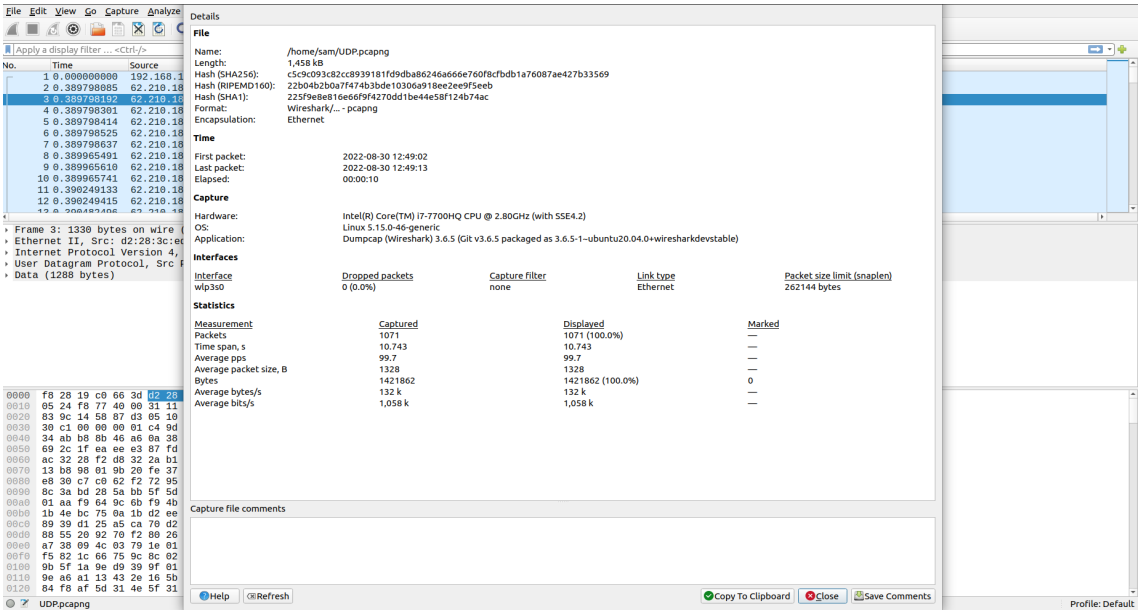
   udp or ip_addr = ¡IP address of iperf client¿

Observation

1. **How many UDP packets are exchanged in this communication between iperf3 client and remote server?**
   1071(by capture file properties)

2. **Who is sending bulk data to whom? What is the average size of the packet sent?**
   iperf client is sending bulk data to remote server. Average packet size by capture file properties are 132 Bytes.

3. **Calculate the throughput (bytes transferred per unit time) for this UDP conversation using UDP's length field. Explain how you calculated this value using Wireshark capture in this experiment along with relevant screenshots. Verify your calculation with the one done by Wireshark using "Capture File properties" as well with the one displayed by iperf3 terminal. If you observe the major difference in your calculation and with the other two listed here, comment why and how?**



