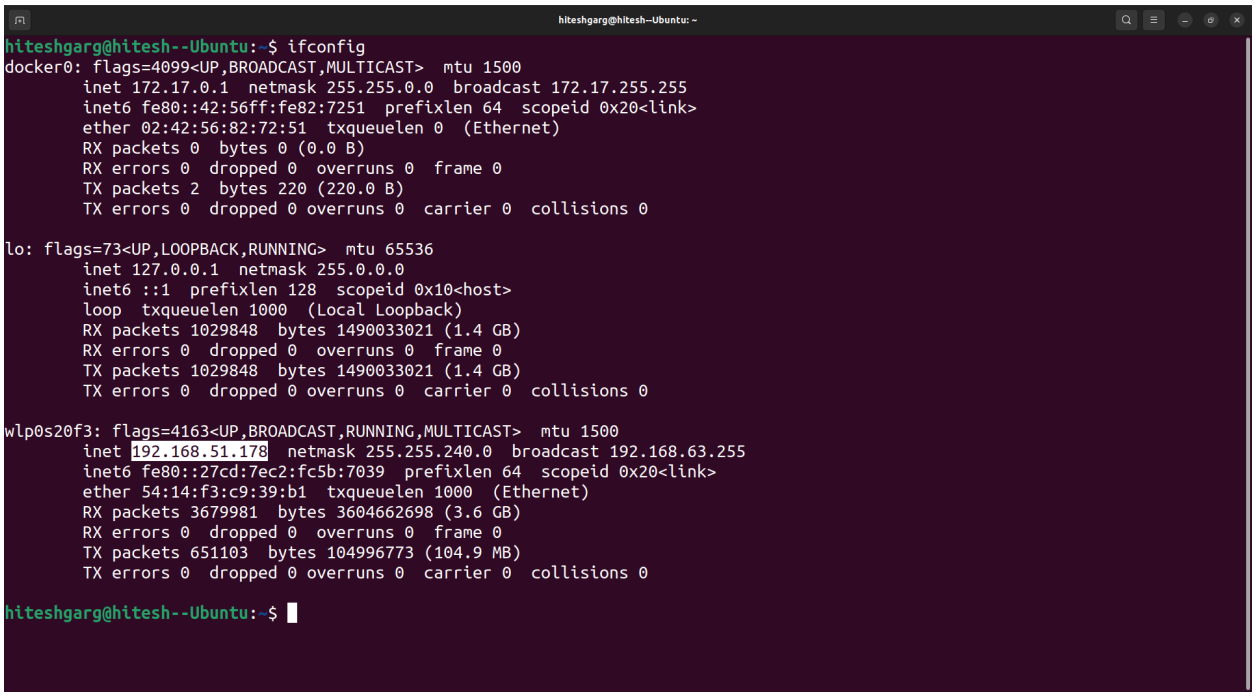
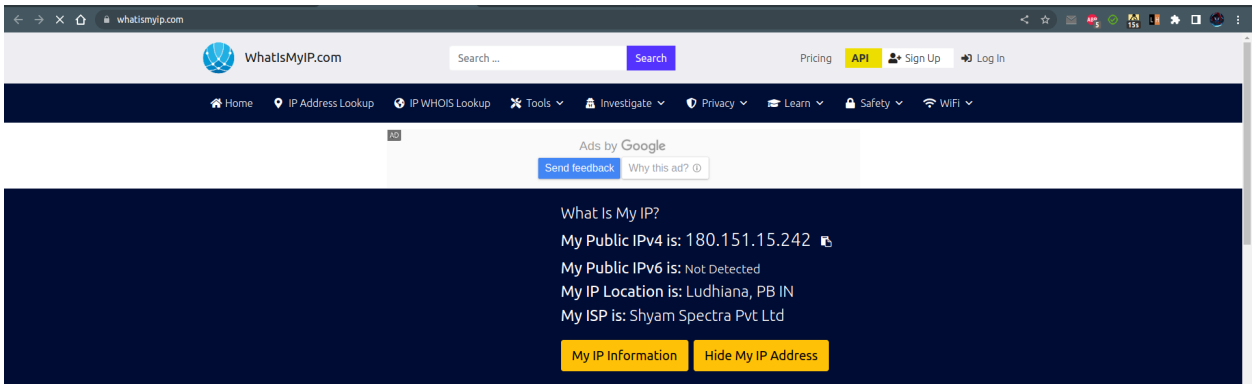
Q1. [1+2]

a) Learn to use the ifconfig command, and figure out the IP address of your network interface. Put a screenshot.



IPv4 address = 192.168.51.178
IPv6 address = f380::27cd:7ec2:fc5b:7039

b) Go to the webpage https://www.whatismyip.com and find out what IP is shown for your machine. Are they identical or different? Why?



IP using ifconfig = 192.168.51.178
IP using whatismyip = 180.151.15.242

The IP that is shown using ipconfig is my local ip address. It is private to my device and is not visible to others while browsing the internet. The IP that whatismyip shows is the ip address that

is provided by my ISP via the router/proxy that I am connected to. In order to resolve the issue of limited ips, the ip address of the router is used to connect to the world. This same router IP will be shown for every laptop/device that would connect to whatismyip using the same ISP.

Q2. nslookup [[2+1] + [2 +1]]

a) Get an authoritative result in nslookup. Put a screenshot. Explain how you did it.

```
hiteshgarg@hitesh--Ubuntu: ~
hiteshgarg@hitesh--Ubuntu:~$ nslookup facebook.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   facebook.com
Address: 31.13.79.35
Name:   facebook.com
Address: 2a03:2880:f144:82:face:b00c:0:25de

hiteshgarg@hitesh--Ubuntu:~$ nslookup -type=soa facebook.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
facebook.com
        origin = a.ns.facebook.com
        mail addr = dns.facebook.com
        serial = 3665155098
        refresh = 14400
        retry = 1800
        expire = 604800
        minimum = 300

Authoritative answers can be found from:
a.ns.facebook.com       internet address = 129.134.30.12
a.ns.facebook.com       has AAAA address 2a03:2880:f0fc:c:face:b00c:0:35

hiteshgarg@hitesh--Ubuntu:~$ nslookup facebook.com a.ns.facebook.com
Server:         a.ns.facebook.com
Address:        129.134.30.12#53

Name:   facebook.com
Address: 157.240.198.35
Name:   facebook.com
Address: 2a03:2880:f144:82:face:b00c:0:25de
```

As seen in the screenshot, I first query facebook.com directly. Since facebook is a very frequently accessed website, the result is returned from the DNS server (a server that caches the data of frequently visited sites so they can be served quickly).

