Network Tools

Part 1:

```
C:\Users\HP\Desktop\SEM 5\COL334\Assignment\Iperf\iperf-3.1.3-win64>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::fd53:6590:f04b:db88%15
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : iitd.ac.in
   Link-local IPv6 Address . . . . . : fe80::e548:7623:ba4e:47da%21
   IPv4 Address. . . . . . . . . . . : 10.184.24.161
   Subnet Mask . . . . . . . . . . . : 255.255.224.0
   Default Gateway . . . . . . . . . : 10.184.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

The IP address of my device:10.184.24.161(IPV4 Address) using IITD Wi-Fi

```
C:\Users\HP\Desktop\SEM 5\COL334\Assignment\Iperf\iperf-3.1.3-win64>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::fd53:6590:f04b:db88%15
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:47ff:8e9d:e548:7623:ba4e:47da
   Temporary IPv6 Address. . . . . . : 2401:4900:47ff:8e9d:7d94:fce0:9fe5:c6af
   Link-local IPv6 Address . . . . . : fe80::e548:7623:ba4e:47da%21
   IPv4 Address. . . . . . . . . . . : 192.168.29.223
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::54c0:1bff:fe89:c5f2%21
                                       192.168.29.197

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\HP\Desktop\SEM 5\COL334\Assignment\Iperf\iperf-3.1.3-win64>
```

On connecting through mobile hotspot the IP address of my device came out to be 198.168.29.223

Thus we can observe that IP address depends on the ISP

Part 2:

```
C:\Users\HP\Desktop\SEM 5\COL334\Assignment\Iperf\iperf-3.1.3-win64>nslookup
Default Server:  dns1.cc.iitd.ac.in
Address:  10.10.2.2

> google.com
Server:  dns1.cc.iitd.ac.in
Address:  10.10.2.2

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4002:81c::200e
          142.250.193.206

> facebook.com
Server:  dns1.cc.iitd.ac.in
Address:  10.10.2.2

Non-authoritative answer:
Name:    facebook.com
Addresses:  2a03:2880:f12f:83:face:b00c:0:25de
          31.13.79.35

>
```

Using default IITD DNS server:

The IP address of google.com- 142.250.193.206

The IP address of facebook.com-157.240.16.35

```
C:\Users\HP\Desktop\SEM 5\COL334\Assignment\Iperf\iperf-3.1.3-win64>nslookup
Default Server:  dns1.cc.iitd.ac.in
Address:  10.10.2.2

> lserver 9.9.9.9
Default Server:  [9.9.9.9]
Address:  9.9.9.9

> google.com
Server:  [9.9.9.9]
Address:  9.9.9.9

Non-authoritative answer:
Name:    google.com
Addresses:  2a00:1450:4006:801::200e
          142.250.200.238

> facebook.com
Server:  [9.9.9.9]
Address:  9.9.9.9

Non-authoritative answer:
Name:    facebook.com
Addresses:  2a03:2880:f128:83:face:b00c:0:25de
          157.240.9.35

>
```

After this I changed DNS server to quadnet DNS server 9.9.9.9 using lserver command and then

The IP address of google.com- 142.250.200.238

The IP address of facebook.com-157.240.9.35

Thus, there is change in Ip address of IP addresses obtained.

Part 3:

```
C:\Users\HP\Desktop\SEM 5\COL334\Assignment\Iperf\iperf-3.1.3-win64>ping google.com

Pinging google.com [142.250.193.206] with 32 bytes of data:
Reply from 142.250.193.206: bytes=32 time=4ms TTL=118
Reply from 142.250.193.206: bytes=32 time=5ms TTL=118
Reply from 142.250.193.206: bytes=32 time=5ms TTL=118
Reply from 142.250.193.206: bytes=32 time=5ms TTL=118

Ping statistics for 142.250.193.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 5ms, Average = 4ms

C:\Users\HP\Desktop\SEM 5\COL334\Assignment\Iperf\iperf-3.1.3-win64>ping -l000 -i 1 google.com
Bad parameter google.com.

C:\Users\HP\Desktop\SEM 5\COL334\Assignment\Iperf\iperf-3.1.3-win64>ping -l 1000 -i 1 google.com

Pinging google.com [142.250.193.206] with 1000 bytes of data:
Reply from 10.184.0.14: TTL expired in transit.
Reply from 10.184.0.14: TTL expired in transit.
Reply from 10.184.0.14: TTL expired in transit.
Reply from 10.184.0.14: TTL expired in transit.

