COL334
Assignment 1

Ishaan Watts
2019PH10629

Network Analysis

1. Local IP Address

IITD wifi

```
ishaanwatts@Ishaans-MacBook-Pro ~ % ipconfig getifaddr en0
10.194.7.124
```

Iphone hotspot

```
ishaanwatts@Ishaans-MacBook-Pro ~ % ipconfig getifaddr en0
172.20.10.4
```

IP address of the local machine changes by changing the ISP

2. Changing DNS

Default DNS --> 10.10.2.2
CloudFare DNS --> 1.1.1.1

a. IITD wifi

i. www.google.com

```
ishaanwatts@Ishaans-MacBook-Pro ~ % nslookup www.google.com
Server:         10.10.2.2
Address:        10.10.2.2#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.206.100

ishaanwatts@Ishaans-MacBook-Pro ~ % nslookup www.google.com 1.1.1.1
Server:         1.1.1.1
Address:        1.1.1.1#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.183.100
```

ii. www.facebook.com

```
ishaanwatts@Ishaans-MacBook-Pro ~ % nslookup www.facebook.com
Server:         10.10.2.2
Address:        10.10.2.2#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

ishaanwatts@Ishaans-MacBook-Pro ~ % nslookup www.facebook.com 1.1.1.1
Server:         1.1.1.1
Address:        1.1.1.1#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
```

b. Iphone Hotspot

i. www.google.com

```
ishaanwatts@Ishaans-MacBook-Pro ~ % nslookup www.google.com
Server:         fe80::586b:14ff:feb9:3164%6
Address:        fe80::586b:14ff:feb9:3164%6#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.193.196

ishaanwatts@Ishaans-MacBook-Pro ~ % nslookup www.google.com 1.1.1.1
Server:         1.1.1.1
Address:        1.1.1.1#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.194.4
```

ii. www.facebook.com

```
ishaanwatts@Ishaans-MacBook-Pro ~ % nslookup www.facebook.com
Server:         fe80::586b:14ff:feb9:3164%6
Address:        fe80::586b:14ff:feb9:3164%6#53

Non-authoritative answer:
www.facebook.com        canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 157.240.239.35

ishaanwatts@Ishaans-MacBook-Pro ~ % nslookup www.facebook.com 1.1.1.1
Server:         1.1.1.1
Address:        1.1.1.1#53

Non-authoritative answer:
www.facebook.com        canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 157.240.239.35
```

We observe that IP address of www.google.com changes on changing the DNS server while it remains unchanged for www.facebook.com

3. Pinging www.google.com

```
ishaanwatts@Ishaans-MacBook-Pro ~ % ping www.google.com -c 4
PING www.google.com (142.250.183.164): 56 data bytes
64 bytes from 142.250.183.164: icmp_seq=0 ttl=116 time=26.269 ms
64 bytes from 142.250.183.164: icmp_seq=1 ttl=116 time=36.388 ms
64 bytes from 142.250.183.164: icmp_seq=2 ttl=116 time=31.347 ms
64 bytes from 142.250.183.164: icmp_seq=3 ttl=116 time=37.791 ms

--- www.google.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 26.269/32.949/37.791/4.540 ms
```

a. Changing packet size

```
ishaanwatts@Ishaans-MacBook-Pro ~ % ping www.google.com -c 4 -s 32
PING www.google.com (142.250.183.164): 32 data bytes
40 bytes from 142.250.183.164: icmp_seq=0 ttl=116 time=28.660 ms
40 bytes from 142.250.183.164: icmp_seq=1 ttl=116 time=27.347 ms
40 bytes from 142.250.183.164: icmp_seq=2 ttl=116 time=28.752 ms
40 bytes from 142.250.183.164: icmp_seq=3 ttl=116 time=94.766 ms

--- www.google.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 27.347/44.881/94.766/28.806 ms
ishaanwatts@Ishaans-MacBook-Pro ~ % ping www.google.com -c 4 -s 128
PING www.google.com (142.250.183.164): 128 data bytes
76 bytes from 142.250.183.164: icmp_seq=0 ttl=116 time=29.173 ms
wrong total length 96 instead of 156
76 bytes from 142.250.183.164: icmp_seq=1 ttl=116 time=29.510 ms
wrong total length 96 instead of 156
76 bytes from 142.250.183.164: icmp_seq=2 ttl=116 time=39.510 ms
wrong total length 96 instead of 156
76 bytes from 142.250.183.164: icmp_seq=3 ttl=116 time=29.350 ms
wrong total length 96 instead of 156

--- www.google.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 29.173/31.886/39.510/4.403 ms
```

```
ishaanwatts@Ishaans-MacBook-Pro ~ % ping www.google.com -c 4 -s 69
PING www.google.com (172.217.27.196): 69 data bytes
76 bytes from 172.217.27.196: icmp_seq=0 ttl=116 time=31.848 ms
wrong total length 96 instead of 97
76 bytes from 172.217.27.196: icmp_seq=1 ttl=116 time=31.925 ms
wrong total length 96 instead of 97
76 bytes from 172.217.27.196: icmp_seq=2 ttl=116 time=32.237 ms
wrong total length 96 instead of 97
76 bytes from 172.217.27.196: icmp_seq=3 ttl=116 time=37.221 ms
wrong total length 96 instead of 97

--- www.google.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 31.848/33.308/37.221/2.264 ms
ishaanwatts@Ishaans-MacBook-Pro ~ % ping www.google.com -c 4 -s 68
PING www.google.com (172.217.27.196): 68 data bytes
76 bytes from 172.217.27.196: icmp_seq=0 ttl=116 time=36.261 ms
76 bytes from 172.217.27.196: icmp_seq=1 ttl=116 time=39.328 ms
76 bytes from 172.217.27.196: icmp_seq=2 ttl=116 time=32.344 ms
76 bytes from 172.217.27.196: icmp_seq=3 ttl=116 time=26.585 ms

--- www.google.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 26.585/33.630/39.328/4.761 ms
```

Shows wrong total length for packet size greater than 68.

b. Changing TTL values

```
ishaanwatts@Ishaans-MacBook-Pro ~ % ping www.google.com -c 4 -s 64 -m 30
PING www.google.com (142.250.183.164): 64 data bytes
72 bytes from 142.250.183.164: icmp_seq=0 ttl=116 time=29.178 ms
72 bytes from 142.250.183.164: icmp_seq=1 ttl=116 time=28.364 ms
72 bytes from 142.250.183.164: icmp_seq=2 ttl=116 time=50.040 ms
72 bytes from 142.250.183.164: icmp_seq=3 ttl=116 time=41.907 ms

--- www.google.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 28.364/37.372/50.040/9.074 ms
ishaanwatts@Ishaans-MacBook-Pro ~ % ping www.google.com -c 4 -s 64 -m 10
PING www.google.com (142.250.183.164): 64 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2

--- www.google.com ping statistics ---
4 packets transmitted, 0 packets received, 100.0% packet loss
ishaanwatts@Ishaans-MacBook-Pro ~ % ping www.google.com -c 4 -s 64 -m 20
PING www.google.com (142.250.183.164): 64 data bytes
72 bytes from 142.250.183.164: icmp_seq=0 ttl=116 time=32.075 ms
72 bytes from 142.250.183.164: icmp_seq=1 ttl=116 time=32.095 ms
72 bytes from 142.250.183.164: icmp_seq=2 ttl=116 time=32.076 ms
72 bytes from 142.250.183.164: icmp_seq=3 ttl=116 time=33.308 ms

--- www.google.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 32.075/32.389/33.308/0.531 ms
```

```
ishaanwatts@Ishaans-MacBook-Pro ~ % ping www.google.com -c 4 -s 64 -m 15
PING www.google.com (142.250.183.164): 64 data bytes
72 bytes from 142.250.183.164: icmp_seq=0 ttl=116 time=31.883 ms
72 bytes from 142.250.183.164: icmp_seq=1 ttl=116 time=32.010 ms
72 bytes from 142.250.183.164: icmp_seq=2 ttl=116 time=32.124 ms
72 bytes from 142.250.183.164: icmp_seq=3 ttl=116 time=32.158 ms

--- www.google.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 31.883/32.044/32.158/0.108 ms
ishaanwatts@Ishaans-MacBook-Pro ~ % ping www.google.com -c 4 -s 64 -m 12
PING www.google.com (142.250.183.164): 64 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2

--- www.google.com ping statistics ---
4 packets transmitted, 0 packets received, 100.0% packet loss
ishaanwatts@Ishaans-MacBook-Pro ~ % ping www.google.com -c 4 -s 64 -m 13
PING www.google.com (142.250.183.164): 64 data bytes
72 bytes from 142.250.183.164: icmp_seq=0 ttl=116 time=31.658 ms
72 bytes from 142.250.183.164: icmp_seq=1 ttl=116 time=40.339 ms
72 bytes from 142.250.183.164: icmp_seq=2 ttl=116 time=42.860 ms
72 bytes from 142.250.183.164: icmp_seq=3 ttl=116 time=31.994 ms

--- www.google.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 31.658/36.713/42.860/4.969 ms
```

Shows request timeout for TTL value less than 13

4. Traceroute using multiple ISPs

    a. IITD wifi

        i. www.iitd.ac.in

```
ishaanwatts@Ishaans-MacBook-Pro ~ % traceroute www.iitd.ac.in
traceroute to www.iitd.ac.in (10.10.211.212), 64 hops max, 52 byte packets
 1  10.194.0.14 (10.194.0.14)  5.520 ms  6.379 ms  2.835 ms
 2  10.254.238.1 (10.254.238.1)  2.777 ms  3.403 ms  2.983 ms
 3  10.254.236.10 (10.254.236.10)  4.239 ms
    10.254.236.18 (10.254.236.18)  3.158 ms  3.314 ms
 4  www.iitd.ac.in (10.10.211.212)  2.690 ms  2.769 ms  2.722 ms
```

Able to route to this site.

        ii. www.google.com

```
ishaanwatts@Ishaans-MacBook-Pro ~ % traceroute -m 30 www.google.com
traceroute to www.google.com (216.58.221.36), 30 hops max, 52 byte packets
 1  10.194.0.14 (10.194.0.14)  3.357 ms  2.869 ms  3.332 ms
 2  10.254.238.5 (10.254.238.5)  3.834 ms  8.123 ms  3.029 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  *traceroute: sendto: Can't assign requested address
traceroute: wrote www.google.com 52 chars, ret=-1
 *traceroute: sendto: Can't assign requested address
traceroute: wrote www.google.com 52 chars, ret=-1
 *
traceroute: sendto: Can't assign requested address
23 traceroute: wrote www.google.com 52 chars, ret=-1
 *traceroute: sendto: Can't assign requested address
traceroute: wrote www.google.com 52 chars, ret=-1
 *traceroute: sendto: Can't assign requested address
traceroute: wrote www.google.com 52 chars, ret=-1
 *
traceroute: sendto: Can't assign requested address
24 traceroute: wrote www.google.com 52 chars, ret=-1
 *traceroute: sendto: Can't assign requested address
traceroute: wrote www.google.com 52 chars, ret=-1
```

iii. www.facebook.com

```
ishaanwatts@Ishaans-MacBook-Pro ~ % traceroute -m 30 www.facebook.com
traceroute to star-mini.c10r.facebook.com (157.240.16.35), 30 hops max, 52 byte packets
 1  10.194.0.14 (10.194.0.14)  3.623 ms  2.903 ms  2.894 ms
 2  10.254.238.5 (10.254.238.5)  3.117 ms  2.979 ms  3.208 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
traceroute: sendto: Can't assign requested address
30 traceroute: wrote star-mini.c10r.facebook.com 52 chars, ret=-1
 * * *
```

