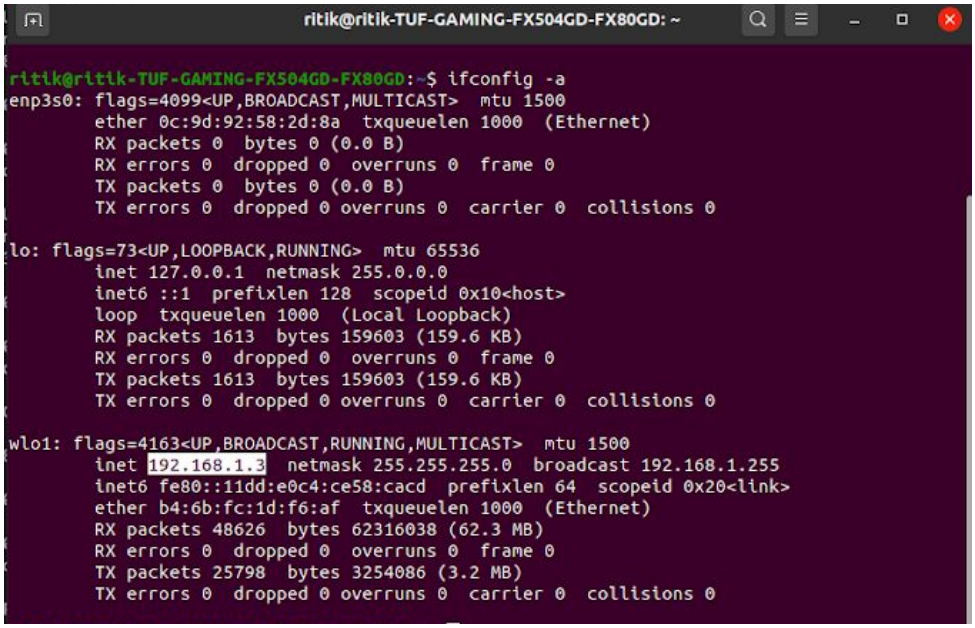
Assignment 2
Ritik Garg | 2018305

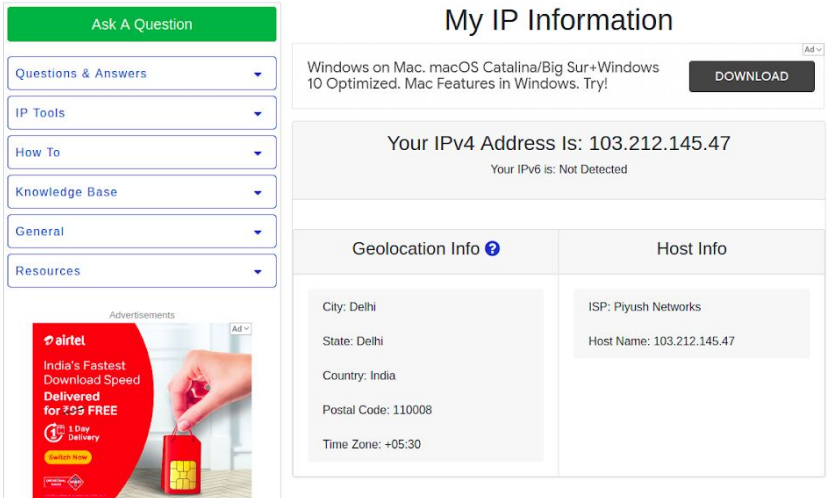
Q1.