Ping statistics for 142.250.193.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\HP\Desktop\SEM 5\COL334\Assignment\Iperf\iperf-3.1.3-win64>ping -l 1000 -i 10 google.com

Pinging google.com [142.250.193.206] with 1000 bytes of data:
Reply from 142.250.193.206: bytes=68 (sent 1000) time=4ms TTL=118
Reply from 142.250.193.206: bytes=68 (sent 1000) time=9ms TTL=118
Reply from 142.250.193.206: bytes=68 (sent 1000) time=7ms TTL=118
Reply from 142.250.193.206: bytes=68 (sent 1000) time=5ms TTL=118

Ping statistics for 142.250.193.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 9ms, Average = 6ms
```

```
C:\Users\HP\Desktop\SEM 5\COL334\Assignment\Iperf\iperf-3.1.3-win64>ping -l 1000 -i 5 google.com

Pinging google.com [2404:6800:4002:810::200e] with 1000 bytes of data:
Reply from 2404:6800:4002:810::200e: TTL expired in transit.
Reply from 2404:6800:4002:810::200e: TTL expired in transit.
Reply from 2404:6800:4002:810::200e: TTL expired in transit.
Reply from 2404:6800:4002:810::200e: TTL expired in transit.

Ping statistics for 2404:6800:4002:810::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\HP\Desktop\SEM 5\COL334\Assignment\Iperf\iperf-3.1.3-win64>ping -l 200 -i 15 google.com

Pinging google.com [2404:6800:4002:810::200e] with 200 bytes of data:
Reply from 2404:6800:4002:810::200e: time=86ms
Reply from 2404:6800:4002:810::200e: time=53ms
Reply from 2404:6800:4002:810::200e: time=145ms
Reply from 2404:6800:4002:810::200e: time=53ms

Ping statistics for 2404:6800:4002:810::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 53ms, Maximum = 145ms, Average = 84ms
```

Part 4:

```
sibasish@LAPTOP-BKAEH353:/mnt/c/Users/HP/Desktop/SEM 5/COL334/Assignment/Iperf/iperf-3.1.3-win64$ traceroute facebook.com
traceroute to facebook.com (157.240.198.35), 30 hops max, 60 byte packets
 1  LAPTOP-BKAEH353.mshome.net (172.21.160.1)  0.400 ms  0.252 ms  0.246 ms
 2  192.168.90.199 (192.168.90.199)  7.361 ms  7.293 ms  10.869 ms
 3  * * *
 4  10.71.70.18 (10.71.70.18)  38.818 ms  49.491 ms  47.658 ms
 5  172.26.105.4 (172.26.105.4)  49.550 ms  49.545 ms  47.654 ms
 6  172.26.105.18 (172.26.105.18)  47.630 ms 172.26.105.19 (172.26.105.19)  49.900 ms  49.888 ms
 7  192.168.44.44 (192.168.44.44)  49.893 ms 192.168.44.42 (192.168.44.42)  45.802 ms 192.168.44.48 (192.168.44.48)  45.747 ms
 8  * * *
 9  * * *
10  * * *
11  * * *
12  ae4.pr02.del1.tfbnw.net (157.240.73.118)  58.314 ms * po102.psw01.del1.tfbnw.net (31.13.24.7)  39.253 ms
13  157.240.38.89 (157.240.38.89)  39.027 ms 157.240.38.67 (157.240.38.67)  49.410 ms po102.psw01.del1.tfbnw.net (31.13.24.7)  49.378 ms
14  edge-star-mini-shv-01-del1.facebook.com (157.240.198.35)  52.525 ms 173.252.67.201 (173.252.67.201)  49.389 ms po102.psw02.del1.tfbnw.net (74.119.78.33)  51.4
93 ms
```

```
sibasish@LAPTOP-BKAEH353:/mnt/c/Users/HP/Desktop/SEM 5/COL334/Assignment/Iperf/iperf-3.1.3-win64$ traceroute google.com
traceroute to google.com (142.250.77.206), 30 hops max, 60 byte packets
 1  LAPTOP-BKAEH353.mshome.net (172.21.160.1)  0.344 ms  0.324 ms  0.319 ms
 2  192.168.90.199 (192.168.90.199)  2.299 ms  2.895 ms  2.890 ms
 3  * * *
 4  10.71.70.18 (10.71.70.18)  46.038 ms  46.033 ms 10.71.70.2 (10.71.70.2)  46.055 ms
 5  172.26.105.4 (172.26.105.4)  45.948 ms  45.990 ms  45.940 ms
 6  172.26.105.18 (172.26.105.18)  45.912 ms 172.26.105.19 (172.26.105.19)  44.170 ms 172.26.105.18 (172.26.105.18)  49.805 ms
 7  192.168.44.48 (192.168.44.48)  44.193 ms 192.168.44.46 (192.168.44.46)  47.192 ms 192.168.44.44 (192.168.44.44)  54.882 ms
 8  * * *
 9  * * *
10  * 142.250.168.56 (142.250.168.56)  157.241 ms *
11  142.250.161.100 (142.250.161.100)  157.232 ms 142.250.47.144 (142.250.47.144)  157.110 ms 142.250.161.100 (142.250.161.100)  157.104 ms
12  142.251.52.218 (142.251.52.218)  157.100 ms * *
13  108.170.251.113 (108.170.251.113)  100.186 ms  100.155 ms 142.251.52.214 (142.251.52.214)  100.207 ms
14  108.170.251.122 (108.170.251.122)  100.158 ms 74.125.244.193 (74.125.244.193)  99.172 ms 108.170.251.98 (108.170.251.98)  99.022 ms
15  del11s08-in-f14.1e100.net (142.250.77.206)  48.048 ms * *
```

After changing ISP

