

# **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 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
        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<IP,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
        ether 00:00:00:00:00:00 txqueuelen 0 (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
    inet 10.10.19.116 netmask 255.255.252.0 broadcast 10.10.19.255
        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
wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.19.116 netmask 255.255.252.0 broadcast 10.10.19.255
        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
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           bom07545-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           kule1s09-in-f66.1:https TIME_WAIT
tcp   0     0  mafia:39634           kule1s09-in-f66.1:https TIME_WAIT
tcp   0     0  mafia:39298           20.207.73.82:https ESTABLISHED
tcp   0     0  mafia:48564           200.221.207.35.bc:https ESTABLISHED
tcp   0     0  mafia:50192           bom07535-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           bom07545-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           bom07532-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-105-199-109-1: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:57290           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.

```
Wed Aug-8 12:42:23am  CPU 14.8% 0 Net 36  mafia ~ 14M 60
> sudo netstat -no -tp | grep brave
tcp      0      0 10.10.18.230:54746    108.158.46.39:443    ESTABLISHED 13788/brave --type= keepalive (3.10/0/0)
tcp      0      0 10.10.18.230:37444    185.199.109.133:443  ESTABLISHED 13788/brave --type= keepalive (44.06/0/0)
tcp      0      0 10.10.18.230:39070    52.1.190.228:443    ESTABLISHED 13788/brave --type= keepalive (35.86/0/0)
tcp      0      0 10.10.18.230:51562    140.82.113.25:443    ESTABLISHED 13788/brave --type= keepalive (8.98/0/0)
tcp      0      0 10.10.18.230:34050    52.139.250.209:443  ESTABLISHED 13788/brave --type= keepalive (25.65/0/0)
tcp      0      0 10.10.18.230:36512    52.24.158.111:443    ESTABLISHED 13788/brave --type= keepalive (18.70/0/0)
```

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.**

```
1 2 3 0
Fri Sep-9 6:41:05pm CPU 5.5% 0 Net 22 mafia ~ 15M 66
> ping google.com
PING google.com (172.217.166.46) 56(84) bytes of data.
64 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=1 ttl=59 time=22.2 ms
59 time=22.2 ms
64 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=2 ttl=59 time=24.6 ms
59 time=23.5 ms
64 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=3 ttl=59 time=25.4 ms
59 time=23.7 ms
64 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=4 ttl=59 time=24.8 ms
59 time=28.8 ms
64 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=5 ttl=59 time=25.2 ms
59 time=28.2 ms
64 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=6 ttl=59 time=30.9 ms
59 time=28.2 ms
64 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=7 ttl=59 time=23.7 ms
59 time=21.2 ms
64 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=8 ttl=
59 time=22.6 ms
64 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=9 ttl=
59 time=25.7 ms
64 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=10 ttl=
=59 time=24.7 ms
--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9011ms
rtt min/avg/max/mdev = 21.172/24.935/28.951/2.713 ms
Fri Sep-9 6:41:18pm CPU 5.5% 0 Net 22 mafia ~ 15M 66
> [REDACTED]

Fri Sep-9 6:41:12pm CPU 5.5% 0 Net 22 mafia ~ 15M 66
> ping stackoverflow.com
PING stackoverflow.com (151.101.129.69) 56(84) bytes of data.
64 bytes from 151.101.129.69 (151.101.129.69): icmp_seq=1 ttl=59 time=22.2 ms
64 bytes from 151.101.129.69 (151.101.129.69): icmp_seq=2 ttl=59 time=24.6 ms
64 bytes from 151.101.129.69 (151.101.129.69): icmp_seq=3 ttl=59 time=25.4 ms
64 bytes from 151.101.129.69 (151.101.129.69): icmp_seq=4 ttl=59 time=23.7 ms
64 bytes from 151.101.129.69 (151.101.129.69): icmp_seq=5 ttl=59 time=24.8 ms
64 bytes from 151.101.129.69 (151.101.129.69): icmp_seq=6 ttl=59 time=25.2 ms
64 bytes from 151.101.129.69 (151.101.129.69): icmp_seq=7 ttl=59 time=30.9 ms
64 bytes from 151.101.129.69 (151.101.129.69): icmp_seq=8 ttl=59 time=23.7 ms
64 bytes from 151.101.129.69 (151.101.129.69): icmp_seq=10 ttl=59 time=68.3 ms
64 bytes from 151.101.129.69 (151.101.129.69): icmp_seq=11 ttl=59 time=28.3 ms
--- stackoverflow.com ping statistics ---
10 packets transmitted, 9 received, 10% packet loss, time 9031ms
rtt min/avg/max/mdev = 22.242/29.870/68.317/13.778 ms
Fri Sep-9 6:41:37pm CPU 5.4% 0 Net 20 mafia ~ 15M 66
64 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=7 ttl= > [REDACTED]
59 time=21.2 ms
64 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=8 ttl=
59 time=22.6 ms
64 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=9 ttl=
59 time=25.7 ms
64 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=10 ttl=
=59 time=24.7 ms
--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9011ms
rtt min/avg/max/mdev = 21.172/24.935/28.951/2.713 ms
Fri Sep-9 6:41:50pm CPU 5.4% 0 Net 20 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=25.5 ms
64 bytes from 20.207.73.82 (20.207.73.82): icmp_seq=2 ttl=114 time=25.9 ms
64 bytes from 20.207.73.82 (20.207.73.82): icmp_seq=3 ttl=114 time=26.6 ms
64 bytes from 20.207.73.82 (20.207.73.82): icmp_seq=4 ttl=114 time=26.4 ms
64 bytes from 20.207.73.82 (20.207.73.82): icmp_seq=5 ttl=114 time=28.2 ms
64 bytes from 20.207.73.82 (20.207.73.82): icmp_seq=6 ttl=114 time=28.3 ms
64 bytes from 20.207.73.82 (20.207.73.82): icmp_seq=7 ttl=114 time=35.0 ms
64 bytes from 20.207.73.82 (20.207.73.82): icmp_seq=8 ttl=114 time=27.8 ms
64 bytes from 20.207.73.82 (20.207.73.82): icmp_seq=9 ttl=114 time=26.4 ms
64 bytes from 20.207.73.82 (20.207.73.82): icmp_seq=10 ttl=114 time=26.3 ms
--- github.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 13328ms
rtt min/avg/max/mdev = 25.540/27.640/35.001/2.613 ms
Fri Sep-9 6:42:31pm CPU 5.4% 0 Net 20 mafia ~ 15M 66
> [REDACTED]
```

```

1 2 3 4 5 8 10
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.le100.net (142.250.182.238): icmp_seq=1 ttl=59 time=19.6 ms
64 bytes from bom07s29-in-f14.le100.net (142.250.182.238): icmp_seq=2 ttl=59 time=21.0 ms
64 bytes from bom07s29-in-f14.le100.net (142.250.182.238): icmp_seq=3 ttl=59 time=22.5 ms
64 bytes from bom07s29-in-f14.le100.net (142.250.182.238): icmp_seq=4 ttl=59 time=21.9 ms
64 bytes from bom07s29-in-f14.le100.net (142.250.182.238): icmp_seq=5 ttl=59 time=20.7 ms
64 bytes from bom07s29-in-f14.le100.net (142.250.182.238): icmp_seq=6 ttl=59 time=19.2 ms
64 bytes from bom07s29-in-f14.le100.net (142.250.182.238): icmp_seq=7 ttl=59 time=26.8 ms
64 bytes from bom07s29-in-f14.le100.net (142.250.182.238): icmp_seq=8 ttl=59 time=20.0 ms
64 bytes from bom07s29-in-f14.le100.net (142.250.182.238): icmp_seq=9 ttl=59 time=21.7 ms
64 bytes from bom07s29-in-f14.le100.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
> []
Fri Sep-9 7:41:36pm CPU 5.9% 0 Net 17 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
> []

Fri Sep-9 7:41:39pm CPU 5.9% 0 Net 17 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
> []

```

```

1 2 5 8 10
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.le100.net (172.217.167.174): icmp_seq=1 ttl=59 time=25.1 ms
64 bytes from bom12s01-in-f14.le100.net (172.217.167.174): icmp_seq=2 ttl=59 time=24.3 ms
64 bytes from bom12s01-in-f14.le100.net (172.217.167.174): icmp_seq=3 ttl=59 time=24.7 ms
64 bytes from bom12s01-in-f14.le100.net (172.217.167.174): icmp_seq=4 ttl=59 time=23.8 ms
64 bytes from bom12s01-in-f14.le100.net (172.217.167.174): icmp_seq=5 ttl=59 time=24.0 ms
64 bytes from bom12s01-in-f14.le100.net (172.217.167.174): icmp_seq=6 ttl=59 time=22.1 ms
64 bytes from bom12s01-in-f14.le100.net (172.217.167.174): icmp_seq=7 ttl=59 time=22.5 ms
64 bytes from bom12s01-in-f14.le100.net (172.217.167.174): icmp_seq=8 ttl=59 time=24.2 ms
64 bytes from bom12s01-in-f14.le100.net (172.217.167.174): icmp_seq=9 ttl=59 time=23.7 ms
64 bytes from bom12s01-in-f14.le100.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
> []
Sat Sep-9 9:33:39am CPU 32.4% 0 Net 122 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
> []
Sat Sep-9 9:33:47am CPU 30.4% 0 Net 123 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.