(a) Command: **ifconfig**

Ip address : **192.168.1.3/24**

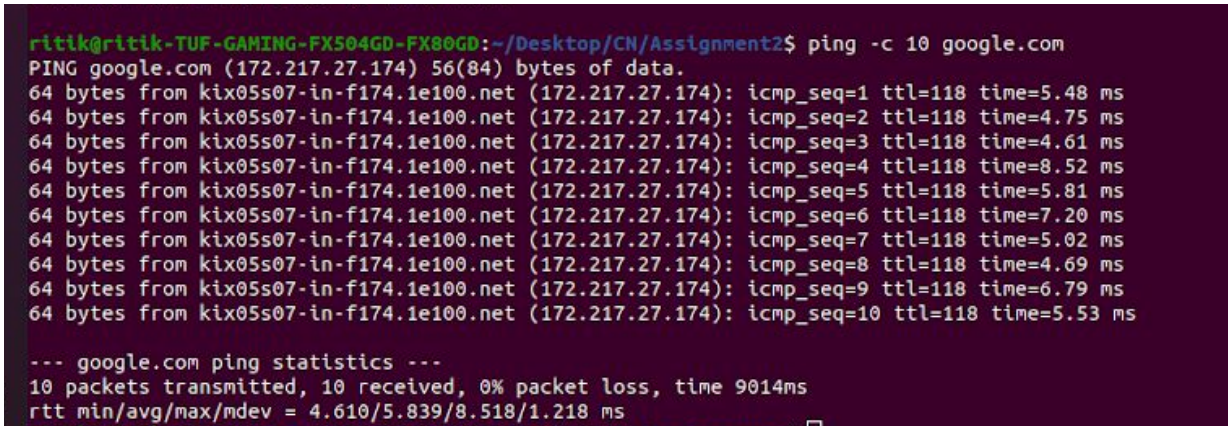


(b) Here my IP address is : **103.212.145.47**. No they are not the same. The IP address shown on WhatsmyIp is the public IP address (external IP). As we are behind the router, it's ip address is checked by the website.



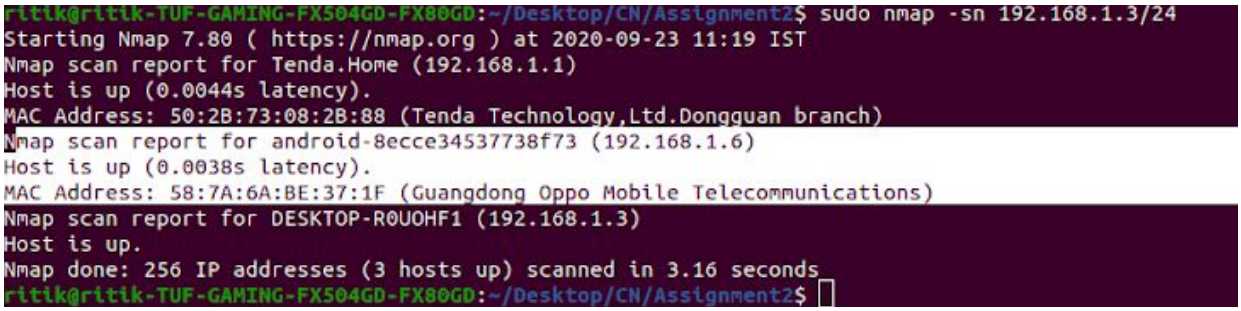
Q2.

(a) Command: **ping -c 10 google.com**



Here the column: ‘time=5.48 ms’ show the latency. For network latency we can see the **min/avg/max/mdev = 4.610/5.839/8.518/1.218**.

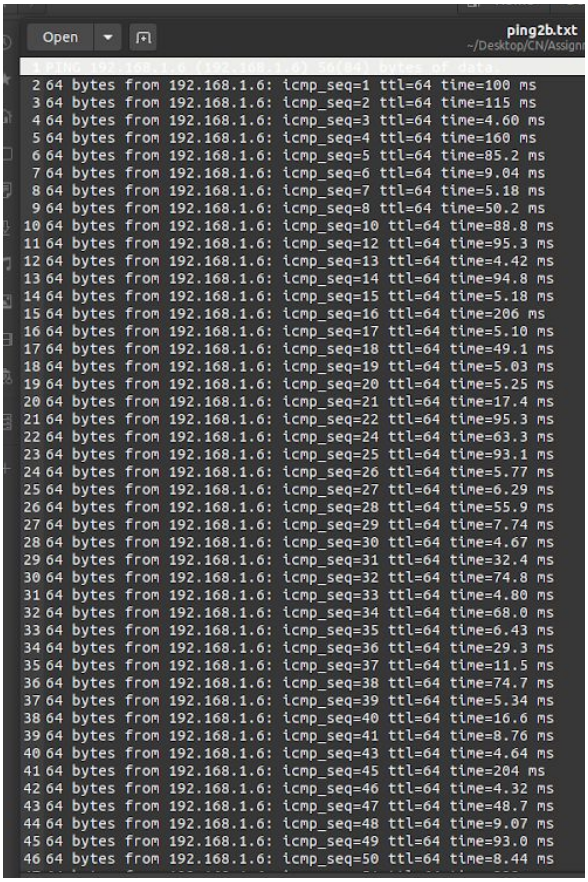
(b) To connect to the different machines on the same network, I will need my IP address and will use broadcasting to get all the devices on the same network.
Command: **sudo nmap -sn 192.168.1.3/24**