Not able to route to facebook and google using IITD wifi

b. IPhone Hotspot

i. www.iitd.ac.in

```
ishaanwatts@Ishaans-MacBook-Pro ~ % traceroute -m 30 www.iitd.ac.in
traceroute to www.iitd.ac.in (103.27.9.24), 30 hops max, 52 byte packets
 1  172.20.10.1 (172.20.10.1)  10.807 ms  4.205 ms  5.464 ms
 2  10.206.31.1 (10.206.31.1)  39.878 ms  28.580 ms  25.693 ms
 3  * * *
 4  10.206.252.229 (10.206.252.229)  59.022 ms *  58.250 ms
 5  125.21.187.189 (125.21.187.189)  49.744 ms  29.872 ms  25.528 ms
 6  182.79.142.236 (182.79.142.236)  81.991 ms
    182.79.189.227 (182.79.189.227)  124.497 ms
    182.79.239.199 (182.79.239.199)  87.768 ms
 7  49.44.220.188 (49.44.220.188)  84.294 ms  72.642 ms
    49.44.129.53 (49.44.129.53)  92.707 ms
 8  * * *
 9  136.232.148.254.static.jio.com (136.232.148.254)  98.637 ms  102.508 ms *
10  * 136.232.148.254.static.jio.com (136.232.148.254)  135.680 ms  91.969 ms
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

ii. www.google.com

```
ishaanwatts@Ishaans-MacBook-Pro ~ % traceroute -m 30 www.google.com
traceroute to www.google.com (142.250.193.196), 30 hops max, 52 byte packets
 1  172.20.10.1 (172.20.10.1)  12.937 ms  6.932 ms  2.980 ms
 2  10.206.31.1 (10.206.31.1)  57.080 ms  24.572 ms  24.613 ms
 3  * * *
 4  10.206.254.165 (10.206.254.165)  164.804 ms *  347.283 ms
 5  125.21.187.185 (125.21.187.185)  33.609 ms  34.246 ms  49.478 ms
 6  142.250.161.56 (142.250.161.56)  46.912 ms  31.122 ms  30.958 ms
 7  * * *
 8  142.251.76.200 (142.251.76.200)  55.076 ms
    142.251.52.228 (142.251.52.228)  31.288 ms  71.151 ms
 9  142.251.54.97 (142.251.54.97)  47.283 ms
    108.170.251.108 (108.170.251.108)  58.914 ms
    142.251.54.97 (142.251.54.97)  71.058 ms
10  del11s17-in-f4.1e100.net (142.250.193.196)  87.012 ms
    74.125.244.193 (74.125.244.193)  45.067 ms  89.066 ms
```

iii. www.facebook.com

```
ishaanwatts@Ishaans-MacBook-Pro ~ % traceroute -m 30 www.facebook.com
traceroute to star-mini.c10r.facebook.com (157.240.198.35), 30 hops max, 52 byte packets
 1  172.20.10.1 (172.20.10.1)  7.854 ms  6.602 ms  3.428 ms
 2  10.206.31.1 (10.206.31.1)  50.607 ms  36.052 ms  27.021 ms
 3  * * *
 4  10.206.252.229 (10.206.252.229)  31.361 ms *  76.700 ms
 5  125.21.187.189 (125.21.187.189)  39.060 ms  38.203 ms  56.037 ms
 6  ae20.pr01.del1.tfbnw.net (157.240.64.120)  50.060 ms  76.206 ms  49.737 ms
 7  po101.psw01.del1.tfbnw.net (157.240.50.155)  31.020 ms
    po101.psw04.del1.tfbnw.net (157.240.50.159)  30.992 ms
    po101.psw02.del1.tfbnw.net (74.119.77.215)  26.963 ms
 8  157.240.38.171 (157.240.38.171)  35.163 ms
    173.252.67.181 (173.252.67.181)  31.943 ms
    157.240.38.161 (157.240.38.161)  48.611 ms
 9  edge-star-mini-shv-01-del1.facebook.com (157.240.198.35)  31.196 ms  29.195 ms  29.804 ms
```

IPhone hotspot was able to traceroute to google and facebook but not iitd.ac.in

Forcing to use IPv6 instead of IPv4

i. www.google.com

```
ishaanwatts@Ishaans-MacBook-Pro ~ % traceroute6 -m 30 www.google.com
traceroute6 to www.google.com (2404:6800:4002:81c::2004) from 2401:4900:2e86:bb7c:c995:24c:668c:b
74a, 30 hops max, 12 byte packets
 1  2401:4900:2e86:bb7c:7054:4adc:b31a:8ac4  6.644 ms  5.744 ms  5.425 ms
 2  2401:4900:2e86:bb7c:0:65:610b:e240  36.933 ms  28.640 ms  40.198 ms
 3  * * *
 4  2401:4900:0:c000::1  65.948 ms  28.286 ms  29.328 ms
 5  2401:4900:0:c001::ff  24.912 ms  29.103 ms  26.502 ms
 6  2404:a800:1a00:803::65  28.133 ms  44.234 ms  39.928 ms
 7  2404:a800::207  80.820 ms  55.443 ms  65.819 ms
 8  2001:4860:1:1::194a  36.858 ms  31.478 ms  40.037 ms
 9  2404:6800:810d::1  36.099 ms
    2404:6800:812c::1  23.863 ms
    2404:6800:8172::1  30.288 ms
10  2001:4860:0:1::5504  28.641 ms
    2001:4860:0:1::15e  33.589 ms
    2001:4860:0:1::538a  55.717 ms
11  2001:4860:0:1::5501  27.588 ms
    2001:4860:0:1::54ff  29.317 ms
    2001:4860:0:11de::c  31.900 ms
12  del11s17-in-x04.1e100.net  26.758 ms
    2001:4860::1c:4001:314a  29.761 ms
    2001:4860:0:1a::1  33.331 ms
```

ii. www.facebook.com

```
ishaanwatts@Ishaans-MacBook-Pro ~ % traceroute6 -m 30 www.facebook.com
traceroute6 to star-mini.c10r.facebook.com (2a03:2880:f144:181:face:b00c:0:25de) from 2401:4
0:2e86:bb7c:c995:24c:668c:b74a, 30 hops max, 12 byte packets
 1  2401:4900:2e86:bb7c:7054:4adc:b31a:8ac4  4.834 ms  6.850 ms  6.146 ms
 2  2401:4900:2e86:bb7c:0:65:610b:e240  27.868 ms  36.166 ms  28.198 ms
 3  * * *
 4  2401:4900:0:c000::5  46.489 ms  26.129 ms  24.971 ms
 5  2401:4900:0:c001::34d  25.005 ms  29.168 ms  31.595 ms
 6  2404:a800:1a00:803::6d  27.920 ms  73.407 ms  48.416 ms
 7  2404:a800::207  34.560 ms  36.869 ms  42.506 ms
 8  ae20.pr04.del1.tfbnw.net  43.774 ms  31.043 ms  30.022 ms
 9  po104.psw02.del1.tfbnw.net  28.717 ms
    po104.psw01.del1.tfbnw.net  39.250 ms
    po104.psw03.del1.tfbnw.net  27.355 ms
10  po8.msw1ah.02.del1.tfbnw.net  27.317 ms
    po3.msw1aq.02.del1.tfbnw.net  29.926 ms
    po2.msw1ad.02.del1.tfbnw.net  32.897 ms
11  edge-star-mini6-shv-02-del1.facebook.com  29.764 ms  30.119 ms  32.745 ms
```

iii. www.iitd.ac.in