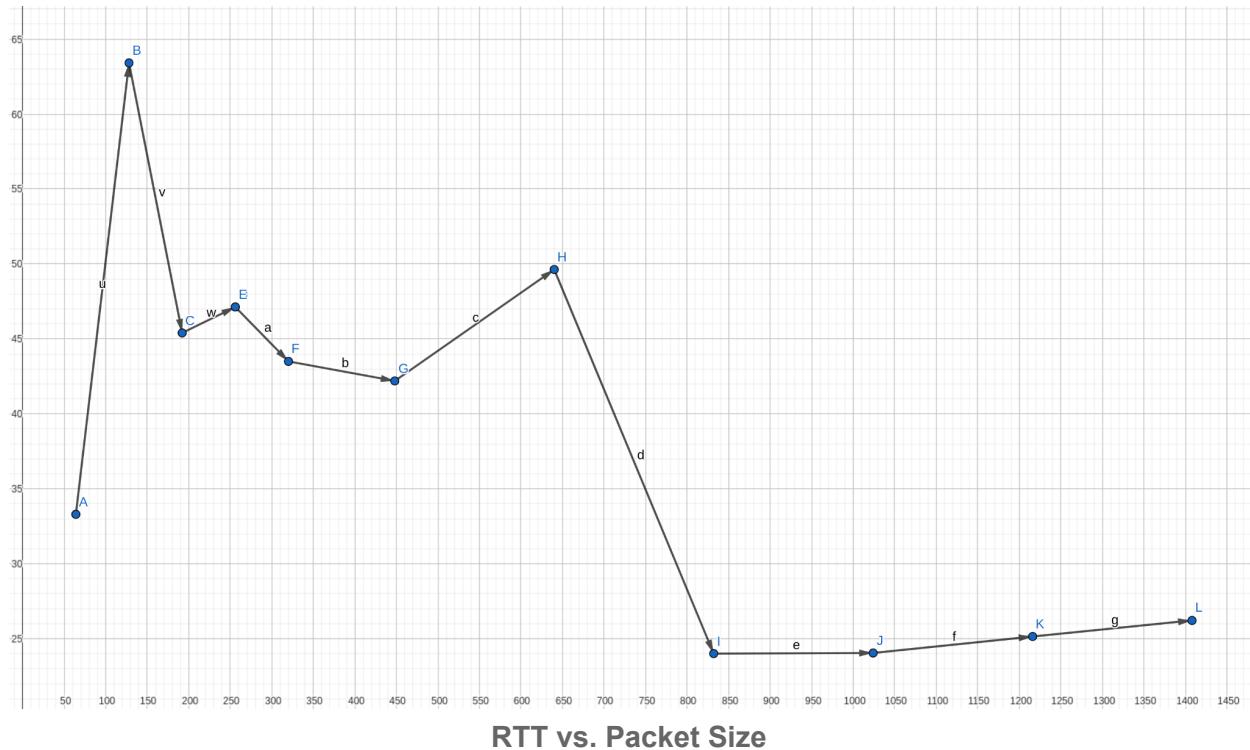
- **Pick one of the above-used hosts and repeat the experiment with different packet sizes ranging from 64 bytes to 2048 bytes. Plot average RTT vs packet size.**

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%.



- 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 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.

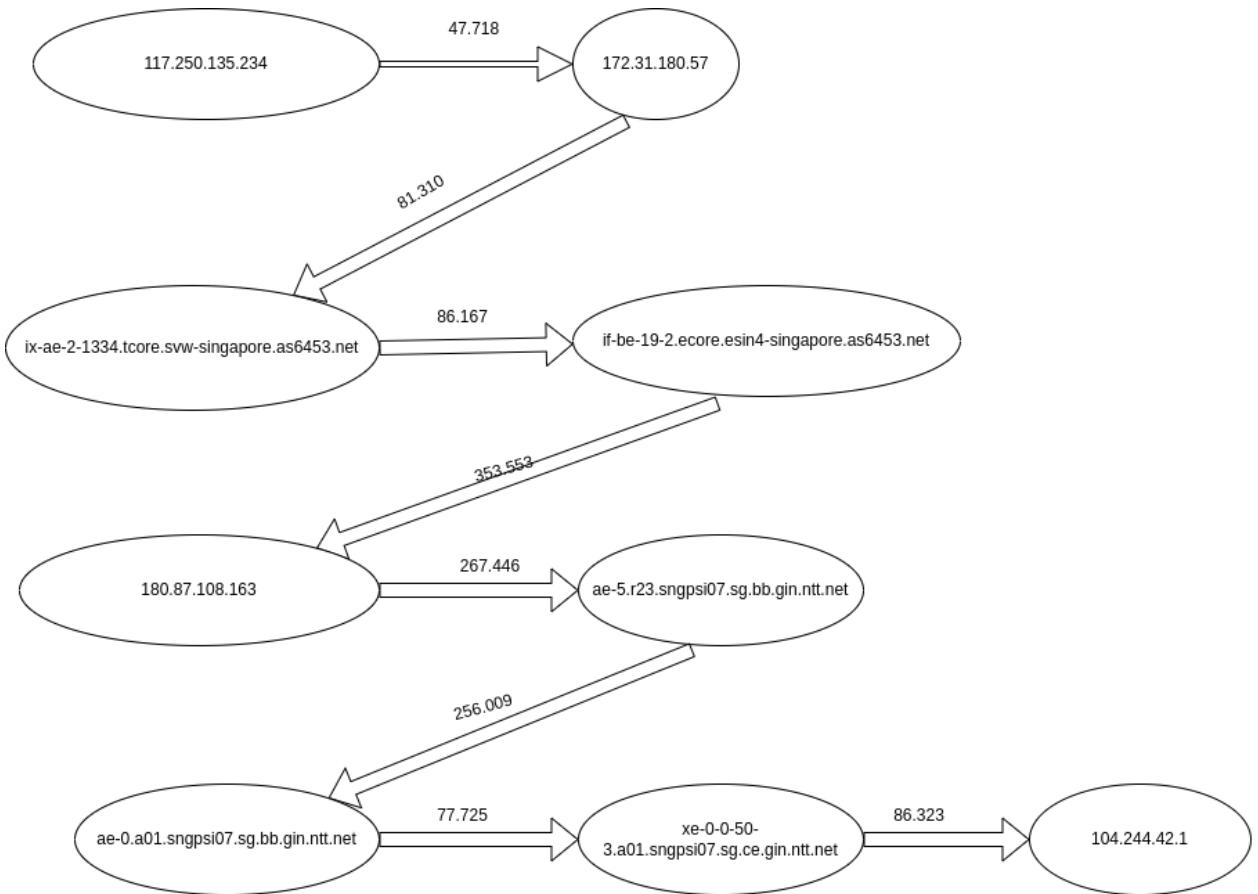
Sometimes a host may block ICMP echo requests for security or any other reasons, at that time it may allow ICMP traffic or different protocols (UDP) used by traceroute, making it a valuable tool for network troubleshooting and diagnostics, even when ping requests are blocked.

