

LAB 1: Basic Networking Tools

Team Members:

1. Name : Abhinav Reddy Gutha
Roll No. : 2103102

2. Name : Nidamanuri Sai Adarsh
Roll No. : 2103123

PART 1: IP and MAC Addresses, and Routing Tables

1. Read up about the ip command in Linux, in particular the “ip addr show” command. You should have a rough understanding of what this command does, what are its options, and how to interpret its output.

a) List the loopback IP address

A)

```
abhinav@ABHINAV:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: bond0: <BROADCAST,MULTICAST,MASTER> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 1e:b5:d1:a0:91:89 brd ff:ff:ff:ff:ff:ff
3: dummy0: <BROADCAST,NOARP> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether ea:5b:2a:df:c4:ba brd ff:ff:ff:ff:ff:ff
4: tunl0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/ipip 0.0.0.0 brd 0.0.0.0
5: sit0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/sit 0.0.0.0 brd 0.0.0.0
6: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:c6:24:1d brd ff:ff:ff:ff:ff:ff
    inet 172.19.94.29/20 brd 172.19.95.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fec6:241d/64 scope link
        valid_lft forever preferred_lft forever
abhinav@ABHINAV:~$
```

Here the loopback IP address is 127.0.0.1/ 8 which can be found on inet in lo interface name.

b) List the IP address used by your computer for connecting to the internet, and state its type (IPv6 or IPv4). Also state what type of interface it belongs to (WiFi/Ethernet etc)

A) 172.19.94.29/20 is the IP address used by my computer for connecting to the internet and it is of IPv4 type. As you can see the eth0 interface name in 6th line of the output of the command, it belongs to the ethernet interface.


c) Find out how many network interfaces your computer has. For each network interface, list down the following information:

- 1. It's type (Ethernet/Wifi/Bluetooth ...)**
- 2. It's MAC address**
- 3. Manufacturer of this NIC (Network Interface Card) (this information can be inferred from the MAC address)**
- 4. IPv4 address or IPv6 address**

A) Here there are two network interfaces in my computer i.e, eth0 and lo. For eth0,

1. It is the ethernet interface.
2. 00:15:5d:c6:24:1d is the MAC address.
3. Microsoft Corporation is the Manufacturer of this NIC based on the DNS checker website.

Result for: **00:15:5D:C6:24:1D**

Address Prefix	00:15:5D
Vendor / Company	Microsoft Corporation
Start Address	00155D000000
End Address	00155DFFFFFF
Company Address	One Microsoft Way Redmond Wa 98052-8300 Us 

4. It is of IPv6 address.

For lo,

1. It is the loopback interface.

2. 00:00:00:00:00:00 is the MAC address.
3. Xerox Corporation is the manufacturer of this NIC based on the DNS website checker.
4. It is of IPv6 address.

2. Your computer may be part of a local network (say a lab-wide or building-wide network within IIT Goa).

a) What is the IP address of this network and what is the range of IP addresses that can belong to individual computers within this network?

A)

```
abhinav@ABHINAV:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.19.94.29 netmask 255.255.240.0 broadcast 172.19.95.255
    inet6 fe80::215:5dff:fec6:241d prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:c6:24:1d txqueuelen 1000 (Ethernet)
    RX packets 124 bytes 217634 (217.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 57 bytes 4166 (4.1 KB)
    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 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

abhinav@ABHINAV:~$
```

The IP address of this network is 172.19.94.29. The range of this IP address that can belong to individual computers within this network is 172.19.80.0 to 172.19.95.255. This is done by keeping the first 20 bits as constant and to obtain the lower limit, we need to assign the remaining bits to 0. To get an upper limit, we need to assign 1 to the remaining bits.

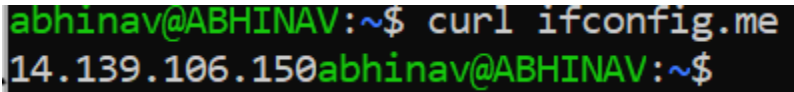
b) What is the max number of hosts that can be uniquely addressed within this local network?