```
ishaanwatts@Ishaans-MacBook-Pro ~ % traceroute6 -m 30 www.iitd.ac.in
traceroute6: nodename nor servname provided, or not known
```

Not able to use IPv6 with www.iitd.ac.in

Forcing to use other routers

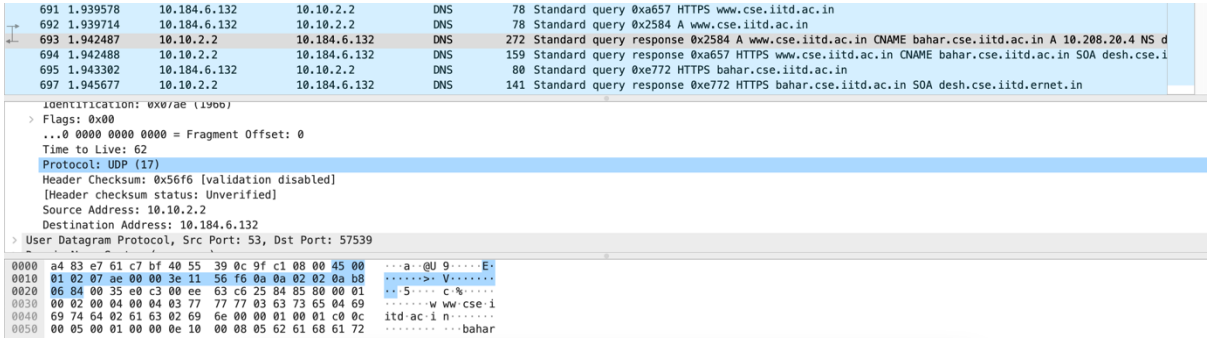
```
ishaanwatts@Ishaans-MacBook-Pro ~ % traceroute -m 30 -I www.google.com
traceroute to www.google.com (142.250.193.196), 30 hops max, 72 byte packets
 1  172.20.10.1 (172.20.10.1)  15.045 ms  7.888 ms  6.268 ms
 2  10.206.31.1 (10.206.31.1)  52.065 ms  27.317 ms  23.533 ms
 3  * * *
 4  10.206.252.229 (10.206.252.229)  90.989 ms *  164.695 ms
 5  125.21.187.189 (125.21.187.189)  47.734 ms  49.850 ms  41.996 ms
 6  72.14.222.116 (72.14.222.116)  35.399 ms  30.223 ms  29.844 ms
 7  209.85.250.11 (209.85.250.11)  53.134 ms  34.712 ms  42.678 ms
 8  142.251.54.97 (142.251.54.97)  37.665 ms  63.967 ms  55.165 ms
 9  del11s17-in-f4.1e100.net (142.250.193.196)  42.523 ms  49.649 ms  83.443 ms
```

Some * * * are resolved

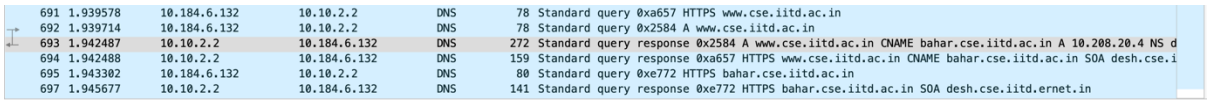
Packet Analysis

DNS Task 1

1. DNS query and response messages sent over UDP

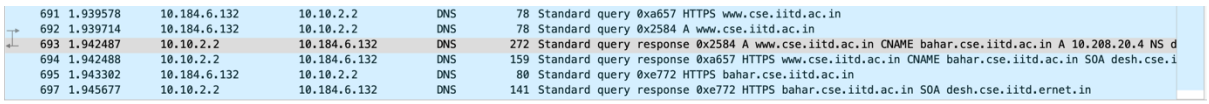


2. 3 queries are sent from my browser to DNS servers as seen in the screenshot



3. 1 DNS server is involved (10.10.2.2) as seen in above screenshot

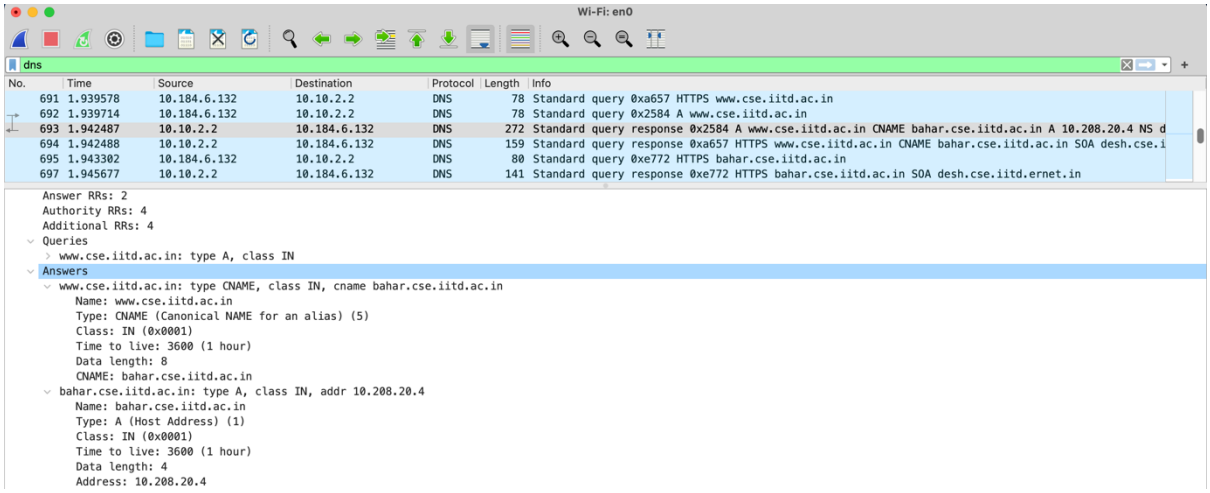
4. DNS server 10.10.2.2 returns the IP Address (693)

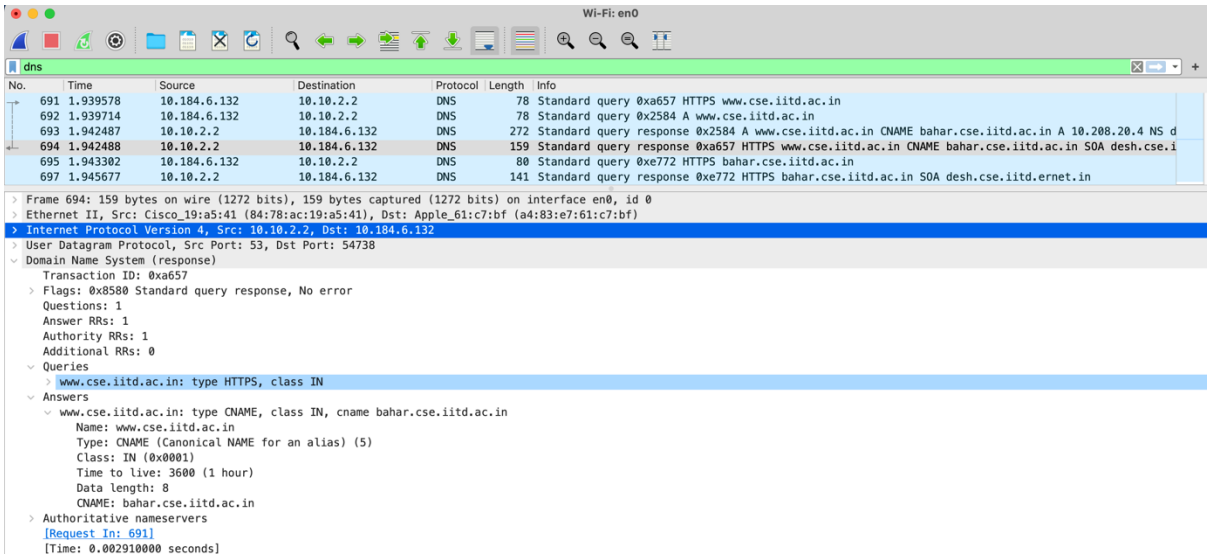



```
ishaanwatts@Ishaans-MacBook-Pro ~ % nslookup www.cse.iitd.ac.in
Server:         10.10.2.2
Address:        10.10.2.2#53

www.cse.iitd.ac.in      canonical name = bahar.cse.iitd.ac.in.
Name:   bahar.cse.iitd.ac.in
Address: 10.208.20.4

ishaanwatts@Ishaans-MacBook-Pro ~ %
```

5. No only one server responds i.e., 10.10.2.2

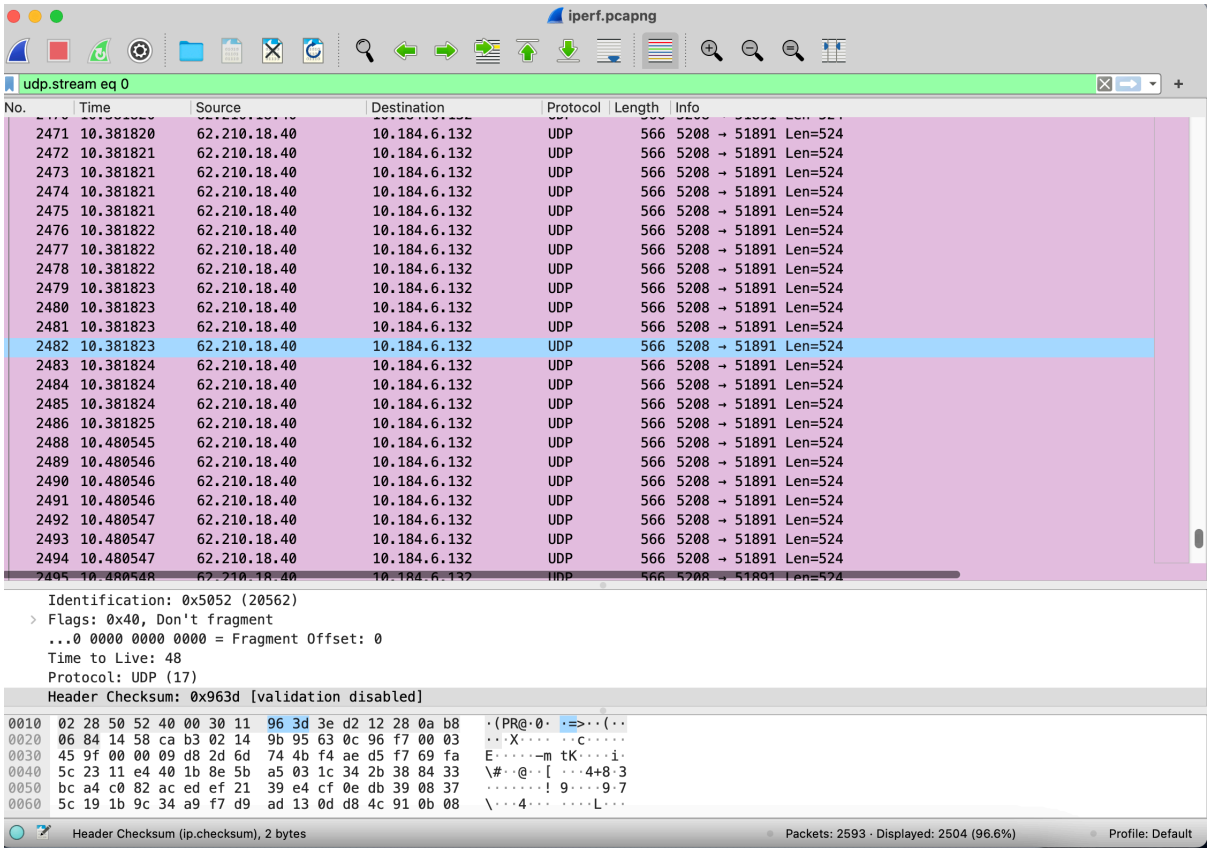
6. Resource records involved in resolving the IP address of the site, mentioning, Name, value, type, TTL appropriately in the complete resolving process of this DNS conversation including query/queries and response/answer(s).

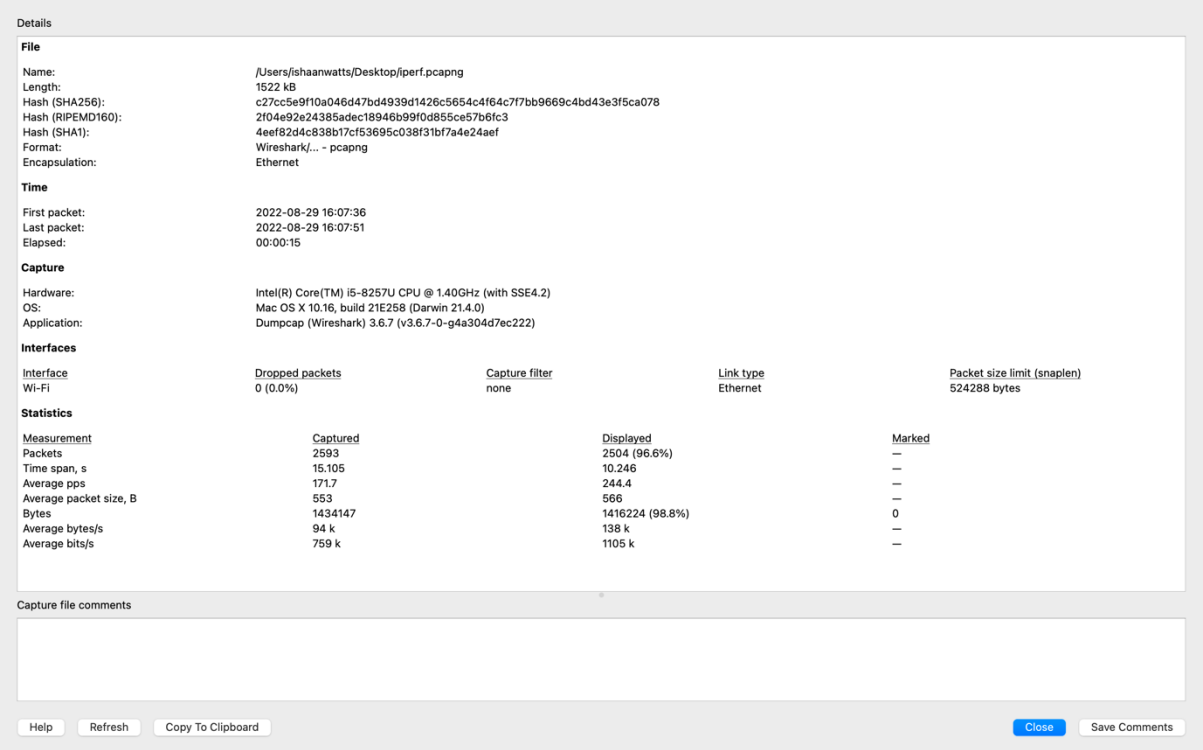

Wi-Fi: en0
dns
No. Time Source Destination Protocol Length Info
691 1.939578 10.184.6.132 10.10.2.2 DNS 78 Standard query 0xa657 HTTPS www.cse.iitd.ac.in
692 1.939714 10.184.6.132 10.10.2.2 DNS 78 Standard query 0x2584 A www.cse.iitd.ac.in
693 1.942487 10.10.2.2 10.184.6.132 DNS 272 Standard query response 0x2584 A www.cse.iitd.ac.in CNAME bahar.cse.iitd.ac.in A 10.208.20.4 NS d
694 1.942488 10.10.2.2 10.184.6.132 DNS 159 Standard query response 0xa657 HTTPS www.cse.iitd.ac.in CNAME bahar.cse.iitd.ac.in SOA desh.cse.i
695 1.943302 10.184.6.132 10.10.2.2 DNS 80 Standard query 0xe772 HTTPS bahar.cse.iitd.ac.in
697 1.945677 10.10.2.2 10.184.6.132 DNS 141 Standard query response 0xe772 HTTPS bahar.cse.iitd.ac.in SOA desh.cse.iitd.ernet.in
Answer RRs: 2
Authority RRs: 4
Additional RRs: 4
Queries
www.cse.iitd.ac.in: type A, class IN
Answers
www.cse.iitd.ac.in: type CNAME, class IN, cname bahar.cse.iitd.ac.in
Name: www.cse.iitd.ac.in
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 3600 (1 hour)
Data length: 8
CNAME: bahar.cse.iitd.ac.in
bahar.cse.iitd.ac.in: type A, class IN, addr 10.208.20.4
Name: bahar.cse.iitd.ac.in
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 3600 (1 hour)
Data length: 4
Address: 10.208.20.4


Wi-Fi: en0
dns
No. Time Source Destination Protocol Length Info
691 1.939578 10.184.6.132 10.10.2.2 DNS 78 Standard query 0xa657 HTTPS www.cse.iitd.ac.in
692 1.939714 10.184.6.132 10.10.2.2 DNS 78 Standard query 0x2584 A www.cse.iitd.ac.in
693 1.942487 10.10.2.2 10.184.6.132 DNS 272 Standard query response 0x2584 A www.cse.iitd.ac.in CNAME bahar.cse.iitd.ac.in A 10.208.20.4 NS d
694 1.942488 10.10.2.2 10.184.6.132 DNS 159 Standard query response 0xa657 HTTPS www.cse.iitd.ac.in CNAME bahar.cse.iitd.ac.in SOA desh.cse.i
695 1.943302 10.184.6.132 10.10.2.2 DNS 80 Standard query 0xe772 HTTPS bahar.cse.iitd.ac.in
697 1.945677 10.10.2.2 10.184.6.132 DNS 141 Standard query response 0xe772 HTTPS bahar.cse.iitd.ac.in SOA desh.cse.iitd.ernet.in
Frame 694: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface en0, id 0
Ethernet II, Src: Cisco_19:a5:41 (84:78:ac:19:a5:41), Dst: Apple_61:c7:bf (a4:83:e7:61:c7:bf)
Internet Protocol Version 4, Src: 10.10.2.2, Dst: 10.184.6.132
User Datagram Protocol, Src Port: 53, Dst Port: 54738
Domain Name System (response)
Transaction ID: 0xa657
Flags: 0x8580 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 1
Additional RRs: 0
Queries
www.cse.iitd.ac.in: type HTTPS, class IN
Answers
www.cse.iitd.ac.in: type CNAME, class IN, cname bahar.cse.iitd.ac.in
Name: www.cse.iitd.ac.in
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 3600 (1 hour)
Data length: 8
CNAME: bahar.cse.iitd.ac.in
Authoritative nameservers
[Request In: 691]
[Time: 0.002910000 seconds]

IPERF TASK 2