- **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

```
Sat Sep 9 5:08:06pm CPU 11.7% 0 Net 22 mafia ~ 15M 69
> traceroute twitter.com
traceroute to twitter.com (104.244.42.1), 30 hops max, 60 byte packets
 1 _gateway (10.10.16.1)  2.028 ms  2.479 ms  2.866 ms
 2 static.ill.117.250.135.234.bsnl.co.in (117.250.135.234)  3.919 ms  4.244 ms  4.221 ms
 3 * *
 4 * *
 5 115.114.89.177.static-Mumbai.vsnl.net.in (115.114.89.177)  20.485 ms  21.352 ms  21.719 ms
 6 172.31.180.57 (172.31.180.57)  47.718 ms  45.457 ms  42.231 ms
 7 ix-ae-2-1334.tcore2.svw-singapore.as6453.net (180.87.15.5)  81.310 ms  78.260 ms  81.719 ms
 8 if-be-19-2.ecore1.esin4-singapore.as6453.net (180.87.15.113)  86.167 ms  82.581 ms  87.570 ms
 9 180.87.108.163 (180.87.108.163)  352.553 ms  352.530 ms  310.346 ms
10 * ae-5.r23.sngpsi07.sg.bb.gin.ntt.net (129.250.5.65)  267.466 ms ae-4.r22.sngpsi07.sg.bb.gin.ntt.net (129.250.5.61)  260.029 ms
11 ae-0.a01.sngpsi07.sg.bb.gin.ntt.net (129.250.2.122)  256.009 ms  255.569 ms ae-1.a01.sngpsi07.sg.bb.gin.ntt.net (129.250.2.240)  262.956 ms
12 xe-0-0-50-3.a01.sngpsi07.sg.ce.gin.ntt.net (116.51.26.110)  77.725 ms  86.953 ms  86.876 ms
13 104.244.42.1 (104.244.42.1)  86.323 ms  86.296 ms  84.841 ms
```

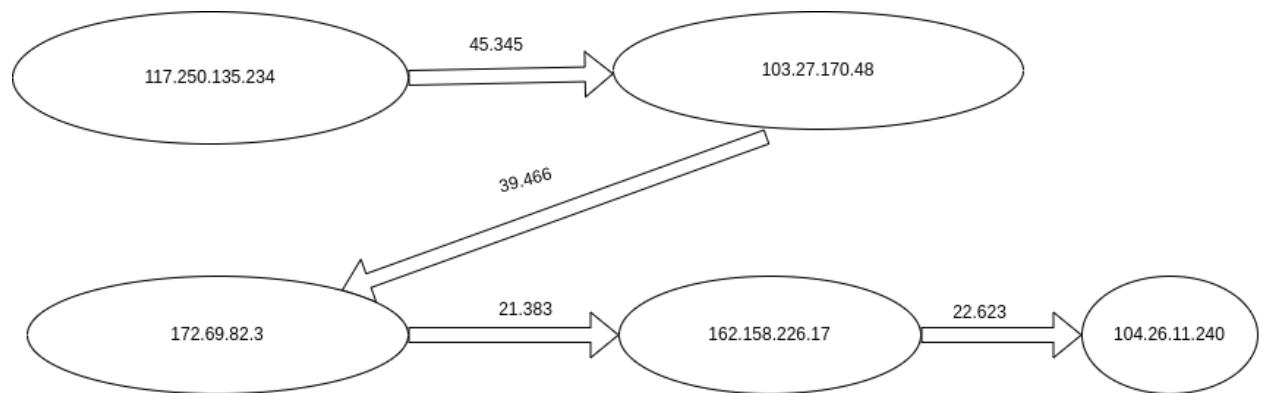
Hops	RTT (ms)
117.250.135.234	3.919
172.31.180.57	47.718
ix-ae-2-1334.tcore2.svw-singapore.as6453.net	81.310
if-be-19-2.ecore1.esin4-singapore.as6453.net	86.167
180.87.108.163	352.553
ae-5.r23.sngpsi07.sg.bb.gin.ntt.net	267.466
ae-0.a01.sngpsi07.sg.bb.gin.ntt.net	256.009
xe-0-0-50-3.a01.sngpsi07.sg.ce.gin.ntt.net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



## 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
```

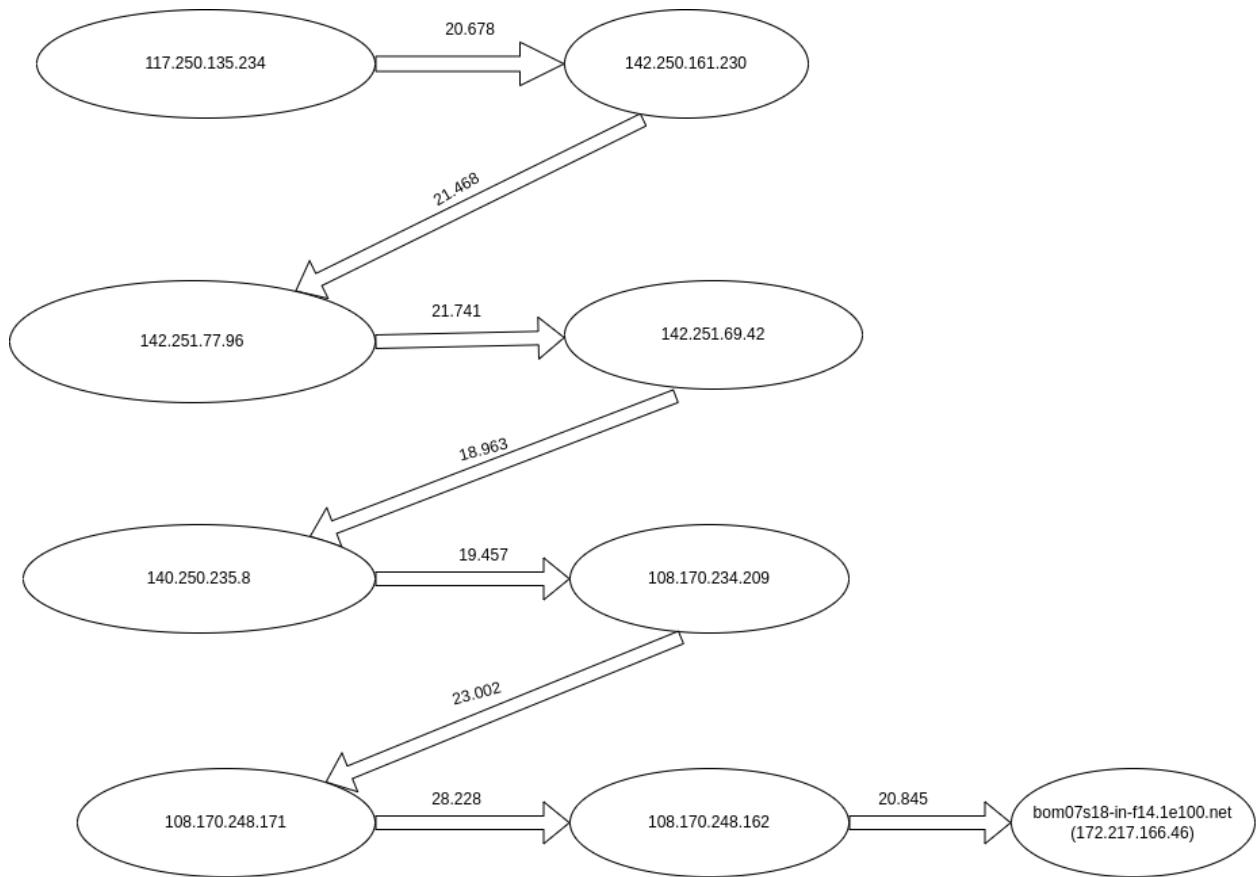
<u>Hops</u>	<u>RTT</u>
117.250.135.234	20.941ms
103.27.170.48	45.345 ms
172.69.82.3	39.466 ms
162.158.226.17	21.383 ms
104.26.11.240	22.623 ms



## 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
```

<u>Hops</u>	<u>RTT</u>
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



# PART 2

# HTTP

## **1. All the GET Requests are as follows:-**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method == "GET" || http.response

No.	Time	Source	Destination	Protocol	Length	Info
1	100.10.16.180	100.10.16.180	100.10.16.180	TLSv1.2	3858	HTTP/1.1 200 OK (text/html)
2	253.3.7820511	100.10.16.180	100.10.16.180	HTTP	712	GET /index.php?pid=css_bootstrap&page=HTTP/1.1
3	255.3.783025	100.10.16.180	100.10.16.180	HTTP	705	GET /index.php?pid=css_bootstrap&select=HTTP/1.1
4	271.3.8840131	100.10.16.180	100.10.16.180	HTTP	716	GET /index.php?pid=css_bootstrap&select=HTTP/1.1
5	273.3.8909612	100.10.16.180	100.10.16.180	HTTP	714	GET /index.php?pid=css_fontawesome&minify=HTTP/1.1
6	275.3.8909615	100.10.16.180	100.10.16.180	HTTP	692	GET /index.php?pid=css_fontawesome&minify=HTTP/1.1
7	281.3.8230851	100.10.16.180	100.10.16.180	HTTP	694	GET /index.php?pid=jq_jqueryuniv HTTP/1.1
8	305.3.058751	100.10.16.180	100.10.16.180	HTTP	707	GET /index.php?pid=jq_bootstrap_select HTTP/1.1
9	337.3.058751	100.10.16.180	100.10.16.180	HTTP	948	GET /index.php?pid=jq_fancybox&script=HTTP/1.1
10	343.3.9989022	100.10.16.180	100.10.16.180	HTTP	8804	HTTP/1.1 200 OK (text/css)
11	407.4.0032099	100.10.16.180	100.10.16.180	HTTP	2493	HTTP/1.1 200 OK (text/css)
12	372.4.0032099	100.10.16.180	100.10.16.180	HTTP	3304	HTTP/1.1 200 OK (text/css)
13	378.4.3984232	100.10.16.180	100.10.16.180	HTTP	697	GET /index.php?pid=jq_bootstrap&minify=HTTP/1.1
14	426.4.3946216	100.10.16.180	100.10.16.180	HTTP	1247	HTTP/1.1 200 OK (text/javascript)
15	429.4.3946216	100.10.16.180	100.10.16.180	HTTP	5005	GET /index.php?pid=js_afili_cryptejis_jhmacsha256 HTTP/1.1
16	428.4.5588393	100.10.16.180	100.10.16.180	HTTP	799	GET /index.php?pid=js_afili_cryptejis_jhmacsha256 HTTP/1.1
17	429.4.5599784	100.10.16.180	100.10.16.180	HTTP	798	GET /index.php?pid=js_afili_cryptejis_jhmacsha256 HTTP/1.1
18	430.4.5599314	100.10.16.180	100.10.16.180	HTTP	794	GET /index.php?pid=js_afili_cryptejis_jhmacsha256 HTTP/1.1
19	431.4.5599314	100.10.16.180	100.10.16.180	HTTP	1778	HTTP/1.1 200 OK (text/javascript)
20	434.4.5318028	100.10.16.180	100.10.16.180	HTTP	798	GET /index.php?pid=js_afili_cryptejis_jhmacsha256 HTTP/1.1
21	435.4.5318028	100.10.16.180	100.10.16.180	HTTP	10	10.10.16.218
22	436.4.6320295	100.10.16.180	100.10.16.180	HTTP	7843	HTTP/1.1 200 OK (text/javascript)
23	437.4.6320295	100.10.16.180	100.10.16.180	HTTP	748	GET /index.php?pid=independence_2023 HTTP/1.1
24	438.4.6330033	100.10.16.180	100.10.16.180	HTTP	948	GET /index.php?pid=indonesia_2023 HTTP/1.1
25	439.4.6330033	100.10.16.180	100.10.16.180	HTTP	746	GET /index.php?pid=img_NEPIKsanjhi HTTP/1.1
26	439.4.6709466	100.10.16.180	100.10.16.180	HTTP	879	HTTP/1.1 200 OK (text/javascript)
27	42.5.7268487	100.10.16.180	100.10.16.180	HTTP	740	GET /index.php?pid=js_afili_cryptejis_jhmacsha253 HTTP/1.1
28	42.5.7268487	100.10.16.180	100.10.16.180	HTTP	740	GET /index.php?pid=js_afili_cryptejis_jhmacsha253 HTTP/1.1
29	93.5.7758333	100.10.16.180	100.10.16.180	HTTP	5935	HTTP/1.1 200 OK (PNG)
30	42.5.7798252	100.10.16.180	100.10.16.180	HTTP	757	GET /index.php?pid=js_afili_cryptejis_jhmacsha253 HTTP/1.1
31	161.4.1240425	100.10.16.180	100.10.16.180	HTTP	747	GET /index.php?pid=js_afili_cryptejis_jhmacsha253 HTTP/1.1
32	117.6.6330756	100.10.16.180	100.10.16.180	HTTP	487	GET / HTTP/1.1