A) Here my netmask is 255.255.240.0. So no. of zeroes are 4 (from 240) + 8 (from 0) = 12. Therefore, the maximum number of hosts that can be uniquely addressed within this local network is $2^{12} = 4096$.

c) What is the IP address for sending broadcast messages to your local network?

A) 172.19.95.255 is the IP address for sending broadcast messages to my local network.

d) What is your publicly-visible IP address (as seen by a server outside of IIT Goa)?

A) The image shows a terminal window with the prompt 'abhinav@ABHINAV:~\$' followed by the command 'curl ifconfig.me'. The output of the command is '14.139.106.150', which is displayed on the same line as the command.

14.139.106.150 is my publicly visible IP address.

3. Just like a router, your computer also maintains a routing table. Each entry in this routing table contains a range of destination IP addresses and the IP address of the “next hop” that should be chosen to forward a packet with the matching destination address. In addition, there is also an entry called “default” which is the route chosen if a destination address does not match any of the other more-specific entries. For a given destination IP address, the entries in the table are searched in the order of the longest prefix to shortest prefix until a match is found. (This is called the “Longest Prefix Match” approach). When a match is found, the computer chooses this entry as the next hop for forwarding the packet. You can view your computer’s routing table using the ip route show command in Linux. Read up about this command to get a rough understanding of what this command does, what are its options, and how to interpret its output.

a) What is your default Gateway’s IP address as shown in the routing table? What is meant by a Gateway?

A)

```
student@user-V530-15ICB: ~
(base) student@user-V530-15ICB:~$ iproute | grep default
Command 'iproute' not found, did you mean:
  command 'ibroute' from deb infiniband-diags (28.0-1ubuntu1)
Try: apt install <deb name>
(base) student@user-V530-15ICB:~$ ip route | grep default
default via 10.250.9.250 dev enp1s0 proto static metric 100
default via 10.196.2.250 dev wlp2s0 proto dhcp metric 20600
(base) student@user-V530-15ICB:~$
```

10.250.9.250 and 10.196.2.250 are my default gateway's IP addresses.
Unlike Router, Gateway is a hardware which acts as a gate of connecting two networks together.

**b) Re-write the first 3 entries of your routing table here in the format:
<destination IP-address/prefix-length>, <next hop's IP address where this
packet should be forwarded>.**

A) <10.196.0.0/20>, <10.250.9.0/24>


```

unix 3 [ ] STREAM CONNECTED 40241 @/tmp/.X11-unix/X0
unix 3 [ ] STREAM CONNECTED 55752 @/tmp/dbus-rETJFR9G6j
unix 3 [ ] STREAM CONNECTED 37480
unix 3 [ ] STREAM CONNECTED 43862
unix 3 [ ] STREAM CONNECTED 45524
unix 3 [ ] STREAM CONNECTED 44534 /run/systemd/journal/std
unix 3 [ ] STREAM CONNECTED 33606
unix 3 [ ] STREAM CONNECTED 41074
unix 3 [ ] STREAM CONNECTED 40979
unix 3 [ ] STREAM CONNECTED 34451 /run/dbus/system_bus_sock
(base) student@user-V530-15ICB:~$ netstat -r
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
default _gateway 0.0.0.0 UG 0 0 0 enp1s0
default _gateway 0.0.0.0 UG 0 0 0 wlp2s0
10.196.0.0 0.0.0.0 255.255.240.0 U 0 0 0 wlp2s0
10.250.9.0 0.0.0.0 255.255.255.0 U 0 0 0 enp1s0
link-local 0.0.0.0 255.255.0.0 U 0 0 0 enp1s0
(base) student@user-V530-15ICB:~$ netstat -r
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
default _gateway 0.0.0.0 UG 0 0 0 enp1s0
default _gateway 0.0.0.0 UG 0 0 0 wlp2s0
10.196.0.0 0.0.0.0 255.255.240.0 U 0 0 0 wlp2s0
10.250.9.0 0.0.0.0 255.255.255.0 U 0 0 0 enp1s0
link-local 0.0.0.0 255.255.0.0 U 0 0 0 enp1s0
(base) student@user-V530-15ICB:~$ ^C
(base) student@user-V530-15ICB:~$

```

c) Sometimes, the next hop's IP address may be shown as 0.0.0.0. Find out what this means (using web search).