```
ishaanwatts — -zsh — 99×24

iperf Done.
[ishaanwatts@Ishaans-MacBook-Pro ~ % 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
[  7] local 10.184.6.132 port 51891 connected to 62.210.18.40 port 5208
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  7]   0.00-1.00   sec   126 KBytes  1.03 Mbits/sec  0.016 ms  0/246 (0%)
[  7]   1.00-2.00   sec   118 KBytes   964 Kbits/sec  0.007 ms  0/230 (0%)
[  7]   2.00-3.00   sec   128 KBytes  1.05 Mbits/sec  0.008 ms  0/250 (0%)
[  7]   3.00-4.00   sec   128 KBytes  1.05 Mbits/sec  0.134 ms  0/251 (0%)
[  7]   4.00-5.00   sec   140 KBytes  1.15 Mbits/sec  0.021 ms  0/274 (0%)
[  7]   5.00-6.00   sec   103 KBytes   842 Kbits/sec  0.087 ms  25/226 (11%)
[  7]   6.00-7.00   sec   141 KBytes  1.15 Mbits/sec  0.016 ms  0/275 (0%)
[  7]   7.00-8.00   sec   115 KBytes   943 Kbits/sec  0.030 ms  0/225 (0%)
[  7]   8.00-9.00   sec   128 KBytes  1.05 Mbits/sec  0.041 ms  0/250 (0%)
[  7]   9.00-10.00  sec   139 KBytes  1.14 Mbits/sec  0.026 ms  0/271 (0%)
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  7]   0.00-10.00  sec  1.26 MBytes  1.06 Mbits/sec  0.000 ms  0/2498 (0%)  sender
[  7]   0.00-10.00  sec  1.24 MBytes  1.04 Mbits/sec  0.026 ms  25/2498 (1%)  receiver