In order to get an authoritative answer, we need to perform a soa (start of authority) query. This would get a list of possible servers that we can query to get an authoritative answer.

We then query facebook.com again with the primary name server as the authoritative server (a.ns.facebook.com) to get an authoritative result.

b) Find out time to live for any website on the local dns. Put a screenshot. Explain in

words (with unit) that after how much time this entry would expire.

Time to live (TTL) refers to the amount of time or “hops” that a packet is set to exist inside a network before being discarded by a router. (source).

```
hiteshgarg@hitesh--U
hiteshgarg@hitesh--Ubuntu:~$ nslookup -debug google.in
Server:         127.0.0.53
Address:        127.0.0.53#53

------------
    QUESTIONS:
        google.in, type = A, class = IN
    ANSWERS:
    ->  google.in
        internet address = 142.250.183.164
        ttl = 300
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Non-authoritative answer:
Name:   google.in
Address: 142.250.183.164
------------
    QUESTIONS:
        google.in, type = AAAA, class = IN
    ANSWERS:
    ->  google.in
        has AAAA address 2404:6800:4002:806::2004
        ttl = 201
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Name:   google.in
Address: 2404:6800:4002:806::2004
```

TTL for IPv4 request: 300 seconds
TTL for IPv6 request: 201 seconds

TTL for google.com is 29s (seconds). This means that the packet to google.com will be discarded after 29s.

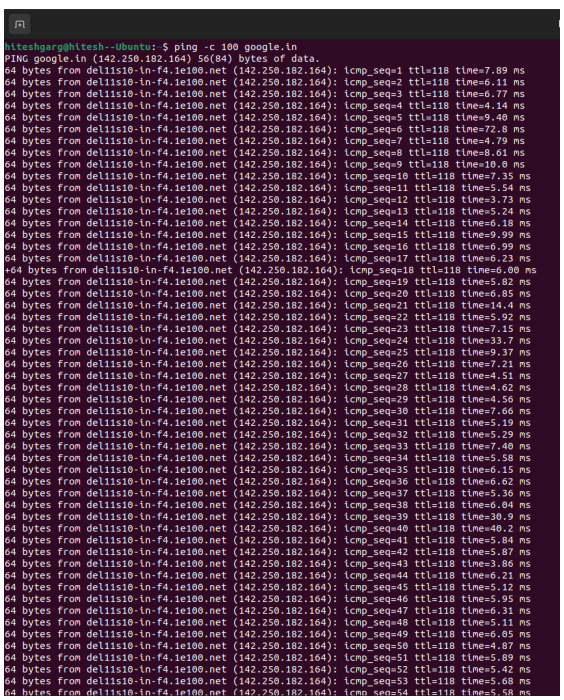
Q3. Run the command, traceroute google.in
a) How many intermediate hosts do you see, what are the IP addresses, compute the average latency to each intermediate host. Put a screenshot. [2+2]
Note that some of the intermediate hosts might not be visible, their IP addresses will come as “*”, ignore those hosts for this assignment.**

```
hiteshgarg@hitesh--Ubuntu:~$ traceroute google.in
traceroute to google.in (216.58.196.196), 30 hops max, 60 byte packets
 1  192.168.48.254 (192.168.48.254)  116.660 ms  116.606 ms  116.590 ms
 2  auth.iiitd.edu.in (192.168.1.99)  59.090 ms  59.074 ms  59.056 ms
 3  180.151.15.241.reverse.spectranet.in (180.151.15.241)  44.692 ms  44.678 ms  44.664 ms
 4  72.14.194.202 (72.14.194.202)  91.642 ms  91.626 ms  91.612 ms
 5  108.170.251.97 (108.170.251.97)  58.954 ms  58.939 ms 108.170.251.113 (108.170.251.113)  91.559 ms
 6  216.239.47.99 (216.239.47.99)  91.548 ms 216.239.56.253 (216.239.56.253)  60.083 ms  60.026 ms
 7  del03s06-in-f4.1e100.net (216.58.196.196)  59.560 ms  46.182 ms  46.124 ms
```

It took 7 intermediate hosts to reach google.com

S. No.	IP Address	Average Latency
1	192.168.48.254	(116.660+116.606+116.590)/3 = 116.618 ms
2	192.168.1.99	(59.090+59.074+59.074)/3 =59.079 ms
3	180.151.15.241	(44.692+44.678+44.664)/3 = 44.678 ms
4	72.14.194.202	(91.642+91.626+91.612)/3 = 91.626 ms
5	108.170.251.97	(58.954+58.939+91.559)/3 = 69.817 ms
6	216.239.47.99	(91.548+60.083+60.026)/3 = 70.552 ms
7	216.58.196.196	(59.560+46.182+46.124)/3 = 50.622ms