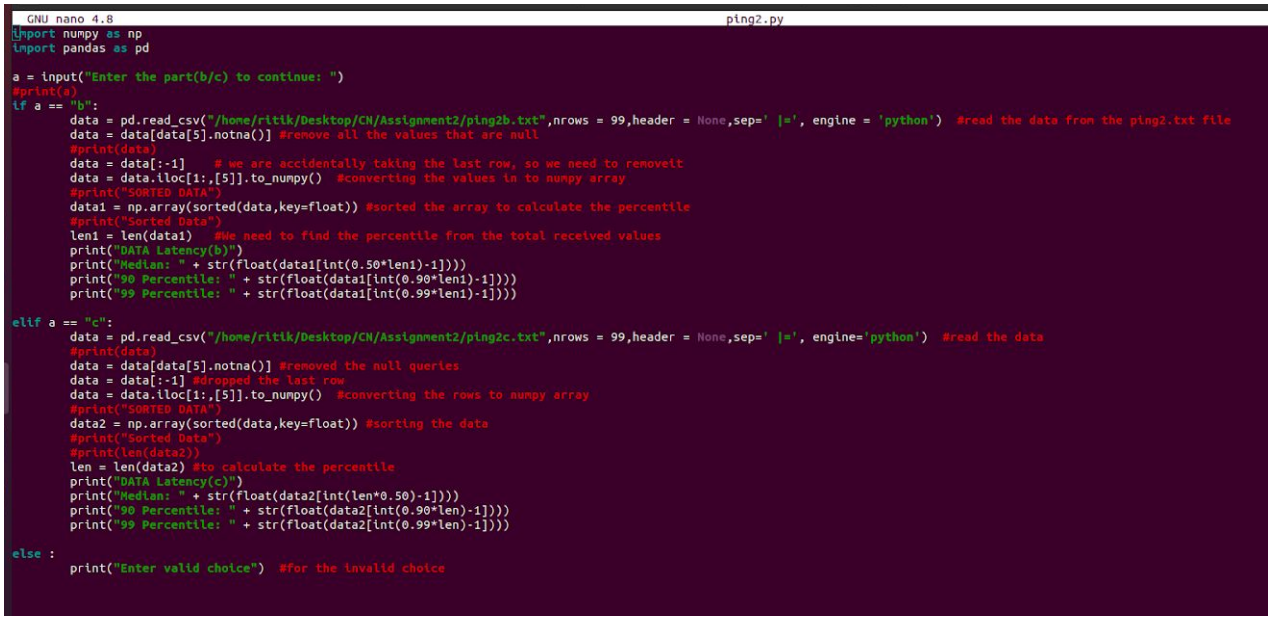
(For configuring the Firewall and to get the IP address of the device: In the WiFi setting options, select the same network and then go to the ip settings and make it static from DHCP to make it visible). Here I got the ip address of my phone and now I will ping that using **ping -c 100 192.168.1.6** and then redirect the output to the another file **ping2b.txt** and then used the python file to sort the ping time value and we can get the median, 90th percentile and 99th percentile (Please find attached the python file).

Command: **ping -c 100 192.168.1.6 > ping2b.txt && python3 ping2.py**

Ping2b.txt:



Ping2.py:



(c). Pinging amazon.com 100 times.

