CN Assignment -1
Basant Solanky (12040430)

PART 1
Basic Networking Tools

1. ifconfig

ifconfig - configure a network interface.
Ifconfig is used to configure the kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary.

- Outputs:-

  • docker0:- The docker0 interface serves as a bridge network in Docker, enabling communication among containers and with the host system.

  • enp4s0:- The enp4s0 Ethernet interface represents a physical network connection.

  • lo (Loopback):- The lo interface enables local communication on the device itself. such as accessing local services via the IP address 127.0.0.1 or by Localhost.

  • wlp0s20f3:- The wlp0s20f3 wireless interface provides connectivity between the host system and wireless networks.

- Options:-

  • ifconfig -a:- Display all interfaces that are currently available, even if down.

  • ifconfig <interface name> up:- This flag causes the interface to be activated. eg. ifconfig wlp0s20f3 up (requires sudo to run).

  • ifconfig <interface name> down:- This flag causes the driver for this in-interface to be shut down. eg. ifconfig wlp0s20f3 down.

  • ifconfig -s:- Displays a simplified summary of network interfaces on the host system.

```
 Mon Aug-8 4:51:36pm   CPU 20.5% 0 Net 16   mafia ~   14M 60
> ifconfig
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        inet6 fe80::42:67ff:fedd:c895  prefixlen 64  scopeid 0x20<link>
        ether 02:42:67:dd:c8:95  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 524  bytes 97705 (97.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp4s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether b0:7b:25:3c:2c:0c  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 11361  bytes 1299069 (1.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11361  bytes 1299069 (1.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vetha31a1d8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::8c2a:d5ff:feef:4565  prefixlen 64  scopeid 0x20<link>
        ether 8e:2a:d5:ef:45:65  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 577  bytes 104439 (104.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.19.116  netmask 255.255.252.0  broadcast 10.10.19.255
        inet6 fe80::1700:7dd2:efba:c295  prefixlen 64  scopeid 0x20<link>
        ether c8:e2:65:6a:e2:94  txqueuelen 1000  (Ethernet)
        RX packets 1593123  bytes 1915708951 (1.9 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 332974  bytes 72417375 (72.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

 Mon Aug-8 5:02:25pm   CPU 20.5% 0 Net 49   mafia ~   14M 60
>
```

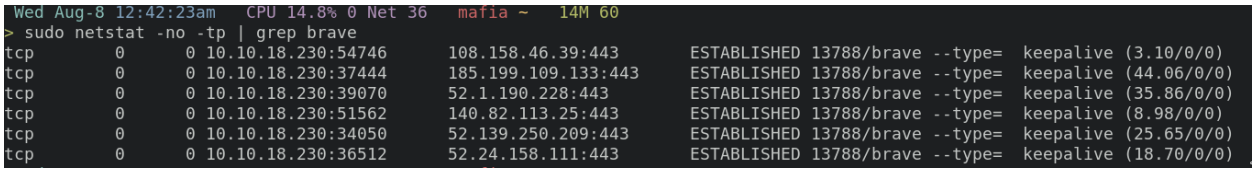
2. netstat

The netstat command is a networking tool for configuration and troubleshooting that may also be used to keep track of network connections. It is an effective tool that may be used to identify network faults, track network activity, and resolve security problems.

- The active TCP port on your system:-

```
 Wed Aug-8 12:41:30am   CPU 15.5% 0 Net 75   mafia ~   14M 60
> netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 mafia:53166             150.138.117.34.bc:https TIME_WAIT
tcp        0      0 mafia:59710             bom07s45-in-f10.1:https TIME_WAIT
tcp        0      0 mafia:46628             104.16.137.15:https     ESTABLISHED
tcp        0      0 mafia:38676             146.75.112.157:https    ESTABLISHED
tcp        0      0 mafia:33570             ec2-54-243-64-124:https ESTABLISHED
tcp        0      0 mafia:39620             kul01s09-in-f66.1:https TIME_WAIT
tcp        0      0 mafia:39634             kul01s09-in-f66.1:https TIME_WAIT
tcp        0      0 mafia:32928             20.207.73.82:https      ESTABLISHED
tcp        0      0 mafia:48564             200.221.207.35.bc:https ESTABLISHED
tcp        0      0 mafia:50192             bom07s35-in-f2.1e:https TIME_WAIT
tcp        0      0 mafia:60476             a23-202-33-114.de:https ESTABLISHED
tcp        0      0 mafia:35834             199.232.45.44:https     ESTABLISHED
tcp        0      0 mafia:54746             server-108-158-46:https ESTABLISHED
tcp        0      0 mafia:36968             bom12s21-in-f10.1:https TIME_WAIT
tcp        0      0 mafia:59700             bom07s45-in-f10.1:https TIME_WAIT
tcp        0      0 mafia:45518             ec2-3-227-101-219:https ESTABLISHED
tcp        0      0 mafia:60586             bom12s16-in-f14.1:https TIME_WAIT
tcp        0      0 mafia:33842             64.52.120.34.bc.g:https ESTABLISHED
tcp        1      0 mafia:37524             8.241.166.254:http      CLOSE_WAIT
tcp        0      0 mafia:38580             bom07s32-in-f5.1e:https ESTABLISHED
tcp        0      0 mafia:45012             104.18.25.173:https     ESTABLISHED
tcp        0      0 mafia:37644             104.18.13.33:https      ESTABLISHED
tcp        0      0 mafia:56432             20.207.73.85:https      ESTABLISHED
tcp        0      0 mafia:37444             cdn-185-199-109-1:https ESTABLISHED
tcp        0      0 mafia:35108             bom12s12-in-f5.1e:https ESTABLISHED
tcp        0      0 mafia:39070             ec2-52-1-190-228.:https ESTABLISHED
tcp       78      0 mafia:60150             ec2-34-205-226-42:https CLOSE_WAIT
tcp        0      0 mafia:54494             20.198.162.76:https     ESTABLISHED
tcp        0      0 mafia:39982             199.232.45.140:https    ESTABLISHED
tcp        0      0 mafia:51562             lb-140-82-113-25-:https ESTABLISHED
tcp        0      0 mafia:38812             a23-202-33-211.de:https ESTABLISHED
tcp        0      0 mafia:57250             20.42.65.89:https       ESTABLISHED
tcp        0      0 mafia:51874             64.52.120.34.bc.g:https ESTABLISHED
tcp        0      0 mafia:38820             a23-202-33-211.de:https ESTABLISHED
tcp        0      0 mafia:51886             64.52.120.34.bc.g:https ESTABLISHED
tcp        0      0 mafia:35106             bom12s12-in-f5.1e:https ESTABLISHED
tcp        0      0 mafia:56436             20.207.73.85:https      ESTABLISHED
tcp        0      0 mafia:34050             52.139.250.209:https    ESTABLISHED
tcp        0      0 mafia:37646             104.18.13.33:https      ESTABLISHED
tcp        0      0 mafia:56620             199.232.45.44:https     ESTABLISHED
tcp        0      0 mafia:39988             199.232.45.140:https    ESTABLISHED
tcp        0      0 mafia:36512             ec2-52-24-158-111:https ESTABLISHED
 Wed Aug-8 12:41:41am   CPU 15.3% 0 Net 41   mafia ~   14M 60
>
```

The PID used by brave-browser is 13788. Some local PORTS used by the browser are:- 54746, 37444, 39070, 51562, 34050,36512 as mentioned in the pic attached below.



HTTPS's well-known port is 443 and all the 6 connections mentioned above are using this standard port.

- The **"-su"** option of netstat can be used to show the statistics of all UDP connections.

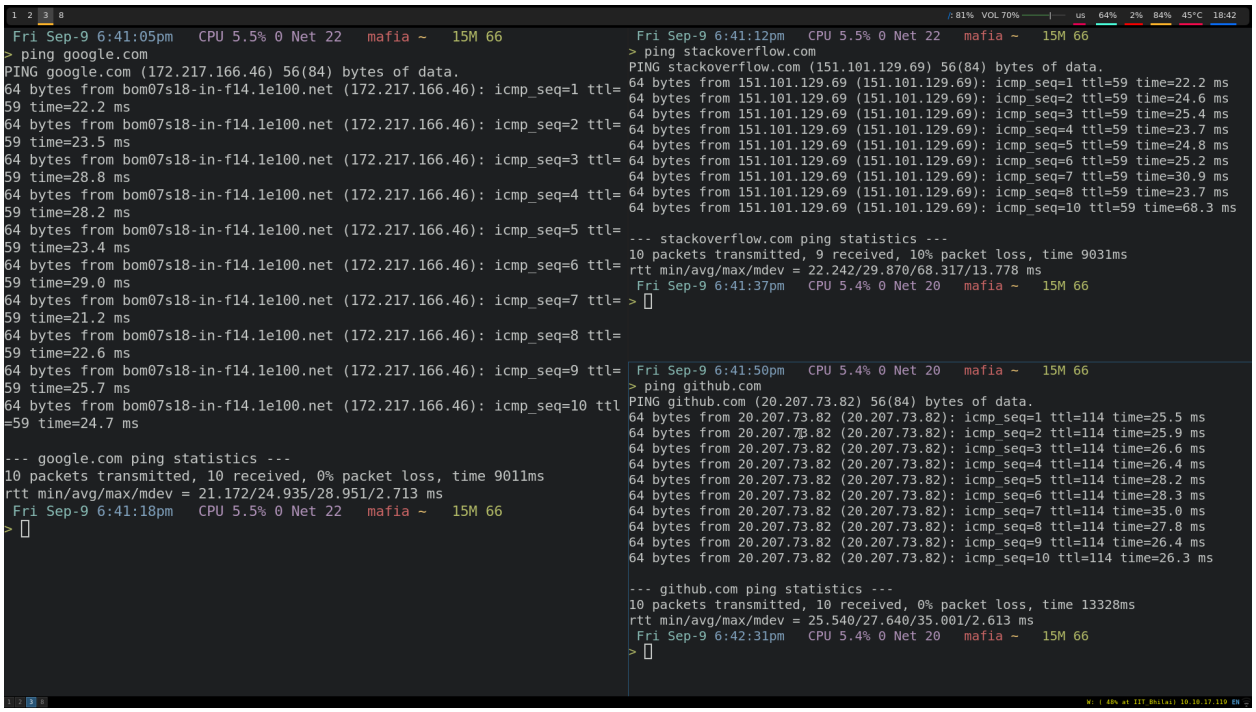
```
 Wed Aug-8 12:43:13am   CPU 14.4% 0 Net 30   mafia ~   14M 60
> netstat -su
IcmpMsg:
    InType0: 10
    InType3: 315
    InType11: 3
    OutType3: 350
    OutType8: 20
Udp:
    102750 packets received
    409 packets to unknown port received
    564 packet receive errors
    33822 packets sent
    564 receive buffer errors
    17 send buffer errors
UdpLite:
IpExt:
    InMcastPkts: 88
    OutMcastPkts: 164
    InBcastPkts: 2
    OutBcastPkts: 4
    InOctets: 214980142
    OutOctets: 13737812
    InMcastOctets: 8794
    OutMcastOctets: 23280
    InBcastOctets: 4200
    OutBcastOctets: 4240
    InNoECTPkts: 198090
    InECT0Pkts: 6
MPTcpExt:
```

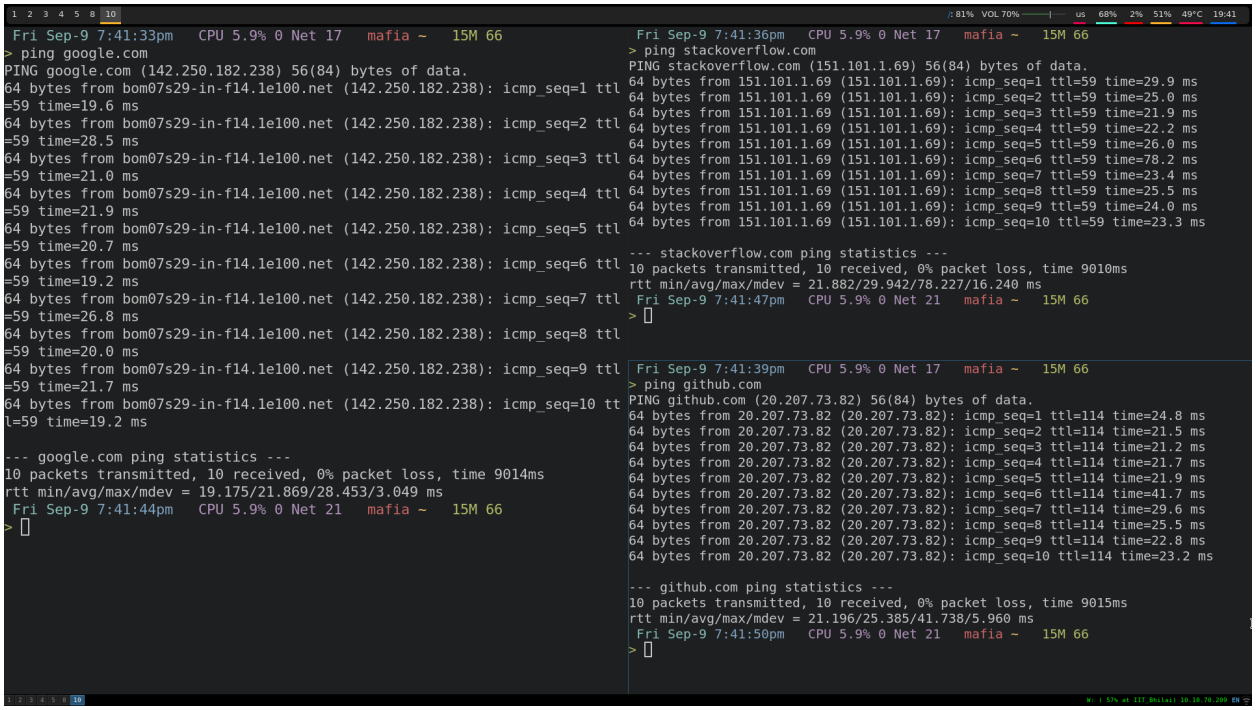
3. ping

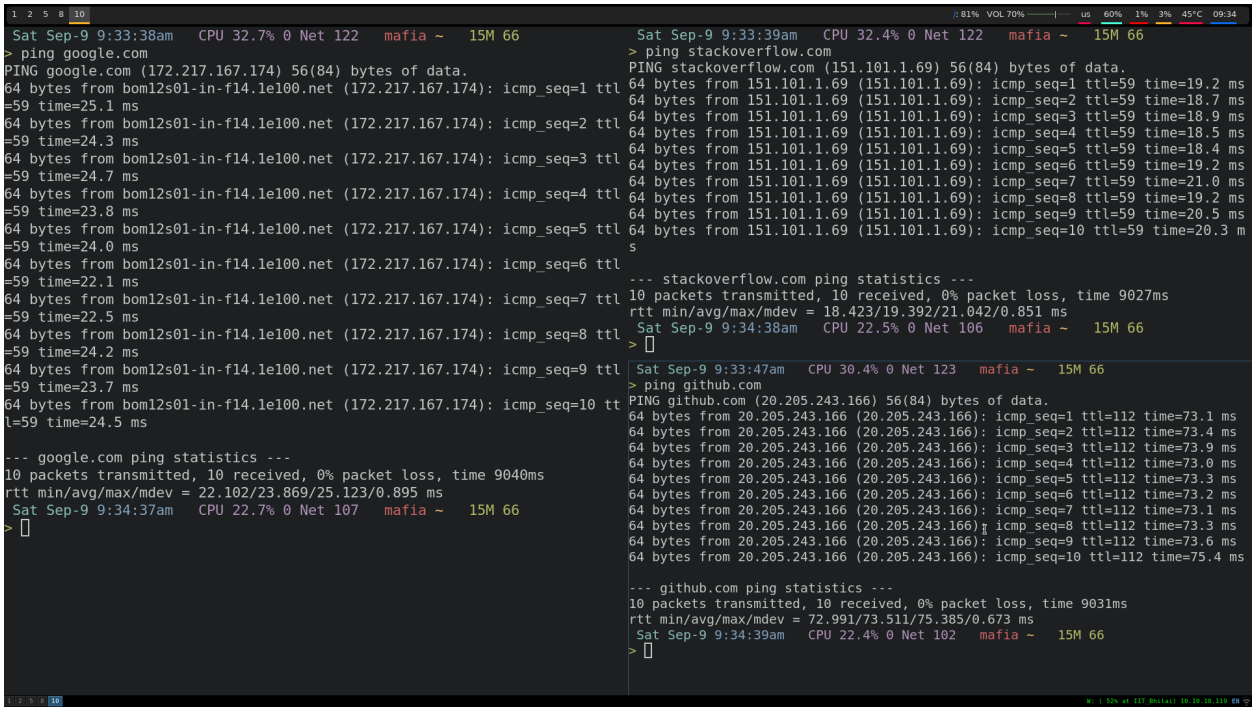
- **What is the use of the ping command?**