A) The next hop's IP address 0.0.0.0 means that the packet is sent to the directly connected host. This is a default destination address. When a local routing table does not have a specific route to send data packets, then it will be sent to the default gateway i.e, local router.

d) You might notice an address that looks like 169.254.x.x. What are such addresses called and what do they indicate?

A) Addresses like 169.254.x.x are called APIPA (Automatic Private IP Addressing) addresses. This plays a crucial role when the DHCP fails to provide a valid IP address. This device can itself create an APIPA IP address like for example 169.254.0.0/20 which is used for communication

across local area networks. Automatic Private IP Addressing) addresses. This plays a crucial role when the DHCP fails to provide a valid IP address. This device can itself create an APIPA IP address like for example 169.254.0.0/20 which is used for communication across local area networks.

PART 2: PING and TRACEROUTE

4. Explore the 'Ping' command, and report the approximate round-trip time for a ping to :

a) www.iitgoa.ac.in

b) www.iceland.is

A) The ping command sends a packet to the destination url to find out the approximate round-trip time.

The syntax of the ping command is: ping <url>

a) The average round-trip time for www.iitgoa.ac.in is:
2.5ms.

b) The average round-trip time for the url www.iceland.is is:
195ms

The image of the execution of the ping command is:

```
adarsh@DESKTOP-PHE98EL:~$ sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-ABknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-ABknS] [-g group] [-h host] [-p prompt] [-u user] [-u user] [command]
usage: sudo [-ABknPS] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host] [-p prompt] [-R directory] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-ABknS] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host] [-p prompt] [-R directory] [-T timeout] [-u user] file ...

adarsh@DESKTOP-PHE98EL:~$ ping www.iitgoa.ac.in
PING www.iitgoa.ac.in (10.250.200.7) 56(84) bytes of data:
64 bytes from bighome.iitgoa.ac.in (10.250.200.7): icmp_seq=1 ttl=62 time=1.87 ms
64 bytes from bighome.iitgoa.ac.in (10.250.200.7): icmp_seq=2 ttl=62 time=2.44 ms
64 bytes from bighome.iitgoa.ac.in (10.250.200.7): icmp_seq=3 ttl=62 time=4.59 ms
64 bytes from bighome.iitgoa.ac.in (10.250.200.7): icmp_seq=4 ttl=62 time=2.71 ms
64 bytes from bighome.iitgoa.ac.in (10.250.200.7): icmp_seq=5 ttl=62 time=2.72 ms
64 bytes from bighome.iitgoa.ac.in (10.250.200.7): icmp_seq=6 ttl=62 time=3.03 ms
64 bytes from bighome.iitgoa.ac.in (10.250.200.7): icmp_seq=7 ttl=62 time=2.67 ms
64 bytes from bighome.iitgoa.ac.in (10.250.200.7): icmp_seq=8 ttl=62 time=2.45 ms
64 bytes from bighome.iitgoa.ac.in (10.250.200.7): icmp_seq=9 ttl=62 time=2.70 ms
64 bytes from bighome.iitgoa.ac.in (10.250.200.7): icmp_seq=10 ttl=62 time=2.17 ms
64 bytes from bighome.iitgoa.ac.in (10.250.200.7): icmp_seq=11 ttl=62 time=2.58 ms
64 bytes from bighome.iitgoa.ac.in (10.250.200.7): icmp_seq=12 ttl=62 time=2.49 ms
64 bytes from bighome.iitgoa.ac.in (10.250.200.7): icmp_seq=13 ttl=62 time=2.54 ms
64 bytes from bighome.iitgoa.ac.in (10.250.200.7): icmp_seq=14 ttl=62 time=4.01 ms
^C
[1]+  Stopped                  ping www.iitgoa.ac.in
adarsh@DESKTOP-PHE98EL:~$ ping www.iceland.is
ping: www.: Name or service not known
adarsh@DESKTOP-PHE98EL:~$ ping www.iceland.is
PING www.iceland.is (45.76.142.217) 56(84) bytes of data:
64 bytes from 45.76.142.217.vultrusercontent.com (45.76.142.217): icmp_seq=1 ttl=45 time=197 ms
64 bytes from 45.76.142.217.vultrusercontent.com (45.76.142.217): icmp_seq=2 ttl=45 time=193 ms
64 bytes from 45.76.142.217.vultrusercontent.com (45.76.142.217): icmp_seq=3 ttl=45 time=193 ms
64 bytes from 45.76.142.217.vultrusercontent.com (45.76.142.217): icmp_seq=4 ttl=45 time=195 ms
64 bytes from 45.76.142.217.vultrusercontent.com (45.76.142.217): icmp_seq=5 ttl=45 time=213 ms
64 bytes from 45.76.142.217.vultrusercontent.com (45.76.142.217): icmp_seq=6 ttl=45 time=195 ms
64 bytes from 45.76.142.217.vultrusercontent.com (45.76.142.217): icmp_seq=7 ttl=45 time=196 ms
64 bytes from 45.76.142.217.vultrusercontent.com (45.76.142.217): icmp_seq=8 ttl=45 time=224 ms
64 bytes from 45.76.142.217.vultrusercontent.com (45.76.142.217): icmp_seq=9 ttl=45 time=196 ms
64 bytes from 45.76.142.217.vultrusercontent.com (45.76.142.217): icmp_seq=10 ttl=45 time=195 ms
64 bytes from 45.76.142.217.vultrusercontent.com (45.76.142.217): icmp_seq=11 ttl=45 time=195 ms
64 bytes from 45.76.142.217.vultrusercontent.com (45.76.142.217): icmp_seq=12 ttl=45 time=203 ms
64 bytes from 45.76.142.217.vultrusercontent.com (45.76.142.217): icmp_seq=13 ttl=45 time=219 ms
64 bytes from 45.76.142.217.vultrusercontent.com (45.76.142.217): icmp_seq=14 ttl=45 time=193 ms
^C
[2]+  Stopped                  ping www.iceland.is
adarsh@DESKTOP-PHE98EL:~$
```