Command: **ping -c 100 amazon.com > ping2c.txt && python3 ping2.py**

```
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop/CN/Assignment2$ ping -c 100 amazon.com > ping2c.txt && python3 ping2.py
Enter the part(b/c) to continue: c
DATA Latency(c)
Median: 413.0
90 Percentile: 525.0
99 Percentile: 644.0
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop/CN/Assignment2$
```

Ping2c.txt:

Open ping2c.txt ~/Desktop/CN/Assignment2

```
1 PING amazon.com (176.32.103.205) 56(84) bytes of data.
2 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=1 ttl=232 time=389 ms
3 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=2 ttl=232 time=413 ms
4 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=3 ttl=232 time=437 ms
5 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=4 ttl=232 time=359 ms
6 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=5 ttl=232 time=382 ms
7 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=6 ttl=232 time=410 ms
8 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=7 ttl=232 time=533 ms
9 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=9 ttl=232 time=357 ms
10 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=10 ttl=232 time=383 ms
11 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=11 ttl=232 time=508 ms
12 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=12 ttl=232 time=532 ms
13 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=13 ttl=232 time=351 ms
14 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=14 ttl=232 time=375 ms
15 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=15 ttl=232 time=404 ms
16 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=16 ttl=232 time=341 ms
17 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=17 ttl=232 time=449 ms
18 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=18 ttl=232 time=371 ms
19 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=19 ttl=232 time=501 ms
20 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=20 ttl=232 time=518 ms
21 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=21 ttl=232 time=440 ms
22 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=22 ttl=232 time=361 ms
23 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=23 ttl=232 time=591 ms
24 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=24 ttl=232 time=518 ms
25 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=25 ttl=232 time=434 ms
26 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=26 ttl=232 time=354 ms
27 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=27 ttl=232 time=596 ms
28 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=28 ttl=232 time=505 ms
29 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=29 ttl=232 time=426 ms
30 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=30 ttl=232 time=562 ms
31 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=31 ttl=232 time=473 ms
32 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=32 ttl=232 time=669 ms
33 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=33 ttl=232 time=420 ms
34 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=34 ttl=232 time=445 ms
35 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=35 ttl=232 time=363 ms
36 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=36 ttl=232 time=390 ms
37 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=37 ttl=232 time=425 ms
38 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=38 ttl=232 time=435 ms
39 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=39 ttl=232 time=356 ms
40 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=40 ttl=232 time=482 ms
41 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=41 ttl=232 time=404 ms
42 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=42 ttl=232 time=530 ms
43 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=43 ttl=232 time=455 ms
44 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=44 ttl=232 time=376 ms
45 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=45 ttl=232 time=501 ms
46 64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=46 ttl=232 time=424 ms
```

(d). Packets dropped:

In (b): 1 packet dropped out of 100.

```
102 --- 192.168.1.6 ping statistics ---
103 100 packets transmitted, 99 received, 1% packet loss, time 99148ms
104 rtt min/avg/max/mdev = 2.814/63.053/213.357/54.294 ms
```

In (c): 1 packet dropped out of 100

```
102 --- amazon.com ping statistics ---
103 100 packets transmitted, 99 received, 1% packet loss, time 99117ms
104 rtt min/avg/max/mdev = 239.520/247.684/321.078/14.275 ms
```

They both have the same packet drop count but latency for amazon.com is higher than for the mobile device because the number of routers in between to reach

amazon.com is more than to reach the mobile device, that's why (c) has more latency than (b).

Q3.

(a). Command: **ping -c 10 -M do -s 2000 google.com**

```
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop/CN/Assignment2$ ping -c 10 -M do -s 2000 google.com
PING google.com(bom07s16-in-x0e.1e100.net (2404:6800:4009:80b::200e)) 2000 data bytes
ping: local error: message too long, mtu: 1500
ping: local error: message too long, mtu: 1500
ping: local error: message too long, mtu: 1500
ping: local error: message too long, mtu: 1500
ping: local error: message too long, mtu: 1500
ping: local error: message too long, mtu: 1500
ping: local error: message too long, mtu: 1500
ping: local error: message too long, mtu: 1500
ping: local error: message too long, mtu: 1500
ping: local error: message too long, mtu: 1500

--- google.com ping statistics ---
10 packets transmitted, 0 received, +10 errors, 100% packet loss, time 9212ms
```

We can see all the 10 packets were dropped as we stopped the fragmentation by **-M do** and changed the size to 2000 by **-s,** due to this they dropped as the maximum mtu is 1500. So, the packet with mtu > 1500 will be dropped. After that the packet should be fragmented to smaller chunks.