b) Send 100 ping messages to google.in, Determine the average latency. Put a Screenshot.[2]



```
hiteshgarg@hitesh--Ubuntu:~$ ping -c 100 google.in
PING google.in (142.250.182.164) 56(84) bytes of data.
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=1 ttl=118 time=7.89 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=2 ttl=118 time=6.11 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=3 ttl=118 time=6.77 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=4 ttl=118 time=4.14 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=5 ttl=118 time=9.40 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=6 ttl=118 time=72.8 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=7 ttl=118 time=4.79 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=8 ttl=118 time=8.61 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=9 ttl=118 time=10.0 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=10 ttl=118 time=7.35 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=11 ttl=118 time=5.54 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=12 ttl=118 time=3.73 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=13 ttl=118 time=5.24 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=14 ttl=118 time=6.18 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=15 ttl=118 time=9.99 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=16 ttl=118 time=6.99 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=17 ttl=118 time=6.23 ms
+64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=18 ttl=118 time=6.00 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=19 ttl=118 time=5.82 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=20 ttl=118 time=6.85 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=21 ttl=118 time=14.4 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=22 ttl=118 time=5.92 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=23 ttl=118 time=7.15 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=24 ttl=118 time=33.7 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=25 ttl=118 time=9.37 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=26 ttl=118 time=7.21 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=27 ttl=118 time=4.51 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=28 ttl=118 time=4.62 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=29 ttl=118 time=4.56 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=30 ttl=118 time=7.66 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=31 ttl=118 time=5.19 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=32 ttl=118 time=5.29 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=33 ttl=118 time=7.40 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=34 ttl=118 time=5.58 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=35 ttl=118 time=6.15 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=36 ttl=118 time=6.62 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=37 ttl=118 time=5.36 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=38 ttl=118 time=6.04 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=39 ttl=118 time=30.9 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=40 ttl=118 time=40.2 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=41 ttl=118 time=5.84 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=42 ttl=118 time=5.87 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=43 ttl=118 time=3.86 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=44 ttl=118 time=6.21 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=45 ttl=118 time=5.12 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=46 ttl=118 time=5.95 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=47 ttl=118 time=6.31 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=48 ttl=118 time=5.11 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=49 ttl=118 time=6.05 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=50 ttl=118 time=4.87 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=51 ttl=118 time=5.89 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=52 ttl=118 time=5.42 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=53 ttl=118 time=5.68 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=54 ttl=118 time=5.58 ms
```

```
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=51 ttl=118 time=5.89 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=52 ttl=118 time=5.42 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=53 ttl=118 time=5.68 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=54 ttl=118 time=5.58 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=55 ttl=118 time=9.03 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=56 ttl=118 time=5.05 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=57 ttl=118 time=4.93 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=58 ttl=118 time=5.40 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=59 ttl=118 time=5.59 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=60 ttl=118 time=4.39 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=61 ttl=118 time=5.99 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=62 ttl=118 time=5.72 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=63 ttl=118 time=5.21 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=64 ttl=118 time=4.95 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=65 ttl=118 time=5.93 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=66 ttl=118 time=5.27 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=67 ttl=118 time=5.92 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=68 ttl=118 time=5.83 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=69 ttl=118 time=6.03 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=70 ttl=118 time=10.9 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=71 ttl=118 time=97.3 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=72 ttl=118 time=3.57 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=73 ttl=118 time=4.75 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=74 ttl=118 time=5.75 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=75 ttl=118 time=4.89 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=76 ttl=118 time=6.71 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=77 ttl=118 time=6.20 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=78 ttl=118 time=5.31 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=79 ttl=118 time=5.42 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=80 ttl=118 time=6.44 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=81 ttl=118 time=5.08 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=82 ttl=118 time=3.87 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=83 ttl=118 time=4.72 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=84 ttl=118 time=5.81 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=85 ttl=118 time=3.65 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=86 ttl=118 time=6.56 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=87 ttl=118 time=6.58 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=88 ttl=118 time=6.66 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=89 ttl=118 time=5.42 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=90 ttl=118 time=5.31 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=91 ttl=118 time=5.68 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=92 ttl=118 time=5.00 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=93 ttl=118 time=3.20 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=94 ttl=118 time=5.59 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=95 ttl=118 time=6.38 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=96 ttl=118 time=5.78 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=97 ttl=118 time=14.6 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=98 ttl=118 time=11.5 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=99 ttl=118 time=4.93 ms
64 bytes from del11s10-in-f4.1e100.net (142.250.182.164): icmp_seq=100 ttl=118 time=5.82 ms

--- google.in ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 99122ms
rtt min/avg/max/mdev = 3.203/8.605/97.318/12.262 ms
hiteshgarg@hitesh--Ubuntu:~$ +
```