  The ping command is used to check the connectivity and response time of a network host, such as a server or a website, by sending packets and receiving responses. Its primary uses include Latency measurements, Troubleshooting, testing connectivity with websites, continuous monitoring, packet information, etc.

- **Select three hosts of your choice on the Internet and experiment with pinging each host 10 times at three different hours of the day.**




Fri Sep-9 7:41:33pm CPU 5.9% 0 Net 17 mafia ~ 15M 66
> ping google.com
PING google.com (142.250.182.238) 56(84) bytes of data.
64 bytes from bom07s29-in-f14.1e100.net (142.250.182.238): icmp_seq=1 ttl=59 time=19.6 ms
64 bytes from bom07s29-in-f14.1e100.net (142.250.182.238): icmp_seq=2 ttl=59 time=28.5 ms
64 bytes from bom07s29-in-f14.1e100.net (142.250.182.238): icmp_seq=3 ttl=59 time=21.0 ms
64 bytes from bom07s29-in-f14.1e100.net (142.250.182.238): icmp_seq=4 ttl=59 time=21.9 ms
64 bytes from bom07s29-in-f14.1e100.net (142.250.182.238): icmp_seq=5 ttl=59 time=20.7 ms
64 bytes from bom07s29-in-f14.1e100.net (142.250.182.238): icmp_seq=6 ttl=59 time=19.2 ms
64 bytes from bom07s29-in-f14.1e100.net (142.250.182.238): icmp_seq=7 ttl=59 time=26.8 ms
64 bytes from bom07s29-in-f14.1e100.net (142.250.182.238): icmp_seq=8 ttl=59 time=20.0 ms
64 bytes from bom07s29-in-f14.1e100.net (142.250.182.238): icmp_seq=9 ttl=59 time=21.7 ms
64 bytes from bom07s29-in-f14.1e100.net (142.250.182.238): icmp_seq=10 ttl=59 time=19.2 ms
--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 19.175/21.869/28.453/3.049 ms
Fri Sep-9 7:41:44pm CPU 5.9% 0 Net 21 mafia ~ 15M 66
> ping stackoverflow.com
PING stackoverflow.com (151.101.1.69) 56(84) bytes of data.
64 bytes from 151.101.1.69 (151.101.1.69): icmp_seq=1 ttl=59 time=29.9 ms
64 bytes from 151.101.1.69 (151.101.1.69): icmp_seq=2 ttl=59 time=25.0 ms
64 bytes from 151.101.1.69 (151.101.1.69): icmp_seq=3 ttl=59 time=21.9 ms
64 bytes from 151.101.1.69 (151.101.1.69): icmp_seq=4 ttl=59 time=22.2 ms
64 bytes from 151.101.1.69 (151.101.1.69): icmp_seq=5 ttl=59 time=26.0 ms
64 bytes from 151.101.1.69 (151.101.1.69): icmp_seq=6 ttl=59 time=78.2 ms
64 bytes from 151.101.1.69 (151.101.1.69): icmp_seq=7 ttl=59 time=23.4 ms
64 bytes from 151.101.1.69 (151.101.1.69): icmp_seq=8 ttl=59 time=25.5 ms
64 bytes from 151.101.1.69 (151.101.1.69): icmp_seq=9 ttl=59 time=24.0 ms
64 bytes from 151.101.1.69 (151.101.1.69): icmp_seq=10 ttl=59 time=23.3 ms
--- stackoverflow.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9010ms
rtt min/avg/max/mdev = 21.882/29.942/78.227/16.240 ms
Fri Sep-9 7:41:47pm CPU 5.9% 0 Net 21 mafia ~ 15M 66
> ping github.com
PING github.com (20.207.73.82) 56(84) bytes of data.
64 bytes from 20.207.73.82 (20.207.73.82): icmp_seq=1 ttl=114 time=24.8 ms
64 bytes from 20.207.73.82 (20.207.73.82): icmp_seq=2 ttl=114 time=21.5 ms
64 bytes from 20.207.73.82 (20.207.73.82): icmp_seq=3 ttl=114 time=21.2 ms
64 bytes from 20.207.73.82 (20.207.73.82): icmp_seq=4 ttl=114 time=21.7 ms
64 bytes from 20.207.73.82 (20.207.73.82): icmp_seq=5 ttl=114 time=21.9 ms
64 bytes from 20.207.73.82 (20.207.73.82): icmp_seq=6 ttl=114 time=41.7 ms
64 bytes from 20.207.73.82 (20.207.73.82): icmp_seq=7 ttl=114 time=29.6 ms
64 bytes from 20.207.73.82 (20.207.73.82): icmp_seq=8 ttl=114 time=25.5 ms
64 bytes from 20.207.73.82 (20.207.73.82): icmp_seq=9 ttl=114 time=22.8 ms
64 bytes from 20.207.73.82 (20.207.73.82): icmp_seq=10 ttl=114 time=23.2 ms
--- github.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9015ms
rtt min/avg/max/mdev = 21.196/25.385/41.738/5.960 ms
Fri Sep-9 7:41:50pm CPU 5.9% 0 Net 21 mafia ~ 15M 66


Sat Sep-9 9:33:38am CPU 32.7% 0 Net 122 mafia ~ 15M 66
> ping google.com
PING google.com (172.217.167.174) 56(84) bytes of data.
64 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=1 ttl=59 time=25.1 ms
64 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=2 ttl=59 time=24.3 ms
64 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=3 ttl=59 time=24.7 ms
64 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=4 ttl=59 time=23.8 ms
64 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=5 ttl=59 time=24.0 ms
64 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=6 ttl=59 time=22.1 ms
64 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=7 ttl=59 time=22.5 ms
64 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=8 ttl=59 time=24.2 ms
64 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=9 ttl=59 time=23.7 ms
64 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=10 ttl=59 time=24.5 ms
--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9040ms
rtt min/avg/max/mdev = 22.102/23.869/25.123/0.895 ms
Sat Sep-9 9:34:37am CPU 22.7% 0 Net 107 mafia ~ 15M 66
> ping stackoverflow.com
PING stackoverflow.com (151.101.1.69) 56(84) bytes of data.
64 bytes from 151.101.1.69 (151.101.1.69): icmp_seq=1 ttl=59 time=19.2 ms
64 bytes from 151.101.1.69 (151.101.1.69): icmp_seq=2 ttl=59 time=18.7 ms
64 bytes from 151.101.1.69 (151.101.1.69): icmp_seq=3 ttl=59 time=18.9 ms
64 bytes from 151.101.1.69 (151.101.1.69): icmp_seq=4 ttl=59 time=18.5 ms
64 bytes from 151.101.1.69 (151.101.1.69): icmp_seq=5 ttl=59 time=18.4 ms
64 bytes from 151.101.1.69 (151.101.1.69): icmp_seq=6 ttl=59 time=19.2 ms
64 bytes from 151.101.1.69 (151.101.1.69): icmp_seq=7 ttl=59 time=21.0 ms
64 bytes from 151.101.1.69 (151.101.1.69): icmp_seq=8 ttl=59 time=19.2 ms
64 bytes from 151.101.1.69 (151.101.1.69): icmp_seq=9 ttl=59 time=20.5 ms
64 bytes from 151.101.1.69 (151.101.1.69): icmp_seq=10 ttl=59 time=20.3 ms
--- stackoverflow.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9027ms
rtt min/avg/max/mdev = 18.423/19.392/21.042/0.851 ms
Sat Sep-9 9:34:38am CPU 22.5% 0 Net 106 mafia ~ 15M 66
> ping github.com
PING github.com (20.205.243.166) 56(84) bytes of data.
64 bytes from 20.205.243.166 (20.205.243.166): icmp_seq=1 ttl=112 time=73.1 ms
64 bytes from 20.205.243.166 (20.205.243.166): icmp_seq=2 ttl=112 time=73.4 ms
64 bytes from 20.205.243.166 (20.205.243.166): icmp_seq=3 ttl=112 time=73.9 ms
64 bytes from 20.205.243.166 (20.205.243.166): icmp_seq=4 ttl=112 time=73.0 ms
64 bytes from 20.205.243.166 (20.205.243.166): icmp_seq=5 ttl=112 time=73.3 ms
64 bytes from 20.205.243.166 (20.205.243.166): icmp_seq=6 ttl=112 time=73.2 ms
64 bytes from 20.205.243.166 (20.205.243.166): icmp_seq=7 ttl=112 time=73.1 ms
64 bytes from 20.205.243.166 (20.205.243.166): icmp_seq=8 ttl=112 time=73.3 ms
64 bytes from 20.205.243.166 (20.205.243.166): icmp_seq=9 ttl=112 time=73.6 ms
64 bytes from 20.205.243.166 (20.205.243.166): icmp_seq=10 ttl=112 time=75.4 ms
--- github.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9031ms
rtt min/avg/max/mdev = 72.991/73.511/75.385/0.673 ms
Sat Sep-9 9:34:39am CPU 22.4% 0 Net 102 mafia ~ 15M 66

Time	Host Name	Avg. RTT (ms)
6:41	google.com	24.93
	stackoverflow.com	29.87
	github.com	27.64
7:41	google.com	21.86
	stackoverflow.com	29.94
	github.com	25.38
9:33	google.com	23.86
	stackoverflow.com	19.39
	github.com	73.51

The RTT tends to be longer the farther apart the source and destination are geographically. This is due to the fact that the data packets must pass via numerous network components, such as routers and switches, as well as actual communication pathways, like fibre-optic cables or satellite links. There are delays in the transfer of data due to these tools and media.

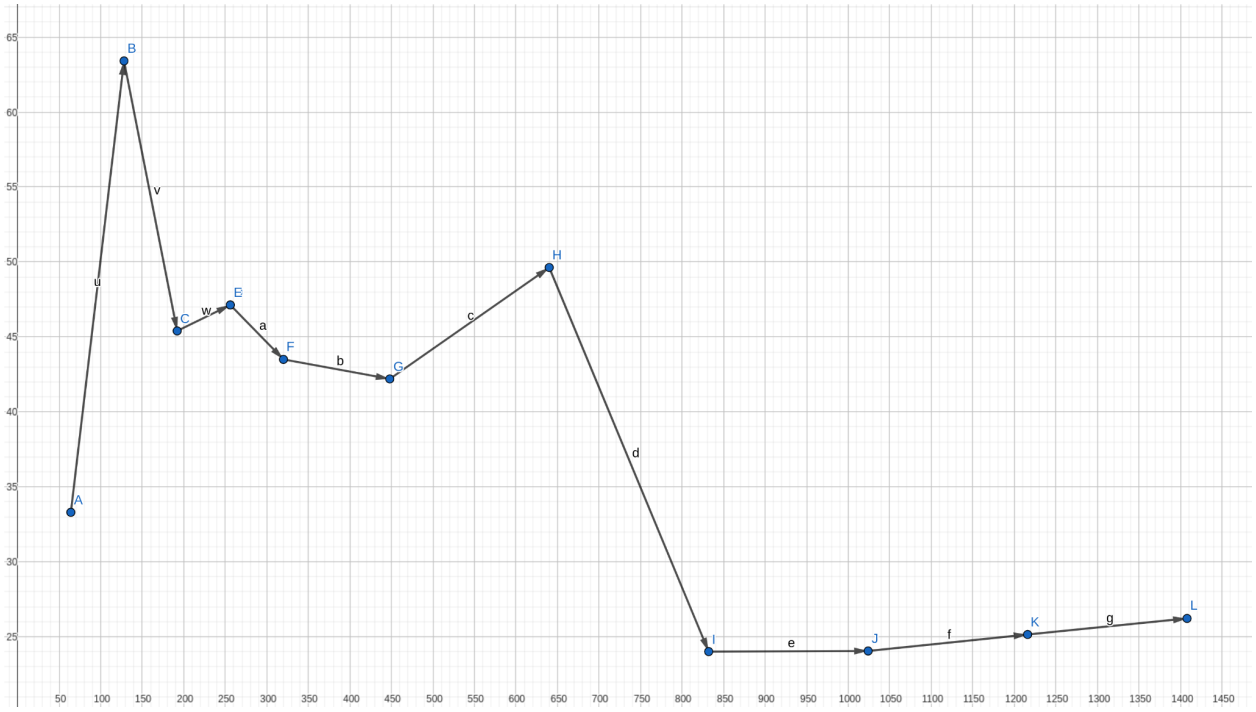
- **Pick one of the above-used hosts and repeat the experiment with different packet sizes ranging from 64 bytes to 2048 bytes. Plot average RTT vs packet size.**

cmd = **ping -c 10 -s <packet-size> google.com.**

Size	Average RTT (ms)
64	33.23

128	63.41
192	45.40
256	47.130
320	43.502
448	42.198
640	49.63
832	24.01
1024	24.05
1216	25.15
1408	26.22
2048 bytes	NA (100% loss)

After 1408 bytes of size packet loss accuracy was 100%.