The throughput measured by iperf is ,

$$1.08 \text{ Mb/sec} = 135 \text{ kB/s}$$

The throughput measured by WireShark is ,

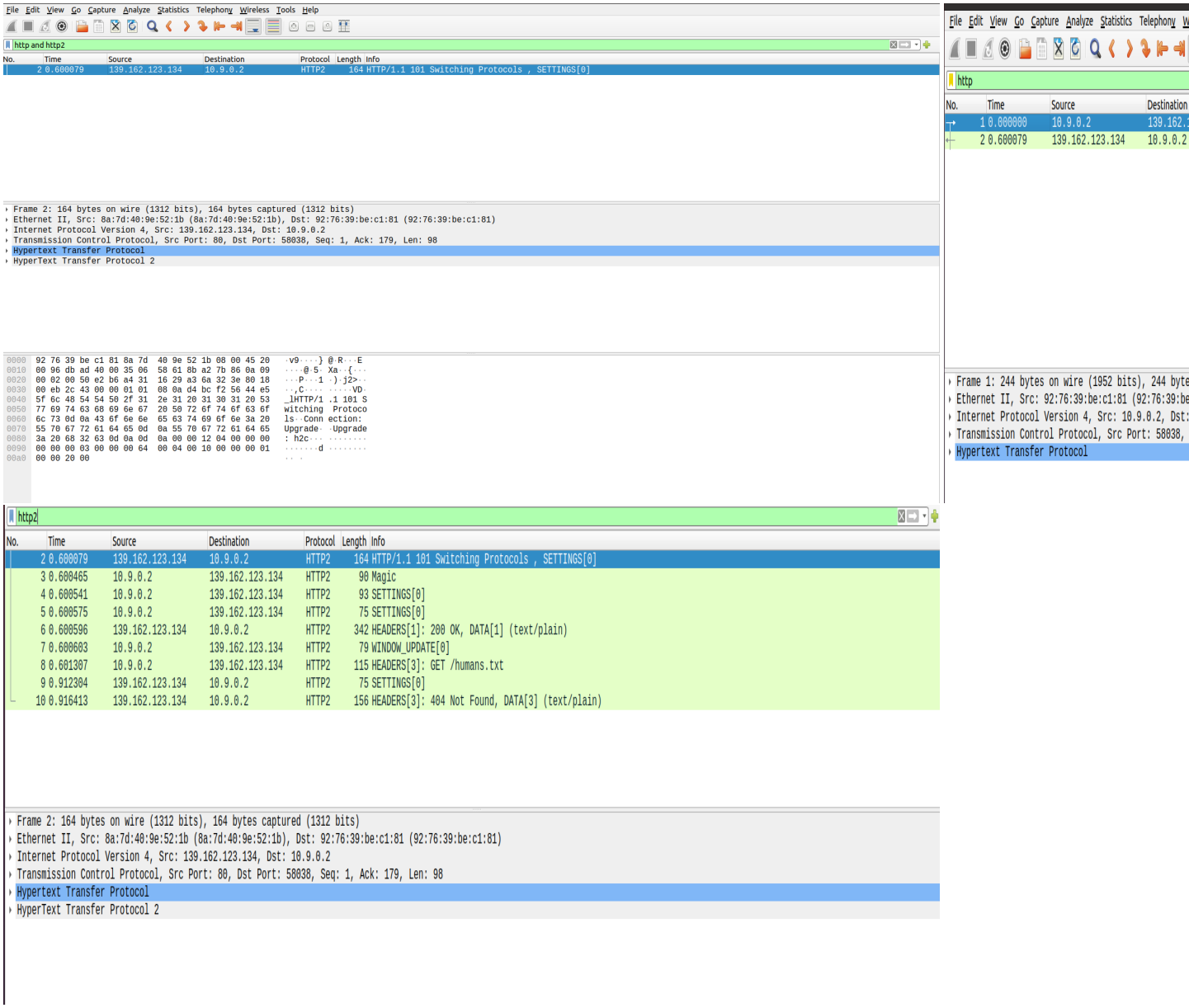
$$132 \text{ kB/s}$$

Using UDP length field,
I calculated the total length of packets captured using length field , there were 2 packets of length 46 and 1069 packets of length 1330, so total byes captured is $1,421,862 = 1421.862KB$. Now i check time field of the last packet, which is equal to $10.742711008s$. So throughput calculated is qual to

$$\frac{1421.862}{10.742711008} \; KB/s \; = \; 132.353 \; KB/s$$

This value matches with the Wireshark , but differs with iperf. This can be beacuse of delay in stopping the capturing process in wirehsark and s

2.3 HTTP Task



1. **How many HTTP/2 and HTTP/1.1 packets are present?**
   After applying the filter hhtp and http2 , only packet shows up(as shown in above figure).
   After applying only http filter 2 packet shows up
   After applying http2 filter 9 packet shows up

2. **How many HTTP/2 packets are exchanged between client and server here before the first object is fetched?**