```
sibasish@LAPTOP-BKAEH353:/mnt/c/Users/HP/Desktop/SEM 5/COL334/Assignment/Iperf/iperf-3.1.3-win64$ traceroute google.com
traceroute to google.com (142.250.67.46), 30 hops max, 60 byte packets
 1  LAPTOP-BKAEH353.mshome.net (172.21.160.1)  0.310 ms  0.401 ms  0.230 ms
 2  192.168.29.197 (192.168.29.197)  4.920 ms  6.216 ms  4.859 ms
 3  192.168.59.1 (192.168.59.1)  34.936 ms  48.838 ms  48.819 ms
 4  192.168.27.57 (192.168.27.57)  63.161 ms 192.168.27.69 (192.168.27.69)  67.724 ms 192.168.27.57 (192.168.27.57)  60.140 ms
 5  192.168.27.109 (192.168.27.109)  63.111 ms 192.168.27.111 (192.168.27.111)  60.012 ms 192.168.27.107 (192.168.27.107)  67.632 ms
 6  nsg-corporate-1.39.185.122.airtel.in (122.185.39.1)  67.625 ms  65.954 ms nsg-corporate-5.39.185.122.airtel.in (122.185.39.5)  88.055 ms
 7  72.14.217.194 (72.14.217.194)  95.286 ms * *
 8  * * *
 9  142.251.76.196 (142.251.76.196)  61.151 ms * *
10  108.170.251.106 (108.170.251.106)  86.930 ms  75.214 ms 74.125.244.195 (74.125.244.195)  86.422 ms
11  * * *
12  74.125.242.145 (74.125.242.145)  116.100 ms 172.253.72.137 (172.253.72.137)  104.178 ms  122.314 ms
13  74.125.242.145 (74.125.242.145)  116.041 ms 108.170.225.89 (108.170.225.89)  85.781 ms  87.220 ms
14  * * *
15  * maa05s12-in-f14.1e100.net (142.250.67.46)  101.866 ms  101.301 ms
sibasish@LAPTOP-BKAEH353:/mnt/c/Users/HP/Desktop/SEM 5/COL334/Assignment/Iperf/iperf-3.1.3-win64$ traceroute facebook.com
traceroute to facebook.com (157.240.239.35), 30 hops max, 60 byte packets
 1  LAPTOP-BKAEH353.mshome.net (172.21.160.1)  0.434 ms  0.390 ms  0.375 ms
 2  192.168.29.197 (192.168.29.197)  3.887 ms  3.491 ms  3.897 ms
 3  192.168.59.1 (192.168.59.1)  56.625 ms  56.611 ms  56.596 ms
 4  192.168.27.81 (192.168.27.81)  62.402 ms 192.168.27.93 (192.168.27.93)  62.380 ms 192.168.27.81 (192.168.27.81)  62.303 ms
 5  192.168.27.105 (192.168.27.105)  62.271 ms  62.262 ms 192.168.27.109 (192.168.27.109)  68.035 ms