RTT vs. Packet Size

- **Explain how the change in packet size, and time of the day impact RTT.**

Larger data packets typically take longer to transfer over a network because they contain more information. The RTT may go up as a result. The time of day has an impact on RTT because of network congestion. Congestion can cause packet queuing during peak hours, lengthening RTT.

4. traceroute

- **What is the use of traceroute tool?**

Traceroute is a network diagnostic tool used to trace the route that data packets take from one device device to another on a network. It provides valuable information about the path and the performance of the data. Here are some of the key uses and benefits of the traceroute tool:- Troubleshooting, Path Analysis, IPA verification, latency analysis, Service provider analysis, etc.

- **Inspect the cases when the traceroute does not find complete paths to some hosts and explain the reasons.**

Challenges with Traceroute commands for today's networks:-

1. Interfaces are not known, only the device IP node. There is no additional detail.
2. Traceroute output is the static text that cannot be acted upon easily.
3. Traceroute is missing historical information.

Ref:- https://www.netbraintech.com/blog/limitations-of-traceroute/

```
Sat Sep-9 11:18:18am   CPU 10.3% 1 Net 41   mafia ~   15M 71
> traceroute google.com
traceroute to google.com (142.251.42.46), 30 hops max, 60 byte packets
 1  _gateway (10.10.16.1)  1.536 ms  1.890 ms  2.233 ms
 2  static.ill.117.250.135.234.bsnl.co.in (117.250.135.234)  3.126 ms  3.505 ms  3.483 ms
 3  * * *
 4  * * *
 5  142.250.161.230 (142.250.161.230)  27.973 ms  27.953 ms 74.125.48.138 (74.125.48.138)  26.851 ms
 6  * * *
 7  142.250.210.182 (142.250.210.182)  28.405 ms 172.253.77.20 (172.253.77.20)  26.551 ms 142.251.77.98 (142.251.77.98)  26.157 ms
 8  108.170.248.195 (108.170.248.195)  28.336 ms 142.251.69.43 (142.251.69.43)  29.770 ms 108.170.248.210 (108.170.248.210)  30.449 ms
 9  bom12s20-in-f14.1e100.net (142.251.42.46)  27.006 ms  19.687 ms  20.670 ms
```

*** * *** are the cases when the traceroute is not able to find the complete paths to google.com.

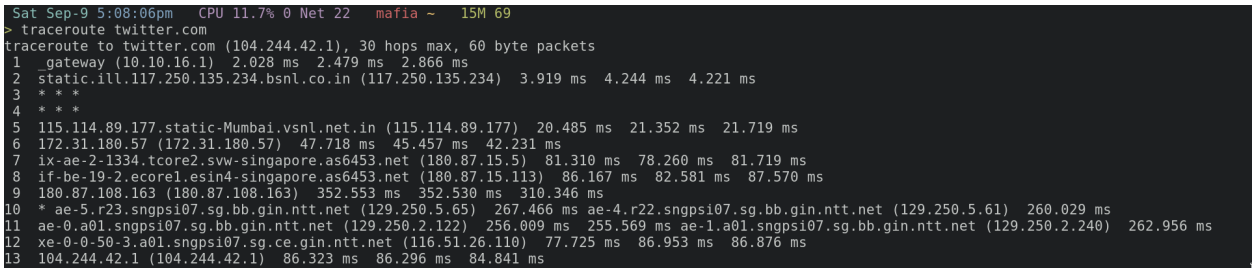
- **Is it possible to find the route to certain hosts which fail to respond with the ping experiment? Give reasoning.**

  Yes, it is possible to find the route to certain hosts even if they fail to respond to a ping experiment. The reason is that the behaviour of the protocol used in ping (ICMP echo request) and the behaviour of the protocol used in the traceroute tool (ICMP traffic or UDP or other) can be different, and network devices may treat them differently for various reasons.

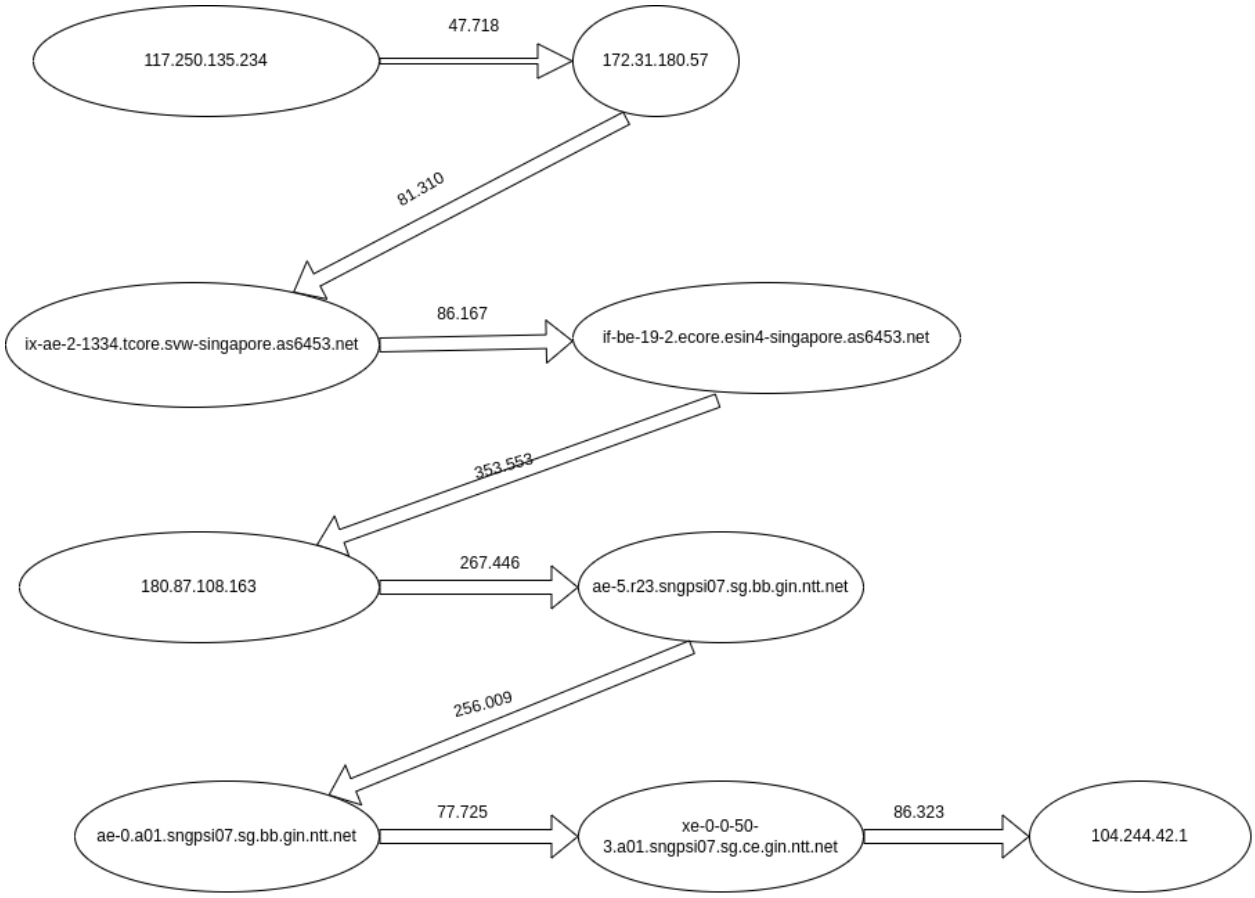
  Sometimes a host may block ICMP echo requests for security or any other reasons, at that time it may allow ICMP traffic or different protocols (UDP) used by traceroute, making it a valuable tool for network troubleshooting and diagnostics, even when ping requests are blocked.

- **Use the traceroute program to find the route to three of your favorite sites on the Internet. Draw a graph of your results, labeling each node with the IP address of the hops between your location and the destinations. The links between them should be marked with the measured delays between each link.**

Twitter.com



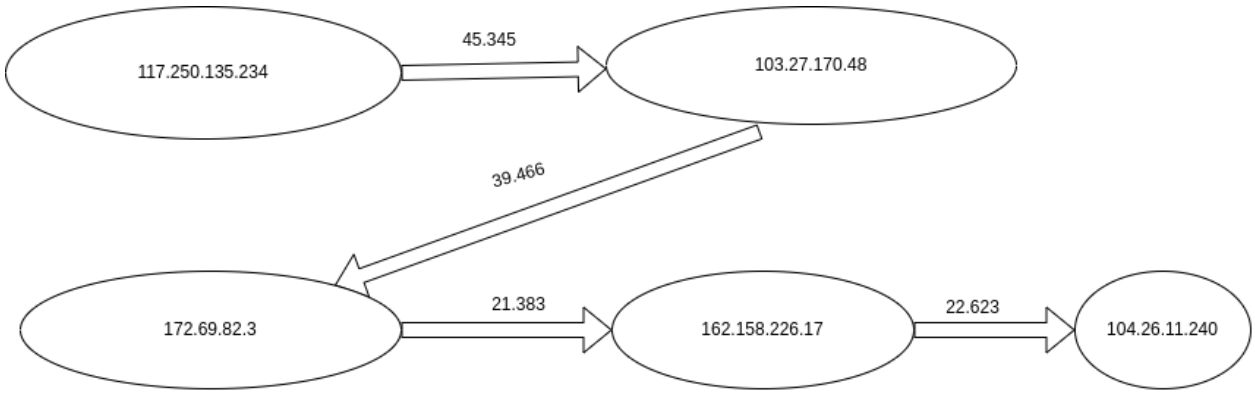
Hops	RTT (ms)
117.250.135.234	3.919
172.31.180.57	47.718
ix-ae-2-1334.tcore2.svw-singapore.as6453.net	81.310
if-be-19-2.ecore1.esin4-singapore.as6453.net	86.167
180.87.108.163	352.553
ae-5.r23.sngpsi07.sg.bb.gin.ntt.net	267.466
ae-0.a01.sngpsi07.sg.bb.gin.ntt.net	256.009
xe-0-0-50-3.a01.sngpsi07.sg.ce.gin.ntt.net	77.725
104.244.42.1	86.323


117.250.135.234
47.718
172.31.180.57
81.310
ix-ae-2-1334.tcore.svw-singapore.as6453.net
86.167
if-be-19-2.ecore.esin4-singapore.as6453.net
353.553
180.87.108.163
267.446
ae-5.r23.sngpsi07.sg.bb.gin.ntt.net
256.009
ae-0.a01.sngpsi07.sg.bb.gin.ntt.net
77.725
xe-0-0-50-
3.a01.sngpsi07.sg.ce.gin.ntt.net
86.323
104.244.42.1

Wireshark.org

```
 Sat Sep-9 6:34:01pm   CPU 11.8% 0 Net 26   mafia ~   15M 69
> traceroute wireshark.org
traceroute to wireshark.org (104.26.11.240), 30 hops max, 60 byte packets
 1  _gateway (10.10.16.1)  44.266 ms  44.203 ms  44.176 ms
 2  static.ill.117.250.135.234.bsnl.co.in (117.250.135.234)  20.941 ms  21.313 ms  21.290 ms
 3  * * *
 4  * * *
 5  103.27.170.48 (103.27.170.48)  45.345 ms  45.601 ms  45.577 ms
 6  172.69.82.3 (172.69.82.3)  39.466 ms  23.397 ms 162.158.226.17 (162.158.226.17)  21.383 ms
 7  104.26.11.240 (104.26.11.240)  22.623 ms  19.703 ms  20.261 ms
```

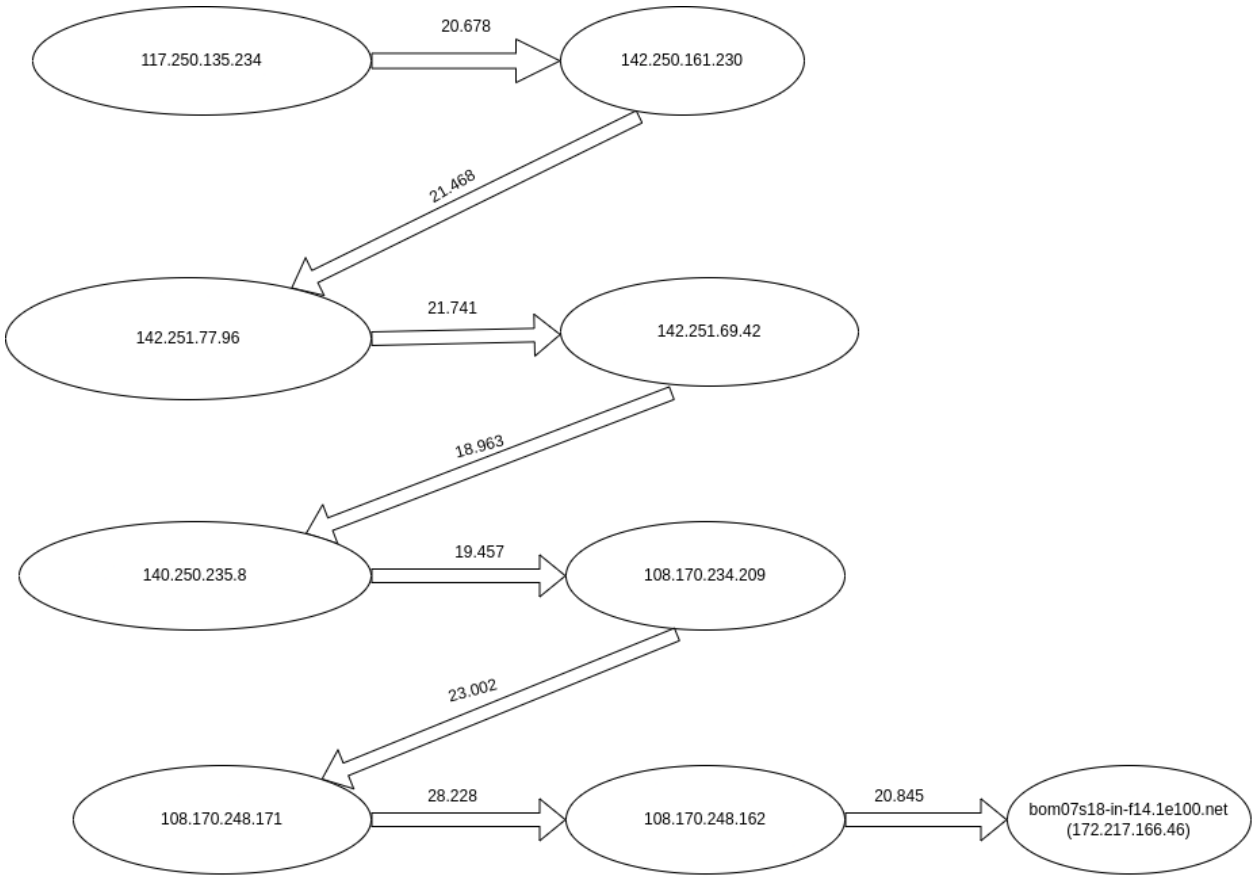
Hops	RTT
117.250.135.234	20.941ms
103.27.170.48	45.345 ms
172.69.82.3	39.466 ms
162.158.226.17	21.383 ms
104.26.11.240	22.623 ms