(b). Command: **sudo netstat -atp**

```
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop/CN/Assignment2$ sudo netstat -atp
[sudo] password for ritik:
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      815/systemd-resolve
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      827/cupsd
tcp        0      0 DESKTOP-R0UOHF1:56752   del03s17-in-f3.1e:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:42856   del03s10-in-f10.1:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:38006   del11s05-in-f14.1:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:57730   del11s07-in-f10.1:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:56256   del03s18-in-f14.1:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:48482   74.125.24.189:https     ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:51116   del03s15-in-f10.1:https ESTABLISHED 3006/firefox
tcp        0      1 DESKTOP-R0UOHF1:52748   5.85.222.35.bc.goo:http SYN_SENT    830/NetworkManager
tcp        0      0 DESKTOP-R0UOHF1:33812   del11s04-in-f10.1:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:54636   ec2-52-35-220-92.:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:34860   ec2-52-2-201-228.:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:48826   del03s14-in-f1.1e:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:57728   del11s07-in-f10.1:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:46750   del03s09-in-f14.1:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:60146   del03s16-in-f2.1e:https TIME_WAIT   -
tcp        0      0 DESKTOP-R0UOHF1:34666   del11s03-in-f13.1:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:42858   del03s10-in-f10.1:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:56278   del03s17-in-f14.1:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:37998   del11s05-in-f14.1:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:46980   sa-in-f189.1e100.:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:33810   del11s04-in-f10.1:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:34594   whatsapp-cdn-shv-:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:38064   del03s17-in-f4.1e:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:42886   del03s09-in-f3.1e:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:60668   del11s04-in-f14.1:https ESTABLISHED 3006/firefox
tcp        0      0 DESKTOP-R0UOHF1:42864   del03s10-in-f10.1:https ESTABLISHED 3006/firefox
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN      827/cupsd
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop/CN/Assignment2$
```

Q4.

(a). To get an authoritative answer for a website, we first need to check for **ns/soa** as it returns one or more authoritative name server records for the domain.

Command: **nslookup -type=ns google.com**

```
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop/CN/Assignment2$ nslookup -type=ns google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns1.google.com.

Authoritative answers can be found from:
```

Now, to get authoritative answers, run **nslookup google.com ns1.google.com**
It will check for the authoritative answer from **ns1.google.com**.

```
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop/CN/Assignment2$ nslookup google.com ns1.google.com
Server:         ns1.google.com
Address:        2001:4860:4802:32::a#53

Name:   google.com
Address: 216.58.200.206
Name:   google.com
Address: 2404:6800:4002:812::200e
```

(b). To get the time to live for the website on the local dns.

Command: **dig google.com**

Here the time 179 (units) is the time. Now we want to get unit

For that I used **+ttlunits** get the time in human readable format (Here the ‘s’ is for seconds).

Command: **dig google.com && dig +ttlunits google.com**

```
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop/CN/Assignment2$ dig google.com && dig +ttlunits google.com

; <<>> DiG 9.16.1-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18974
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             179     IN      A       142.250.67.238

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Wed Sep 23 18:35:10 IST 2020
;; MSG SIZE  rcvd: 55


; <<>> DiG 9.16.1-Ubuntu <<>> +ttlunits google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57575
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             2m59s   IN      A       142.250.67.238

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Wed Sep 23 18:35:10 IST 2020
;; MSG SIZE  rcvd: 55
```

On comparing the time, it came out to be in seconds i.e. **179secs ≡ 2m59secs**
So, it will change after 179sec.