33	1354.6.1310438	100.10.16.180	100.10.16.180	HTTP	12027	HTTP/1.1 200 OK (JPEG_JFIF_image)
34	1359.6.1310438	100.10.16.180	100.10.16.180	HTTP	753	GET /index.php?pid=js_afili_cryptejis_jhmacsha253 HTTP/1.1
35	1359.6.1310438	100.10.16.180	100.10.16.180	HTTP	1383	GET /index.php?pid=js_afili_cryptejis_jhmacsha253 HTTP/1.1
36	1359.6.1330731	100.10.16.180	100.10.16.180	HTTP	1384	HTTP/1.1 200 OK (PNG)
37	1359.6.1330731	100.10.16.180	100.10.16.180	HTTP	743	GET /index.php?pid=js_afili_cryptejis_jhmacsha253 HTTP/1.1
38	16.6.6337232	100.10.16.180	100.10.16.180	HTTP	753	GET /index.php?pid=js_afili_cryptejis_jhmacsha253 HTTP/1.1
39	2810.6.6709466	100.10.16.180	100.10.16.180	HTTP	719	GET /filestreamingservice/files/b057032_1280_4798_8244-3c63b0c7e137P1=10938999048P2=4046P=28A4:RFA32xJk01RgnPR50lipyjJH2fwn2bb1Mn9Lh7361oEY5N2fu1n128ab0
40	771.7.5426262	100.10.16.180	100.10.16.180	HTTP	1257	HTTP/1.1 200 OK (application/x-chrome-extension)
41	323.7.5426262	100.10.16.180	100.10.16.180	HTTP	745	GET /index.php?pid=js_afili_cryptejis_jhmacsha253 HTTP/1.1
42	364.7.9987459	100.10.16.180	100.10.16.180	HTTP	8155	HTTP/1.1 200 OK (JPEG_JFIF_image)
43	364.7.9987459	100.10.16.180	100.10.16.180	HTTP	745	GET /index.php?pid=js_afili_cryptejis_jhmacsha253 HTTP/1.1
44	364.7.9987459	100.10.16.180	100.10.16.180	HTTP	3055	HTTP/1.1 200 OK (text/html)
45	3712.7.6330817	100.10.16.180	100.10.16.180	HTTP	387	HTTP/1.1 200 OK
46	3712.7.6330817	100.10.16.180	100.10.16.180	HTTP	742	GET /index.php?pid=unikeydy_22 HTTP/1.1
47	3712.7.6330817	100.10.16.180	100.10.16.180	HTTP	387	HTTP/1.1 200 OK (text/html)
48	3812.7.1397191	100.10.16.180	100.10.16.180	HTTP	643	HTTP/1.1 413 Request Entity Too Large (text/html)
49	4012.7.2901168	100.10.16.180	100.10.16.180	HTTP	742	GET /index.php?pid=unikeydy_22 HTTP/1.1
50	4012.7.2901168	100.10.16.180	100.10.16.180	HTTP	579	HTTP/1.1 200 OK (text/html)
51	4156.7.3892549	100.10.16.180	100.10.16.180	HTTP	643	HTTP/1.1 413 Request Entity Too Large (text/html)
52	4156.7.3892549	100.10.16.180	100.10.16.180	HTTP	748	GET /index.php?pid=js_afili_cryptejis_jhmacsha253 HTTP/1.1
53	4193.7.4210952	100.10.16.180	100.10.16.180	HTTP	3055	HTTP/1.1 200 OK (text/html)
54	4193.7.4210952	100.10.16.180	100.10.16.180	HTTP	745	GET /index.php?pid=director_lith HTTP/1.1
55	4193.7.4210952	100.10.16.180	100.10.16.180	HTTP	748	GET /index.php?pid=js_afili_cryptejis_jhmacsha253 HTTP/1.1
56	4218.7.4805296	100.10.16.180	100.10.16.180	HTTP	307	HTTP/1.1 200 OK (text/html)
57	4218.7.4805296	100.10.16.180	100.10.16.180	HTTP	570	HTTP/1.1 200 OK (text/plain)
58	4478.7.9909385	100.10.16.180	100.10.16.180	HTTP	750	GET /index.php?pid=js_afili_cryptejis_jhmacsha253 HTTP/1.1
59	16.19.6358611	100.10.16.180	100.10.16.180	HTTP	746	GET /index.php?pid=js_afili_cryptejis_jhmacsha253 HTTP/1.1
60	7037.16.6358611	100.10.16.180	100.10.16.180	HTTP	744	GET /index.php?pid=js_afili_cryptejis_jhmacsha253 HTTP/1.1
61	8992.16.337942	100.10.16.180	100.10.16.180	HTTP	738	GET /index.php?pid=news HTTP/1.1
62	9783.16.386233	100.10.16.180	100.10.16.180	HTTP	738	GET /index.php?pid=news HTTP/1.1
63	9891.16.7871446	100.10.16.180	100.10.16.180	HTTP	738	GET /index.php?pid=news HTTP/1.1
64	9891.16.7871446	100.10.16.180	100.10.16.180	HTTP	738	GET /index.php?pid=news HTTP/1.1

## 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_cryptojshmacsha256 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](http://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.

**Details**

**File**

Name:	/home/mafia/Pictures/http-file.pcapng
Length:	36 MB
Hash (SHA256):	26db0264e679b4d0de192b9436fb80b0adec9d6b6988ae17c7d65bb586a0a0d0
Hash (RIPEMD160):	a588177780d087685db4e323b3108fd563bd7291
Hash (SHA1):	c62f175b540dd086edd47f488387ce6240540808
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

**Time**

First packet:	2023-08-30 04:52:07
Last packet:	2023-08-30 04:53:53
Elapsed:	00:01:45

**Capture**

Hardware:	Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz (with SSE4.2)
OS:	Linux 6.2.0-31-generic
Application:	Dumpcap (Wireshark) 3.6.2 (Git v3.6.2 packaged as 3.6.2-2)

**Interfaces**

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
wlp0s20f3	0 (0.0%)	none	Ethernet	262144 bytes

**Statistics**

Measurement	Captured	Displayed	Marked
Packets	16095	63 (0.4%)	—
Time span, s	105.575	14.710	—
Average pps	152.5	4.3	—
Average packet size, B	2240	1484	—
Bytes	36049168	93490 (0.3%)	0
Average bytes/s	341 k	6,355	—
Average bits/s	2,731 k	50 k	—

[ ]

**Capture file comments**

### 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

Step-2

Step-3

Step-4

Step-5

The screenshot shows a NetworkMiner capture window. A GET request is selected, labeled 'Step-1'. The response, labeled 'Step-2', is a JPEG file named 'img\_NEPKiSamajh.jpg'. Below the main pane, a context menu is open over the response item, with 'Step-3' pointing to 'File Interchange Format'. Under 'Step-4', 'Copy' is selected, with 'Step-5' pointing to 'As Hex Stream'. The bottom status bar shows 'Packets: 16095 - Displayed: 63 (0.4%)'.

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](https://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.

The screenshot shows a browser window with the URL 'codepen.io/abdhash/full/jdRNjd'. The page title is 'Hex to image'. A text input field contains a long hex string. Below it, a preview area shows the 'NEPKiSamajh' logo. At the bottom, there is a 'Convert' button.