 6  nsg-corporate-1.39.185.122.airtel.in (122.185.39.1)  62.196 ms nsg-corporate-5.39.185.122.airtel.in (122.185.39.5)  65.154 ms  59.253 ms
 7  ae20.pr03.del1.tfbnw.net (157.240.70.152)  65.086 ms  291.816 ms ae20.pr02.del1.tfbnw.net (157.240.69.238)  291.770 ms
 8  po103.psw02.del1.tfbnw.net (74.119.78.135)  72.477 ms po102.psw04.del1.tfbnw.net (157.240.50.169)  72.460 ms po103.psw02.del1.tfbnw.net (74.119.78.135)  72.45
9 ms
 9  173.252.67.223 (173.252.67.223)  48.928 ms 157.240.39.83 (157.240.39.83)  72.438 ms 157.240.39.143 (157.240.39.143)  48.911 ms
10  edge-star-mini-shv-02-del1.facebook.com (157.240.239.35)  72.446 ms  72.443 ms  72.440 ms
```

We can force traceroute to use IPV4 by using

traceroute -4 www.google.com

and we can use traceroute to 10.*.*.* to traceroute to a private IP and we can use -I flag to force the routers to reply.

Packet Analyzer

Part 1(DNS)

Subtask 1:

DNS Query and response messages are sent over UDP

Subtask 2:

1 DNS query is sent from browser to DNS Server

Subtask 3:

1 Local DNS Server and 4 authoritative servers are involved

Subtask 4:

The dns1.cc.iitd.ernet.in replies with actual IP address

Subtask 5:

Yes, all DNS servers respond

Subtask 6:

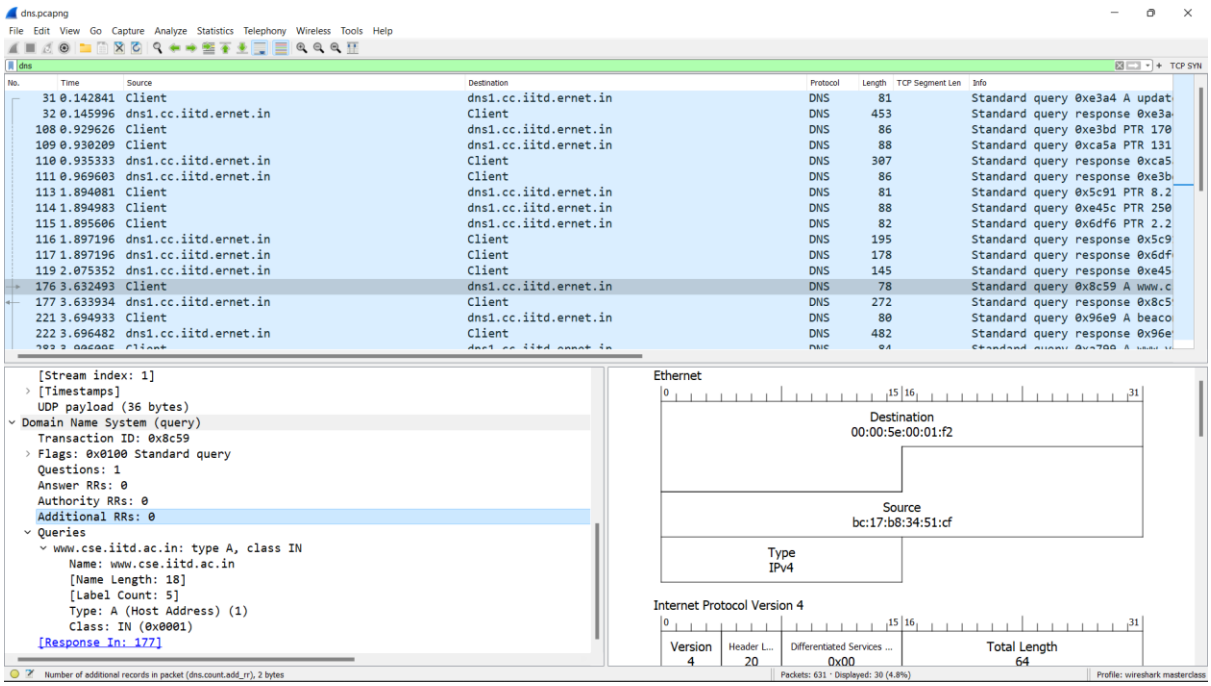
Name: www.cse.iitd.ac.in, bahar.cse.iitd.ac.in

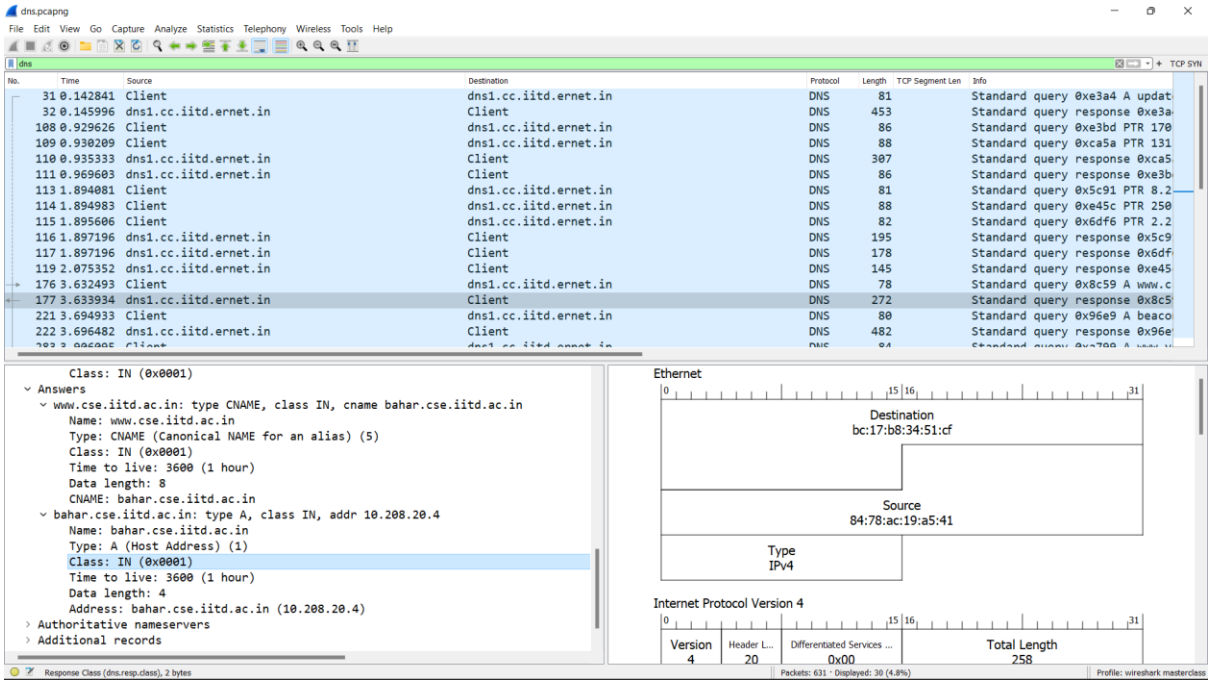
Value: 10.208.20.4

Type: CNAME, A

Class: IN(0x0001)

TTL: 3600s(1 hour)




dns.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
TCP SYN
No. Time Source Destination Protocol Length TCP Segment Len Info
31 0.142841 Client dns1.cc.iitd.ernet.in DNS 81 Standard query 0xe3a4 A updat
32 0.145996 dns1.cc.iitd.ernet.in Client DNS 453 Standard query response 0xe3a
108 0.929626 Client dns1.cc.iitd.ernet.in DNS 86 Standard query 0xe3bd PTR 170
109 0.930209 Client dns1.cc.iitd.ernet.in DNS 88 Standard query 0xca5a PTR 131
110 0.935333 dns1.cc.iitd.ernet.in Client DNS 307 Standard query response 0xca5