Q5. Command: **traceroute -z 12345 -q 5 -f 4 -m 7 google.com**

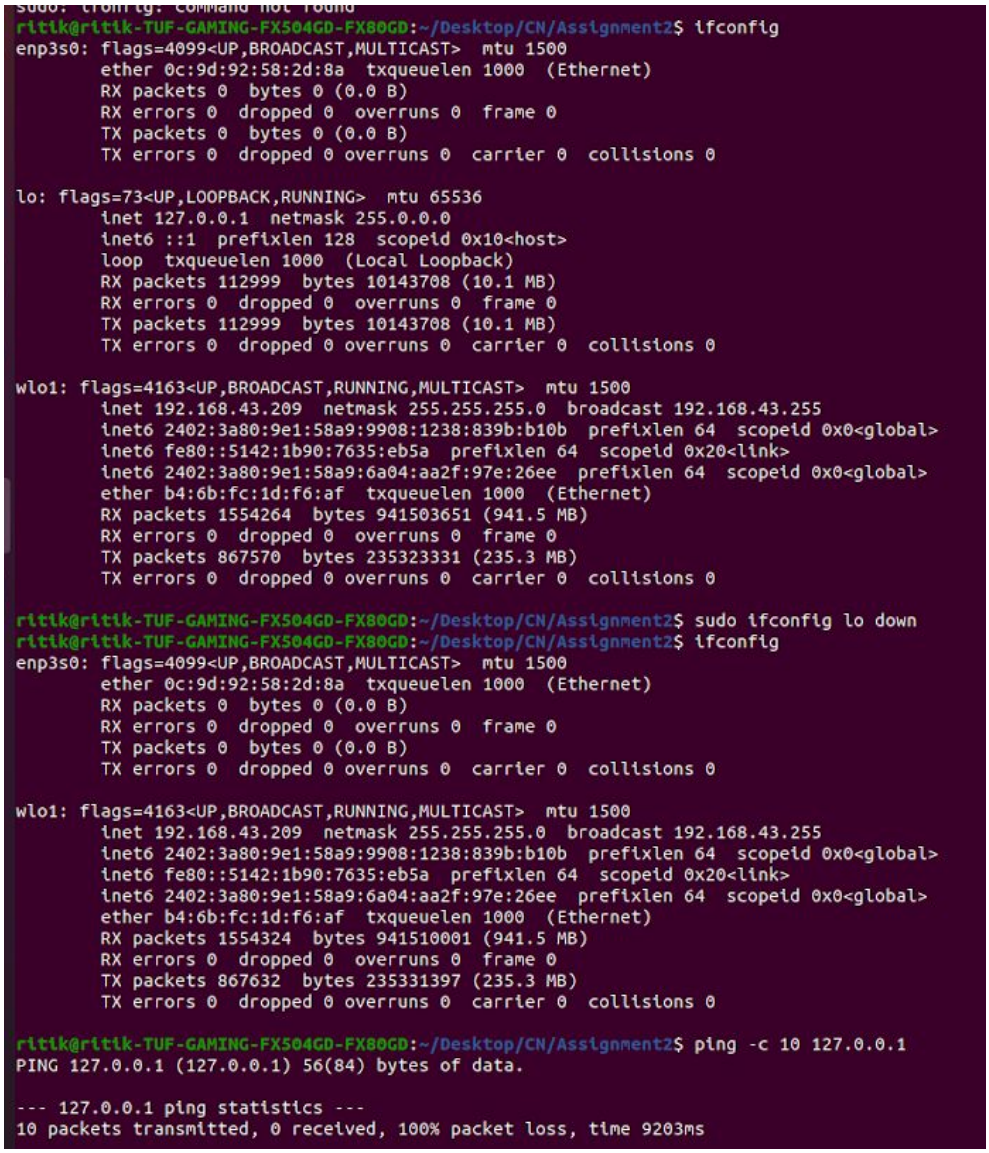
- **-z 12345:** wait for 12345 milliseconds
- **-q 5:** sends 5 probes for each hop sent
- **-f 4 -m 7:** displays the 4th to 7th hop

```
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop/CN/Assignment2$ traceroute -z 12345 -q 5  google.com
traceroute to google.com (172.217.27.174), 30 hops max, 60 byte packets
 1  Tenda.Home (192.168.1.1)  2.890 ms  3.928 ms  4.063 ms  3.947 ms  5.983 ms
 2  103.212.145.1 (103.212.145.1)  6.474 ms  6.693 ms  6.223 ms  7.943 ms  11.048 ms
 3  * * * * *
 4  103.56.231.1 (103.56.231.1)  10.244 ms *  8.936 ms *  7.816 ms
 5  209.85.172.217 (209.85.172.217)  6.648 ms  25.880 ms  6.805 ms  6.425 ms  21.820 ms
 6  74.125.243.97 (74.125.243.97)  8.772 ms  9.915 ms 74.125.244.193 (74.125.244.193)  7.515 ms 74.125.243.97 (74.125.243.97)  6.750 ms  7.634 ms
 7  172.253.67.97 (172.253.67.97)  8.605 ms  9.284 ms 172.253.67.95 (172.253.67.95)  10.246 ms 172.253.67.97 (172.253.67.97)  8.442 ms  7.840 ms
 8  kix05s07-in-f14.1e100.net (172.217.27.174)  8.897 ms  10.191 ms  7.086 ms  5.132 ms  8.439 ms
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop/CN/Assignment2$ traceroute -z 12345 -q 5 -f 4 -m 4 google.com
traceroute to google.com (172.217.27.174), 4 hops max, 60 byte packets
 4  * 103.56.231.1 (103.56.231.1)  9.686 ms *  14.251 ms *
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop/CN/Assignment2$ traceroute -z 12345 -q 5 -f 4 -m 7 google.com
traceroute to google.com (172.217.27.174), 7 hops max, 60 byte packets
 4  103.56.231.1 (103.56.231.1)  24.319 ms *  9.837 ms *  10.243 ms
 5  209.85.172.217 (209.85.172.217)  6.484 ms  9.433 ms  15.122 ms  13.088 ms  6.025 ms
 6  74.125.243.97 (74.125.243.97)  8.912 ms 74.125.244.193 (74.125.244.193)  7.540 ms  6.597 ms 74.125.243.97 (74.125.243.97)  8.131 ms 74.125.244.193 (74.125.244.193)  6.
 7  172.253.67.95 (172.253.67.95)  7.202 ms  6.961 ms 172.253.67.97 (172.253.67.97)  7.899 ms  9.230 ms 172.253.67.95 (172.253.67.95)  11.497 ms
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop/CN/Assignment2$ man traceroute
```