iperf Done.
ishaanwatts@Ishaans-MacBook-Pro ~ %
```





Details

File

Name:	/Users/ishaanwatts/Desktop/iperf.pcapng
Length:	1522 kB
Hash (SHA256):	c27cc5e9f10a046d47bd4939d1426c5654c4f64c7f7bb9669c4bd43e3f5ca078
Hash (RIPEMD160):	2f04e92e24385adec18946b99f0d855ce57b6fc3
Hash (SHA1):	4eef82d4c838b17cf53695c038f31bf7a4e24aef
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2022-08-29 16:07:36
Last packet:	2022-08-29 16:07:51
Elapsed:	00:00:15

Capture

Hardware:	Intel(R) Core(TM) i5-8257U CPU @ 1.40GHz (with SSE4.2)
OS:	Mac OS X 10.16, build 21E258 (Darwin 21.4.0)
Application:	Dumpcap (Wireshark) 3.6.7 (v3.6.7-0-g4a304d7ec222)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Wi-Fi	0 (0.0%)	none	Ethernet	524288 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	2593	2504 (96.6%)	—
Time span, s	15.105	10.246	—
Average pps	171.7	244.4	—
Average packet size, B	553	566	—
Bytes	1434147	1416224 (98.8%)	0
Average bytes/s	94 k	138 k	—
Average bits/s	759 k	1105 k	—

Capture file comments

Help Refresh Copy To Clipboard Close Save Comments

1. As we can see from file properties capture, 2504 UDP packets are exchanged in this communication between iperf3 client and remote server.

2. Bulk data is being sent from the remote server (62.210.18.40 port 5208) to the iperf3 client (10.184.6.132 port 51891) as seen in the wireshark capture.

   Average packet size is 566 bytes in file properties capture.

3. Throughput = $\frac{\text{average packet size * number of packets sent}}{\text{capture time}}$

   $= \frac{566*2504}{10}$

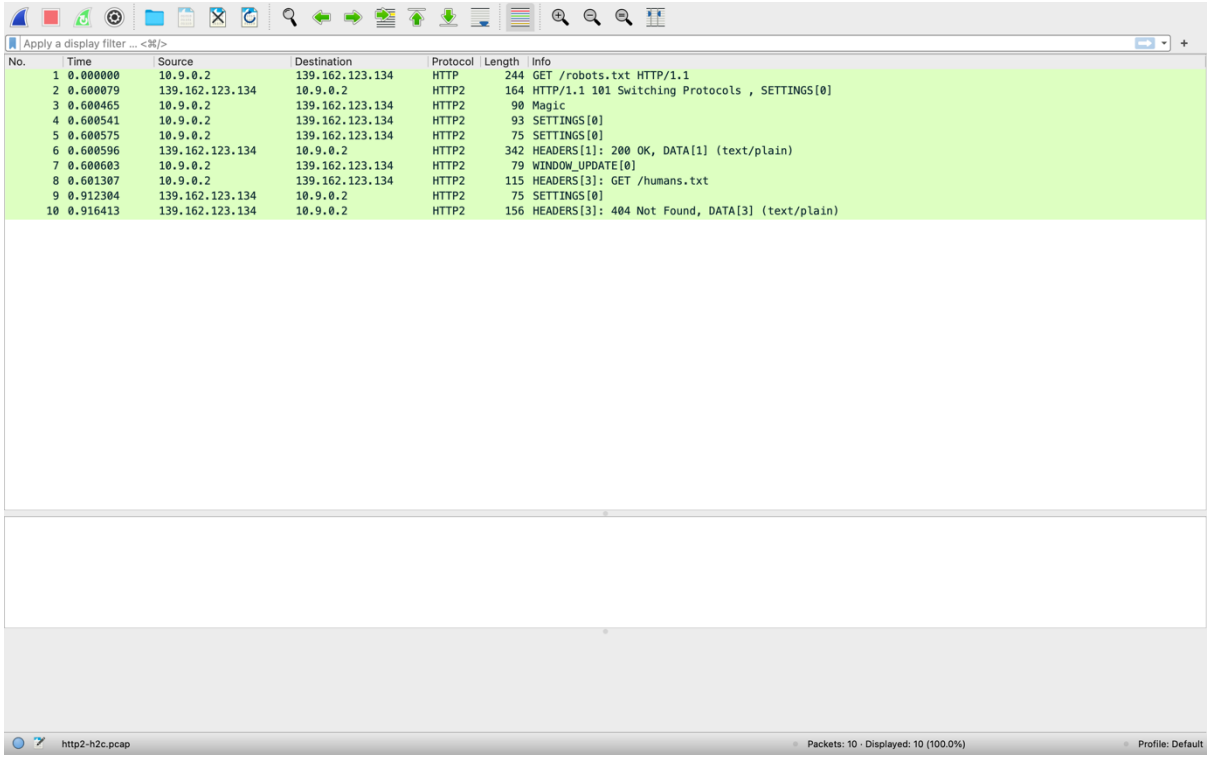
   = 141,726.4 bytes/sec

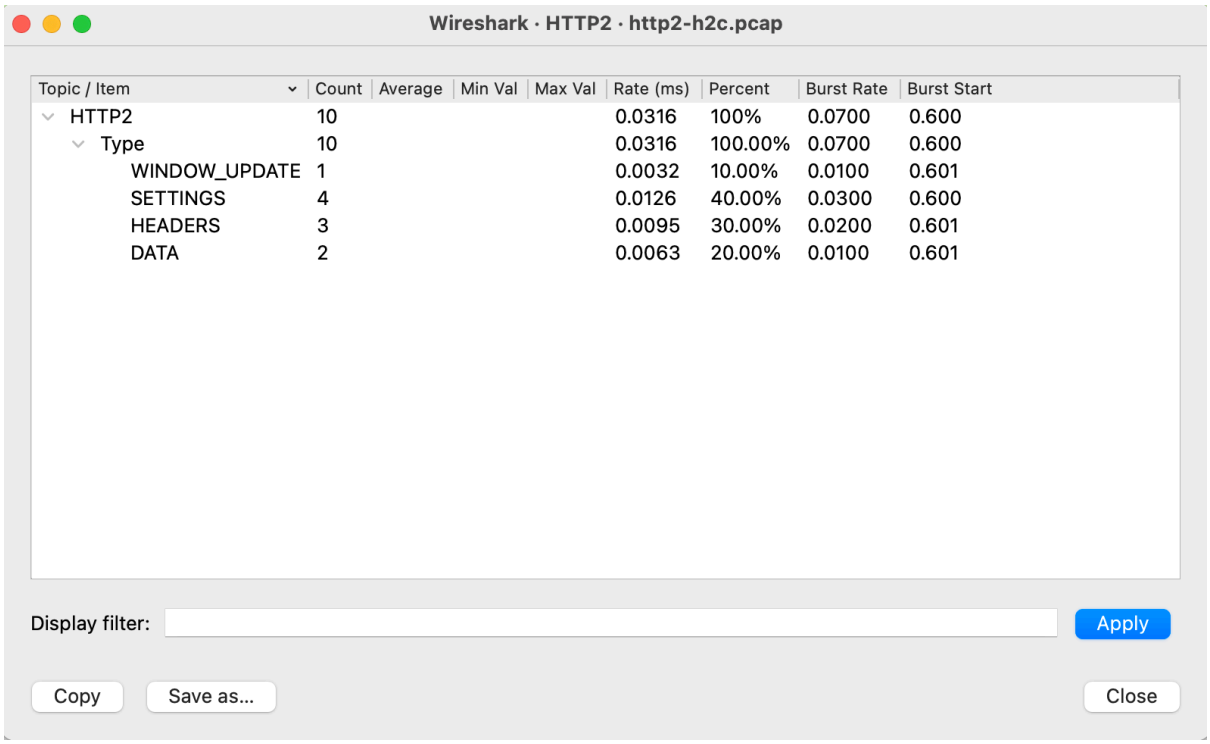
   Calculated value = 141,726.4 bytes/sec
   Observed value in wireshark = 138k bytes/sec
   % error = 2.7

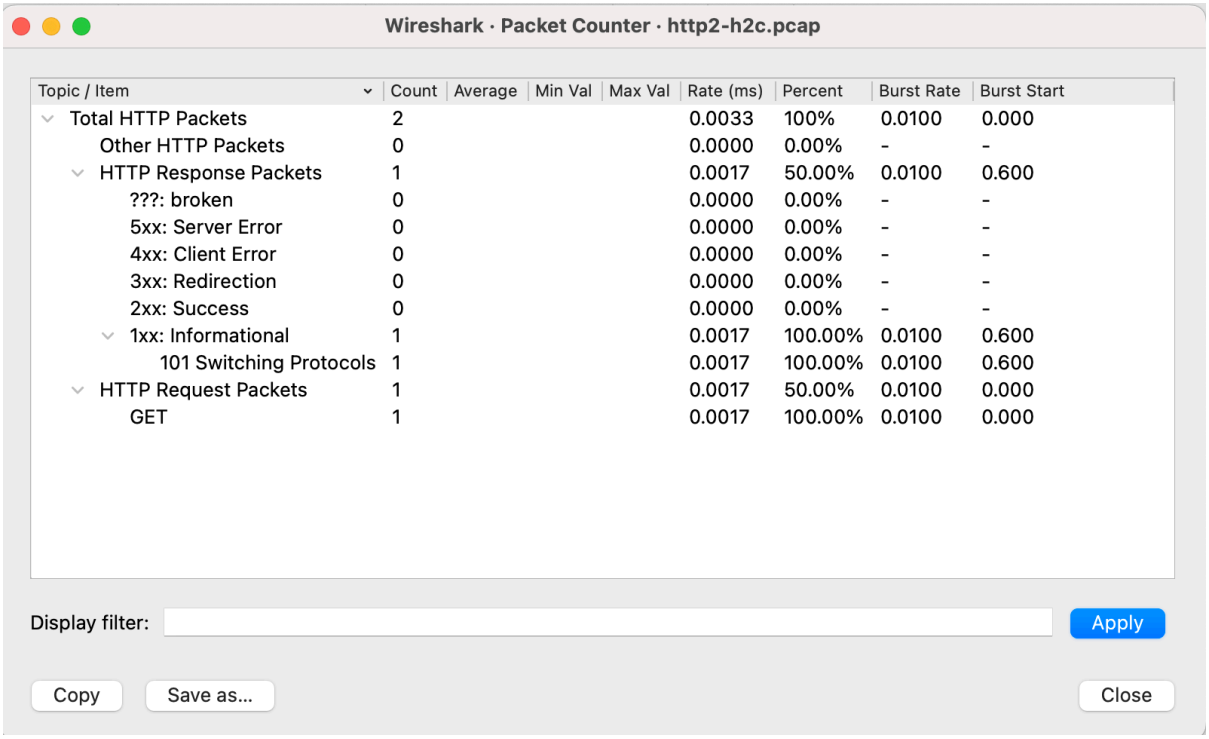
   Calculated bit rate = 141,726.4/125000
   = 1.1338112 Mbits/sec
   Observed bit rate in terminal = 1.06 Mbits/sec
   % error = 6.6

   The difference is due to packet loss and extra packets due to some other procedures

HTTP Task 3


Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
1 0.000000 10.9.0.2 139.162.123.134 HTTP 244 GET /robots.txt HTTP/1.1
2 0.600079 139.162.123.134 10.9.0.2 HTTP2 164 HTTP/1.1 101 Switching Protocols , SETTINGS[0]
3 0.600465 10.9.0.2 139.162.123.134 HTTP2 90 Magic
4 0.600541 10.9.0.2 139.162.123.134 HTTP2 93 SETTINGS[0]
5 0.600575 10.9.0.2 139.162.123.134 HTTP2 75 SETTINGS[0]
6 0.600596 139.162.123.134 10.9.0.2 HTTP2 342 HEADERS[1]: 200 OK, DATA[1] (text/plain)
7 0.600603 10.9.0.2 139.162.123.134 HTTP2 79 WINDOW_UPDATE[0]
8 0.601307 10.9.0.2 139.162.123.134 HTTP2 115 HEADERS[3]: GET /humans.txt
9 0.912304 139.162.123.134 10.9.0.2 HTTP2 75 SETTINGS[0]
10 0.916413 139.162.123.134 10.9.0.2 HTTP2 156 HEADERS[3]: 404 Not Found, DATA[3] (text/plain)
http2-h2c.pcap
Packets: 10 · Displayed: 10 (100.0%)
Profile: Default


Wireshark · HTTP2 · http2-h2c.pcap
Topic / Item Count Average Min Val Max Val Rate (ms) Percent Burst Rate Burst Start
HTTP2 10 0.0316 100% 0.0700 0.600
Type 10 0.0316 100.00% 0.0700 0.600
WINDOW_UPDATE 1 0.0032 10.00% 0.0100 0.601
SETTINGS 4 0.0126 40.00% 0.0300 0.600
HEADERS 3 0.0095 30.00% 0.0200 0.601
DATA 2 0.0063 20.00% 0.0100 0.601
Display filter:
Apply
Copy
Save as...
Close



1. From the above statistic captures

   HTTP/1.1 packets --> 2
   HTTP/2 packets --> 10

2. 4 HTTP/2 packets are exchanged between client and server here before the first object is fetched (2-5)

```
2 0.600079    139.162.123.134    10.9.0.2           HTTP2    164 HTTP/1.1 101 Switching Protocols , SETTINGS[0]
3 0.600465    10.9.0.2           139.162.123.134    HTTP2     90 Magic
4 0.600541    10.9.0.2           139.162.123.134    HTTP2     93 SETTINGS[0]
5 0.600575    10.9.0.2           139.162.123.134    HTTP2     75 SETTINGS[0]
6 0.600596    139.162.123.134    10.9.0.2           HTTP2    342 HEADERS[1]: 200 OK, DATA[1] (text/plain)
```

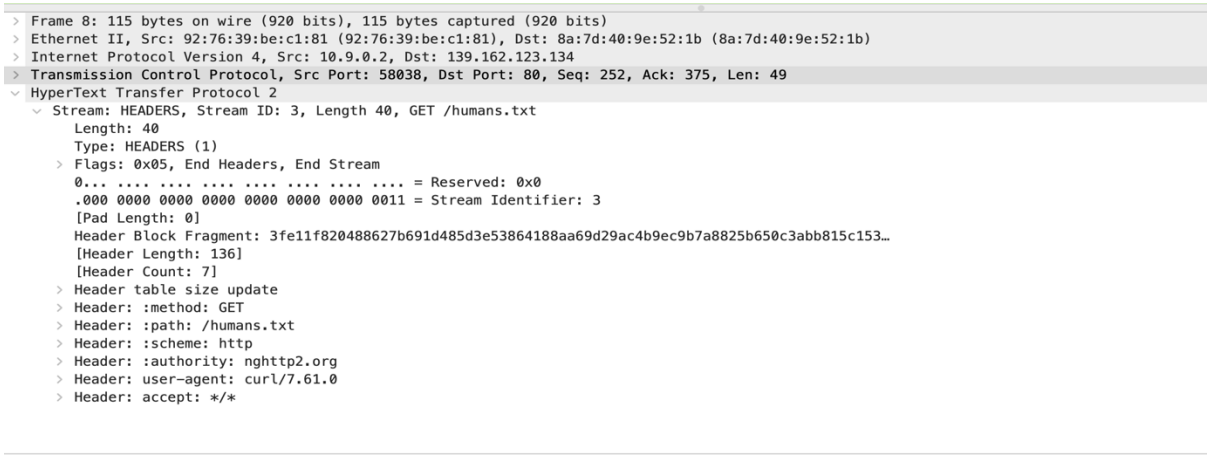
3. HTTP/1.1 use a textual format with fields like HOST, User-Agent, Accept, Connection, Upgrade

   HTTP/2 uses a binary protocol which provides efficient compression of header fields and stream with an identifier.

HTTP/1.1

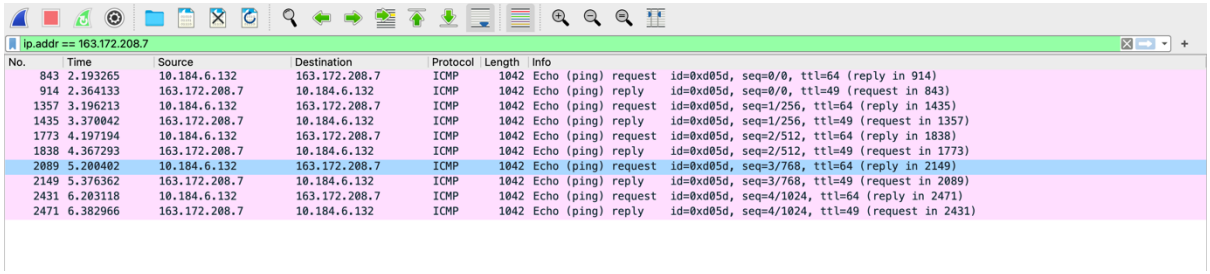
```
Hypertext Transfer Protocol
  GET /robots.txt HTTP/1.1\r\n
  Host: nghttp2.org\r\n
  User-Agent: curl/7.61.0\r\n
  Accept: */*\r\n
  Connection: Upgrade, HTTP2-Settings\r\n
  Upgrade: h2c\r\n
  HTTP2-Settings: AAMAAABkAARAAAAAAAIAAAAA\r\n
  \r\n
  [Full request URI: http://nghttp2.org/robots.txt]
  [HTTP request 1/1]
  [Response in frame: 2]
```

HTTP/2


Frame 8: 115 bytes on wire (920 bits), 115 bytes captured (920 bits)
Ethernet II, Src: 92:76:39:be:c1:81 (92:76:39:be:c1:81), Dst: 8a:7d:40:9e:52:1b (8a:7d:40:9e:52:1b)
Internet Protocol Version 4, Src: 10.9.0.2, Dst: 139.162.123.134
Transmission Control Protocol, Src Port: 58038, Dst Port: 80, Seq: 252, Ack: 375, Len: 49
HyperText Transfer Protocol 2
Stream: HEADERS, Stream ID: 3, Length 40, GET /humans.txt
Length: 40
Type: HEADERS (1)
Flags: 0x05, End Headers, End Stream
0... .... = Reserved: 0x0
.000 0000 0000 0000 0000 0000 0000 0011 = Stream Identifier: 3
[Pad Length: 0]
Header Block Fragment: 3fe11f820488627b691d485d3e53864188aa69d29ac4b9ec9b7a8825b650c3abb815c153…
[Header Length: 136]
[Header Count: 7]
Header table size update
Header: :method: GET
Header: :path: /humans.txt
Header: :scheme: http
Header: :authority: nghttp2.org
Header: user-agent: curl/7.61.0
Header: accept: */*

PING Task 4