## 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:

(ip.dst == 10.10.16.218 && http) || http.request.method == "GET"

No.	Time	Source	Destination	Protocol	Length	Info
1	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	1024	GET /index.php?id=1
2	10:10:16.218	10.10.16.219	10.10.16.219	TLSv1.2	3658	HTTP/1.1 200 OK (text/html)
3	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	712	GET /index.php?id=css_bootstrapmin HTTP/1.1
4	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	710	GET /index.php?id=css_bootstrap_select HTTP/1.1
5	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	714	GET /index.php?id=css_fontrawmin HTTP/1.1
6	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	693	GET /index.php?id=css_fontrawmin HTTP/1.1
7	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	694	GET /index.php?id=js_jquery_min HTTP/1.1
8	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	781	GET /index.php?id=js_bootstrap_select HTTP/1.1
9	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	848	GET /index.php?id=js_independent HTTP/1.1
10	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	8880	HTTP/1.1 200 OK (text/css)
11	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	2493	HTTP/1.1 200 OK (text/css)
12	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	1884	HTTP/1.1 200 OK (text/css)
13	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	697	GET /index.php?id=js_bootstrapmin HTTP/1.1
14	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	1247	HTTP/1.1 200 OK (text/javascript)
15	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	987	GET /index.php?id=js_effl_cryptoj_s_hmacsha256 HTTP/1.1
16	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	789	GET /index.php?id=js_effl_cryptoj_s_embedbase64 HTTP/1.1
17	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	784	GET /index.php?id=js_effl_cryptoj_s_independence_min HTTP/1.1
18	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	739	GET /index.php?id=js_logo_min HTTP/1.1
19	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	1778	HTTP/1.1 200 OK (text/javascript)
20	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	789	GET /index.php?id=js_independent_min HTTP/1.1
21	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	7843	HTTP/1.1 200 OK (text/javascript)
22	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	748	GET /index.php?id=js_independence_2023 HTTP/1.1
23	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	688	GET /index.php?id=js_independence_min HTTP/1.1
24	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	746	GET /index.php?id=js_independence_NEKPSIminj HTTP/1.1
25	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	879	HTTP/1.1 200 OK (text/javascript)
26	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	748	GET /index.php?id=js_independence_neksi_2023 HTTP/1.1
27	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	5835	HTTP/1.1 200 OK (png)
28	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	754	GET /index.php?id=js_laravelEnvironmentDay2023 HTTP/1.1
29	10:10:16.218	10.10.16.219	10.10.16.219	HTTP	747	GET /index.php?id=js_laravelCarousel HTTP/1.1

4 | Transport Layer Security

HyperText Transfer Protocol

GET /index.php?id=1 HTTP/1.1

Host: www.libthlibal.ac.in\h\nConnection: keep-alive\h\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win32; rv:109.0) Gecko/20100101 Firefox/109.0\h\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7\h\nReferer: https://www.libthlibal.ac.in/\h\nSec-Fetch-Dest: document\h\nSec-Fetch-Mode: navigate\h\nSec-Fetch-Site: none\h\nSec-Fetch-User: ?1\h\nUpgrade-Insecure-Requests: 1\h\nAccept-Encoding: gzip, deflate, br\h\nAccept-Language: en-us,en;q=0.9,\h\nCookie: PHPSESSID=abef07b1dd4a2b93149e0c135\h\n

[Full request URI: https://www.libthlibal.ac.in/]

[HTTP Headers]

[Response in frame: 253]

09800 17:45:54.743648 CR 10.10.16.219 10.10.16.218 10.10.16.218 GET / HT TLS/1.3

09820 6c 61 69 62 61 63 26 69 66 6d 8a 43 6f 6e 66 65 lat:ac:1.n\_comme

09830 63 74 69 67 66 26 20 65 65 70 62 61 6c 69 76 ction:k.eep.aliv

09840 66 72 6d 69 75 6d 22 36 76 3d 21 31 34 88 22 hroism\":\";t16\":16

09850 65 22 38 76 3d 22 31 31 38 22 2c 20 22 46 67 74 e\":\";v11\";\p>09860 3d 41 3f 42 72 61 06 64 22 3b 76 3d 22 39 22 \";A\`Brand\":\";N\`

Frame (796 bytes) Decrypted TLS (701 bytes)

● 2 Text item (text), 16 bytes

Packets: 16095 - Disposed: 71 (0.4%)

Profile: Default

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:-

The screenshot shows a NetworkMiner interface with a single captured packet highlighted. The packet details are as follows:

No.	Time	Source	Destination	Protocol	Length	Info
100	10:16:21.000	10.16.21.10	10.16.21.10	HTTP	790	GET / HTTP/1.1
101	10:16:21.011	10.16.21.10	10.16.21.10	HTTP	3658	HTTP/1.1 200 OK (text/html)
205	10:16:21.021	10.16.21.10	10.16.21.10	HTTP	103	/index.php?pid=css_bootstrapmin HTTP/1.1
206	10:16:21.022	10.16.21.10	10.16.21.10	HTTP	765	/index.php?pid=css_style HTTP/1.1
207	10:16:21.023	10.16.21.10	10.16.21.10	HTTP	104	/index.php?pid=css_minimizedbootstrapmin HTTP/1.1

The packet details pane shows the raw hex and ASCII data for the response, which includes the HTML content of the IIT Bhilai homepage. The packet bytes pane shows the raw hex and ASCII data for the request and response.

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

```
(File Edit View Go Capture Analyze Statistics Telephone Wireless Tools Help

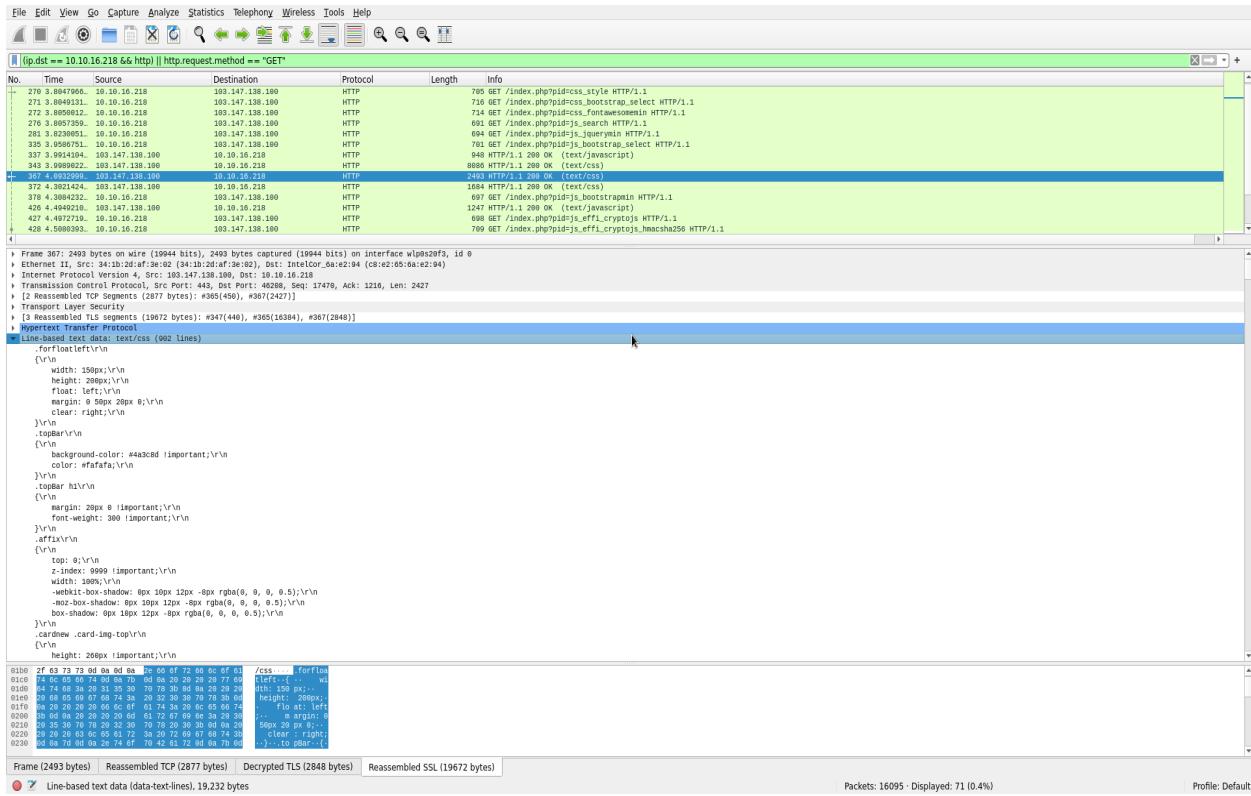
R [(ip.dst == "10.10.10.218 && http) || http.request.method == "GET"]

No.    Time       Source          Destination     Protocol Length Info
1.  0.000000  10.10.10.218  10.10.10.218  HTTP   706 GET / HTTP/1.1
2.  0.000000  10.10.10.218  10.10.10.218  TLSv1.2 3658 HTTP/1.1 200 OK (text/html)