111 0.969603 dns1.cc.iitd.ernet.in Client DNS 86 Standard query response 0xe3b
113 1.894081 Client dns1.cc.iitd.ernet.in DNS 81 Standard query 0x5c91 PTR 8.2
114 1.894983 Client dns1.cc.iitd.ernet.in DNS 88 Standard query 0xe45c PTR 250
115 1.895606 Client dns1.cc.iitd.ernet.in DNS 82 Standard query 0x6df6 PTR 2.2
116 1.897196 dns1.cc.iitd.ernet.in Client DNS 195 Standard query response 0x5c9
117 1.897196 dns1.cc.iitd.ernet.in Client DNS 178 Standard query response 0x6df
119 2.075352 dns1.cc.iitd.ernet.in Client DNS 145 Standard query response 0xe45
176 3.632493 Client dns1.cc.iitd.ernet.in DNS 78 Standard query 0x8c59 A www.c
177 3.633934 dns1.cc.iitd.ernet.in Client DNS 272 Standard query response 0x8c5
221 3.694933 Client dns1.cc.iitd.ernet.in DNS 80 Standard query 0x96e9 A beaco
222 3.696482 dns1.cc.iitd.ernet.in Client DNS 482 Standard query response 0x96e
Class: IN (0x0001)
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: bahar.cse.iitd.ac.in (10.208.20.4)
Authoritative nameservers
Additional records
Ethernet
0 15 16 31
Destination
bc:17:b8:34:51:cf
Source
84:78:ac:19:a5:41
Type
IPv4
Internet Protocol Version 4
0 15 16 31
Version
4
Header L...
20
Differentiated Services ...
0x00
Total Length
258
Response Class (dns.resp.class), 2 bytes
Packets: 631 · Displayed: 30 (4.8%)
Profile: wireshark masterclass

Part 2:

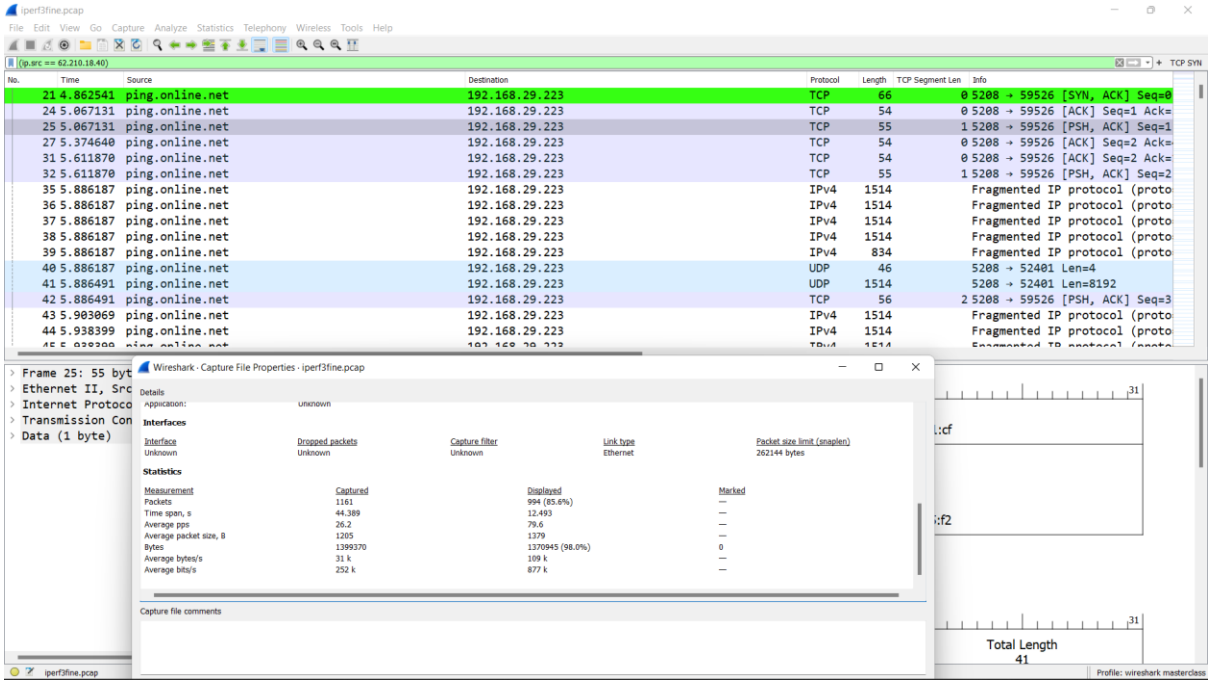
Subtask 1:

165 UDP packets are exchanged between iperf3 client and remote server.

Subtask 2:

The remote server is sending bulk data to the iperf client

Average size of packet sent is around 1205 bytes.



Subtask 3:

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	165	100.0	225114	173 k	0	0	0
Ethernet	100.0	165	1.0	2310	1776	0	0	0
Internet Protocol Version 4	100.0	165	1.5	3300	2537	0	0	0
User Datagram Protocol	100.0	165	0.6	1320	1014	0	0	0
Data	100.0	165	593.2	1335304	1026 k	165	1335304	1026 k