5. Read up about the traceroute command. You can view its manual by typing `man traceroute` in the Linux terminal. Get a broad idea of what this command does, how it works and how to interpret its output. (Note the “-m” option in traceroute, which you may need to tweak in order to get proper results. Also note the difference between `traceroute -l`, `traceroute -T` and `traceroute -U`). Briefly explain (in 4-5 sentences) how traceroute works, by utilizing the TTL field in the Network-layer header.

A) The mechanisms behind the working of traceroute is quite interesting. First it would send a data packet with the TTL (Time to Live) value of 1. This will send the packet to the nearest router and after that the packet perishes. It is because as the TTL value is equal to 1, this means that after reaching one router, the TTL value decreases by 1 unit. Now the value of TTL will be 0. This would kill up the data packet. This will get notified to the user. After that, we will send another packet but now with TTL value of 2. This process continues until the data packet reaches the destination address. Now, we will get a much detailed map of how a packet would flow to the destination address from the user.

6. Consider the website <https://alaska.gov/>. We wish to check if the web server for this site is indeed located physically in Alaska, and trace the route that our packets take to reach this web server.

- a) Find out the IP address of this webserver.
- b) Use the traceroute command to trace the path followed by packets flowing from your computer to this web server. How many total hops were taken to reach the destination ?
- c) Some hops may not be shown (appearing as * * * in the output of the traceroute command. What do these lines mean?
- d) Traceroute does 3 trials (sends 3 messages) to each hop by default. What is the command to get traceroute to do 5 trials instead?
- e) What is the average round-trip delay (in mili-seconds) for reaching the final destination?
- f) Use online services such as “ipinfo.io” to find and list the geographical location (City, State, Country) where the last hop is located.