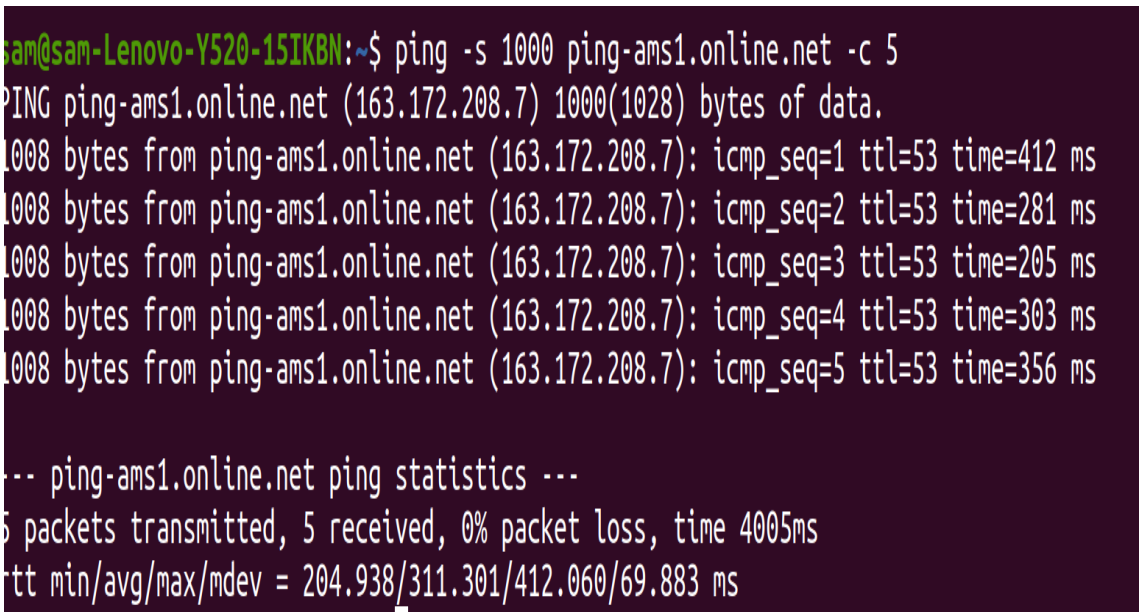
   Data is recieved at NO.6 . Before that 4 HTTP/2 packets are exchnaged between client and server.

3. **What main difference do you observe in headers of HTTP/2 packets displayed here, compared to the headers of HTTP/1.1 packets**

   The main difference we can see that HTTP/1.1 uses the plain text format , while we can see that HTTP/2 encodes its headers in binary format.

2.4 Ping task

I reduced the packet size to 1000, as for 3500 , there was 100% packet loss. I am connected to Airtel Mobile Hotspot.



1. **How many total IP packets are exchanged in the communication between your host and the remote server representing ping-ams1.online.net ?**

   After applying the icmp filter, there were 10 packets exchanged.

2. **What is the size of each ping request sent from your host to remote server?**

   From the length field, it was 1042 bytes for each ping request.

3. **. Make a table for each ping request packet sent from your host to remote, the respective field indicating it, if the request packet is fragmented or not. If packet is fragmented (add details on number of IP fragments and on each fragment), Time of sending each individual fragment/packet, length of the individual fragment/packet), time of receiving ping response, the respective field indicating if response packet is fragmented or not, if response packet is fragmented, include the number of IP fragments, total actual length of data carried by the respective fragment in respective ping request and response.**
   None of the response packet and resuest packet was fragmented.

S No.	Fragmented(Req.)	Time of Req (in s)	Time of Res.(in s)	Fragmented(Req)	Total length of data carried(in bytes)
1	No	0.000000000	0.412037617	No	992
2	No	1.001260243	1.282382643	No	992
3	No	2.002409995	2.207317331	No	992
4	No	3.003636956	3.306282091	No	992
5	No	4.005265355	4.360917974	No	992