3.  0.000000  10.10.10.218  10.10.10.218  HTTP   712 GET /index.php?pid=css_bootstrapadmin HTTP/1.1
4.  0.000000  10.10.10.218  10.10.10.218  HTTP   716 GET /index.php?pid=css_bootstrapselect HTTP/1.1
5.  0.000000  10.10.10.218  10.10.10.218  HTTP   714 GET /index.php?pid=css_fontawesomeadmin HTTP/1.1
6.  0.000000  10.10.10.218  10.10.10.218  HTTP   693 GET /index.php?pid=css_jquerymin HTTP/1.1
7.  0.000000  10.10.10.218  10.10.10.218  HTTP   694 GET /index.php?pid=js_jquerymin HTTP/1.1
8.  0.000000  10.10.10.218  10.10.10.218  HTTP   761 GET /index.php?pid=js_bootstrapselect HTTP/1.1
9.  0.000000  10.10.10.218  10.10.10.218  HTTP   648 GET /index.php?pid=js_bootstrapselect HTTP/1.1
10. 0.000000  10.10.10.218  10.10.10.218  HTTP   8886 HTTP/1.1 200 OK (text/css)
11. 0.000000  10.10.10.218  10.10.10.218  HTTP   4493 HTTP/1.1 200 OK (text/css)
12. 0.000000  10.10.10.218  10.10.10.218  HTTP   1867 HTTP/1.1 200 OK (text/css)
13. 0.000000  10.10.10.218  10.10.10.218  HTTP   697 GET /index.php?pid=js_bootstrapadmin HTTP/1.1

[12 bytes] [Decrypted TLS (617 bytes)]
```

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**

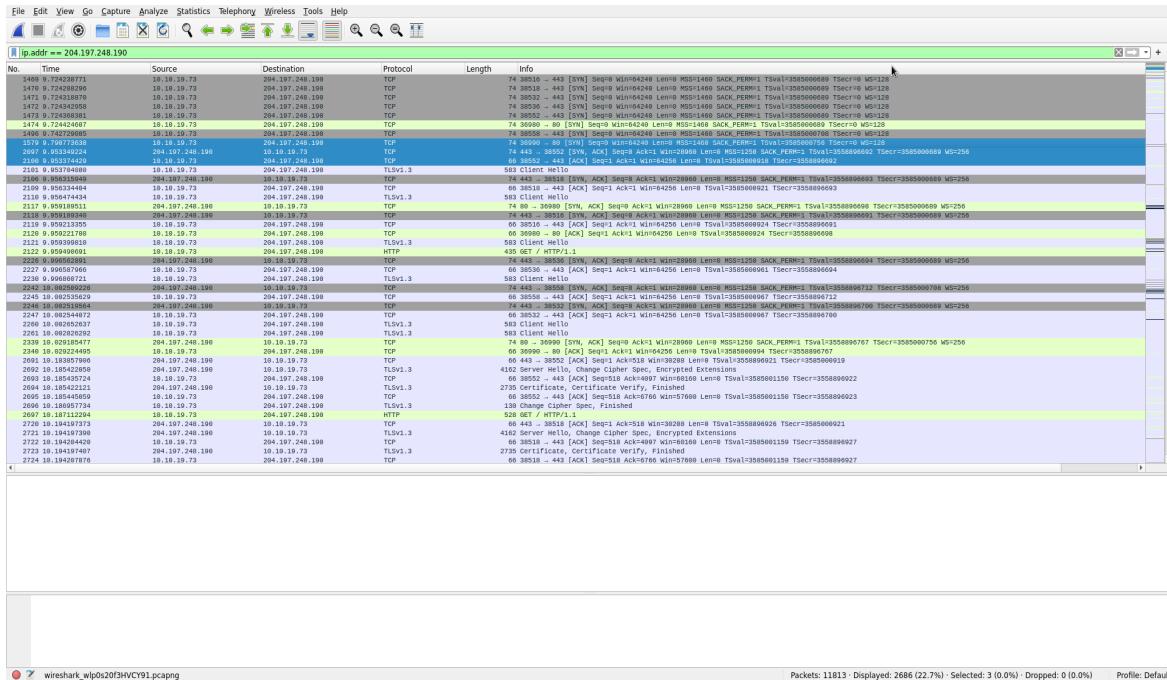
- a) the end-to-end process of web page loading using Wireshark.

- 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.

No.	Time	Source	Destination	Protocol	Length	Info	okk
212	9.19.094960	10.19.19.73	204.197.248.190	HTTP	438	GET / degreeprograms.php HTTP/1.1	0.000000000
2328	10.2443398	10.19.19.73	204.197.248.190	HTTP	540	GET /degreeprograms.php HTTP/1.1	0.000000000
8556	15.455029	10.19.19.73	204.197.248.190	HTTP	741	GET /database/query.dataTables.min.js HTTP/1.1	0.000071308
8555	15.454957	10.19.19.73	204.197.248.190	HTTP	757	GET /database/buttons.buttonsTables.min.css HTTP/1.1	0.0001033959
8554	15.454956	10.19.19.73	204.197.248.190	HTTP	768	GET /database/buttons.buttonsTables.min.css HTTP/1.1	0.0001033959
4940	13.369762	10.19.19.73	204.197.248.190	HTTP	730	GET /js/jquery-1.11.1.min.js HTTP/1.1	0.002272854
9795	17.210866	10.19.19.73	204.197.248.190	HTTP	729	GET /database/vfs_fonts.js HTTP/1.1	0.005256301
8987	15.454956	10.19.19.73	204.197.248.190	HTTP	769	GET /fonts/roboto/roboto-900.woff2 HTTP/1.1	0.000000000
2727	19.194739	10.19.19.73	204.197.248.190	HTTP	539	GET /careers.php HTTP/1.1	0.0076277664
4066	13.378718	10.19.19.73	204.197.248.190	HTTP	721	GET /js/menumuord.js HTTP/1.1	0.008556269
9040	23.495988	10.19.19.73	204.197.248.190	HTTP	778	GET /images/news/gif/Happy1/1	0.000000000
9041	23.495989	10.19.19.73	204.197.248.190	HTTP	781	GET /images/news/gif/Happy1/1	0.000000000
4068	12.819267	10.19.19.73	204.197.248.190	HTTP	736	GET /css/all_min.css HTTP/1.1	0.012529123
8595	15.666861	10.19.19.73	204.197.248.190	HTTP	729	GET /database/szslp-min_js HTTP/1.1	0.019737612
4941	13.369762	10.19.19.73	204.197.248.190	HTTP	733	GET /js/jquery-1.11.1.min.js HTTP/1.1	0.000000000
2779	10.216090	10.19.19.73	204.197.248.190	HTTP	543	GET /phdprograms.php HTTP/1.1	0.021260666
8607	15.688767	10.19.19.73	204.197.248.190	HTTP	731	GET /database/pchake.min_js HTTP/1.1	0.021905364
11325	23.453853	10.19.19.73	204.197.248.190	HTTP	798	GET /css/bootstrap/bootstrap.min.css HTTP/1.1	0.032000040
8552	15.453853	10.19.19.73	204.197.248.190	HTTP	723	GET /js/typewriter.js HTTP/1.1	0.03556946
9797	18.014162	10.19.19.73	204.197.248.190	HTTP	781	GET /images/slider/slides3.jpg HTTP/1.1	0.027606269
11327	23.455029	10.19.19.73	204.197.248.190	HTTP	793	GET /images/news/thumbnail/1/1_f_125X125.png HTTP/1.1	0.032000040
2827	18.232364	10.19.19.73	204.197.248.190	HTTP	542	GET /database/buttons.buttonsTables.min.css HTTP/1.1	0.023653819
11154	22.514366	10.19.19.73	204.197.248.190	HTTP	794	GET /images/news/thumbnail1/amrc_125X125.png HTTP/1.1	0.036962304
11143	22.477464	10.19.19.73	204.197.248.190	HTTP	787	GET /images/news/thumbnail1/VA_TN.png HTTP/1.1	0.057869092
11142	22.477465	10.19.19.73	204.197.248.190	HTTP	774	GET /images/news/thumbnail1/VA_TN.png HTTP/1.1	0.10374141
11464	23.254436	10.19.19.73	204.197.248.190	HTTP	796	GET /images/news/thumbnail1/hydrus_125X125.png HTTP/1.1	0.098885151
11248	22.865826	10.19.19.73	204.197.248.190	HTTP	792	GET /images/news/thumbnail1/armaul_TN.png HTTP/1.1	0.103805623
11423	23.365928	10.19.19.73	204.197.248.190	HTTP	787	GET /images/news/thumbnail1/armaul_TN.png HTTP/1.1	0.103805623
11422	23.365929	10.19.19.73	204.197.248.190	HTTP	795	GET /images/news/thumbnail1/hindi_125X125.png HTTP/1.1	0.11497537
11319	23.006849	10.19.19.73	204.197.248.190	HTTP	792	GET /images/news/thumbnail1/muskaan_TN.png HTTP/1.1	0.118419216
11347	23.177223	10.19.19.73	204.197.248.190	HTTP	798	GET /images/news/thumbnail1/yantra_andra_125X125.png HTTP/1.1	0.120372996
11189	22.658197	10.19.19.73	204.197.248.190	HTTP	791	GET /images/news/thumbnail1/oneapi_TN.png HTTP/1.1	0.143830454
11598	24.614788	10.19.19.73	204.197.248.190	HTTP	774	GET /images/news/thumbnail1/fa-brands-400x400w2.png HTTP/1.1	0.159354122
3026	10.443167	10.19.19.73	204.197.248.190	HTTP	742	GET /database/buttons.buttonsTables.min.css HTTP/1.1	0.159354095
8589	15.647124	10.19.19.73	204.197.248.190	HTTP	742	GET /database/buttons.buttonsTables.min.css HTTP/1.1	0.192095169
3268	10.443167	10.19.19.73	204.197.248.190	HTTP	528	GET /database/buttons.buttonsTables.min.css HTTP/1.1	0.197088054
9040	15.647125	10.19.19.73	204.197.248.190	HTTP	781	GET /images/slider/slides2.jpg HTTP/1.1	0.212000000
9771	17.295549	10.19.19.73	204.197.248.190	HTTP	742	GET /database/buttons.buttons.min_js HTTP/1.1	0.225764613
9929	17.755011	10.19.19.73	204.197.248.190	HTTP	730	GET /database/buttons.print.min_js HTTP/1.1	0.227543671
20962	21.942536	10.19.19.73	204.197.248.190	HTTP	528	GET /database/buttons.print.min_js HTTP/1.1	0.232000000
11090	22.179838	10.19.19.73	204.197.248.190	HTTP	793	GET /images/news/thumbnail1/125X125.png HTTP/1.1	0.233457617