Average latency for 100 ping to google.in = 8.605 ms

c) Send 100 ping messages to columbia.edu, Determine the average latency. Put a Screenshot.[2]

```
hiteshgarg@hitesh--Ubuntu: ~
hiteshgarg@hitesh--Ubuntu:~$ ping -c 100 columbia.edu
PING columbia.edu (128.59.105.24) 56(84) bytes of data.
64 bytes from columbiauniversity.info (128.59.105.24): icmp_seq=1 ttl=234 time=307 ms
64 bytes from www.neurotheory.columbia.edu (128.59.105.24): icmp_seq=2 ttl=234 time=338 ms
64 bytes from p-i-r.org (128.59.105.24): icmp_seq=3 ttl=234 time=262 ms
64 bytes from www.neurotheory.columbia.edu (128.59.105.24): icmp_seq=4 ttl=234 time=293 ms
64 bytes from childpolicy.org (128.59.105.24): icmp_seq=5 ttl=234 time=326 ms
64 bytes from vii.org (128.59.105.24): icmp_seq=6 ttl=234 time=353 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=7 ttl=234 time=283 ms
64 bytes from neurotheory.columbia.edu (128.59.105.24): icmp_seq=8 ttl=234 time=314 ms
64 bytes from columbiauniversity.us (128.59.105.24): icmp_seq=9 ttl=234 time=343 ms
64 bytes from gutenberg-e.org (128.59.105.24): icmp_seq=10 ttl=234 time=270 ms
64 bytes from p-i-r.org (128.59.105.24): icmp_seq=11 ttl=234 time=311 ms
64 bytes from old.columbia.university (128.59.105.24): icmp_seq=12 ttl=234 time=246 ms
64 bytes from p-i-r.org (128.59.105.24): icmp_seq=13 ttl=234 time=263 ms
64 bytes from gutenberg-e.org (128.59.105.24): icmp_seq=14 ttl=234 time=293 ms
64 bytes from childpolicy.org (128.59.105.24): icmp_seq=15 ttl=234 time=324 ms
64 bytes from vii.org (128.59.105.24): icmp_seq=16 ttl=234 time=356 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=17 ttl=234 time=284 ms
64 bytes from vii.org (128.59.105.24): icmp_seq=18 ttl=234 time=316 ms
64 bytes from vii.org (128.59.105.24): icmp_seq=19 ttl=234 time=345 ms
64 bytes from teachtechaward.org (128.59.105.24): icmp_seq=20 ttl=234 time=244 ms
64 bytes from old.columbia.university (128.59.105.24): icmp_seq=21 ttl=234 time=244 ms
64 bytes from www.neurotheory.columbia.edu (128.59.105.24): icmp_seq=22 ttl=234 time=331 ms
64 bytes from p-i-r.org (128.59.105.24): icmp_seq=23 ttl=234 time=262 ms
64 bytes from vii.org (128.59.105.24): icmp_seq=24 ttl=234 time=277 ms
64 bytes from neurotheory.columbia.edu (128.59.105.24): icmp_seq=25 ttl=234 time=321 ms
64 bytes from old.columbia.university (128.59.105.24): icmp_seq=26 ttl=234 time=331 ms
64 bytes from p-i-r.org (128.59.105.24): icmp_seq=27 ttl=234 time=254 ms
64 bytes from columbiauniversity.info (128.59.105.24): icmp_seq=28 ttl=234 time=308 ms
64 bytes from columbiauniversity.us (128.59.105.24): icmp_seq=29 ttl=234 time=346 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=30 ttl=234 time=342 ms
64 bytes from gutenberg-e.org (128.59.105.24): icmp_seq=31 ttl=234 time=247 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=32 ttl=234 time=247 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=33 ttl=234 time=259 ms
64 bytes from neurotheory.columbia.edu (128.59.105.24): icmp_seq=34 ttl=234 time=287 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=35 ttl=234 time=357 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=36 ttl=234 time=246 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=37 ttl=234 time=275 ms
64 bytes from vii.org (128.59.105.24): icmp_seq=38 ttl=234 time=326 ms
64 bytes from childpolicy.org (128.59.105.24): icmp_seq=39 ttl=234 time=334 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=40 ttl=234 time=246 ms
64 bytes from childpolicy.org (128.59.105.24): icmp_seq=41 ttl=234 time=292 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=42 ttl=234 time=291 ms
64 bytes from columbiauniversity.net (128.59.105.24): icmp_seq=43 ttl=234 time=355 ms
64 bytes from old.columbia.university (128.59.105.24): icmp_seq=44 ttl=234 time=286 ms
64 bytes from teachtechaward.org (128.59.105.24): icmp_seq=45 ttl=234 time=314 ms
64 bytes from neurotheory.columbia.edu (128.59.105.24): icmp_seq=46 ttl=234 time=348 ms
64 bytes from p-i-r.org (128.59.105.24): icmp_seq=47 ttl=234 time=257 ms
64 bytes from columbiauniversity.org (128.59.105.24): icmp_seq=48 ttl=234 time=246 ms
64 bytes from vii.org (128.59.105.24): icmp_seq=49 ttl=234 time=339 ms
64 bytes from p-i-r.org (128.59.105.24): icmp_seq=50 ttl=234 time=243 ms
64 bytes from neurotheory.columbia.edu (128.59.105.24): icmp_seq=51 ttl=234 time=292 ms
```

```
hiteshgarg@hitesh-Ubuntu: ~
64 bytes from columbiauniversity.info (128.59.105.24): icmp_seq=53 ttl=234 time=250 ms
64 bytes from neurotheory.columbia.edu (128.59.105.24): icmp_seq=54 ttl=234 time=247 ms
64 bytes from www.neurotheory.columbia.edu (128.59.105.24): icmp_seq=55 ttl=234 time=315 ms
64 bytes from columbiauniversity.org (128.59.105.24): icmp_seq=56 ttl=234 time=342 ms
64 bytes from columbiauniversity.net (128.59.105.24): icmp_seq=57 ttl=234 time=373 ms
64 bytes from teachtechaward.org (128.59.105.24): icmp_seq=58 ttl=234 time=304 ms
64 bytes from childpolicy.org (128.59.105.24): icmp_seq=59 ttl=234 time=330 ms
64 bytes from teachtechaward.org (128.59.105.24): icmp_seq=60 ttl=234 time=256 ms
64 bytes from columbiauniversity.us (128.59.105.24): icmp_seq=61 ttl=234 time=363 ms
64 bytes from vii.org (128.59.105.24): icmp_seq=62 ttl=234 time=302 ms
64 bytes from childpolicy.org (128.59.105.24): icmp_seq=63 ttl=234 time=247 ms
64 bytes from columbiauniversity.us (128.59.105.24): icmp_seq=64 ttl=234 time=363 ms
64 bytes from columbiauniversity.info (128.59.105.24): icmp_seq=65 ttl=234 time=292 ms
64 bytes from columbiauniversity.info (128.59.105.24): icmp_seq=66 ttl=234 time=322 ms
64 bytes from p-i-r.org (128.59.105.24): icmp_seq=67 ttl=234 time=243 ms
64 bytes from p-i-r.org (128.59.105.24): icmp_seq=68 ttl=234 time=247 ms
64 bytes from p-i-r.org (128.59.105.24): icmp_seq=69 ttl=234 time=314 ms
64 bytes from p-i-r.org (128.59.105.24): icmp_seq=70 ttl=234 time=264 ms
64 bytes from old.columbia.university (128.59.105.24): icmp_seq=71 ttl=234 time=476 ms
64 bytes from childpolicy.org (128.59.105.24): icmp_seq=72 ttl=234 time=302 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=73 ttl=234 time=333 ms
64 bytes from vii.org (128.59.105.24): icmp_seq=74 ttl=234 time=486 ms
64 bytes from childpolicy.org (128.59.105.24): icmp_seq=75 ttl=234 time=407 ms
64 bytes from teachtechaward.org (128.59.105.24): icmp_seq=76 ttl=234 time=246 ms
64 bytes from columbiauniversity.info (128.59.105.24): icmp_seq=77 ttl=234 time=265 ms
64 bytes from childpolicy.org (128.59.105.24): icmp_seq=78 ttl=234 time=280 ms
64 bytes from www.neurotheory.columbia.edu (128.59.105.24): icmp_seq=79 ttl=234 time=516 ms
64 bytes from p-i-r.org (128.59.105.24): icmp_seq=80 ttl=234 time=315 ms
64 bytes from www.neurotheory.columbia.edu (128.59.105.24): icmp_seq=81 ttl=234 time=271 ms
64 bytes from columbiauniversity.info (128.59.105.24): icmp_seq=82 ttl=234 time=307 ms
64 bytes from childpolicy.org (128.59.105.24): icmp_seq=83 ttl=234 time=246 ms
64 bytes from old.columbia.university (128.59.105.24): icmp_seq=84 ttl=234 time=259 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=85 ttl=234 time=247 ms
64 bytes from columbiauniversity.us (128.59.105.24): icmp_seq=86 ttl=234 time=321 ms
64 bytes from columbiauniversity.us (128.59.105.24): icmp_seq=87 ttl=234 time=360 ms
64 bytes from old.columbia.university (128.59.105.24): icmp_seq=88 ttl=234 time=245 ms
64 bytes from childpolicy.org (128.59.105.24): icmp_seq=89 ttl=234 time=244 ms
64 bytes from old.columbia.university (128.59.105.24): icmp_seq=90 ttl=234 time=340 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=91 ttl=234 time=267 ms
64 bytes from old.columbia.university (128.59.105.24): icmp_seq=92 ttl=234 time=258 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=93 ttl=234 time=326 ms
64 bytes from neurotheory.columbia.edu (128.59.105.24): icmp_seq=94 ttl=234 time=254 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=95 ttl=234 time=287 ms
64 bytes from p-i-r.org (128.59.105.24): icmp_seq=96 ttl=234 time=244 ms
64 bytes from columbiauniversity.us (128.59.105.24): icmp_seq=97 ttl=234 time=245 ms
64 bytes from p-i-r.org (128.59.105.24): icmp_seq=98 ttl=234 time=245 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=99 ttl=234 time=305 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=100 ttl=234 time=335 ms

--- columbia.edu ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 103772ms
rtt min/avg/max/mdev = 242.934/301.052/516.361/52.175 ms
hiteshgarg@hitesh--Ubuntu:~$
```