A) Given website to apply traceroute is : <https://alaska.gov.in/>

Now we have to trace the route for the packet to the server of <https://alaska.gov.in/>, we do this by using the command traceroute.

The general syntax for the traceroute command is: traceroute <ip address>.

- a) Now firstly to find the ip address of the url <https://alaska.gov.in/> we will use the dig command, [dig alaska.gov.in] Now we will get the ip address of the given url, which is: 158.145.65.37.

```
adarsh@DESKTOP-PHE98EL:~$ dig alaska.gov

;<<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> alaska.gov
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38474
;; flags: qr rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;alaska.gov.                IN      A

;; ANSWER SECTION:
alaska.gov.                 0       IN      A      158.145.65.37

;; Query time: 349 msec
;; SERVER: 172.17.0.1#53(172.17.0.1) (UDP)
;; WHEN: Wed Jan 18 23:29:34 IST 2023
;; MSG SIZE rcvd: 54
```

- b) Now we will use the traceroute command to trace the path followed by the packets from our computer to the destination web server. The command to perform this operation is [traceroute 158.145.65.37]. Now after getting the responses from the routers using the traceroute we have to find out the total number of hops taken to reach the destination server by the packet.(As we are not getting response from the majority of the routers for the alaska.gov website we are trying this command on www.nasa.gov). The ip address of www.nasa.gov which was used by us for traceroute is 13.227.138.59 by using the dig command.

```
adarsh@DESKTOP-PHE98EL:~$ dig www.nasa.gov

; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> www.nasa.gov
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61610
;; flags: qr rd ad; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.nasa.gov.                IN      A

;; ANSWER SECTION:
www.nasa.gov.                0      IN      CNAME   www.nasawestprime.com.
www.nasawestprime.com.      0      IN      CNAME   d30etcnkn29cv0.cloudfront.net.
d30etcnkn29cv0.cloudfront.net. 0 IN      A       13.227.138.59
d30etcnkn29cv0.cloudfront.net. 0 IN      A       13.227.138.113
d30etcnkn29cv0.cloudfront.net. 0 IN      A       13.227.138.67
d30etcnkn29cv0.cloudfront.net. 0 IN      A       13.227.138.2

;; Query time: 3069 msec
;; SERVER: 172.30.48.1#53(172.30.48.1) (UDP)
;; WHEN: Thu Jan 19 16:04:25 IST 2023
;; MSG SIZE rcvd: 234
```

Now after executing the command traceroute the packet reaches the www.nasa.gov web server after 22 hops.(it takes 22 hops to reach the www.nasa.gov server).

```

adarsh@DESKTOP-PHE98EL:~$ traceroute -m 100 13.227.138.59
traceroute to 13.227.138.59 (13.227.138.59), 100 hops max, 60 byte packets
 1  DESKTOP-PHE98EL.mshome.net (172.30.48.1)  0.265 ms  0.232 ms  0.219 ms
 2  10.196.2.250 (10.196.2.250)  2.796 ms  2.785 ms  2.775 ms
 3  firewall.iitgoa.ac.in (10.250.209.251)  2.719 ms  2.713 ms  2.707 ms
 4  14.139.106.145 (14.139.106.145)  3.222 ms  3.217 ms  3.211 ms
 5  10.155.103.129 (10.155.103.129)  64.391 ms  64.386 ms  64.380 ms
 6  * * *
 7  * 10.255.232.201 (10.255.232.201)  59.005 ms *
 8  10.152.7.38 (10.152.7.38)  59.049 ms 10.152.7.214 (10.152.7.214)  63.495 ms 10.152.7.38 (10.152.7.38)  63.480 ms
 9  10.152.7.214 (10.152.7.214)  67.258 ms  65.863 ms 10.152.7.38 (10.152.7.38)  65.134 ms
10  10.152.7.234 (10.152.7.234)  68.922 ms  65.129 ms 99.82.176.10 (99.82.176.10)  65.211 ms
11  52.95.65.223 (52.95.65.223)  62.861 ms 52.95.65.213 (52.95.65.213)  62.865 ms 52.95.65.211 (52.95.65.211)  65.761 ms
12  52.95.67.59 (52.95.67.59)  65.854 ms * 52.95.65.213 (52.95.65.213)  65.727 ms
13  * 52.95.67.77 (52.95.67.77)  73.650 ms *
14  * * *
15  * * *
16  52.95.66.122 (52.95.66.122)  69.086 ms * 52.95.66.54 (52.95.66.54)  64.526 ms
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * server-13-227-138-59.bom50.r.cloudfront.net (13.227.138.59)  17.087 ms
adarsh@DESKTOP-PHE98EL:~$