```
ishaanwatts@Ishaans-MacBook-Pro ~ % ping -s 1000 ping-ams1.online.net -c 5
PING ping-ams1.online.net (163.172.208.7): 1000 data bytes
1008 bytes from 163.172.208.7: icmp_seq=0 ttl=49 time=171.019 ms
1008 bytes from 163.172.208.7: icmp_seq=1 ttl=49 time=174.035 ms
1008 bytes from 163.172.208.7: icmp_seq=2 ttl=49 time=170.310 ms
1008 bytes from 163.172.208.7: icmp_seq=3 ttl=49 time=176.184 ms
1008 bytes from 163.172.208.7: icmp_seq=4 ttl=49 time=180.024 ms

--- ping-ams1.online.net ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 170.310/174.314/180.024/3.552 ms
```



ip.addr == 163.172.208.7

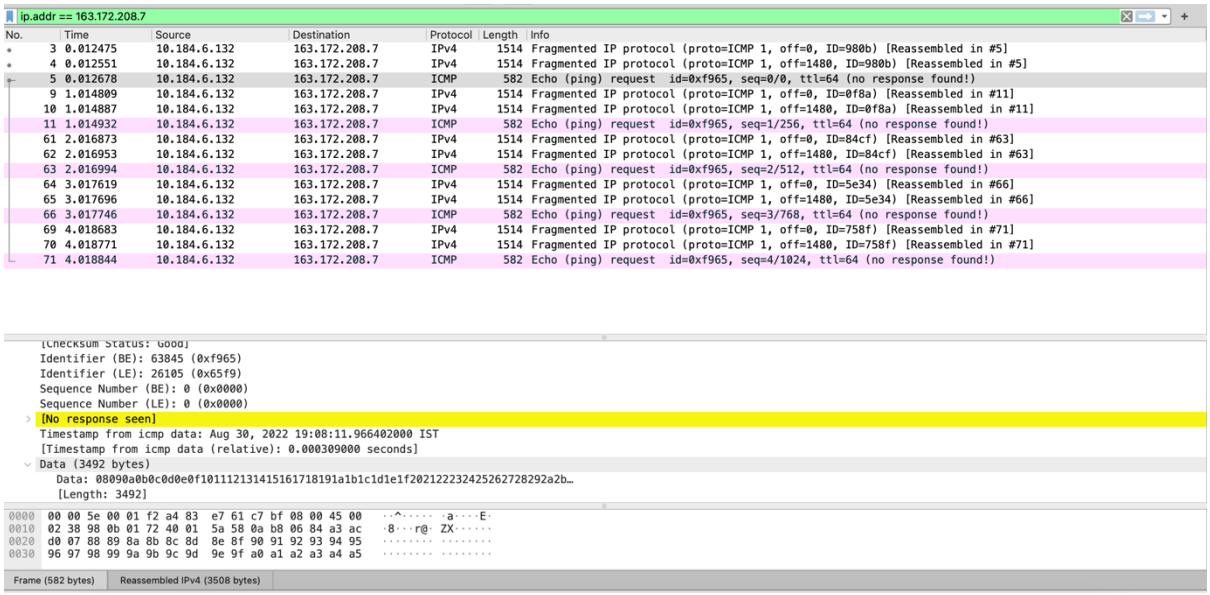
No.	Time	Source	Destination	Protocol	Length	Info
843	2.193265	10.184.6.132	163.172.208.7	ICMP	1042	Echo (ping) request id=0xd05d, seq=0/0, ttl=64 (reply in 914)
914	2.364133	163.172.208.7	10.184.6.132	ICMP	1042	Echo (ping) reply id=0xd05d, seq=0/0, ttl=49 (request in 843)
1357	3.196213	10.184.6.132	163.172.208.7	ICMP	1042	Echo (ping) request id=0xd05d, seq=1/256, ttl=64 (reply in 1435)
1435	3.370042	163.172.208.7	10.184.6.132	ICMP	1042	Echo (ping) reply id=0xd05d, seq=1/256, ttl=49 (request in 1357)
1773	4.197194	10.184.6.132	163.172.208.7	ICMP	1042	Echo (ping) request id=0xd05d, seq=2/512, ttl=64 (reply in 1838)
1838	4.367293	163.172.208.7	10.184.6.132	ICMP	1042	Echo (ping) reply id=0xd05d, seq=2/512, ttl=49 (request in 1773)
2089	5.200402	10.184.6.132	163.172.208.7	ICMP	1042	Echo (ping) request id=0xd05d, seq=3/768, ttl=64 (reply in 2149)
2149	5.376362	163.172.208.7	10.184.6.132	ICMP	1042	Echo (ping) reply id=0xd05d, seq=3/768, ttl=49 (request in 2089)
2431	6.203118	10.184.6.132	163.172.208.7	ICMP	1042	Echo (ping) request id=0xd05d, seq=4/1024, ttl=64 (reply in 2471)
2471	6.382966	163.172.208.7	10.184.6.132	ICMP	1042	Echo (ping) reply id=0xd05d, seq=4/1024, ttl=49 (request in 2431)

a. Size = 1000 bytes

1. 10 IP packets are exchanged in the communication between host (10.184.6.132) and the remote server (163.172.208.7) representing ping-ams1.online.net

2. 1042 bytes is the size of each ping request sent from host to remote server

3. The packets are not fragmented as the size is smaller.



ip.addr == 163.172.208.7

No.	Time	Source	Destination	Protocol	Length	Info
3	0.012475	10.184.6.132	163.172.208.7	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=980b) [Reassembled in #5]
4	0.012551	10.184.6.132	163.172.208.7	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=980b) [Reassembled in #5]
5	0.012678	10.184.6.132	163.172.208.7	ICMP	582	Echo (ping) request id=0xf965, seq=0/0, ttl=64 (no response found!)
9	1.014809	10.184.6.132	163.172.208.7	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0f8a) [Reassembled in #11]
10	1.014887	10.184.6.132	163.172.208.7	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=0f8a) [Reassembled in #11]
11	1.014932	10.184.6.132	163.172.208.7	ICMP	582	Echo (ping) request id=0xf965, seq=1/256, ttl=64 (no response found!)
61	2.016873	10.184.6.132	163.172.208.7	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=84cf) [Reassembled in #63]
62	2.016953	10.184.6.132	163.172.208.7	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=84cf) [Reassembled in #63]
63	2.016994	10.184.6.132	163.172.208.7	ICMP	582	Echo (ping) request id=0xf965, seq=2/512, ttl=64 (no response found!)
64	3.017619	10.184.6.132	163.172.208.7	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=5e34) [Reassembled in #66]
65	3.017696	10.184.6.132	163.172.208.7	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=5e34) [Reassembled in #66]
66	3.017746	10.184.6.132	163.172.208.7	ICMP	582	Echo (ping) request id=0xf965, seq=3/768, ttl=64 (no response found!)
69	4.018683	10.184.6.132	163.172.208.7	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=758f) [Reassembled in #71]
70	4.018771	10.184.6.132	163.172.208.7	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=758f) [Reassembled in #71]
71	4.018844	10.184.6.132	163.172.208.7	ICMP	582	Echo (ping) request id=0xf965, seq=4/1024, ttl=64 (no response found!)


```
[Checksum Status: Good]
Identifier (BE): 63845 (0xf965)
Identifier (LE): 26105 (0x65f9)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[No response seen]
Timestamp from icmp data: Aug 30, 2022 19:08:11.966402000 IST
[Timestamp from icmp data (relative): 0.000309000 seconds]
Data (3492 bytes)
  Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b…
  [Length: 3492]
```

```
0000  00 00 5e 00 01 f2 a4 83  e7 61 c7 bf 08 00 45 00   ··^····· ·a····E·
0010  02 38 98 0b 01 72 40 01  5a 58 0a b8 06 84 a3 ac   ·8···r@· ZX······
0020  d0 07 88 89 8a 8b 8c 8d  8e 8f 90 91 92 93 94 95   ········ ········
0030  96 97 98 99 9a 9b 9c 9d  9e 9f a0 a1 a2 a3 a4 a5   ········ ········
```

Frame (582 bytes) | Reassembled IPv4 (3508 bytes)

```
ishaanwatts@Ishaans-MacBook-Pro ~ % ping -s 3500 ping-ams1.online.net -c 5
PING ping-ams1.online.net (163.172.208.7): 3500 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3

--- ping-ams1.online.net ping statistics ---
5 packets transmitted, 0 packets received, 100.0% packet loss
```

b. Size = 3500 bytes

1. 15 IP packets are exchanged in the communication between host (10.184.6.132) and the remote server (163.172.208.7) representing ping-ams1.online.net. 10 of them are IPv4 packets while 5 are ICMP.

2. Each IPv4 packet is of size 1514 Bytes.
   ICMP is of 582 Bytes each.
   The IPv4 packets are fragmented and the total size of each ping sent is (1514+1514+582) 3610 bytes as seen in the PING terminal

3. Table

No.	Source	Destination	Protocol	Fragmented	Fragments	Size	Time	Response
1	10.184.6.132	163.172.208.7	IPv4	Yes	0-1479	1480	0.012475	
2	10.184.6.132	163.172.208.7	IPv4	Yes	1480-2959	1480	0.012551	
3	10.184.6.132	163.172.208.7	ICMP	No	2960-3507	548	0.012678	None
4	10.184.6.132	163.172.208.7	IPv4	Yes	0-1479	1480	1.014809	
5	10.184.6.132	163.172.208.7	IPv4	Yes	1480-2959	1480	1.014887	
6	10.184.6.132	163.172.208.7	ICMP	No	2960-3507	548	1.014932	None
7	10.184.6.132	163.172.208.7	IPv4	Yes	0-1479	1480	2.016873	
8	10.184.6.132	163.172.208.7	IPv4	Yes	1480-2959	1480	2.016953	
9	10.184.6.132	163.172.208.7	ICMP	No	2960-3507	548	2.016994	None
10	10.184.6.132	163.172.208.7	IPv4	Yes	0-1479	1480	3.017619	
11	10.184.6.132	163.172.208.7	IPv4	Yes	1480-2959	1480	3.017696	
12	10.184.6.132	163.172.208.7	ICMP	No	2960-3507	548	3.017746	None
13	10.184.6.132	163.172.208.7	IPv4	Yes	0-1479	1480	4.018683	
14	10.184.6.132	163.172.208.7	IPv4	Yes	1480-2959	1480	4.018771	
15	10.184.6.132	163.172.208.7	ICMP	No	2960-3507	548	4.018844	None

TRACEROUTE TASK 5

a. Packet size --> 3500