Q6. First we will make the loopback ifconfig down to make in STALE mode (no ping can be done to the device).

For this: **sudo ifconfig lo down**

This command will set the device in stale mode and the device can't ping to itself.



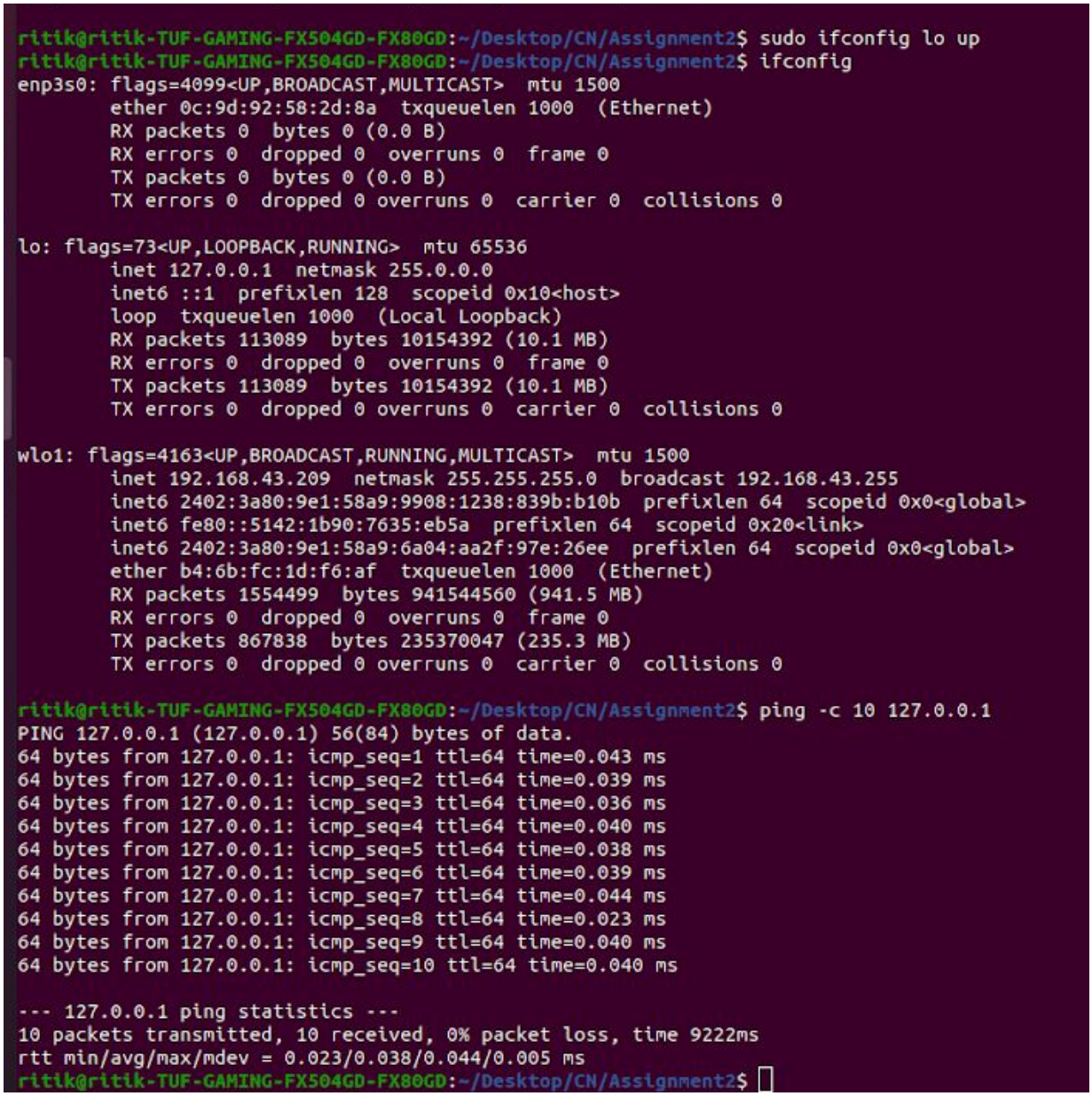
.