Google.com

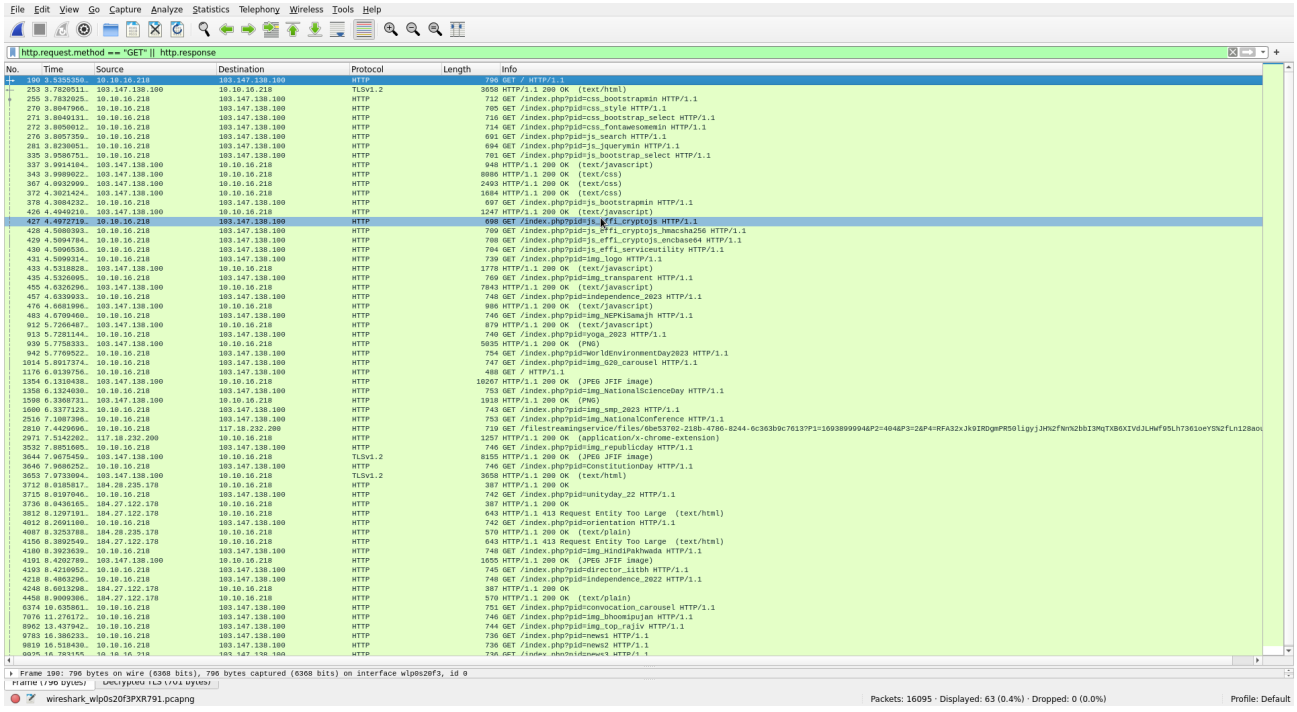
```
Sat Sep-9 6:39:12pm   CPU 11.9% 0 Net 32   mafia ~   15M 69
> traceroute google.com
traceroute to google.com (172.217.166.46), 30 hops max, 60 byte packets
 1  _gateway (10.10.16.1)  1.446 ms  1.811 ms  2.117 ms
 2  static.ill.117.250.135.234.bsnl.co.in (117.250.135.234)  2.811 ms  3.106 ms  3.083 ms
 3  * * *
 4  * * *
 5  142.250.161.230 (142.250.161.230)  20.678 ms 74.125.48.138 (74.125.48.138)  35.228 ms 142.250.161.230 (142.250.161.230)  21.006 ms
 6  * * *
 7  142.251.77.96 (142.251.77.96)  21.468 ms 142.251.69.42 (142.251.69.42)  21.741 ms 142.250.235.8 (142.250.235.8)  18.963 ms
 8  108.170.234.209 (108.170.234.209)  19.457 ms 108.170.248.171 (108.170.248.171)  23.002 ms 108.170.248.162 (108.170.248.162)  28.228 ms
 9  bom07s18-in-f14.1e100.net (172.217.166.46)  20.845 ms 108.170.248.209 (108.170.248.209)  21.610 ms  21.478 ms
```

Hops	RTT
117.250.135.234	2.811 ms
142.250.161.230	20.678 ms
142.251.77.96	21.468 ms
142.251.69.42	21.741 ms
142.250.235.8	18.963 ms
108.170.234.209	19.457 ms
108.170.248.171	23.002 ms
108.170.248.162	28.228 ms
bom07s18-in-f14.1e100.net (172.217.166.46)	20.845 ms


117.250.135.234
20.678
142.250.161.230
21.468
142.251.77.96
21.741
142.251.69.42
18.963
140.250.235.8
19.457
108.170.234.209
23.002
108.170.248.171
28.228
108.170.248.162
20.845
bom07s18-in-f14.1e100.net
(172.217.166.46)

PART 2
HTTP

1. All the GET Requests are as follows:-

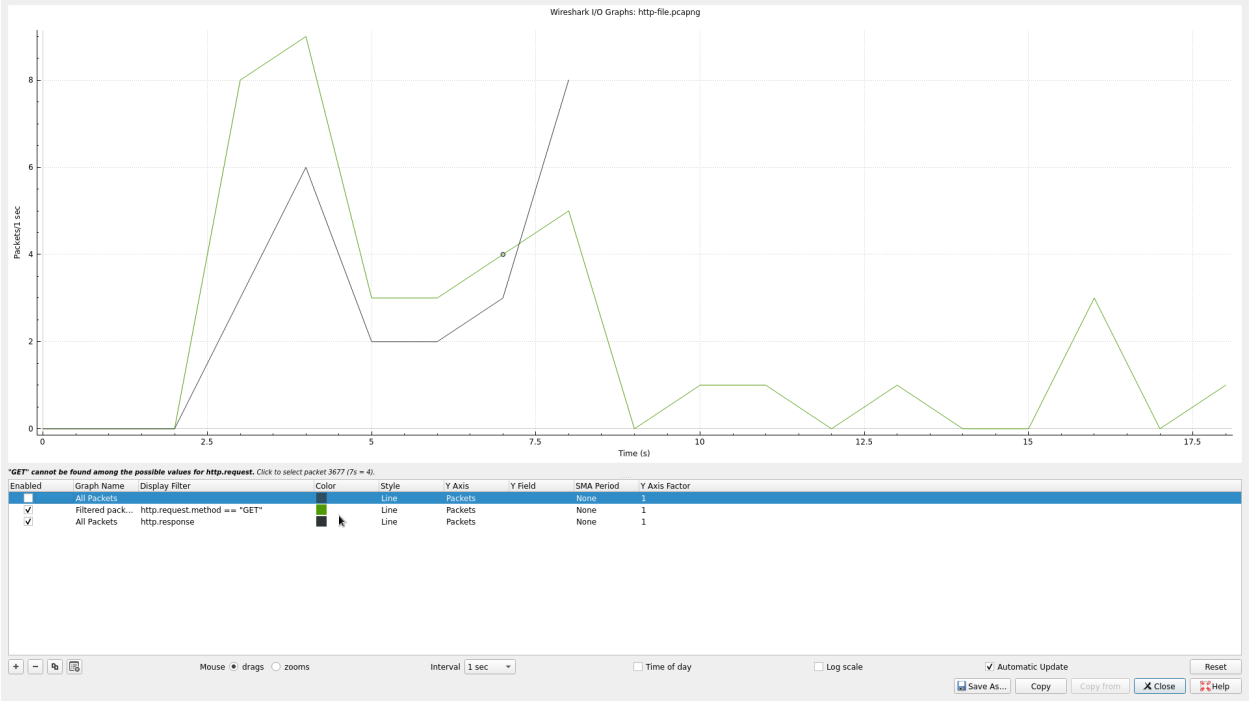


Statistics→ HTTP→ Packer Counter

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total HTTP Packets	88				0.0009	100%	0.0800	4.495
Other HTTP Packets	12				0.0001	13.64%	0.0500	103.117
HTTP Response Packets	24				0.0002	27.27%	0.0400	7.968
???: broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	2				0.0000	8.33%	0.0100	8.130
413 Request Entity Too Large	2				0.0000	100.00%	0.0100	8.130
3xx: Redirection	0				0.0000	0.00%	-	-
2xx: Success	22				0.0002	91.67%	0.0400	7.968
200 OK	22				0.0002	100.00%	0.0400	7.968
1xx: Informational	0				0.0000	0.00%	-	-
HTTP Request Packets	52				0.0005	59.09%	0.0600	3.783
SEARCH	4				0.0000	7.69%	0.0100	66.983
PUT	4				0.0000	7.69%	0.0200	26.932
POST	2				0.0000	3.85%	0.0100	8.020
OPTIONS	3				0.0000	5.77%	0.0200	7.759
GET	39				0.0004	75.00%	0.0600	3.783

Total Number of GET Requests = 39.

We are required to plot the I/O graph for the entered packets and packets sent by the filter **“http.response || http.request.method == “GET” “**



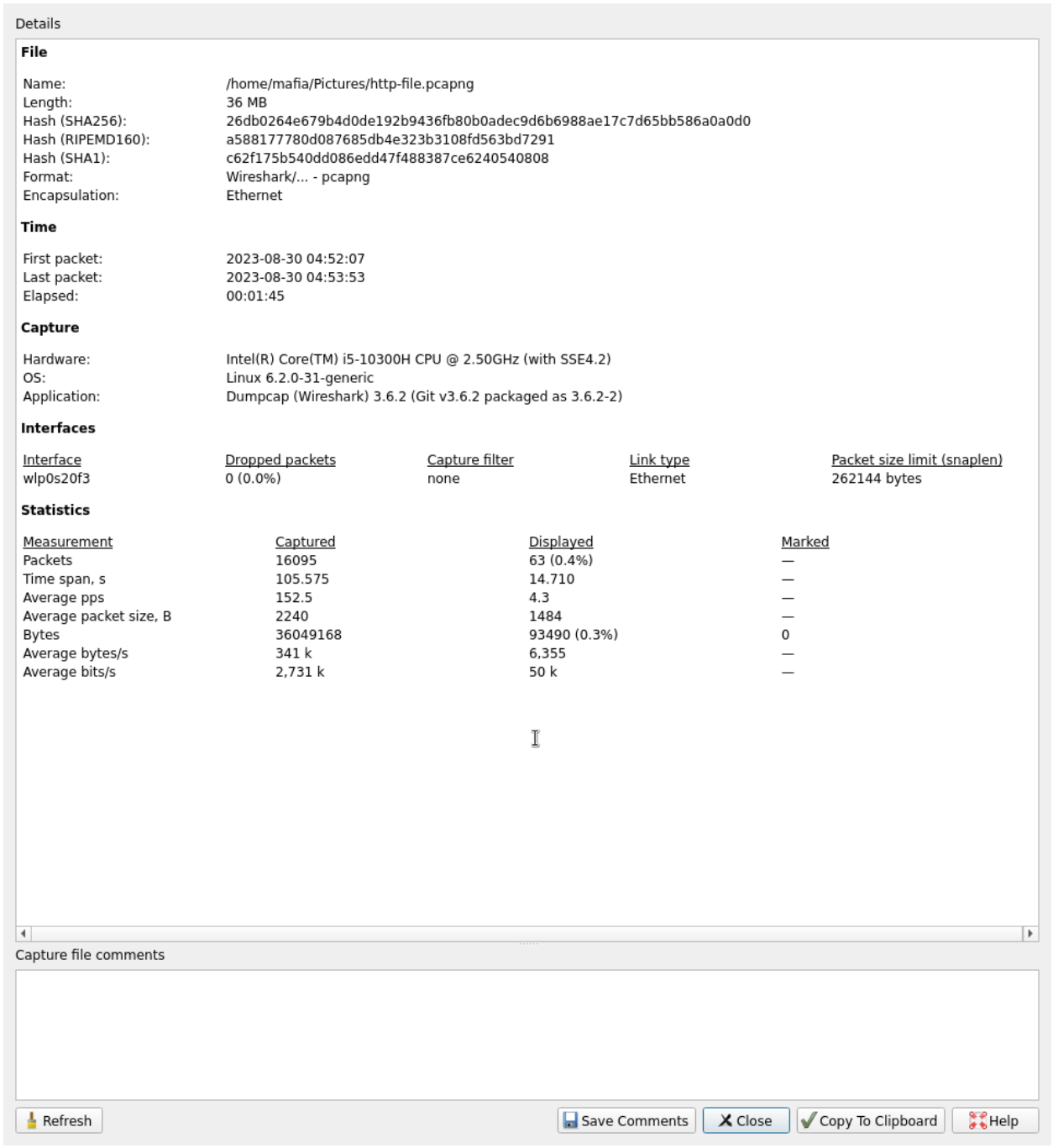
The graph between GET Req and http.response is shown above.

5. The total amount of data

GET Req	Size of Data Received
GET / HTTP/1.1\r\n	File Data: 32959 bytes
GET /index.php?pid=css_style HTTP/1.1\r\n	File Data: 19232 bytes

GET /index.php?pid=css_bootstrap_select	File Data: 6065 bytes
GET /index.php?pid=css_fontawesomemin HTTP/1.1\r\n	File Data: 31004 bytes
GET /index.php?pid=js_search HTTP/1.1\r\n	File Data: 379 bytes
GET /index.php?pid=js_jquerymin HTTP/1.1\r\n	File Data: 116840 bytes
GET /index.php?pid=js_bootstrapmin HTTP/1.1\r\n	File Data: 37045 bytes
GET /index.php?pid=js_effi_cryptojs HTTP/1.1\r\n	File Data: 47944 bytes
GET /index.php?pid=js_effi_cryptojs_hmacsha256 HTTP/1.1\r\n	File Data: 302 bytes
GET /index.php?pid=js_effi_serviceutility HTTP/1.1\r\n	File Data: 5361 bytes
GET /index.php?pid=img_logo HTTP/1.1\r\n	File Data: 9425 bytes
GET /index.php?pid=img_transparent HTTP/1.1\r\n	File Data: 883299 bytes
GET /index.php?pid=img_NEPKiSamajh HTTP/1.1\r\n	File Data: 487958 bytes
GET / HTTP/1.1\r\n	File Data: 32959 bytes
GET /index.php?pid=img_NationalScienceDay HTTP/1.1\r\n	File Data: 311578 bytes
GET /index.php?pid=img_smp_2023 HTTP/1.1\r\n	File Data: 281614 bytes
GET /filestreamingservice/files/ HTTP/1.1\r\n	File Data: 106799 bytes

The Total amount of data received when we access www.iitbhilai.ac.in is the summation of all the entries in the second column i.e. **28107630 bytes.** We are getting approx 28MB of data. And the below image shows 36MB.