2.5 Traceroute Task

```
sam@sam-Lenovo-Y520-15IKBN:~$ traceroute -q 5 ping-ams1.online.net 1000
traceroute to ping-ams1.online.net (163.172.208.7), 30 hops max, 1000 byte packets
 1  _gateway (192.168.131.212)  6.972 ms  6.943 ms  7.001 ms  7.135 ms  7.249 ms
 2  10.50.96.4 (10.50.96.4)  173.890 ms  173.840 ms  173.789 ms  179.421 ms  179.369 ms
 3  10.50.96.154 (10.50.96.154)  177.946 ms  177.894 ms  177.843 ms  177.793 ms 10.50.96.202 (10.50.9
6.202)  177.743 ms
 4  * * * * *
 5  10.206.30.25 (10.206.30.25)  166.063 ms * * * 10.206.30.153 (10.206.30.153)  189.720 ms
 6  dsl-ncr-dynamic-017.24.23.125.airtelbroadband.in (125.23.24.17)  189.637 ms dsl-ncr-dynamic-029.2
4.23.125.airtelbroadband.in (125.23.24.29)  189.698 ms dsl-ncr-dynamic-017.24.23.125.airtelbroadband.
in (125.23.24.17)  189.533 ms  189.482 ms dsl-ncr-dynamic-029.24.23.125.airtelbroadband.in (125.23.24
.29)  189.433 ms
 7  182.79.146.236 (182.79.146.236)  226.334 ms  226.318 ms 116.119.61.204 (116.119.61.204)  205.971
ms 116.119.61.206 (116.119.61.206)  205.880 ms 116.119.61.204 (116.119.61.204)  205.825 ms
 8  * * * * *
 9  195.154.2.103 (195.154.2.103)  237.696 ms  243.181 ms  243.123 ms  586.508 ms  580.841 ms
10  62.210.0.135 (62.210.0.135)  580.750 ms  618.348 ms  618.334 ms  618.203 ms  585.060 ms
11  grokouik.poneytelecom.eu (62.210.175.218)  574.697 ms  574.616 ms  580.171 ms  312.839 ms  312.75
3 ms
12  195.154.2.104 (195.154.2.104)  312.699 ms  312.796 ms  290.262 ms  290.492 ms  290.478 ms
13  51.158.8.27 (51.158.8.27)  290.465 ms 51.158.8.168 (51.158.8.168)  290.181 ms 51.158.8.27 (51.158
.8.27)  290.158 ms  290.144 ms  290.400 ms
14  51.158.143.1 (51.158.143.1)  290.369 ms  290.235 ms  290.344 ms 51.158.143.3 (51.158.143.3)  290.
319 ms 51.158.143.1 (51.158.143.1)  384.441 ms
15  ping-ams1.online.net (163.172.208.7)  551.612 ms  551.595 ms  551.581 ms  552.114 ms  551.590 ms
```

I reduced the packet size to 1000, as for 3500 the packets were getting blocked after few hops. I am connected to Airtel Mobi;e hotspot.

1. How many hops are involved in finding the route to this $ping - ams1.online.net$?
   It took 15 hops as can be seen in the above image.

2. **How many total IP packets are exchanged in the communication to get the final traceroute output of ping-ams1.online.net? How many of them are sent from client to remote machine (server/router) ? How many of them are sent from the remote machine (hop/server/router) to the local client ? Tabulate this with an entry for a router/server and the client too?**

   I applied the filter ICMP, as used by ping , and the number of packets displayed were - 70. All the packets were TTL expired or destination was unreachable. I tried several times over different networks but still same issue. All 70 packets were sent from the remote machine (hop/server/router) to the local client

3. **Which fields in the IP datagram always change from one datagram to the next within this series of IP packets sent by your host/client ? Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?**

   Fields which always chnages are :

   - Time to live : Due to traceroute
   - Identification : there must be unique id for packets.
   - Header Checksum : Checksum is dependent on the header, so it must change

   Fields which stays constant are

   - Version: this is beacuse we are using IPv4 for all packets
   - source IP : this is because only one source
   - Destination IP : this is beacause all packets are send to single destination
   - Length and Differentiated Services Field: this is because we are interested in ICMP packets.

   Fields which must stay constant are same same Fields which changes and filed must change are same as field which changes.