We can see first the loopback was on, then we made it down. Now if we try to ping it **Ping -c 10 127.0.0.1**, we can see all the packets lost.

Then, I made the loopback interface up, using **sudo ifconfig lo up.**

Now, If i again ping the device back using **ping -c 10 127.0.0.1**

We can see all the packets were received.



Q7. Command: **dig google.com** to get the ip address
The ip address was: **142.250.67.238**

```
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop/CN/Assignment2$ dig  google.com

; <<>> DiG 9.16.1-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40585
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             281     IN      A       142.250.67.238

;; Query time: 43 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Wed Sep 23 17:47:17 IST 2020
;; MSG SIZE  rcvd: 55
```

Now if we do reverse domain lookup
Command: **dig -x 142.250.67.238**

```
itik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop/CN/Assignment2$ dig  -x 142.250.67.238

 <<>> DiG 9.16.1-Ubuntu <<>> -x 142.250.67.238
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24856
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
 EDNS: version: 0, flags:; udp: 65494
; QUESTION SECTION:
238.67.250.142.in-addr.arpa.   IN      PTR

; ANSWER SECTION:
38.67.250.142.in-addr.arpa. 84046 IN   PTR     bom07s24-in-f14.1e100.net.

; Query time: 3 msec
; SERVER: 127.0.0.53#53(127.0.0.53)
; WHEN: Wed Sep 23 17:48:00 IST 2020
; MSG SIZE  rcvd: 95
```

Now if we search for the IP address 8.8.8.8, Command: **dig -x 8.8.8.8**

```
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop/CN/Assignment2$ dig  -x 8.8.8.8

; <<>> DiG 9.16.1-Ubuntu <<>> -x 8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33541
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;8.8.8.8.in-addr.arpa.          IN      PTR

;; ANSWER SECTION:
8.8.8.8.in-addr.arpa.   83937   IN      PTR     dns.google.

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Wed Sep 23 17:48:28 IST 2020
;; MSG SIZE  rcvd: 73
```

We can see that Ip address that we got on reverse dns lookup, is also from google.

Technical details

IP address	**142.250.67.238**
Hostname	bom07s24-in-f14.1e100.net
Type	Public
CIDR	142.250.67.238/24

Location of IP address 142.250.67.238

Lookup information about the location associated with the IP address 142.250.67.238.

City	not provided
Country	United States (US) *(99% confidence)*
Continent	North America (NA)
Time zone	America/Chicago

ASN and ISP for IP address 142.250.67.238

General traits like organisation, autonomous system number (ASN) and ISP associated with the IP address 142.250.67.238.

ISP	Google
Organization	Google
User type	business
Autonomous system number (ASN)	15169
Autonomous system organization	GOOGLE
Anonymous proxy?	No
Satellite provider?	No

Registered and represented country

Details about the country in which the ISP has registered the IP address 142.250.67.238. Furthermore, if available, the represented country. For instance, the country represented by an overseas military base or embassy.

Registered country	United States (US)
Represented country	Not Provided

Location on the map for IP address 142.250.67.238