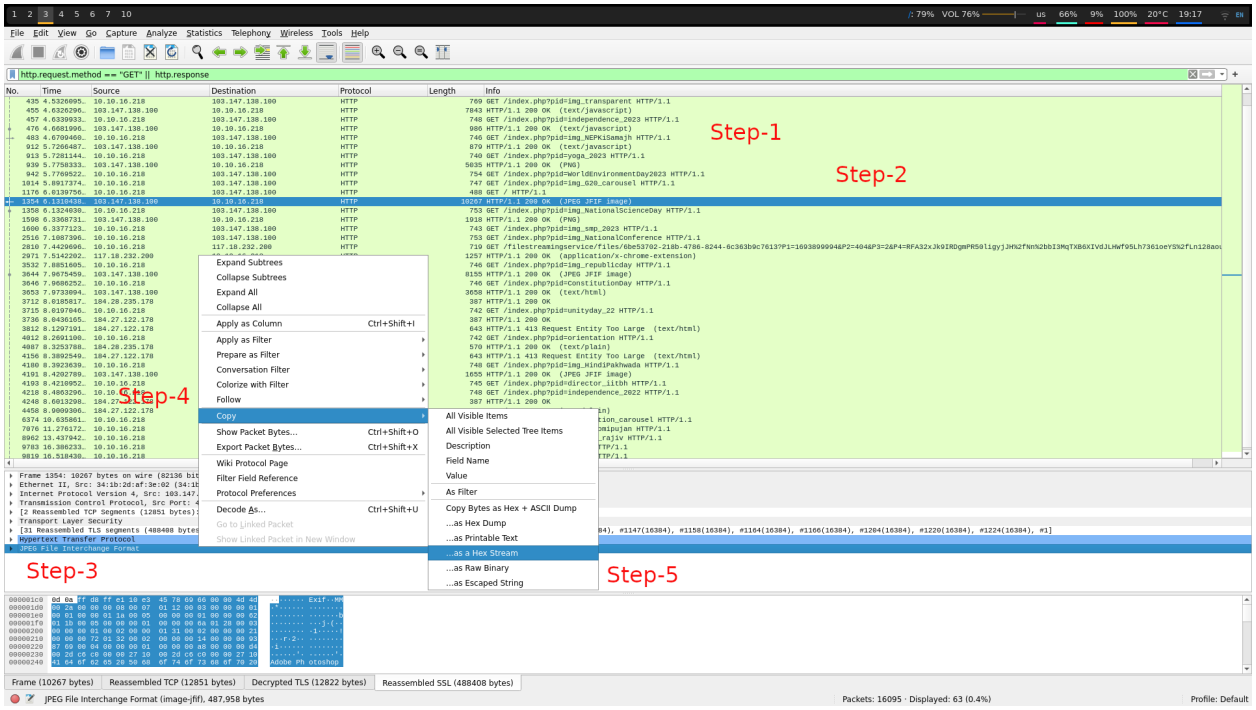


3. The Image is reconstructed by the hex editor.

Getting Image response for this GET Req:-

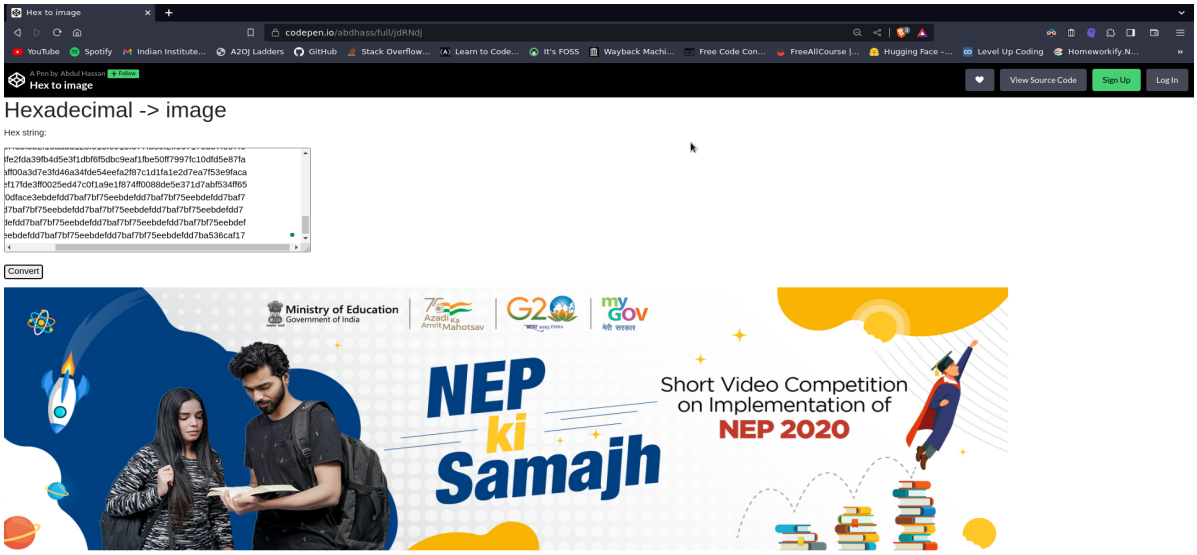
GET /index.php?pid=img_NEPKiSamajh HTTP/1.1\r\n

These steps are to be followed mentioned in the image below.



Step-1: GET /index.php?pid=img_NEPKiSamajh HTTP/1.1\r\n
Step-2: HTTP response for the step-1
Step-3: JPEG file interchangeable format, that is where the hex code of the image is available.
Step-4: Coping the necessary content.
Step-5: Coping as HEX Stream.

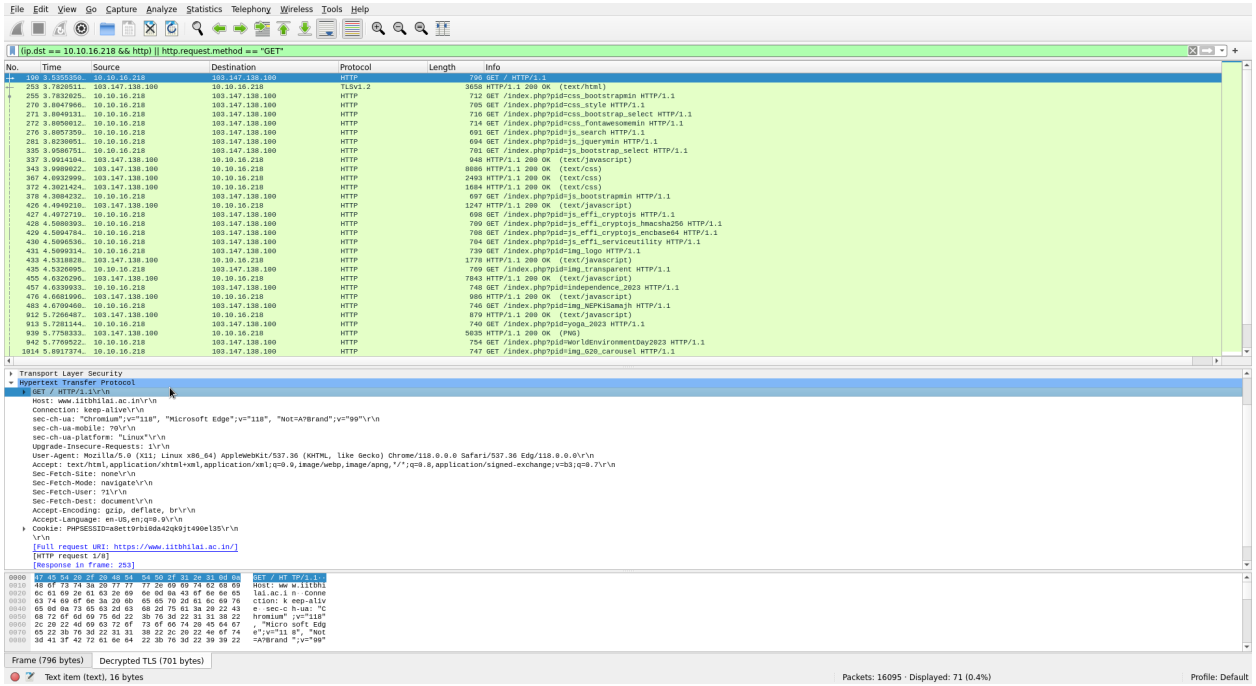
After that, we are using the **codepen.io** online tool to convert the hex stream to jpeg format. Pasting the copied hex code in the website we are getting the desired output as mentioned below.



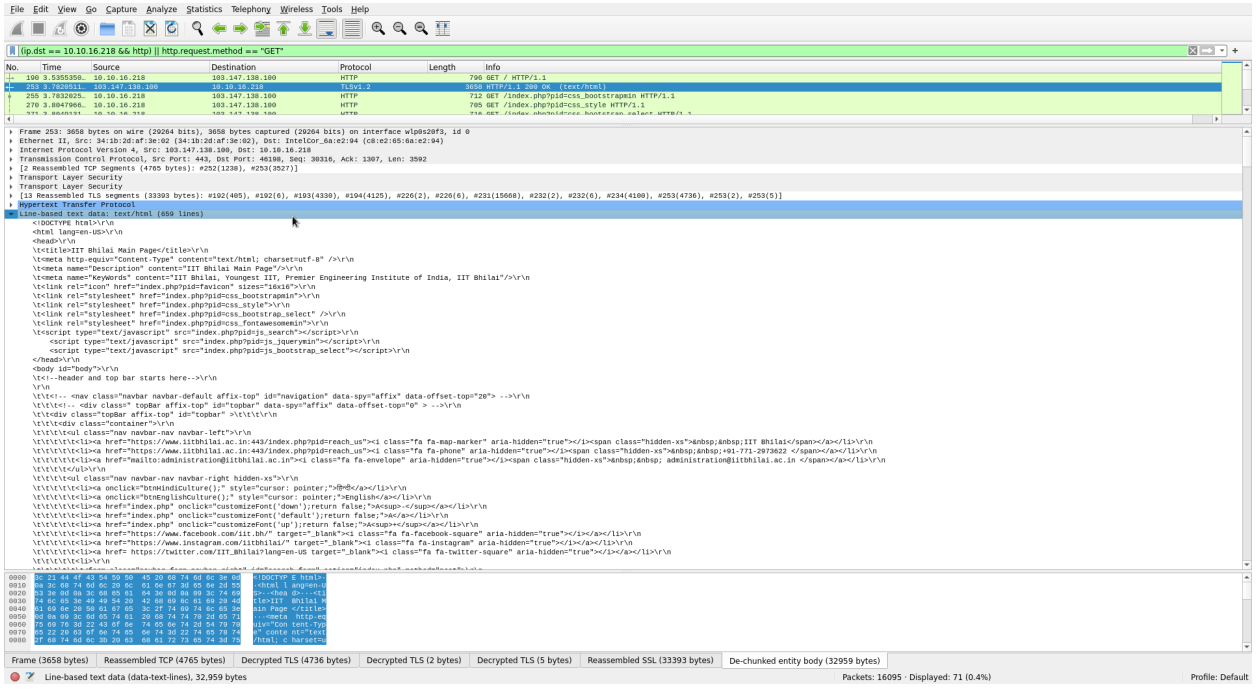
4. HTTP Conditional GET:

a) The first get message that we get is: GET / HTTP/1.1\r\n
Here we are not seeing any “IF-MODIFIED-SINCE” line in the HTTP GET because this is the first GET Req after starting to capture the packets in Wireshark.

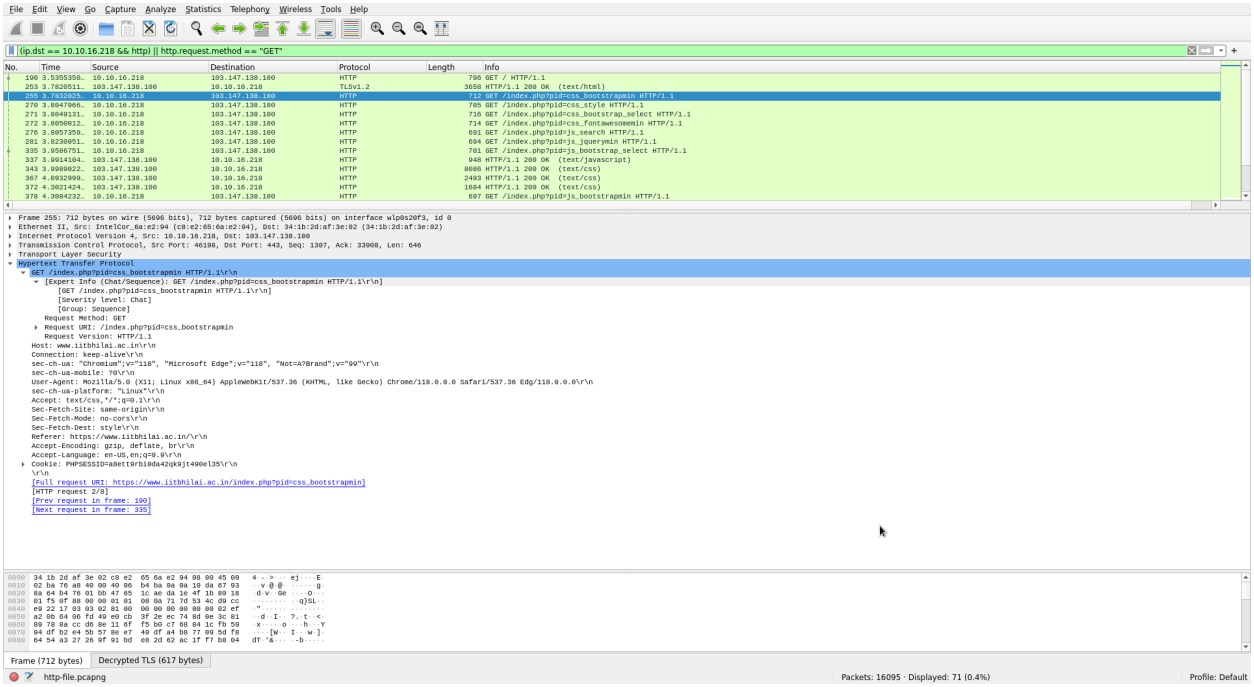
b)
This is the first GET Req:



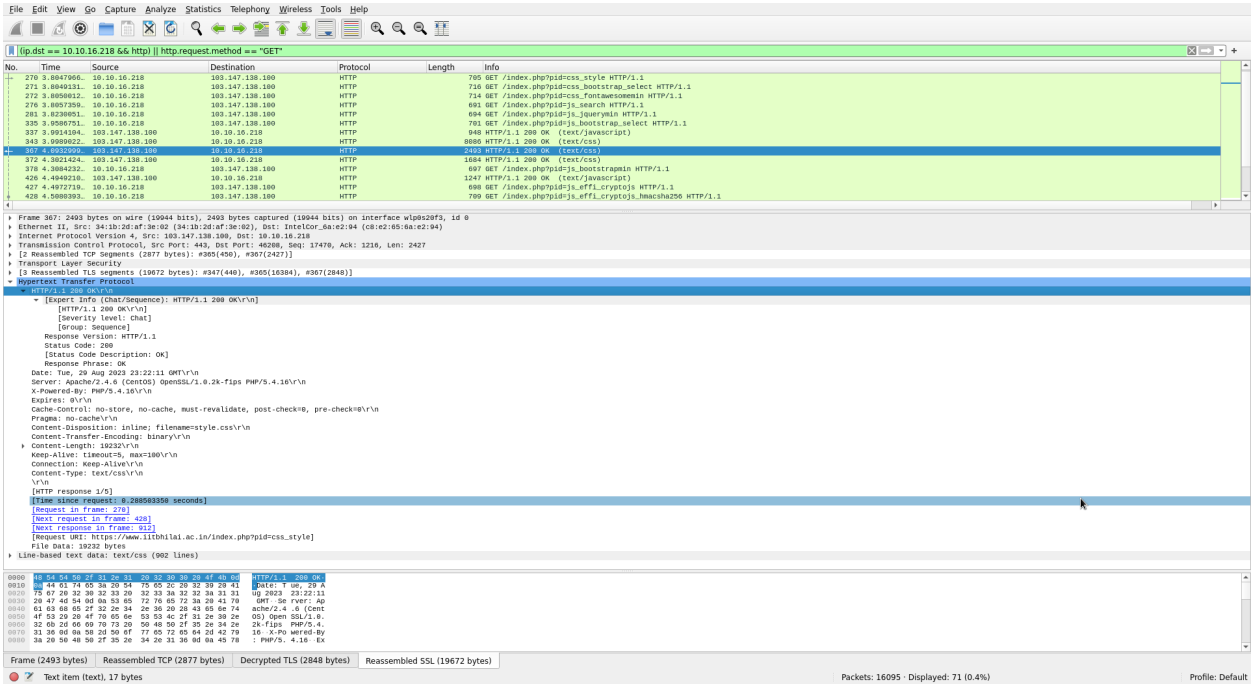
In the first GET Req, we can say that the server has explicitly returned the contents of the file in the response message as HTML code attached below:-



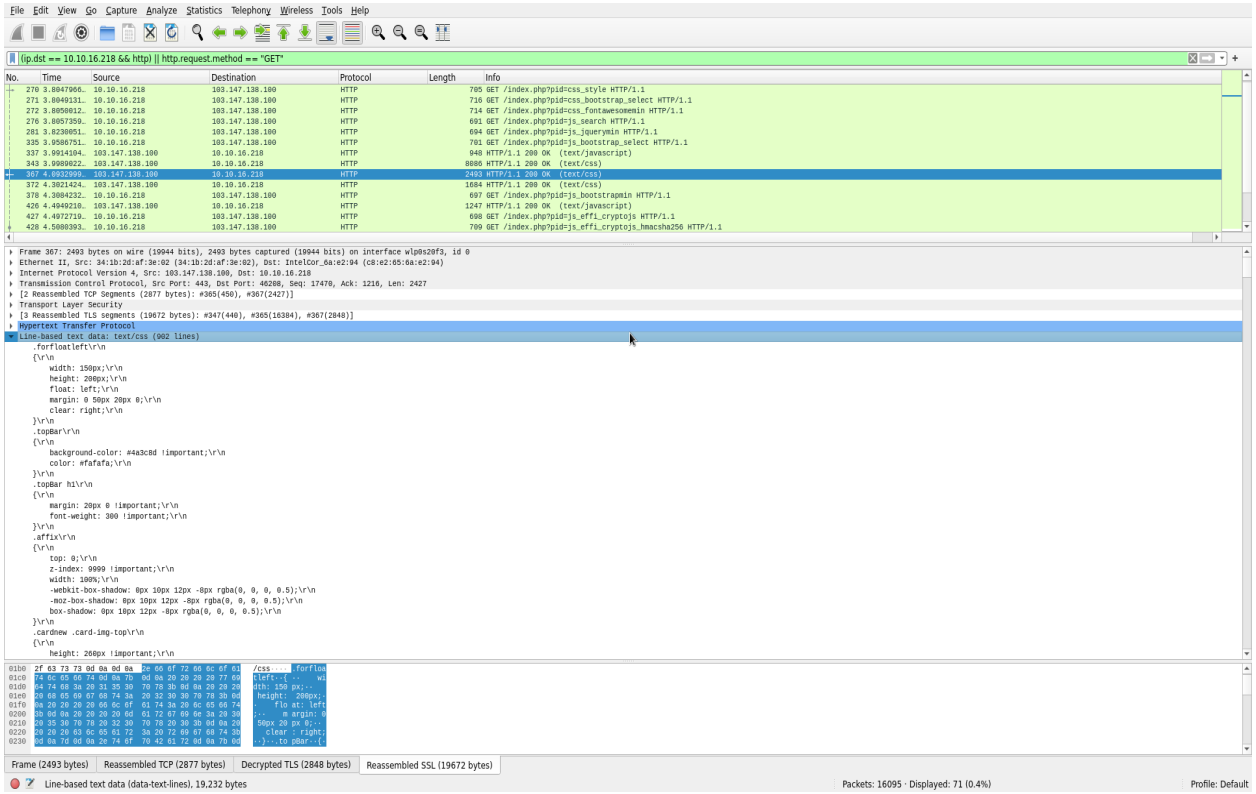
c) No, we can't find any "IF-MODIFIED-SINCE" line in the HTTP GET request. (as we can see in the image below).



d) **"HTTP/1.1 200 OK\r\n"** This is the response for the second request and the response code is 200 which can be seen in the image below.



Yes, the server explicitly returned the response in the form of text/CSS of the respective GET Req, which can be seen in the image below.



CSS Style Information:- The HTTP response contains a CSS file named “style.css” with 902 lines of CSS code.

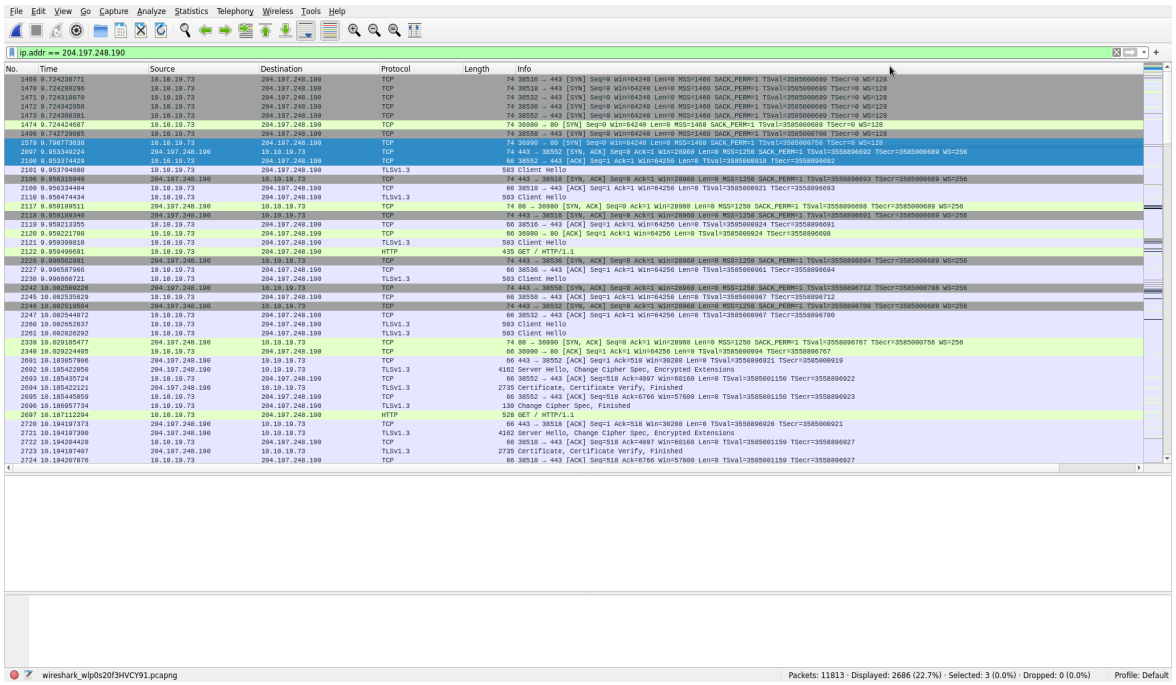
5. Surf a website (other than google.com):- iitmandi.ac.in

a) the end-to-end process of web page loading using Wireshark.

- **DNS Resolution**

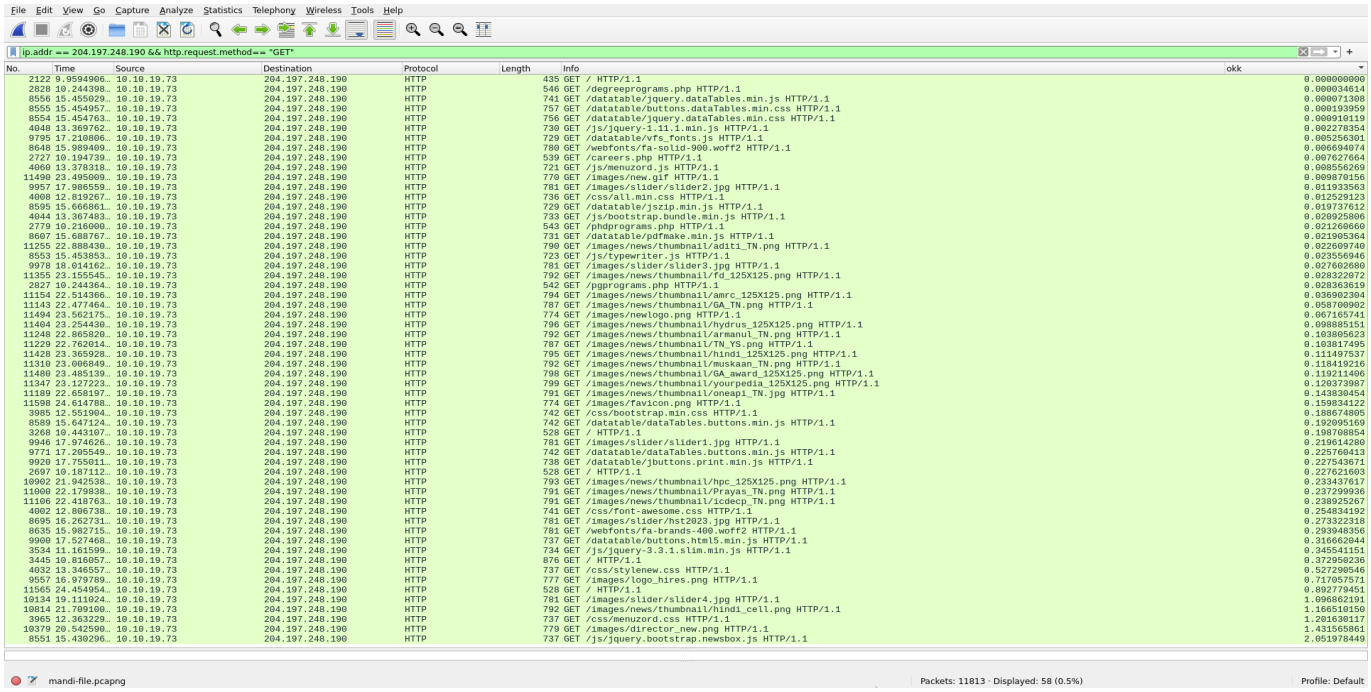
  Initially, our goal is to locate the IP address of the server hosting the desired HTML page. In this instance, we are accessing the page https://www.iitmandi.ac.in/. Since this webpage had been visited before, the DNS lookup process didn't require reaching the authoritative DNS server. This is due to the browser having cached the IP address information.

- **TCP Handshake**
  The TCP handshake is a 3-way process used to establish a connection between two devices in a network, involving an SYN, SYN-ACK and ACK.

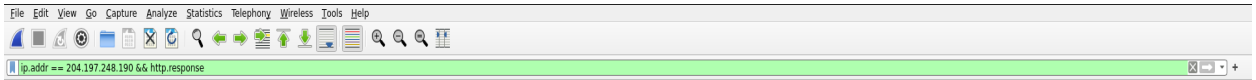


The corresponding image is attached where the handshake is observed between the host and the https://www.iitmandi.ac.in/ (in blue colour).

- **HTTP Request**
  Once a secure connection is established through TLS handshakes, the browser proceeds to initiate specific GET requests aimed at retrieving webpage data from the server. These requests typically encompass various types of resources, including HTML, CSS, and JavaScript files, as well as embedded content like images and GIFs.



- **HTTP Response**
  The web server sends back an HTTP response containing the requested webpage's content. WIreshark captures the HTTP response packets, showing response status codes, headers, and content.