```
ishaanwatts@Ishaans-MacBook-Pro ~ % traceroute -q 5 ping-ams1.online.net 3500
traceroute to ping-ams1.online.net (163.172.208.7), 64 hops max, 3500 byte packets
 1  172.20.10.1 (172.20.10.1)  21.121 ms  7.692 ms  4.830 ms  5.357 ms  6.267 ms
 2  192.168.31.16 (192.168.31.16)  67.649 ms  43.565 ms  40.029 ms  36.202 ms  33.791 ms
 3  * * * * *
 4  * * * * *
 5  dsl-tn-dynamic-121.222.22.125.airtelbroadband.in (125.22.222.121)  68.445 ms  43.918 ms  49.637 ms
40.249 ms  55.243 ms
 6  116.119.49.38 (116.119.49.38)  164.616 ms  160.165 ms  159.155 ms  198.322 ms  165.840 ms
 7  * * * * *
 8  195.154.2.103 (195.154.2.103)  207.141 ms  191.889 ms  188.749 ms  195.965 ms  204.797 ms
 9  62.210.0.135 (62.210.0.135)  194.281 ms  198.141 ms  201.353 ms  190.202 ms  189.153 ms
10  grokouik.poneytelecom.eu (62.210.175.218)  205.938 ms  246.724 ms  196.053 ms  191.657 ms  193.926 m
s
11  195.154.2.104 (195.154.2.104)  210.881 ms  203.883 ms  207.899 ms  200.269 ms  213.010 ms
12  * * * * *
13  * * * * *
14  * * * * *
15  * * * * *
16  * * * * *
17  * * * * *
18  * * * * *
19  * * * * *
20  * * * * *
21  * * * * *
22  * * * * *
23  * * * * *
24  * * * * *
25  * * * * *
26  * * * * *
27  * * * * *
```

Not able to traceroute

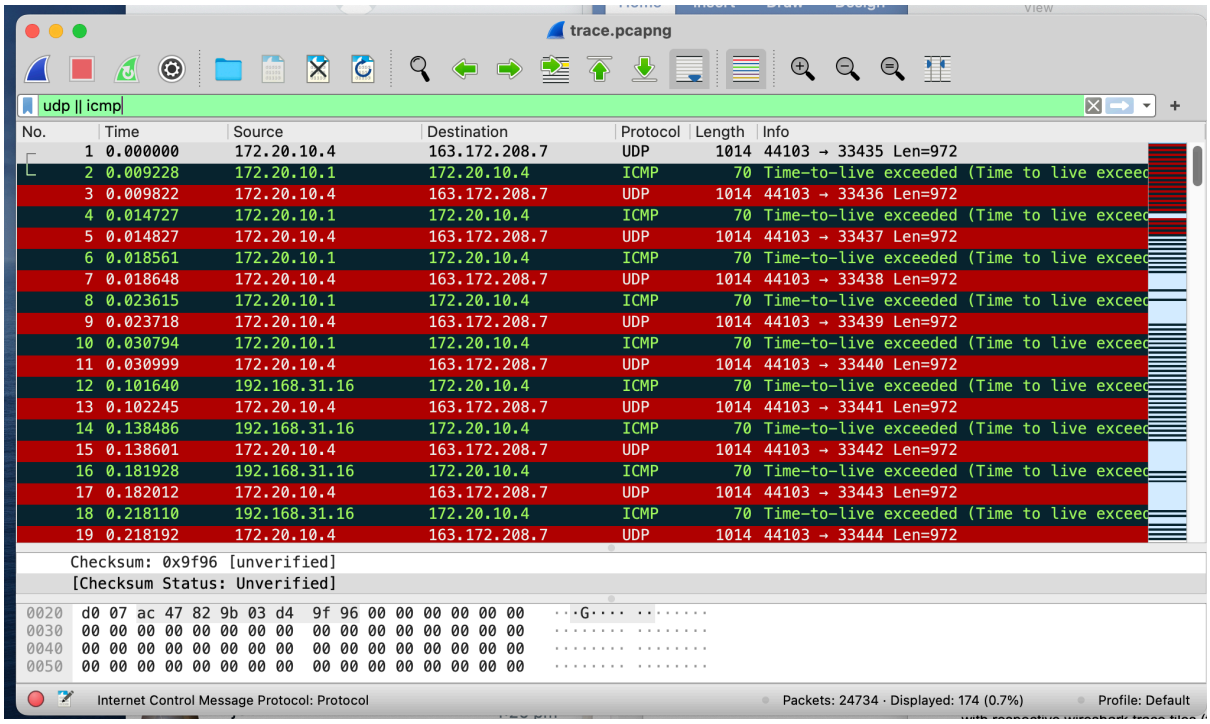
b. Packet size --> 1000

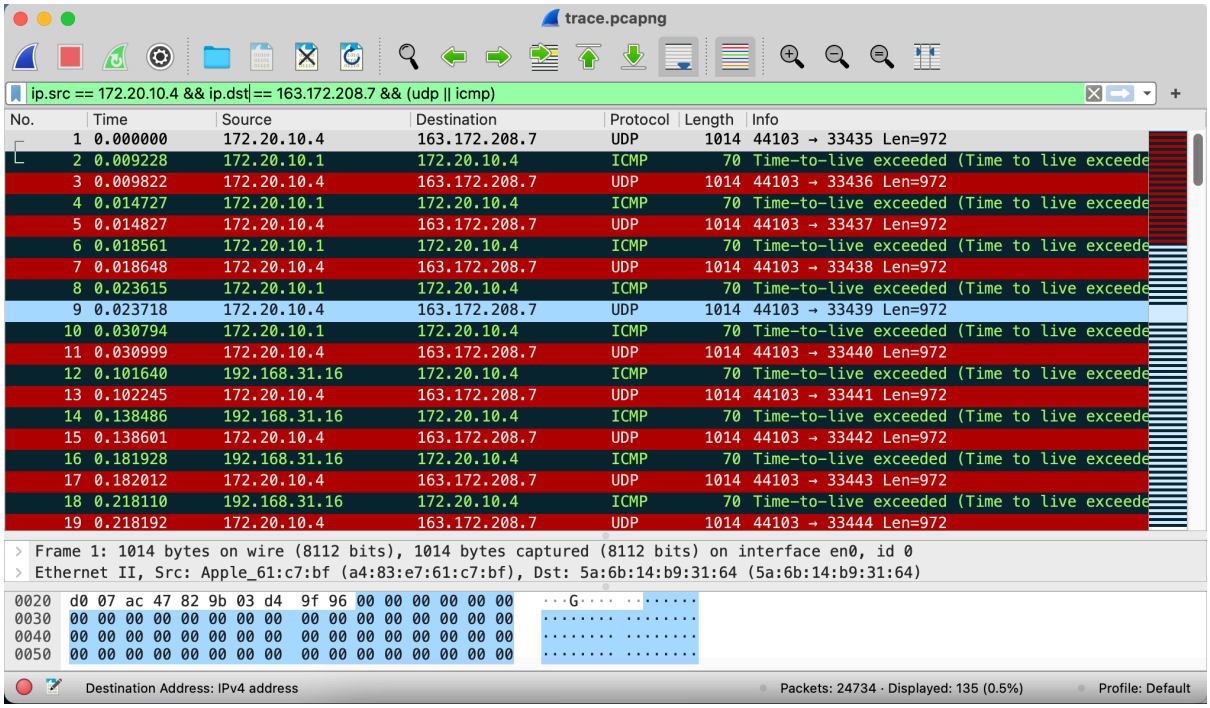
```
ishaanwatts@Ishaans-MacBook-Pro ~ % traceroute -q 5 ping-ams1.online.net 1000
traceroute to ping-ams1.online.net (163.172.208.7), 64 hops max, 1000 byte packets
 1  172.20.10.1 (172.20.10.1)  9.570 ms  4.998 ms  3.813 ms  5.053 ms  7.226 ms
 2  192.168.31.16 (192.168.31.16)  70.756 ms  36.350 ms  43.409 ms  36.171 ms  35.157 ms
 3  192.168.13.160 (192.168.13.160)  40.111 ms  43.047 ms  58.611 ms  44.923 ms  39.932 ms
 4  192.168.13.48 (192.168.13.48)  39.836 ms
    192.168.13.38 (192.168.13.38)  39.977 ms
    192.168.13.68 (192.168.13.68)  36.597 ms
    192.168.13.48 (192.168.13.48)  37.526 ms
    192.168.13.68 (192.168.13.68)  52.341 ms
 5  dsl-tn-dynamic-121.222.22.125.airtelbroadband.in (125.22.222.121)  41.291 ms  41.676 ms  35.846 ms
58.013 ms  37.682 ms
 6  116.119.61.232 (116.119.61.232)  151.327 ms  155.380 ms
    182.79.189.122 (182.79.189.122)  166.669 ms
    116.119.61.204 (116.119.61.204)  192.092 ms
    116.119.61.232 (116.119.61.232)  170.206 ms
 7  * * * * *
 8  195.154.2.103 (195.154.2.103)  204.113 ms  193.416 ms  195.101 ms  189.680 ms  228.723 ms
 9  62.210.0.135 (62.210.0.135)  193.949 ms  397.678 ms  183.721 ms  208.109 ms  200.763 ms
10  grokouik.poneytelecom.eu (62.210.175.218)  311.745 ms  205.107 ms  182.081 ms  199.286 ms  193.013 m
s
11  195.154.2.104 (195.154.2.104)  190.383 ms  235.936 ms  199.912 ms  206.655 ms  201.987 ms
12  51.158.8.168 (51.158.8.168)  201.863 ms  212.512 ms
    51.158.8.27 (51.158.8.27)  193.357 ms  224.617 ms  215.358 ms
13  51.158.143.3 (51.158.143.3)  212.652 ms  312.986 ms  249.786 ms