```

- c) After executing the traceroute command we will see that in the output there are *** in some of the places. Basically traceroute command works on the principle of TTL(time to live) of the packet which means after completing the no of hops equal to TTL the packet gets destroyed and a response is sent to user that the packet is destroyed then we will get the ip address of the responding server. Nowadays many servers are designed not to respond to users if a packet gets destroyed due to completion of TTL. so whenever the traceroute gets no response in return from the routers it represents this 'no-response' with * * *.
- d) Generally traceroute sends 3 trails to each and every router in the path. But we can modify it using the command [traceroute -q <no of trails> <ip address>]. We can modify it to 5 trails using the command traceroute -q 5 <ip_address>.
- e) The average round trip delay for reaching the destination is 60.39.
- f) Using online services such as ipinfo.io we can find the geolocation of the ip address where the last hop is located.
The geo location of the last hop which is ip address: 13.227.138.59 according to ipinfo.io is : Mumbai, Maharashtra, India.

The image of the details is as follows:

Showing results for 13.227.138.59

Copy API link

Geolocation

Copy JSON

“	hostname	"server-13-227-138-59.bom50.r.cloudfront.net"
“	city	"Mumbai"
“	region	"Maharashtra"
“	country	"IN"
“	loc	"19.0728,72.8826"
“	org	"AS16509 Amazon.com, Inc."
“	postal	"400070"
“	timezone	"Asia/Kolkata"

PART 3: PACKET SNIFFING USING WIRESHARK

7. Find out the IP address of “www.iitgoa.ac.in”. Now start up wireshark selecting “any” Interface. Apply a filter “ip.addr == <the ip address you found for iit goa>” for example, “ip.addr==10.250.36.36”. Now, open a web browser and open IIT Goa’s website. Observe the traffic captured in Wireshark for this filter.

- Look out for the SYN, SYN/ACK, ACK sequence of packets. What protocol is being used at the Transport Layer?
- Examine the first SYN packet. Observe how the packet corresponding to each layer of the TCP/IP stack is wrapped inside the packet of the lower layers. Examine the IP datagram and its header. What are the source and destination IP addresses for this packet? Check if the destination IP address matches that of www.iitgoa.ac.in. List your observations.

c) Examine the transport-layer segment in the first SYN packet. What are the source and the destination port numbers for the first SYN message?

d) Now remove all filters, and take a broad view of all packets flowing through the interface. What kind of packets make up a majority of the traffic to your computer/device?

A)

Wireshark packet capture showing a TLSv1.2 connection. The first SYN packet is at sequence 298. The majority of traffic consists of TLSv1.2 packets.