Average latency for 100 ping to columbia.edu = 301.052 ms

d) Add up the ping latency of all the intermediate hosts and compare with (b). Are they matching, explain?[1+1]

```
hiteshgarg@hitesh--Ubuntu: ~
hiteshgarg@hitesh--Ubuntu:~$ ping 192.168.48.254 -c 3
PING 192.168.48.254 (192.168.48.254) 56(84) bytes of data.
64 bytes from 192.168.48.254: icmp_seq=1 ttl=255 time=9.53 ms
64 bytes from 192.168.48.254: icmp_seq=2 ttl=255 time=4.91 ms
64 bytes from 192.168.48.254: icmp_seq=3 ttl=255 time=6.79 ms

--- 192.168.48.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 4.911/7.079/9.533/1.897 ms
```

```
hiteshgarg@hitesh--Ubuntu: ~
hiteshg...   hiteshg...   hiteshg...   hiteshg...   hiteshg...
hiteshgarg@hitesh--Ubuntu:~$ ping 192.168.1.99 -c 3
PING 192.168.1.99 (192.168.1.99) 56(84) bytes of data.
64 bytes from 192.168.1.99: icmp_seq=1 ttl=254 time=17.8 ms
64 bytes from 192.168.1.99: icmp_seq=2 ttl=254 time=2.97 ms
64 bytes from 192.168.1.99: icmp_seq=3 ttl=254 time=3.51 ms

--- 192.168.1.99 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.973/8.088/17.781/6.857 ms
hiteshgarg@hitesh--Ubuntu:~$
```

```
hiteshgarg@hitesh--Ubuntu: ~
hiteshgarg@hit...   hiteshgarg@hit...   hiteshgarg@hit...   hiteshg
hiteshgarg@hitesh--Ubuntu:~$ ping 180.151.15.241 -c 3
PING 180.151.15.241 (180.151.15.241) 56(84) bytes of data.
64 bytes from 180.151.15.241: icmp_seq=1 ttl=62 time=5.83 ms
64 bytes from 180.151.15.241: icmp_seq=2 ttl=62 time=13.3 ms
64 bytes from 180.151.15.241: icmp_seq=3 ttl=62 time=10.7 ms

--- 180.151.15.241 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 5.834/9.924/13.255/3.076 ms
hiteshgarg@hitesh--Ubuntu:~$
```

```
hiteshgarg@hitesh--Ubuntu: ~
hiteshgarg@hitesh--U...   hiteshgarg@hitesh--U...   hiteshgarg@hitesh--U
hiteshgarg@hitesh--Ubuntu:~$ ping 72.14.194.202 -c 3
PING 72.14.194.202 (72.14.194.202) 56(84) bytes of data.
64 bytes from 72.14.194.202: icmp_seq=1 ttl=60 time=7.41 ms
64 bytes from 72.14.194.202: icmp_seq=2 ttl=60 time=8.10 ms
64 bytes from 72.14.194.202: icmp_seq=3 ttl=60 time=22.4 ms

--- 72.14.194.202 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 7.414/12.622/22.350/6.884 ms
hiteshgarg@hitesh--Ubuntu:~$
```

```
hiteshgarg@hitesh--Ubuntu: ~
hiteshgarg@hit...   hiteshgarg@hit...   hiteshgarg@hit...   hitesh
hiteshgarg@hitesh--Ubuntu:~$ ping 108.170.251.97 -c 3
PING 108.170.251.97 (108.170.251.97) 56(84) bytes of data.
64 bytes from 108.170.251.97: icmp_seq=1 ttl=57 time=7.77 ms
64 bytes from 108.170.251.97: icmp_seq=2 ttl=57 time=11.6 ms
64 bytes from 108.170.251.97: icmp_seq=3 ttl=57 time=6.54 ms

--- 108.170.251.97 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 6.540/8.624/11.563/2.137 ms
hiteshgarg@hitesh--Ubuntu:~$
```

```
hiteshgarg@hitesh--Ubuntu:~$ ping 216.239.47.99 -c 3
PING 216.239.47.99 (216.239.47.99) 56(84) bytes of data.

--- 216.239.47.99 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2038ms
```

```
hiteshgarg@hitesh--Ubuntu:~$ ping 216.58.196.196 -c 3
PING 216.58.196.196 (216.58.196.196) 56(84) bytes of data.
64 bytes from 216.58.196.196: icmp_seq=1 ttl=118 time=5.63 ms
64 bytes from 216.58.196.196: icmp_seq=2 ttl=118 time=5.71 ms
64 bytes from 216.58.196.196: icmp_seq=3 ttl=118 time=56.4 ms

--- 216.58.196.196 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 5.627/22.574/56.387/23.909 ms
hiteshgarg@hitesh--Ubuntu:~$
```