    51.158.143.1 (51.158.143.1)  202.788 ms  202.676 ms
14  ping-ams1.online.net (163.172.208.7)  192.414 ms  217.565 ms  188.375 ms  198.299 ms  187.414 ms
```

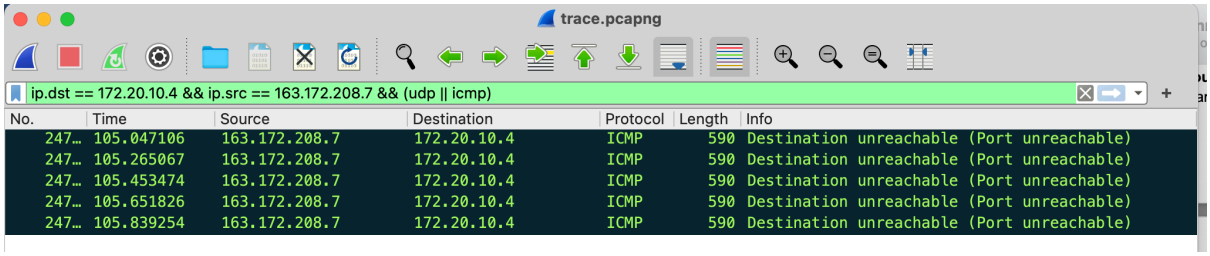
1. 14 hops are involved in finding the route to this ping-ams1.online.net

2. Table

S. No.	Src	Dst	Packets
1	Total		174
2	172.20.10.4	163.172.208.7	135
3	163.172.208.7	172.20.10.4	5



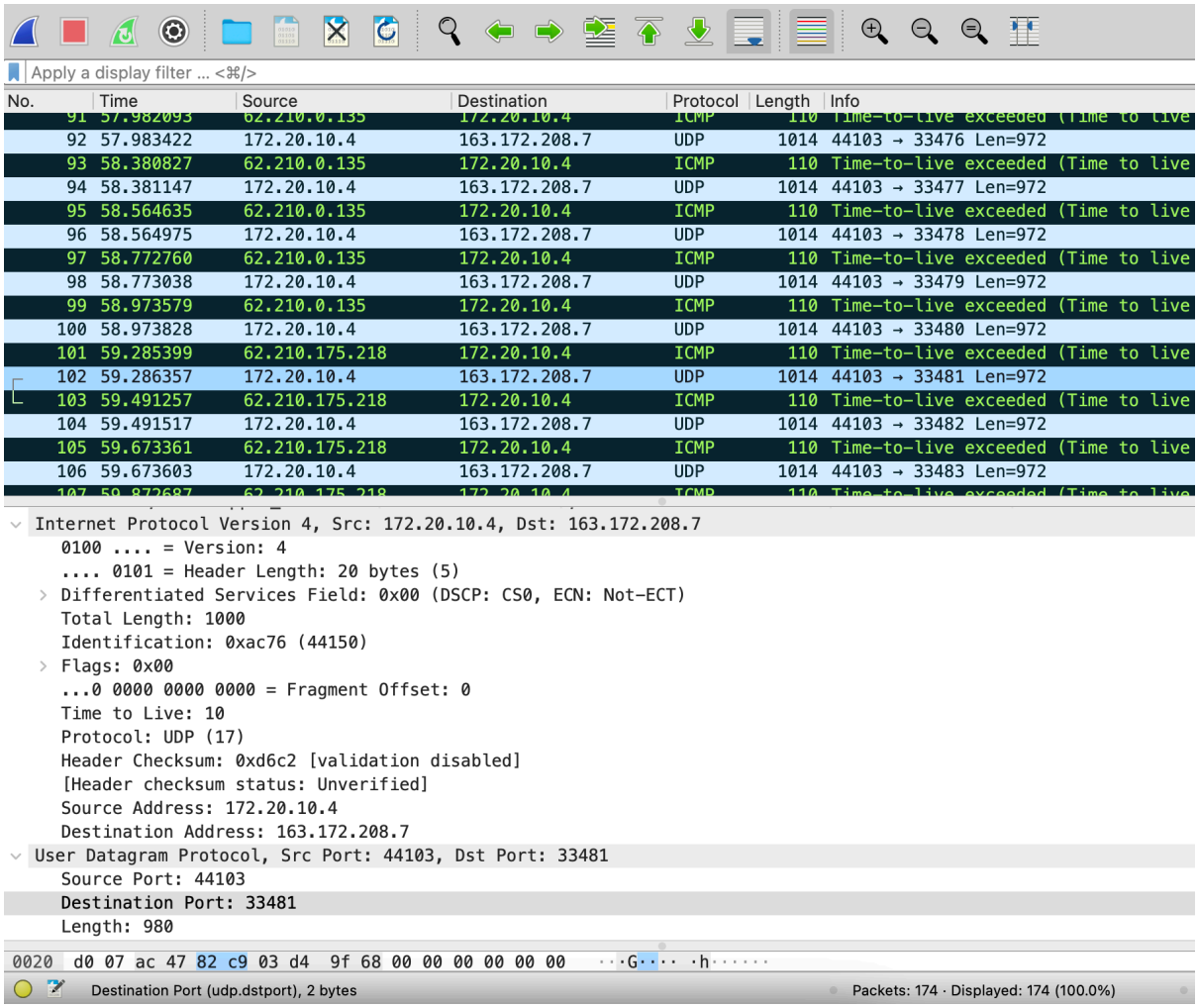


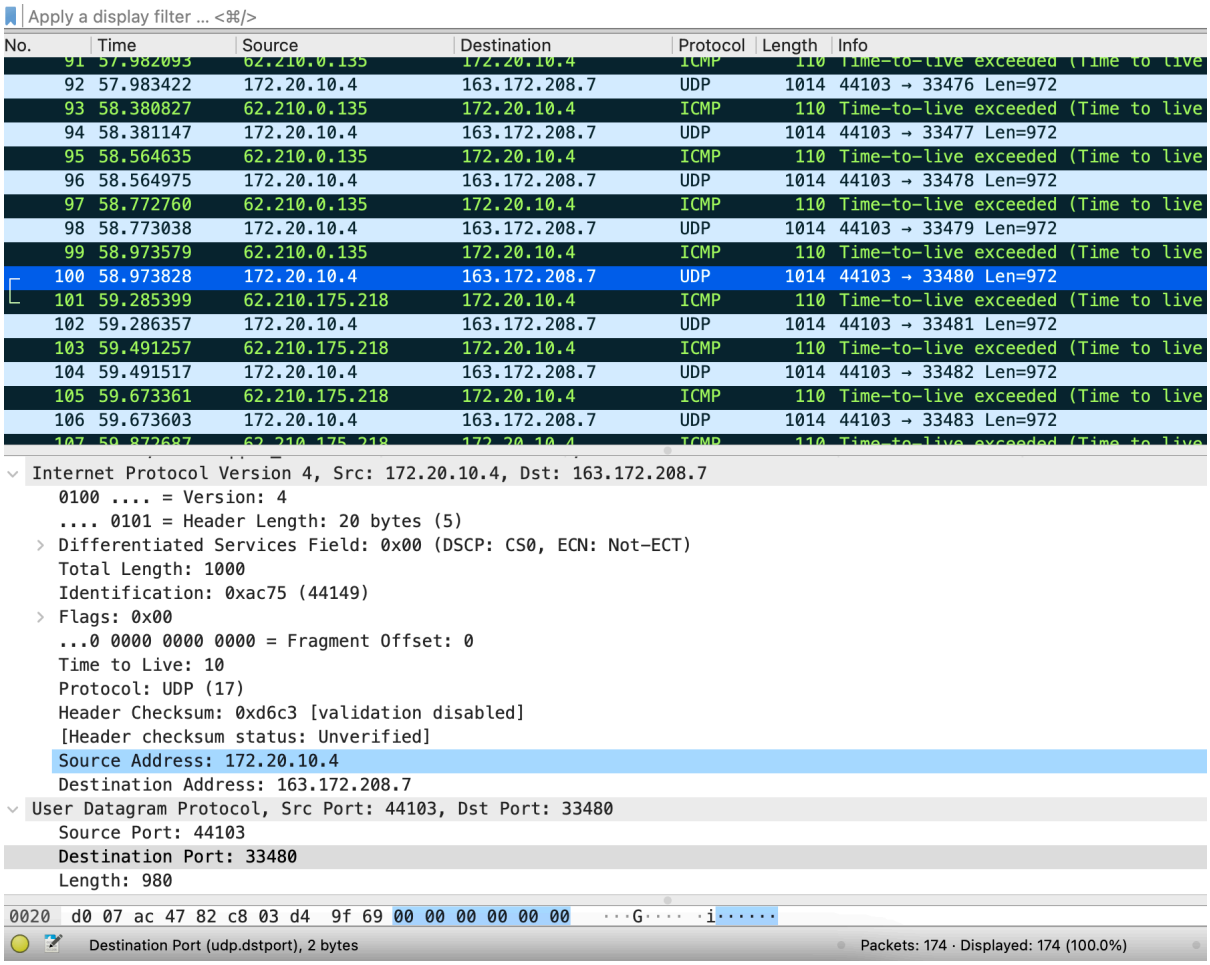


3. The Source port (44103), length (980 bytes) and Data (972 bytes) remain the same.

The fields that stay constant across all IP datagrams are source and destination IP since we are sending from and to the same source and destination respectively. Same version i.e. IPv4 for all packets. The header length is also same.

The fields that must change are Identification since every packet has a different ID, Time to live as traceroute increases each subsequent packet, the header checksum also changes since the header changes. The destination port is also different.




Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
91 57.982093 62.210.0.135 172.20.10.4 ICMP 110 Time-to-live exceeded (Time to live
92 57.983422 172.20.10.4 163.172.208.7 UDP 1014 44103 → 33476 Len=972
93 58.380827 62.210.0.135 172.20.10.4 ICMP 110 Time-to-live exceeded (Time to live
94 58.381147 172.20.10.4 163.172.208.7 UDP 1014 44103 → 33477 Len=972
95 58.564635 62.210.0.135 172.20.10.4 ICMP 110 Time-to-live exceeded (Time to live
96 58.564975 172.20.10.4 163.172.208.7 UDP 1014 44103 → 33478 Len=972
97 58.772760 62.210.0.135 172.20.10.4 ICMP 110 Time-to-live exceeded (Time to live
98 58.773038 172.20.10.4 163.172.208.7 UDP 1014 44103 → 33479 Len=972
99 58.973579 62.210.0.135 172.20.10.4 ICMP 110 Time-to-live exceeded (Time to live
100 58.973828 172.20.10.4 163.172.208.7 UDP 1014 44103 → 33480 Len=972
101 59.285399 62.210.175.218 172.20.10.4 ICMP 110 Time-to-live exceeded (Time to live
102 59.286357 172.20.10.4 163.172.208.7 UDP 1014 44103 → 33481 Len=972
103 59.491257 62.210.175.218 172.20.10.4 ICMP 110 Time-to-live exceeded (Time to live
104 59.491517 172.20.10.4 163.172.208.7 UDP 1014 44103 → 33482 Len=972
105 59.673361 62.210.175.218 172.20.10.4 ICMP 110 Time-to-live exceeded (Time to live
106 59.673603 172.20.10.4 163.172.208.7 UDP 1014 44103 → 33483 Len=972
Internet Protocol Version 4, Src: 172.20.10.4, Dst: 163.172.208.7
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1000
Identification: 0xac75 (44149)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 10
Protocol: UDP (17)
Header Checksum: 0xd6c3 [validation disabled]
[Header checksum status: Unverified]
Source Address: 172.20.10.4
Destination Address: 163.172.208.7
User Datagram Protocol, Src Port: 44103, Dst Port: 33480
Source Port: 44103
Destination Port: 33480
Length: 980
0020 d0 07 ac 47 82 c8 03 d4 9f 69 00 00 00 00 00 00
Destination Port (udp.dstport), 2 bytes
Packets: 174 · Displayed: 174 (100.0%)