```
C:\Users\HP\Desktop\SEM 5\COL334\Assignment\Iperf\iperf-3.1.3-win64>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
[  4] local 192.168.29.223 port 61037 connected to 62.210.18.40 port 5208
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-1.00   sec   136 KBytes  1.11 Mbits/sec  145.806 ms  0/17 (0%)
[  4]   1.00-2.02   sec   112 KBytes   906 Kbits/sec  75.382 ms  0/14 (0%)
[  4]   2.02-3.00   sec   152 KBytes  1.26 Mbits/sec  37.276 ms  0/19 (0%)
[  4]   3.00-4.01   sec   128 KBytes  1.04 Mbits/sec  25.323 ms  0/16 (0%)
[  4]   4.01-5.00   sec   120 KBytes   984 Kbits/sec  19.196 ms  0/15 (0%)
[  4]   5.00-6.00   sec   128 KBytes  1.05 Mbits/sec  19.007 ms  0/16 (0%)
[  4]   6.00-7.01   sec  72.0 KBytes   584 Kbits/sec  16.384 ms  0/9 (0%)
[  4]   7.01-8.01   sec   192 KBytes  1.58 Mbits/sec  43.297 ms  0/24 (0%)
[  4]   8.01-9.00   sec   120 KBytes   988 Kbits/sec  28.831 ms  0/15 (0%)
[  4]   9.00-10.01  sec   128 KBytes  1.04 Mbits/sec  30.881 ms  0/16 (0%)
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-10.01  sec  1.28 MBytes  1.07 Mbits/sec  41.418 ms  0/162 (0%)
[  4] Sent 162 datagrams