11106	22.418763	10.19.19.73	204.197.248.190	HTTP	791	GET /images/news/thumbnail1/Prayas_TN.png HTTP/1.1	0.237299936
4069	15.647125	10.19.19.73	204.197.248.190	HTTP	745	GET /images/news/thumbnail1/vidya_125X125.png HTTP/1.1	0.253000000
8695	16.262731	10.19.19.73	204.197.248.190	HTTP	781	GET /images/slider/slides2.jpg HTTP/1.1	0.273322318
8635	15.082715	10.19.19.73	204.197.248.190	HTTP	781	GET /webfonts/fa-brands-400x400w2.png HTTP/1.1	0.293948356
9041	15.647125	10.19.19.73	204.197.248.190	HTTP	737	GET /database/buttons.buttonsTables.min.css HTTP/1.1	0.345541151
3534	11.161599	10.19.19.73	204.197.248.190	HTTP	734	GET /js/jquery-3.3.1.slim.min_js HTTP/1.1	0.345541151
3445	10.816057	10.19.19.73	204.197.248.190	HTTP	876	GET /HTTP/1.1	0.372950236
4068	15.647125	10.19.19.73	204.197.248.190	HTTP	777	GET /images/logo_hires.png HTTP/1.1	0.372950236
9557	18.879789	10.19.19.73	204.197.248.190	HTTP	528	GET /HTTP/1.1	0.717857571
11565	24.454954	10.19.19.73	204.197.248.190	HTTP	765	GET /images/slider/slides1.jpg HTTP/1.1	0.892779451
11348	23.454954	10.19.19.73	204.197.248.190	HTTP	792	GET /images/news/thumbnail1/hindi_cell.png HTTP/1.1	1.166518150
19814	21.789180	10.19.19.73	204.197.248.190	HTTP	737	GET /css/menumuord.css HTTP/1.1	1.2016301017
3965	12.363229	10.19.19.73	204.197.248.190	HTTP	777	GET /images/director_new.png HTTP/1.1	1.431565861
18370	20.542599	10.19.19.73	204.197.248.190	HTTP	737	GET /js/jquery.bootstrap.newsbox.js HTTP/1.1	2.051978449
8551	15.439296	10.19.19.73	204.197.248.190	HTTP	737	GET /js/jquery.bootrap.newsbox.js HTTP/1.1	2.051978449

Packets: 11813 Displayed: 58 (0.5%) Profile: Default

## • 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.

No.	Time	Source	Destination	Protocol	Length	Info	okk
2761	10.2112892	204.197.248.190	10.19.19.73	HTTP	549	HTTP/1.1 301 Moved Permanently (text/html)	0.000000000
4961	13.817792	204.197.248.190	10.19.19.73	TLSv1.3	4995	HTTP/1.1 299 OK (text/css)	0.000000000
9778	17.288326	204.197.248.190	10.19.19.73	HTTP	246	HTTP/1.1 299 OK (application/javascript)	0.004240113
8646	15.985559	204.197.248.190	10.19.19.73	HTTP	1869	HTTP/1.1 299 OK (text/css)	0.006749999
9956	17.982724	204.197.248.190	10.19.19.73	HTTP	603	HTTP/1.1 404 Not Found (text/html)	0.018343437
4944	17.810791	204.197.248.190	10.19.19.73	HTTP	2149	HTTP/1.1 299 OK (text/css)	0.019342370
8689	15.647125	204.197.248.190	10.19.19.73	HTTP	1626	HTTP/1.1 299 OK (application/javascript)	0.019342370
8695	15.687169	204.197.248.190	10.19.19.73	HTTP	1849	HTTP/1.1 299 OK (application/javascript)	0.023980468
9776	18.012381	204.197.248.190	10.19.19.73	TLSv1.3	2516	HTTP/1.1 299 OK (application/javascript)	0.026262646
5082	13.669593	204.197.248.190	10.19.19.73	HTTP	7149	HTTP/1.1 299 OK (application/javascript)	0.044517557
11519	23.669593	204.197.248.190	10.19.19.73	TLSv1.3	2839	HTTP/1.1 299 OK (PNG)	0.048882639
3664	11.817792	204.197.248.190	10.19.19.73	TLSv1.3	2816	HTTP/1.1 299 OK (text/html)	0.144652012
3983	12.558663	204.197.248.190	10.19.19.73	HTTP	324	HTTP/1.1 299 OK (application/javascript)	0.145293992
9444	17.972381	204.197.248.190	10.19.19.73	TLSv1.3	4105	HTTP/1.1 299 OK (PNG)	0.219687875
8587	15.645086	204.197.248.190	10.19.19.73	HTTP	4013	HTTP/1.1 299 OK (text/css)	0.229373032
9917	17.526269	204.197.248.190	10.19.19.73	TLSv1.3	6019	HTTP/1.1 299 OK (application/javascript)	0.229373032
8541	15.424713	204.197.248.190	10.19.19.73	HTTP	2737	HTTP/1.1 299 OK (application/javascript)	0.235558624
9797	18.012381	204.197.248.190	10.19.19.73	TLSv1.3	4247	HTTP/1.1 299 OK (application/javascript)	0.244517557
3837	11.669393	204.197.248.190	10.19.19.73	HTTP	123	HTTP/1.1 299 OK (text/html)	0.245941458
3998	12.882573	204.197.248.190	10.19.19.73	HTTP	178	HTTP/1.1 299 OK (text/html)	0.251970756
8524	15.882573	204.197.248.190	10.19.19.73	HTTP	2942	HTTP/1.1 299 OK (text/css)	0.291687875
8996	17.452610	204.197.248.190	10.19.19.73	TLSv1.3	6469	HTTP/1.1 299 OK (font/woff2)	0.318883341
3969	12.495318	204.197.248.190	10.19.19.73	TLSv1.3	2482	HTTP/1.1 299 OK (text/html)	0.376143399
11534	23.994168	204.197.248.190	10.19.19.73	TLSv1.3	16662	HTTP/1.1 299 OK (PNG)	0.384512248
11492	23.566719	204.197.248.190	10.19.19.73	HTTP	2736	HTTP/1.1 299 OK (PNG)	0.406516471
3930	12.035166	204.197.248.190	10.19.19.73	TLSv1.3	3664	HTTP/1.1 299 OK (text/html)	0.434773070
4900	13.817771	204.197.248.190	10.19.19.73	TLSv1.3	1108	HTTP/1.1 299 OK (text/css)	0.472852370
4026	13.340185	204.197.248.190	10.19.19.73	TLSv1.3	5019	HTTP/1.1 299 OK (text/css)	0.527093826
11518	23.566719	204.197.248.190	10.19.19.73	TLSv1.3	8019	HTTP/1.1 299 OK (font/woff2)	0.580000000
11584	25.101302	204.197.248.190	10.19.19.73	HTTP	4074	HTTP/1.1 299 OK (font/woff2)	0.613256454
11552	23.154194	204.197.248.190	10.19.19.73	TLSv1.3	4647	HTTP/1.1 299 OK (PNG)	0.239374446
9545	16.961838	204.197.248.190	10.19.19.73	HTTP	1195	HTTP/1.1 299 OK (application/javascript)	0.976247869
3568	11.269888	204.197.248.190	10.19.19.73	TLSv1.3	2441	HTTP/1.1 299 OK (text/html)	0.998519701
16123	19.167915	204.197.248.190	10.19.19.73	TLSv1.3	2853	HTTP/1.1 299 OK (JPEG/JFIF image)	1.094564429
8517	15.189163	204.197.248.190	10.19.19.73	HTTP	4844	HTTP/1.1 299 OK (application/javascript)	1.326852979
11091	22.409886	204.197.248.190	10.19.19.73	HTTP	922	HTTP/1.1 299 OK (JPEG/JFIF image), Alert (Level: Warning, Description: Close Notify)	3.29291075

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

1469.72

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.**

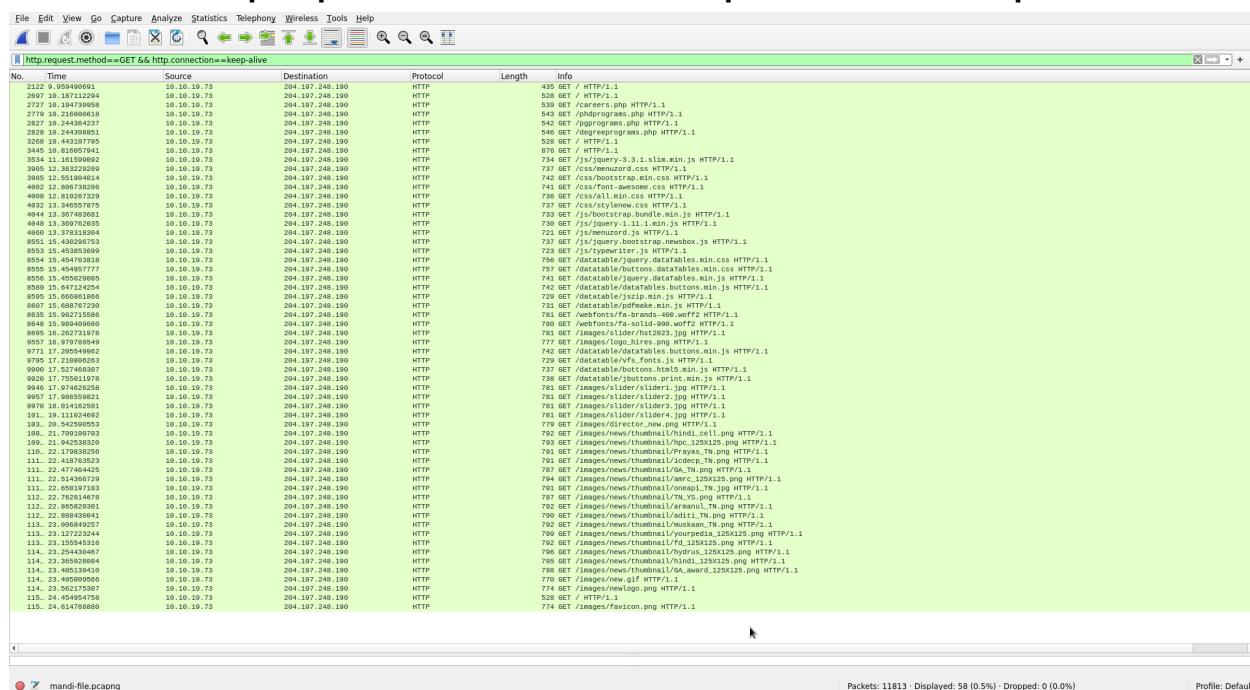
c) How many connections are used to download this page

Ethernet · 8	IPv4 · 59	IPv6 · 7	TCP · 85	UDP · 68						
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	
10.10.19.73	47534	52.178.17.2	443	80	42 k	42	37 k	38	4,	
10.10.19.73	33402	204.79.197.203	443	4	628	2	369	2		