No.	Time	Source	Destination	Protocol	Length	Info
298	18.882659	10.196.7.187	10.250.200.7	TCP	66	49743 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
299	18.883966	10.196.7.187	10.250.200.7	TCP	66	49744 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
300	18.903396	10.250.200.7	10.196.7.187	TCP	66	443 → 49743 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
301	18.903629	10.196.7.187	10.250.200.7	TCP	54	49743 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
302	18.903763	10.250.200.7	10.196.7.187	TCP	66	443 → 49744 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
303	18.903820	10.196.7.187	10.250.200.7	TCP	54	49744 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
304	18.904051	10.196.7.187	10.250.200.7	TLSv1.2	571	Client Hello
305	18.904286	10.196.7.187	10.250.200.7	TLSv1.2	571	Client Hello
306	18.943591	10.250.200.7	10.196.7.187	TCP	54	443 → 49743 [ACK] Seq=1 Ack=518 Win=30336 Len=0
307	18.945381	10.250.200.7	10.196.7.187	TCP	54	443 → 49744 [ACK] Seq=1 Ack=518 Win=30336 Len=0
308	18.947408	10.250.200.7	10.196.7.187	TLSv1.2	1514	Server Hello
309	18.948978	10.250.200.7	10.196.7.187	TLSv1.2	988	Certificate, Server Key Exchange, Server Hello Done
310	18.949198	10.196.7.187	10.250.200.7	TCP	54	49743 → 443 [ACK] Seq=518 Ack=2395 Win=131328 Len=0
311	18.950527	10.250.200.7	10.196.7.187	TLSv1.2	1514	Server Hello
312	18.950527	10.250.200.7	10.196.7.187	TLSv1.2	988	Certificate, Server Key Exchange, Server Hello Done
313	18.950730	10.196.7.187	10.250.200.7	TCP	54	49744 → 443 [ACK] Seq=518 Ack=2395 Win=131328 Len=0
314	18.952292	10.196.7.187	10.250.200.7	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
315	18.952716	10.196.7.187	10.250.200.7	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
316	18.952889	10.196.7.187	10.250.200.7	TLSv1.2	774	Application Data
317	18.958993	10.250.200.7	10.196.7.187	TCP	54	443 → 49743 [ACK] Seq=2395 Ack=1364 Win=31744 Len=0
318	18.969012	10.250.200.7	10.196.7.187	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
319	18.969012	10.250.200.7	10.196.7.187	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
321	19.009018	10.196.7.187	10.250.200.7	TCP	54	49743 → 443 [ACK] Seq=1364 Ack=2669 Win=131072 Len=0
322	19.009284	10.196.7.187	10.250.200.7	TCP	54	49744 → 443 [ACK] Seq=644 Ack=2669 Win=131072 Len=0
370	20.690159	10.250.200.7	10.196.7.187	TLSv1.2	551	Application Data

Frame 312: 988 bytes on wire (7904 bits), 988 bytes captured (7904 bits) on interface \Device\NPF_{A...}

Ethernet II, Src: ExtremeL_9a:82:da (00:04:96:9a:82:da), Dst: Chongin_ac:79:cf (d4:1b:81:ac:79:cf)

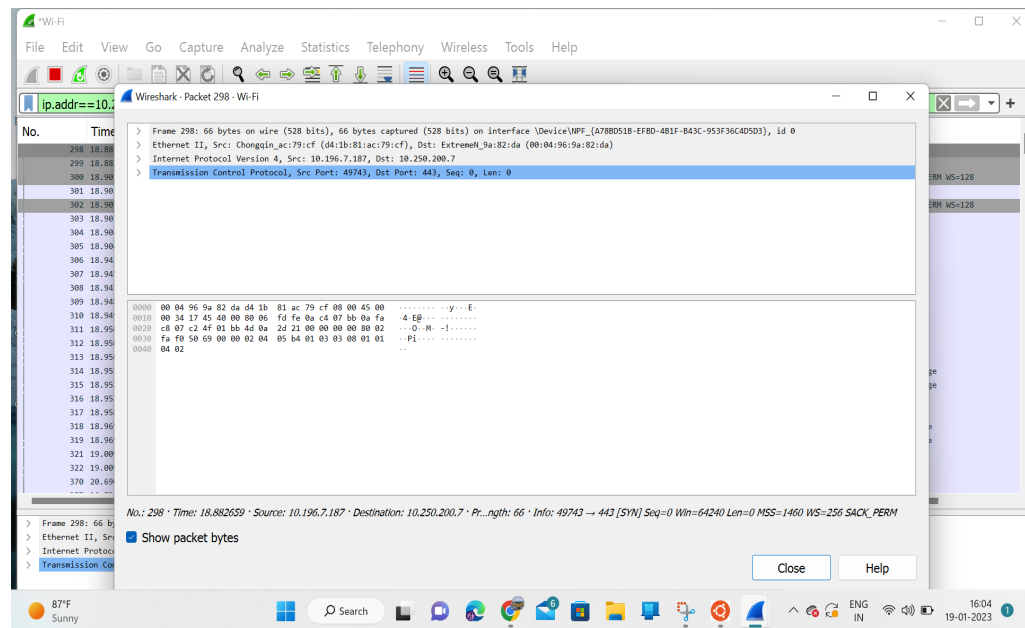
Internet Protocol Version 4, Src: 10.250.200.7, Dst: 10.196.7.187