IP Address	Average latency (traceroute)	Average latency (ping)
192.168.48.254	116.618 ms	7.079 ms
192.168.1.99	59.079 ms	8.088 ms
180.151.15.241	44.678 ms	9.924 ms
72.14.194.202	91.626 ms	12.622 ms
108.170.251.97	69.817 ms	8.624
216.239.47.99	70.552 ms	-
216.58.196.196	50.622 ms	22.574

Average latency from traceroute for all intermediate hops is greater than the average latency from 3 pings. This is because of the difference between traceroute and ping nature. Traceroute finds the path taken to the server along with each intermediate step it took and the time taken for each step. This means that the traceroute will stop at each step (hop) and sends back an acknowledgement to identify that hop. Ping, on the other hand, just checks whether the destination is reachable or not. Since ping is not concerned with the intermediate steps it takes, it is much faster than traceroute and hence the low latency. (reference)

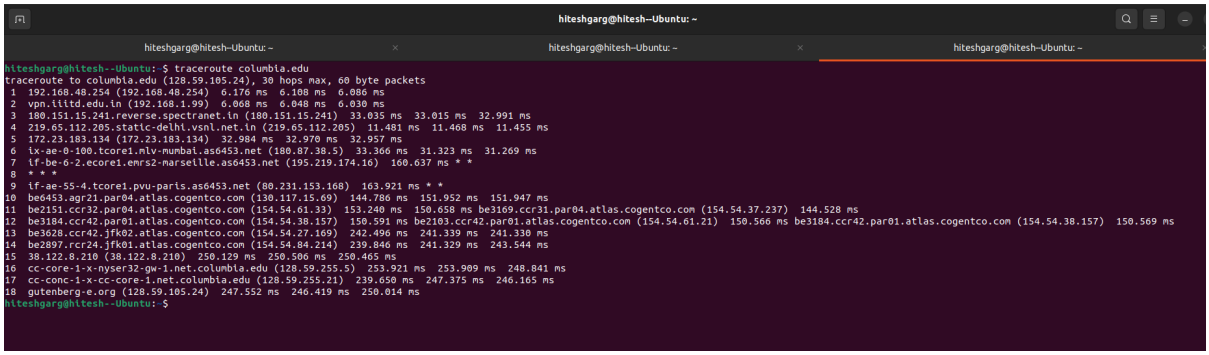
e) Take the maximum of ping latency amongst the intermediate hosts and compare with (b). Are they matching,explain? [1+1]

IP Address	Maximum latency (traceroute)	Maximum latency (ping)
192.168.48.254	116.660 ms	9.53 ms
192.168.1.99	59.090 ms	17.8 ms
180.151.15.241	44.692 ms	13.3 ms
72.14.194.202	91.642 ms	22.4ms
108.170.251.97	91.559 ms	11.6
216.239.47.99	91.548 ms	-
216.58.196.196	59.560 ms	56.4

We can see a general trend that maximum latency from ping is less than maximum latency from traceroute. The reason for this is already explained in the above part that the ping command

only cares about whether the destination is reachable or not and not the intermediate hops and hence is faster. Whereas the traceroute command also cares about the intermediate hops and time it takes to reach them along with the destination and hence is slower. This is what is reflected in the above table.

f) Traceroute columbia.edu. Compare the number of hops between google.in and columbia.edu (between the traceroute result of google.in and columbia.edu). Can you explain the reason for the latency difference between google.in and columbia.edu?



The number of hops to reach columbia.edu is 18 while for google.in is 7. The number of hops for google is significantly less than columbia. More the number of hops, the more time it will take to reach each step (hop) and send an acknowledgement back to the host. Due to this time in sending back an acknowledgment from each hop, the latency of columbia is much higher than google.

Q4. [2+1] Make your ping command fail for 127.0.0.1 (with 100% packet loss). Explain how you do it. Put a screenshot that it failed.

```
hiteshgarg@hitesh--Ubuntu:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:4c:35:71:cb  txqueuelen 0  (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 13698  bytes 1492597 (1.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13698  bytes 1492597 (1.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.51.178  netmask 255.255.240.0  broadcast 192.168.63.255
        inet6 fe80::27cd:7ec2:fc5b:7039  prefixlen 64  scopeid 0x20<link>
        ether 54:14:f3:c9:39:b1  txqueuelen 1000  (Ethernet)
        RX packets 1404344  bytes 744978420 (744.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 317368  bytes 104452138 (104.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

hiteshgarg@hitesh--Ubuntu:~$ sudo ifconfig lo down
[sudo] password for hiteshgarg:
hiteshgarg@hitesh--Ubuntu:~$ ping 127.0.0.1 -c 10
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.

--- 127.0.0.1 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9214ms

hiteshgarg@hitesh--Ubuntu:~$ sudo ifconfig lo up
hiteshgarg@hitesh--Ubuntu:~$ ping 127.0.0.1 -c 10
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.041 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.048 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.048 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.057 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.048 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.048 ms
64 bytes from 127.0.0.1: icmp_seq=7 ttl=64 time=0.046 ms
64 bytes from 127.0.0.1: icmp_seq=8 ttl=64 time=0.053 ms
64 bytes from 127.0.0.1: icmp_seq=9 ttl=64 time=0.050 ms
64 bytes from 127.0.0.1: icmp_seq=10 ttl=64 time=0.050 ms

--- 127.0.0.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9219ms
rtt min/avg/max/mdev = 0.041/0.048/0.057/0.004 ms
hiteshgarg@hitesh--Ubuntu:~$
```