10.10.19.73	48892	23.217.111.75	443	2	132	1	66	1		
10.10.19.73	48898	23.217.111.75	443	2	132	1	66	1		
10.10.19.73	56046	23.217.111.42	443	2	132	1	66	1		
10.10.19.73	46758	142.250.182.228	443	17	6,181	9	1,193	8	4,	
10.10.19.73	59020	108.158.46.47	443	2	132	1	66	1		
10.10.19.73	55718	142.250.192.35	443	15	7,044	8	1,127	7	5,	
10.10.19.73	42014	13.107.5.80	443	25	11 k	13	2,242	12	8,	
10.10.19.73	55266	104.244.42.65	443	90	94 k	39	3,714	51	9,	
10.10.19.73	39170	108.158.61.64	443	199	381 k	95	7,437	104	3,	
10.10.19.73	58550	103.102.166.224	443	89	62 k	39	4,285	50	5,	
10.10.19.73	53946	23.45.149.34	443	360	413 k	169	13 k	191	40	
10.10.19.73	41274	115.124.96.90	443	21	15 k	11	1,719	10		
10.10.19.73	38834	108.158.46.25	443	20	9,149	11	1,722	9	7,	
10.10.19.73	54128	216.58.203.1	443	21	14 k	11	1,337	10		
10.10.19.73	37098	142.250.192.78	443	19	9,764	10	1,259	9	8,	
10.10.19.73	38516	204.197.248.190	443	66	68 k	32	3,382	34	6,	
10.10.19.73	38518	204.197.248.190	443	56	72 k	23	2,580	33		
10.10.19.73	38532	204.197.248.190	443	83	103 k	33	3,229	50	10	
10.10.19.73	38536	204.197.248.190	443	50	58 k	24	2,653	26		
10.10.19.73	38552	204.197.248.190	443	78	103 k	31	3,097	47	10	
10.10.19.73	36980	204.197.248.190	80	11	1,594	6	773	5		
10.10.19.73	38558	204.197.248.190	443	53	51 k	24	2,649	29		
10.10.19.73	36990	204.197.248.190	80	3	214	2	140	1		
10.10.19.73	38564	204.197.248.190	443	376	1,105 k	163	22 k	213	1,08	
10.10.19.73	57078	173.194.52.167	443	2	132	1	66	1		
10.10.19.73	38580	204.197.248.190	443	137	288 k	57	6,371	80	28	
10.10.19.73	38582	204.197.248.190	443	481	1,218 k	202	16 k	279	1,20	
10.10.19.73	38590	204.197.248.190	443	180	434 k	84	9,666	96	42	
10.10.19.73	38594	204.197.248.190	443	186	560 k	80	10 k	106	54	
10.10.19.73	38604	204.197.248.190	443	532	1,320 k	215	21 k	317	1,29	
10.10.19.73	47918	40.79.141.154	443	607	420 k	126	377 k	481		
10.10.19.73	60094	13.89.179.10	443	12	7,561	9	1,083	3	6,	
10.10.19.73	47934	40.79.141.154	443	12	7,778	7	1,073	5	6,	
10.10.19.73	60106	13.89.179.10	443	48	14 k	28	6,064	20	8,	
10.10.19.73	38608	204.197.248.190	443	191	541 k	83	7,643	108	53	
10.10.19.73	59706	52.24.158.111	443	10	1,930	4	891	6	1,	
10.10.19.73	60112	13.89.179.10	443	15	8,001	10	1,295	5	6,	
10.10.19.73	33682	151.101.2.137	443	2	132	1	66	1		
10.10.19.73	60734	108.158.46.39	443	23	9,899	12	2,556	11	7,	
10.10.19.73	35318	204.197.248.190	443	41	73 k	18	3,310	23		
10.10.19.73	35320	204.197.248.190	443	77	133 k	34	5,061	43	12	
10.10.19.73	35322	204.197.248.190	443	22	33 k	10	2,067	12		
10.10.19.73	35334	204.197.248.190	443	63	95 k	30	3,165	33		
10.10.19.73	33376	204.79.197.203	443	2	108	1	54	1		
10.10.19.73	52802	204.79.197.219	443	2	108	1	54	1		
10.10.19.73	47510	52.178.17.2	443	2	108	1	54	1		
10.10.19.73	52786	204.79.197.219	443	2	108	1	54	1		
10.10.19.73	56572	204.79.197.239	443	2	108	1	54	1		
10.10.19.73	60050	142.250.199.142	443	2	132	1	66	1		
10.10.19.73	56280	142.250.67.163	443	2	132	1	66	1		
10.10.19.73	56512	104.18.13.33	443	2	132	1	66	1		
10.10.19.73	34850	20.198.118.190	443	2	108	1	54	1		
10.10.19.73	34330	117.239.141.112	443	2	132	1	66	1		
10.10.19.73	34788	142.250.192.65	443	2	132	1	66	1		
10.10.19.73	34798	142.250.192.65	443	2	132	1	66	1		
10.10.19.73	34810	142.250.192.65	443	2	132	1	66	1		
10.10.19.73	34794	142.250.192.65	443	2	132	1	66	1		
10.10.19.73	56038	23.217.111.42	443	2	132	1	66	1		

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

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.

The screenshot shows the Wireshark interface with the following details:

- Frame 8695:** 78 bytes on wire (6248 bits), 781 bytes captured (6248 bits) on interface wlp8s0f3, id 0
- Frame 1 (1st bytes):** Encapsulated ICA (TCP) layer 0
- Protocol:** Hypertext Transfer Protocol: Protocol
- Packets:** 11813 - Displayed: 98 (0.8%)
- Profile:** Default

The 'Columns' configuration dialog is open, showing the following settings:

Column	Type	Field Occurrence
Displayed	Text	
Title	Text	
No.	Number	
Time	Date/Time	
Source	Source Address	
Destination	Destination Address	
Protocol	Protocol	
Length	Length	
Info	Information	

Other tabs visible in the dialog include Appearance, Font and Colors, Layout, Capture, Buttons, Name Resolution, and Advanced.

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.iitbihilai.ac.in](http://www.iitbihilai.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.iitbihilai.ac.in +cmd

; <>> Dig 9.18.12-0ubuntu0.22.04.2-Ubuntu <>> +norecurse @a.root-servers.net www.iitbihilai.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.iitbihilai.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:dc0:1::12
ns4.registry.in.    172800  IN      A      37.209.198.12
ns4.registry.in.    172800  IN      AAAA     2001:dc0:4::12
ns5.registry.in.    172800  IN      A      156.154.100.20
ns5.registry.in.    172800  IN      AAAA     2001:502:zed0::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:dc0:3::12
ns2.registry.in.    172800  IN      A      37.209.194.12
ns2.registry.in.    172800  IN      AAAA     2001:dc0:2::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.iitbihilai.ac.in" by [\*\*dig +norecurse @a.root-servers.net www.iitbihilai.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.iitbihilai.ac.in](http://www.iitbihilai.ac.in)

cmd: **dig @dns1.iitbihilai.ac.in +norecurse www.iitbihilai.ac.in +noall +answer**

After performing these 4 steps we will be able to find the address of [www.iitbihilai.ac.in](http://www.iitbihilai.ac.in).

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

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

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

### [www.github.com](http://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](http://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
```