iperf Done.
```

Analysing the data and length of each packet we can get that

Total UDP length =46*2+8192*163=1335388bytes

Total number of bits=8*1335388=10682460

Time of transaction =time of last packet-time of first packet=11.443904-1.038893=10.405011

Throughput=Total number of bits/time of transaction=1026664.94057bits/s=1.03Mbits/s

The bandwidth according to Iperf terminal is 1.07Mbits/s for UDP transmission

Value from Wireshark=173Kbits/s

The difference for Wireshark is because it also calculated the IPV4 protocol data and the headers also included in the packets

Calculated value and iperf3 value are almost same but are different from Wireshark capture file properties

Wireshark · Capture File Properties · iperf_final.pcap

Details

File

Name:	C:\Users\HP\Desktop\SEM 5\COL334\Assignment\Assignment1\iperf_final.pcap
Length:	1388 kB
Hash (SHA256):	a3692aa01075d39a90437ab1a45c579000b5ac5b574ccddf7d2a16f2cd44237d
Hash (RIPEMD160):	45b1b2b70a9a07f51b82e98cc68eda9cf33b690a
Hash (SHA1):	9f0b622ff87e21f80bd090030a9926e88c243444
Format:	Wireshark/tcpdump/... - pcap
Encapsulation:	Ethernet
Snapshot length:	262144

Time

First packet:	2022-08-30 18:02:15
Last packet:	2022-08-30 18:02:28
Elapsed:	00:00:12

Capture

Hardware:	Unknown
OS:	Unknown
Application:	Unknown

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	1009	165 (16.4%)	—
Time span, s	12.781	10.405	—
Average pps	78.9	15.9	—
Average packet size, B	1360	1364	—
Bytes	1372125	225114 (16.4%)	0
Average bytes/s	107 k	21 k	—
Average bits/s	858 k	173 k	—

Wireshark · Protocol Hierarchy Statistics · iperf3fine.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	1161	100.0	1399370	252 k	0	0	0
Ethernet	100.0	1161	1.2	16254	2929	0	0	0
Internet Protocol Version 6	1.0	12	0.0	480	86	0	0	0
Transmission Control Protocol	0.7	8	0.1	1633	294	3	72	12
Transport Layer Security	0.3	4	0.1	1460	263	4	1460	263
Data	0.1	1	0.0	1	0	1	1	0
Internet Control Message Protocol v6	0.3	4	0.0	120	21	4	120	21
Internet Protocol Version 4	98.6	1145	1.6	22900	4127	0	0	0
User Datagram Protocol	17.3	201	0.1	1608	289	0	0	0
Domain Name System	3.1	36	0.2	2568	462	36	2568	462
Data	14.2	165	95.4	1335304	240 k	165	1335304	240 k
Transmission Control Protocol	11.1	129	1.3	18391	3314	78	7763	1399
Transport Layer Security	3.4	39	0.9	12859	2317	38	8322	1499
Data	1.1	13	0.0	579	104	13	579	104
Data	70.2	815	79.8	1117120	201 k	815	1117120	201 k
Address Resolution Protocol	0.3	4	0.0	112	20	4	112	20

Part 3:

HTTP Task

Subtask 1: No of HTTP2 packets present are 10

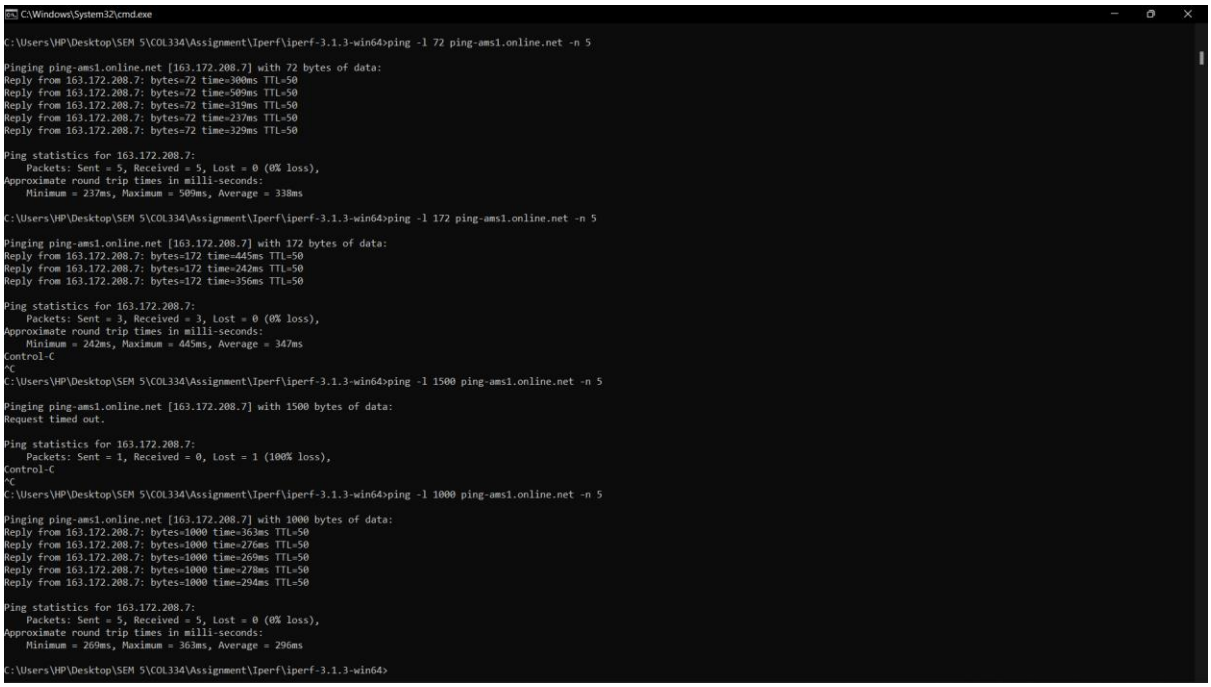
No of HTTP/1.1 packets present are 2

Subtask 2: The data comes after 5 packets