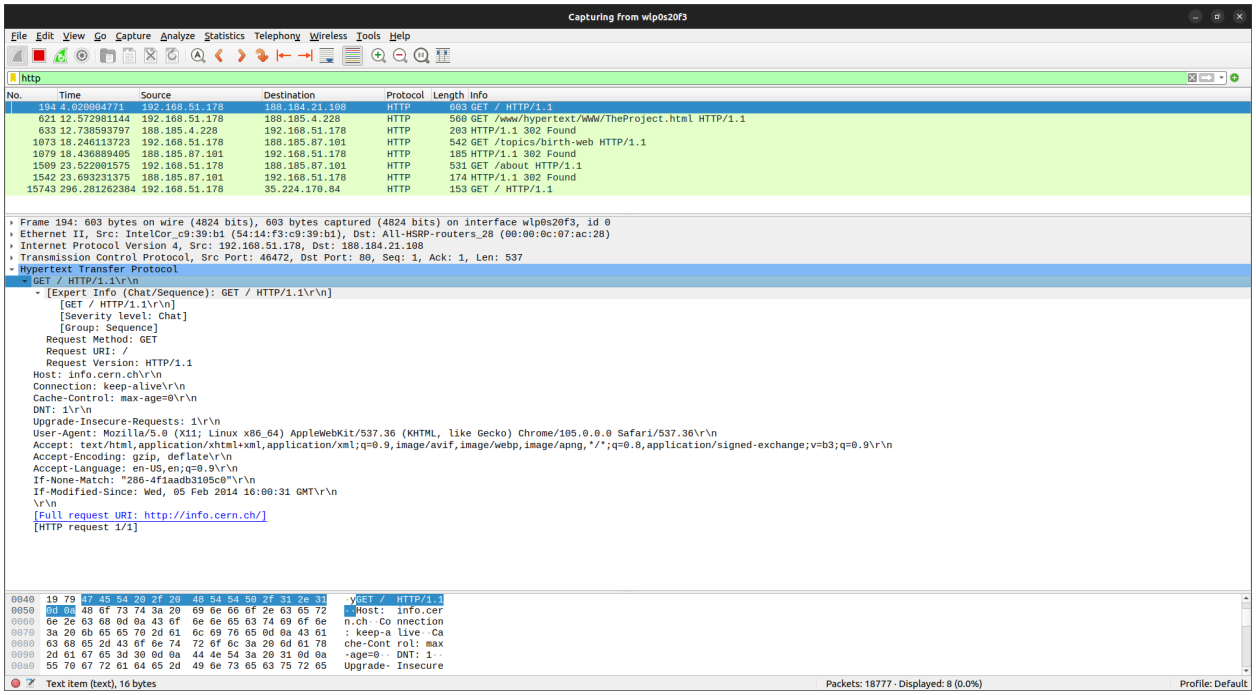
The ip 127.0.0.1 corresponds to the local server. In order to get a 100% packet loss, we need to down the server (lo) so every packet sent to it would miss. This is achieved using the sudo ifconfig lo down command. As we can see, after that we can get a 100% packet loss.

Then we up the server again and ping it. We can see that after upping the server, we are 0% packet loss.

Q5. [2+2+2+1] Use your web browser to retrieve the http://info.cern.ch web page. While retrieving the web page, use wireshark/tshark/tcpdump at your machine to capture the communication between your machine and the web server. You may need to filter the required

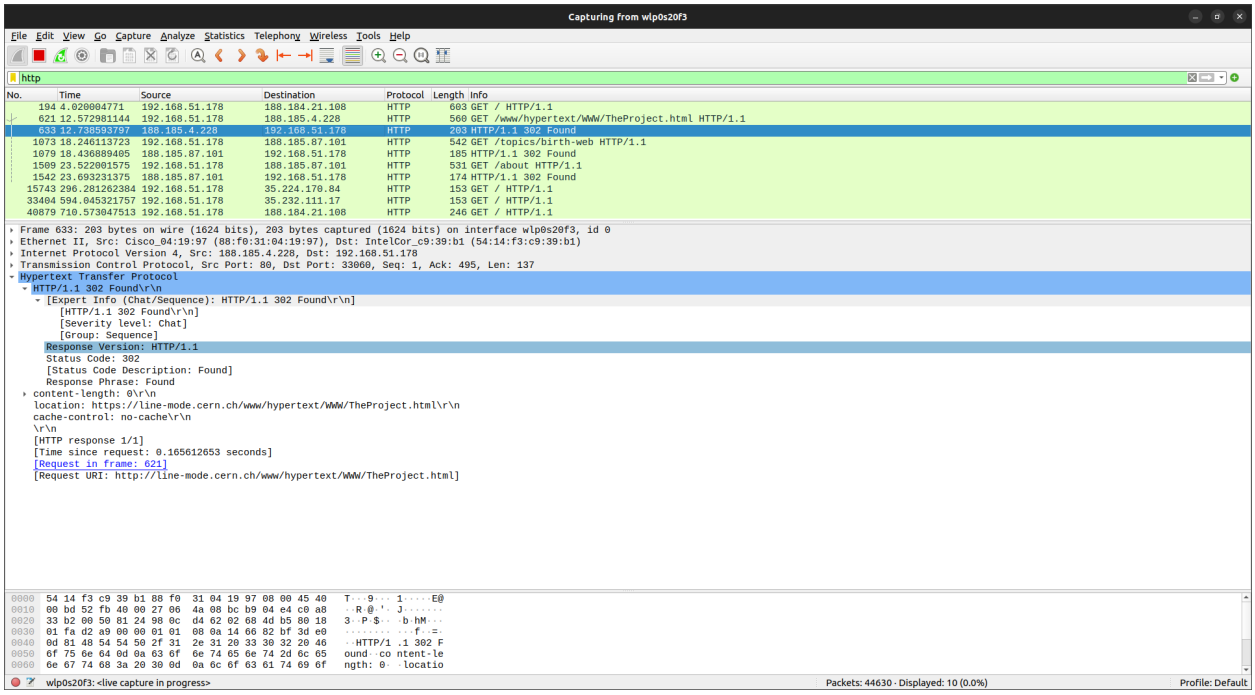
packets. Put the screenshot of HTTP request and response messages. Explain the following details for each captured packet.