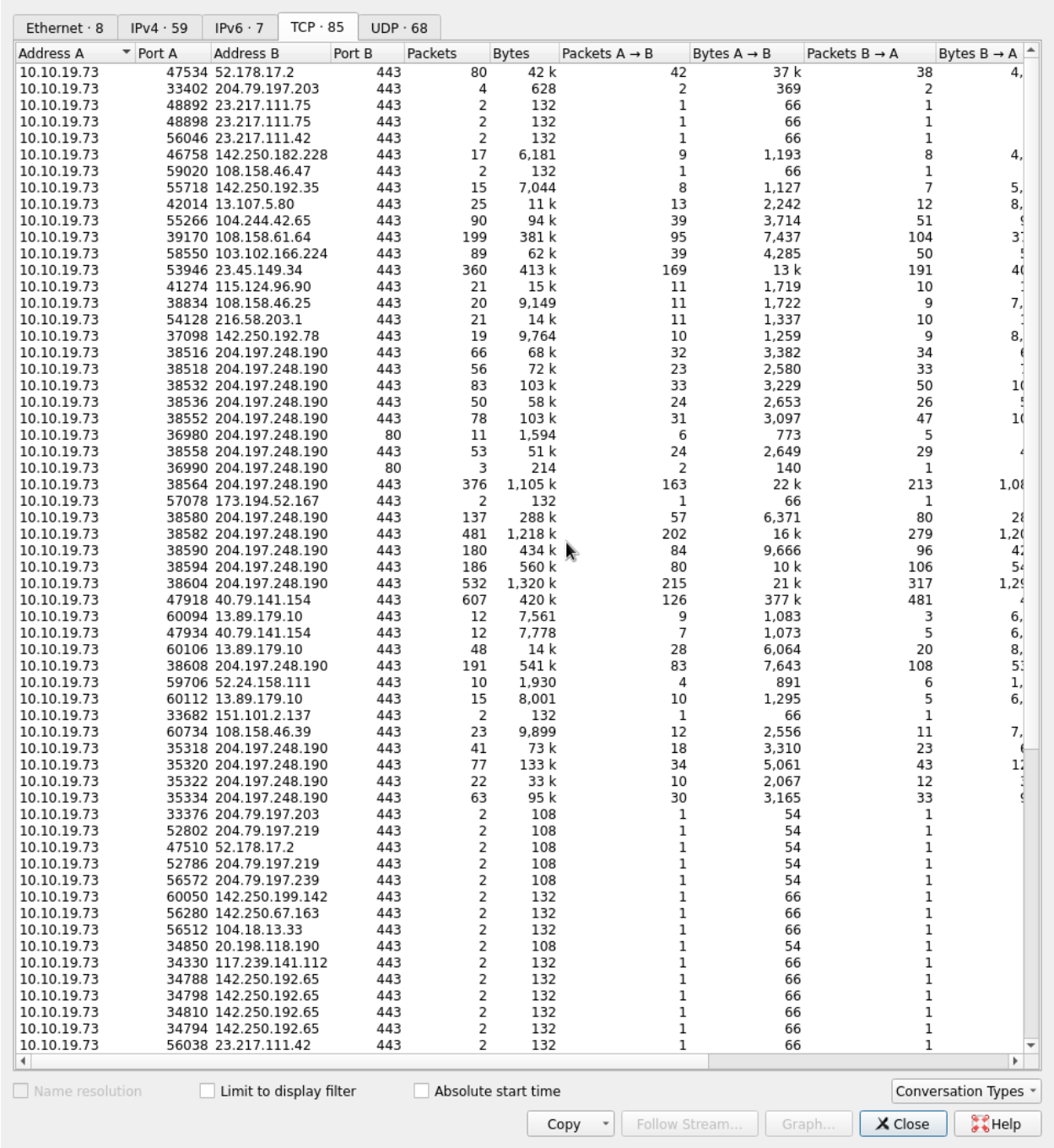
b) How much time did it take to load the page?

The first packet is received on t1 = 9.72 (mentioned in image)

The Last packet is received on t2 = 28.00 (mentioned in image)

Therefore the total time it took to load the page was = **18.28 sec.**

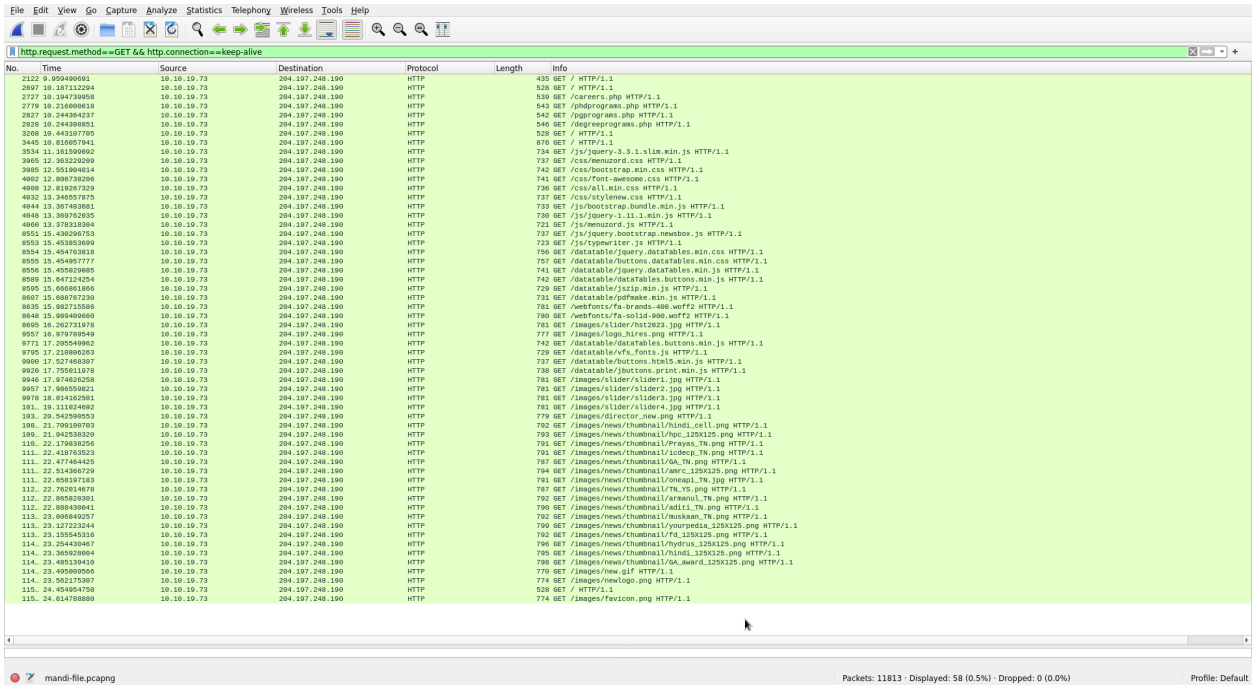
c) How many connections are used to download this page



There were 85 TCP connections used to download the page.

d) Persistent or Non-persistent connections?

Filter used = **“http.request.method==GET && http.connection==keep-alive”**

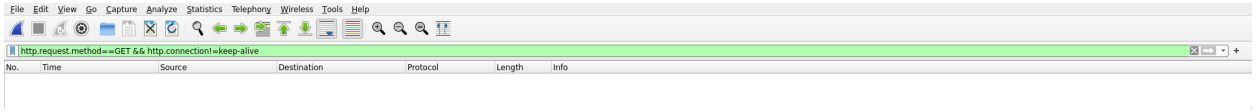


There were 58 persistent connections.

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total HTTP Packets	114				0.0075	100%	0.1800	10.719
Other HTTP Packets	20				0.0013	17.54%	0.1800	10.719
HTTP Response Packets	36				0.0024	31.58%	0.0300	13.818
???: broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	1				0.0001	2.78%	0.0100	17.983
404 Not Found	1				0.0001	100.00%	0.0100	17.983
3xx: Redirection	1				0.0001	2.78%	0.0100	10.211
301 Moved Permanently	1				0.0001	100.00%	0.0100	10.211
2xx: Success	34				0.0022	94.44%	0.0300	13.818
200 OK	34				0.0022	100.00%	0.0300	13.818
1xx: Informational	0				0.0000	0.00%	-	-
HTTP Request Packets	58				0.0038	50.88%	0.0500	10.187
GET	58				0.0038	100.00%	0.0500	10.187

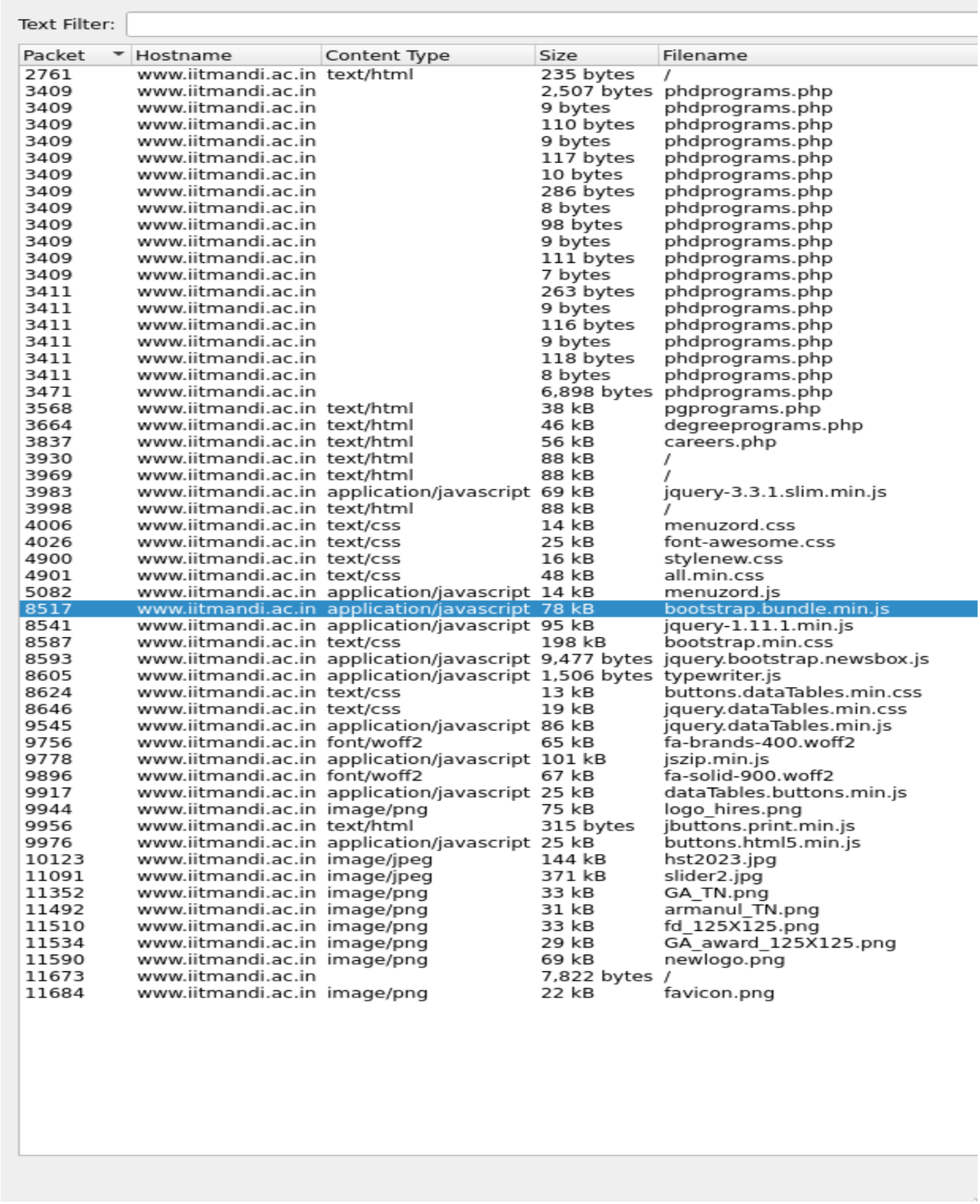
Filter used = **“http.request.method==GET && http.connection!=keep-alive”**

There were no non-persistent connections.



e) How many objects have been transferred on these connections?

Total HTTP Objects are: 56



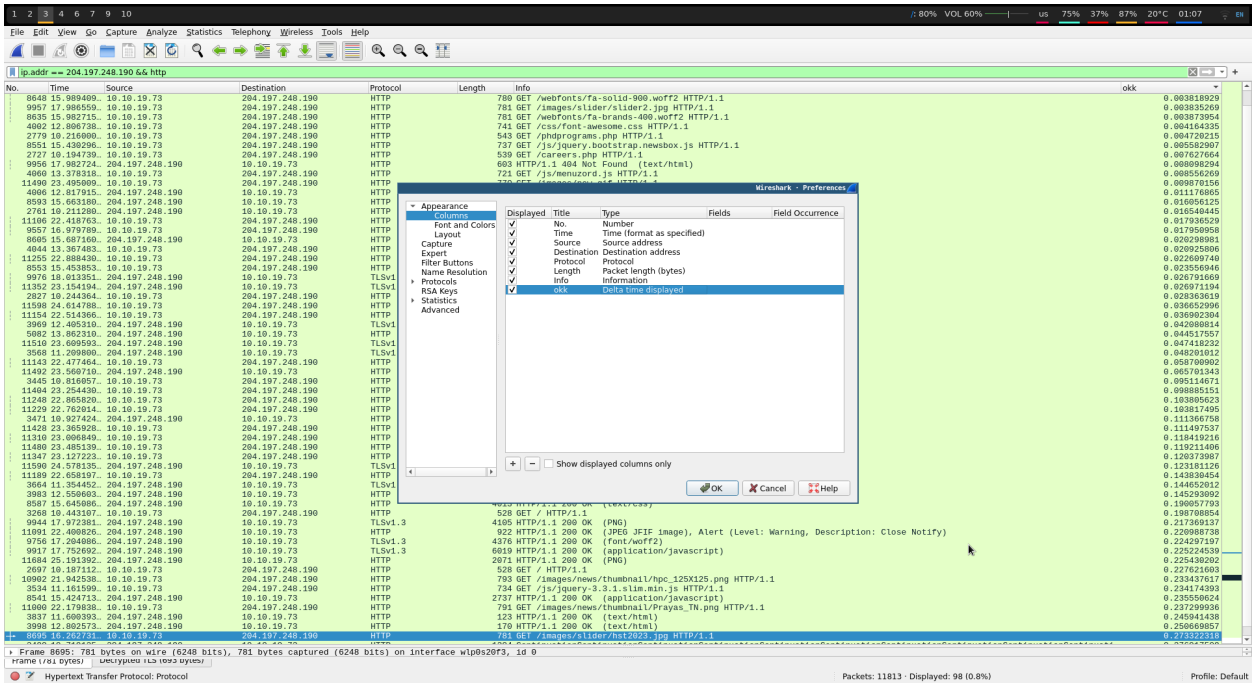
Text Filter:

Packet	Hostname	Content Type	Size	Filename
2761	www.iitmandi.ac.in	text/html	235 bytes	/
3409	www.iitmandi.ac.in		2,507 bytes	phdprograms.php
3409	www.iitmandi.ac.in		9 bytes	phdprograms.php
3409	www.iitmandi.ac.in		110 bytes	phdprograms.php
3409	www.iitmandi.ac.in		9 bytes	phdprograms.php
3409	www.iitmandi.ac.in		117 bytes	phdprograms.php
3409	www.iitmandi.ac.in		10 bytes	phdprograms.php
3409	www.iitmandi.ac.in		286 bytes	phdprograms.php
3409	www.iitmandi.ac.in		8 bytes	phdprograms.php
3409	www.iitmandi.ac.in		98 bytes	phdprograms.php
3409	www.iitmandi.ac.in		9 bytes	phdprograms.php
3409	www.iitmandi.ac.in		111 bytes	phdprograms.php
3409	www.iitmandi.ac.in		7 bytes	phdprograms.php
3411	www.iitmandi.ac.in		263 bytes	phdprograms.php
3411	www.iitmandi.ac.in		9 bytes	phdprograms.php
3411	www.iitmandi.ac.in		116 bytes	phdprograms.php
3411	www.iitmandi.ac.in		9 bytes	phdprograms.php
3411	www.iitmandi.ac.in		118 bytes	phdprograms.php
3411	www.iitmandi.ac.in		8 bytes	phdprograms.php
3471	www.iitmandi.ac.in		6,898 bytes	phdprograms.php
3568	www.iitmandi.ac.in	text/html	38 kB	pgprograms.php
3664	www.iitmandi.ac.in	text/html	46 kB	degreeprograms.php
3837	www.iitmandi.ac.in	text/html	56 kB	careers.php
3930	www.iitmandi.ac.in	text/html	88 kB	/
3969	www.iitmandi.ac.in	text/html	88 kB	/
3983	www.iitmandi.ac.in	application/javascript	69 kB	jquery-3.3.1.slim.min.js
3998	www.iitmandi.ac.in	text/html	88 kB	/
4006	www.iitmandi.ac.in	text/css	14 kB	menuzord.css
4026	www.iitmandi.ac.in	text/css	25 kB	font-awesome.css
4900	www.iitmandi.ac.in	text/css	16 kB	stylenew.css
4901	www.iitmandi.ac.in	text/css	48 kB	all.min.css
5082	www.iitmandi.ac.in	application/javascript	14 kB	menuzord.js
8517	www.iitmandi.ac.in	application/javascript	78 kB	bootstrap.bundle.min.js
8541	www.iitmandi.ac.in	application/javascript	95 kB	jquery-1.11.1.min.js
8587	www.iitmandi.ac.in	text/css	198 kB	bootstrap.min.css
8593	www.iitmandi.ac.in	application/javascript	9,477 bytes	jquery.bootstrap.newsbox.js
8605	www.iitmandi.ac.in	application/javascript	1,506 bytes	typewriter.js
8624	www.iitmandi.ac.in	text/css	13 kB	buttons.dataTables.min.css
8646	www.iitmandi.ac.in	text/css	19 kB	jquery.dataTables.min.css
9545	www.iitmandi.ac.in	application/javascript	86 kB	jquery.dataTables.min.js
9756	www.iitmandi.ac.in	font/woff2	65 kB	fa-brands-400.woff2
9778	www.iitmandi.ac.in	application/javascript	101 kB	jszip.min.js
9896	www.iitmandi.ac.in	font/woff2	67 kB	fa-solid-900.woff2
9917	www.iitmandi.ac.in	application/javascript	25 kB	dataTables.buttons.min.js
9944	www.iitmandi.ac.in	image/png	75 kB	logo_hires.png
9956	www.iitmandi.ac.in	text/html	315 bytes	jbuttons.print.min.js
9976	www.iitmandi.ac.in	application/javascript	25 kB	buttons.html5.min.js
10123	www.iitmandi.ac.in	image/jpeg	144 kB	hst2023.jpg
11091	www.iitmandi.ac.in	image/jpeg	371 kB	slider2.jpg
11352	www.iitmandi.ac.in	image/png	33 kB	GA_TN.png
11492	www.iitmandi.ac.in	image/png	31 kB	armanul_TN.png
11510	www.iitmandi.ac.in	image/png	33 kB	fd_125X125.png
11534	www.iitmandi.ac.in	image/png	29 kB	GA_award_125X125.png
11590	www.iitmandi.ac.in	image/png	69 kB	newlogo.png
11673	www.iitmandi.ac.in		7,822 bytes	/
11684	www.iitmandi.ac.in	image/png	22 kB	favicon.png

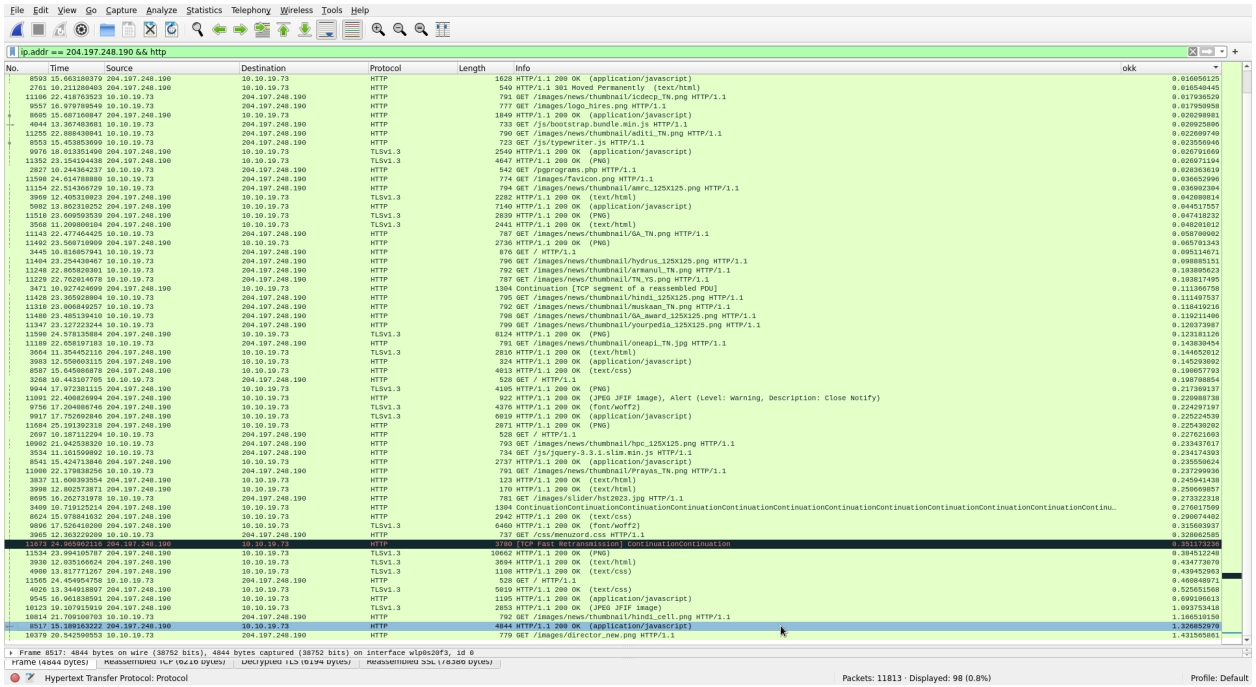
File -> Export Objects -> HTTP

f) Which object took the longest time to download?

Added a column of Delta time delayed and sorting so that we can find the packet that took the longest to receive.



Edit -> Preferences -> Column ->Add new -> Delta time delayed (drop-down menu)



The entry in blue took the longest time = **1.32 sec**

3568	www.iitmandi.ac.in	text/html	38 kB	pgprograms.php
3664	www.iitmandi.ac.in	text/html	46 kB	degreeprograms.php
3837	www.iitmandi.ac.in	text/html	56 kB	careers.php
3930	www.iitmandi.ac.in	text/html	88 kB	/
3969	www.iitmandi.ac.in	text/html	88 kB	/
3983	www.iitmandi.ac.in	application/javascript	69 kB	jquery-3.3.1.slim.min.js
3998	www.iitmandi.ac.in	text/html	88 kB	/
4006	www.iitmandi.ac.in	text/css	14 kB	menuzord.css
4026	www.iitmandi.ac.in	text/css	25 kB	font-awesome.css
4900	www.iitmandi.ac.in	text/css	16 kB	stylenew.css
4901	www.iitmandi.ac.in	text/css	48 kB	all.min.css
5082	www.iitmandi.ac.in	application/javascript	14 kB	menuzord.js
8517	www.iitmandi.ac.in	application/javascript	78 kB	bootstrap.bundle.min.js
8541	www.iitmandi.ac.in	application/javascript	95 kB	jquery-1.11.1.min.js
8587	www.iitmandi.ac.in	text/css	198 kB	bootstrap.min.css
8593	www.iitmandi.ac.in	application/javascript	9,477 bytes	jquery.bootstrap.newsbox.js
8605	www.iitmandi.ac.in	application/javascript	1,506 bytes	typewriter.js

File -> Export Objects -> HTTP

This particular object in blue takes the longest time.

PART 3
DNS

- **Use dig to ask the root server the address of www.iitbhilai.ac.in, without recursion.**

```
 Fri Sep-9 7:09:22pm   CPU 5.4% 0 Net 16   mafia ~   15M 66
> dig +norecurse @a.root-servers.net www.iitbhilai.ac.in +cmd

; <<>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<>> +norecurse @a.root-servers.net www.iitbhilai.ac.in +cmd
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57040
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 13

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.iitbhilai.ac.in.           IN      A

;; AUTHORITY SECTION:
in.                     172800  IN      NS      ns1.registry.in.
in.                     172800  IN      NS      ns4.registry.in.
in.                     172800  IN      NS      ns5.registry.in.
in.                     172800  IN      NS      ns6.registry.in.
in.                     172800  IN      NS      ns3.registry.in.
in.                     172800  IN      NS      ns2.registry.in.

;; ADDITIONAL SECTION:
ns1.registry.in.        172800  IN      A       37.209.192.12
ns1.registry.in.        172800  IN      AAAA    2001:dcd:1::12
ns4.registry.in.        172800  IN      A       37.209.198.12
ns4.registry.in.        172800  IN      AAAA    2001:dcd:4::12
ns5.registry.in.        172800  IN      A       156.154.100.20
ns5.registry.in.        172800  IN      AAAA    2001:502:2eda::20
ns6.registry.in.        172800  IN      A       156.154.101.20
ns6.registry.in.        172800  IN      AAAA    2001:502:ad09::20
ns3.registry.in.        172800  IN      A       37.209.196.12
ns3.registry.in.        172800  IN      AAAA    2001:dcd:3::12
ns2.registry.in.        172800  IN      A       37.209.194.12
ns2.registry.in.        172800  IN      AAAA    2001:dcd:2::12

;; Query time: 132 msec
;; SERVER: 198.41.0.4#53(a.root-servers.net) (UDP)
;; WHEN: Fri Sep 01 19:09:28 IST 2023
;; MSG SIZE  rcvd: 429

 Fri Sep-9 7:09:28pm   CPU 5.4% 0 Net 17   mafia ~   15M 66
>
```

Step 1: The IP address of one of the root name servers is:- "a.root-servers.net".

Step 2: Now we will perform a query search on the root server to find "www.iitbhillai.ac.in" by **dig +norecurse @a.root-servers.net www.iitbhilai.ac.in this command**.

Step 3: Select one of the **.in** servers:- @ns1.registry.in.
The root server will respond with a referral to the authoritative name servers for the **.in** top-level domain.

Step 4: Select one of the authority servers from the above step and we will get 2 DNS servers related to **www.iitbhilai.ac.in**
cmd: **dig @dns1.iitbhilai.ac.in +norecurse www.iitbhilai.ac.in +noall +answer**

After performing these 4 steps we will be able to find the address of www.iitbhilai.ac.in.

```
 Fri Sep-9 7:18:32pm   CPU 5.3% 0 Net 16   mafia ~   15M 66
> dig +norecurse @ns1.registry.in www.iitbhilai.ac.in +noall  +authority  +addition +answer
iitbhilai.ac.in.        3600    IN      NS      dns1.iitbhilai.ac.in.
iitbhilai.ac.in.        3600    IN      NS      dns2.iitbhilai.ac.in.
dns2.iitbhilai.ac.in.   3600    IN      A       103.147.138.111
dns1.iitbhilai.ac.in.   3600    IN      A       103.147.138.110
 Fri Sep-9 7:19:14pm   CPU 5.3% 0 Net 16   mafia ~   15M 66
> dig  @dns1.iitbhilai.ac.in +norecurse www.iitbhilai.ac.in +noall +answer
www.iitbhilai.ac.in.    10800   IN      A       103.147.138.100
 Fri Sep-9 7:19:27pm   CPU 5.3% 0 Net 16   mafia ~   15M 66
> dig  @dns1.iitbhilai.ac.in +norecurse www.iitbhilai.ac.in +noall +authority
iitbhilai.ac.in.        10800   IN      NS      dns1.iitbhilai.ac.in.
 Fri Sep-9 7:20:10pm   CPU 5.3% 0 Net 14   mafia ~   15M 66
> dig  @dns1.iitbhilai.ac.in +norecurse www.iitbhilai.ac.in +noall +additional
dns1.iitbhilai.ac.in.   10800   IN      A       103.147.138.110
```

<www.iitbhilai.ac.in. → 103.147.138.100>

- **List all the name servers involved to find out the IP address of the www.iitbhilai.ac.in.**
    1. @a.root-servers.net
    2. @ns1.registry.in
    3. @dns1.iitbhilai.ac.in
- **Do the same exercise for 2 more websites with different top-level domains (.com, .edu, .org, etc.)**

www.github.com

```
 Fri Sep-9 7:49:26pm   CPU 6.0% 0 Net 17   mafia ~   15M 66
> dig @a.root-servers.net +norecurse www.github.com +noall +answer +authority
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.
 Fri Sep-9 7:49:34pm   CPU 6.0% 0 Net 17   mafia ~   15M 66
> dig @m.gtld-servers.net +norecurse www.github.com +noall +answer +authority
github.com.             172800  IN      NS      ns-520.awsdns-01.net.
github.com.             172800  IN      NS      ns-421.awsdns-52.com.
github.com.             172800  IN      NS      ns-1707.awsdns-21.co.uk.
github.com.             172800  IN      NS      ns-1283.awsdns-32.org.
github.com.             172800  IN      NS      dns1.p08.nsone.net.
github.com.             172800  IN      NS      dns2.p08.nsone.net.
github.com.             172800  IN      NS      dns3.p08.nsone.net.
github.com.             172800  IN      NS      dns4.p08.nsone.net.
 Fri Sep-9 7:49:37pm   CPU 6.0% 0 Net 17   mafia ~   15M 66
> dig @ns-520.awsdns-01.net +norecurse www.github.com +noall +answer
www.github.com.         3600    IN      CNAME   github.com.
github.com.             60      IN      A       20.207.73.82
```

www.wireshark.org

```
 Fri Sep-9 7:50:33pm   CPU 6.0% 0 Net 29   mafia ~   15M 66
> dig @a.root-servers.net +norecurse www.wireshark.org +noall +answer +authority
org.                    172800  IN      NS      a0.org.afilias-nst.info.
org.                    172800  IN      NS      a2.org.afilias-nst.info.
org.                    172800  IN      NS      b0.org.afilias-nst.org.
org.                    172800  IN      NS      b2.org.afilias-nst.org.
org.                    172800  IN      NS      c0.org.afilias-nst.info.
org.                    172800  IN      NS      d0.org.afilias-nst.org.
 Fri Sep-9 7:50:51pm   CPU 6.0% 0 Net 28   mafia ~   15M 66
> dig @b2.org.afilias-nst.org +norecurse www.wireshark.org +noall +answer +authority
wireshark.org.          3600    IN      NS      cody.ns.cloudflare.com.
wireshark.org.          3600    IN      NS      olga.ns.cloudflare.com.
 Fri Sep-9 7:51:23pm   CPU 6.0% 0 Net 27   mafia ~   15M 66
> dig @cody.ns.cloudflare.com www.wireshark.org +noall +answer
www.wireshark.org.      300     IN      A       104.26.11.240
www.wireshark.org.      300     IN      A       172.67.75.39
www.wireshark.org.      300     IN      A       104.26.10.240
```