Subtask 3:

In HTTP 1.1 header is in plain text format whereas in HTTP 2 header is in compressed and encoded format.

Part 4:



Subtask 1:

10 IP packets *are exchanged in the communication between your host and the remote server representing ping-ams1.online.net*

Subtask 2:

Size of each ping request from host to remote server is 1042 Bytes.

Subtask 3:

Packets from host to server

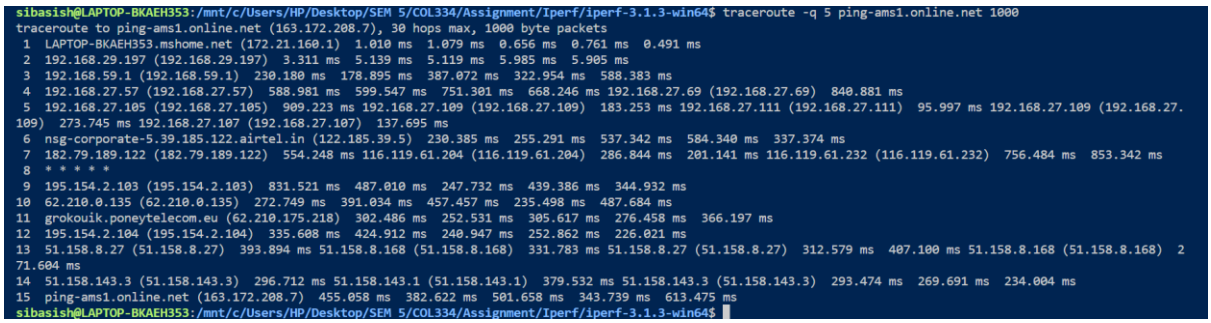
Packet no	Source IP	Destination IP	Fragmented	Length	More Fragments	Don't Fragment	Time
59	192.68.90.223	163.172.208.7	NO	1042	Not Set	Not Set	4.080035
62	192.68.90.223	163.172.208.7	NO	1042	Not Set	Not Set	5.089114
71	192.68.90.223	163.172.208.7	NO	1043	Not Set	Not Set	6.117962
75	192.68.90.223	163.172.208.7	NO	1043	Not Set	Not Set	7.127614
77	192.68.90.223	163.172.208.7	NO	1043	Not Set	Not Set	8.145428

Packets from server to host

Packet no	Source IP	Destination IP	Fragmented	Length	More Fragments	Don't Fragment	Time
60	163.172.208.7	192.68.90.223	NO	1042	Not Set	Not Set	4.386703
67	163.172.208.7	192.68.90.223	NO	1042	Not Set	Not Set	5.322727
74	163.172.208.7	192.68.90.223	NO	1043	Not Set	Not Set	6.428730
76	163.172.208.7	192.68.90.223	NO	1043	Not Set	Not Set	7.551122
78	163.172.208.7	192.68.90.223	NO	1043	Not Set	Not Set	8.484536

We can know if the packet is fragmented or not if we check the more fragmented and don't fragmented flags in the packet.

Part 5:



Subtask 1:

No of hops involved =15

Subtask 2:

Total number of packets exchanged in the transmission is 148

Packets from client to remote machine =78

Packets from remote machine to client =70

Sl. no	IP address of remote machine	No of packets sent to client	No of packets received from client
1	172.21.160.1		
2	192.168.29.197	5	5
3	192.168.59.1	5	5
4	192.168.27.57	4	5
5	192.168.27.105	1	5
6	122.185.39.5	5	5
7	182.79.189.122	1	5
8	*	*	*

9	195.154.2.103	5	5
10	62.210.0.135	5	5
11	62.210.175.218	5	5
12	195.154.2.104	5	5
13	51.158.8.27	3	5
14	51.158.143.3	4	5
15	163.172.208.7	10	5

Subtask 3:

The fields which are same are:

i)Internet Protocol Version: As we have used IPv4 protocol for all packets.

ii) length of packets: As these, all are ICMP packets, so they have the same length.

iii)destination IP: As we are the ones to receive the packets.

iv)Protocol: These are all ICMP packets.

v) Type of ICMP messages: All are TTL exceeded type messages

The fields which are different are:

i)Port numbers: port number for source and destination are different

ii) Packet ID: IP packets must have different ids.

iii)Time to live: subsequent packet has greater TTL.

iv)checksum: As the header changes, so checksum also should change.