- **For HTTP request packets**
  - **HTTP request type**
  - **User agent type**
  - **HTTP request packet's URL**



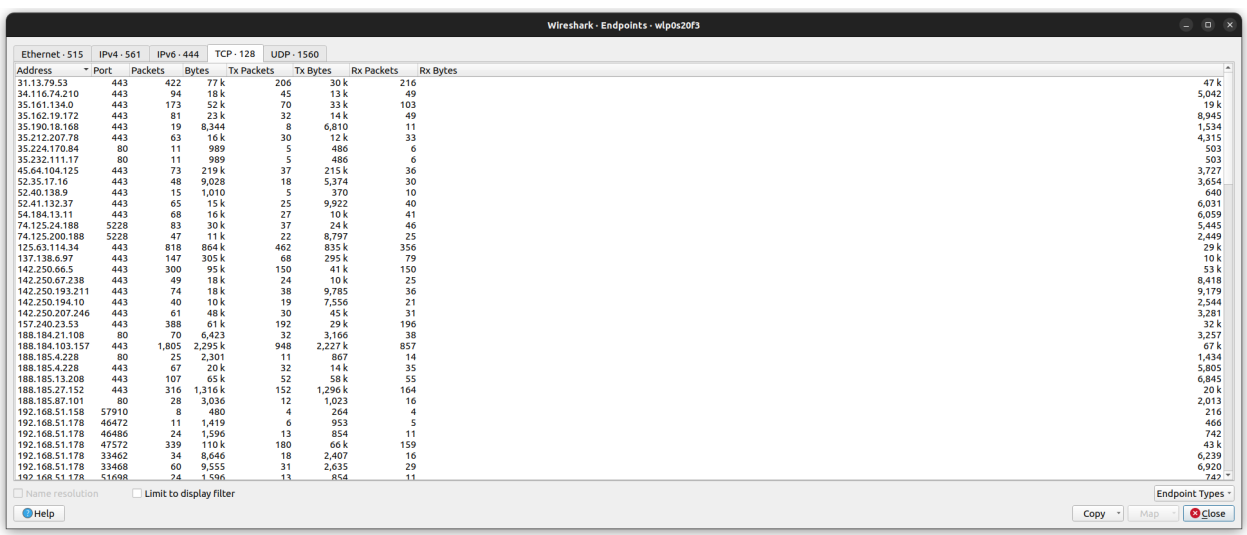
HTTP Request Type: GET
User agent type: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
HTTP request packet's URL: http://info.cern.ch/

- **For HTTP response packets**
  - **HTTP response code**
  - **HTTP response description**
  - **Name and version of the web server**



HTTP response code: 302
HTTP response description: Found
Name and version of the web server: Apache\r\n and (version = HTTP/1.1)

● How many web objects get downloaded? Were they over the same TCP connection or different connections?



We can see from the above screenshot that 128 packets have downloaded and they are downloaded over different TCP connections.

● From this tell if it is HTTP persistent or non-persistent?

```
Hypertext Transfer Protocol
  HTTP/1.1 302 Found\r\n
```

We can see that we have HTTP 1.1 as the connection, which is persistent.

Q6. [1+1] Note: perform this test after Q5

a) Write the command to display all active tcp connections with pids

```
hiteshgarg@hitesh--Ubuntu:~$ netstat --tcp -p -a
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      -
tcp        0      0 hitesh--Ubuntu:40288    sa-in-f188.1e100.n:5228 ESTABLISHED 2852/chrome --type=
tcp        0      0 hitesh--Ubuntu:60946    del11s17-in-f19.1:https ESTABLISHED 2852/chrome --type=
tcp        0      0 hitesh--Ubuntu:33998    ec2-35-162-19-172:https ESTABLISHED -
tcp        0      0 hitesh--Ubuntu:55196    whatsapp-cdn-shv-:https ESTABLISHED 2852/chrome --type=
tcp        0      0 hitesh--Ubuntu:48464    bom07s35-in-f5.1e:https ESTABLISHED 2852/chrome --type=
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN      -
hiteshgarg@hitesh--Ubuntu:~$
```

b) Determine the state of the TCP connection(s) to this server http://info.cern.ch

```
hiteshgarg@hitesh--Ubuntu:~$ netstat -at info.cern.ch
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 hitesh--Ubuntu:56884    whatsapp-cdn-shv-:https ESTABLISHED
tcp        0      0 hitesh--Ubuntu:44836    sd-in-f188.1e100.n:5228 ESTABLISHED
tcp        0      0 hitesh--Ubuntu:56422    bom12s21-in-f5.1e:https ESTABLISHED
tcp        0      0 hitesh--Ubuntu:58600    21.4.120.34.bc.go:https ESTABLISHED
tcp        0      0 hitesh--Ubuntu:45638    webafs706.cern.ch:http  ESTABLISHED
tcp        0      0 hitesh--Ubuntu:35204    59.107.201.35.bc.:https ESTABLISHED
tcp        0      0 hitesh--Ubuntu:42362    del12s04-in-f14.1:https ESTABLISHED
tcp        0      0 hitesh--Ubuntu:43280    104.16.124.175:https    ESTABLISHED
tcp        0      0 hitesh--Ubuntu:38694    236.234.111.34.bc:https ESTABLISHED
tcp        0      0 hitesh--Ubuntu:47732    a-0001.a-msedge.n:https ESTABLISHED
tcp        0      0 hitesh--Ubuntu:40320    104.16.204.22:https     ESTABLISHED
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
hiteshgarg@hitesh--Ubuntu:~$
```

As we can see from the above screenshot, the connection to cern is established.