Transmission Control Protocol, Src Port: 443, Dst Port: 49744, Seq: 1461, Ack: 518, Len: 934

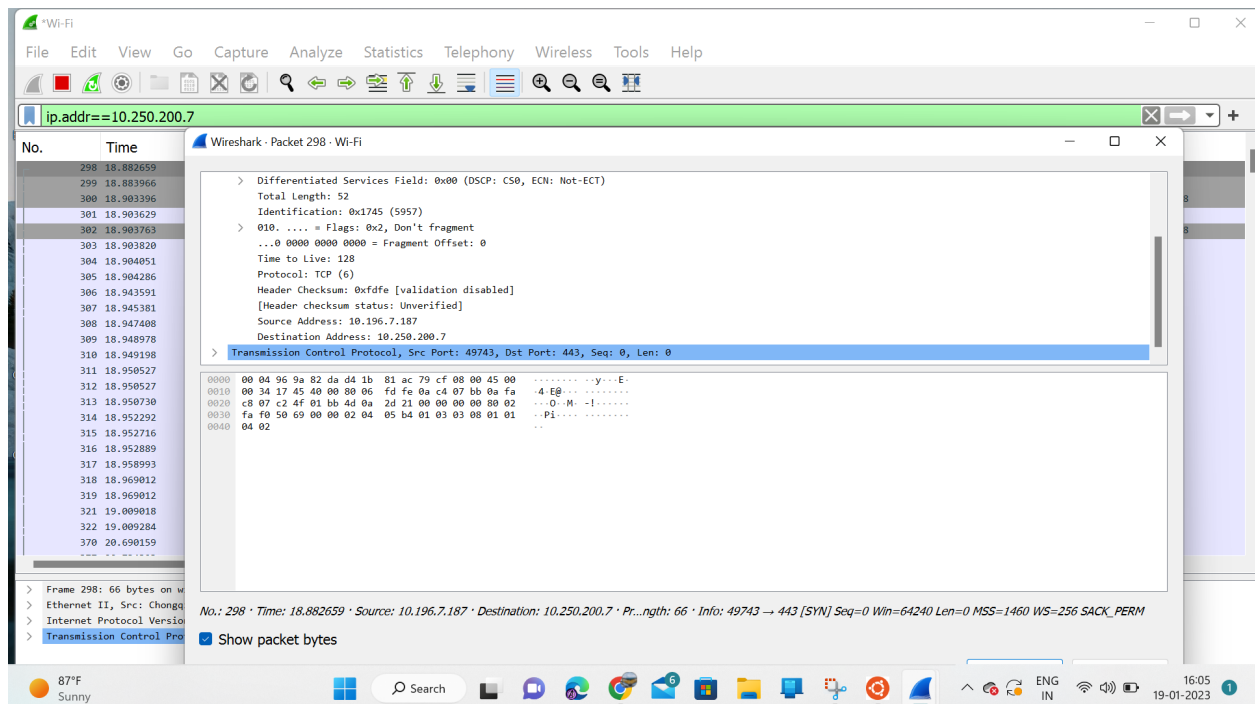
[2 Reassembled TCP Segments (1962 bytes): #311(1375), #312(587)]

TCP protocol is being used at the transport layer for the SYN, SYN/ACK, ACK sequence of packets.

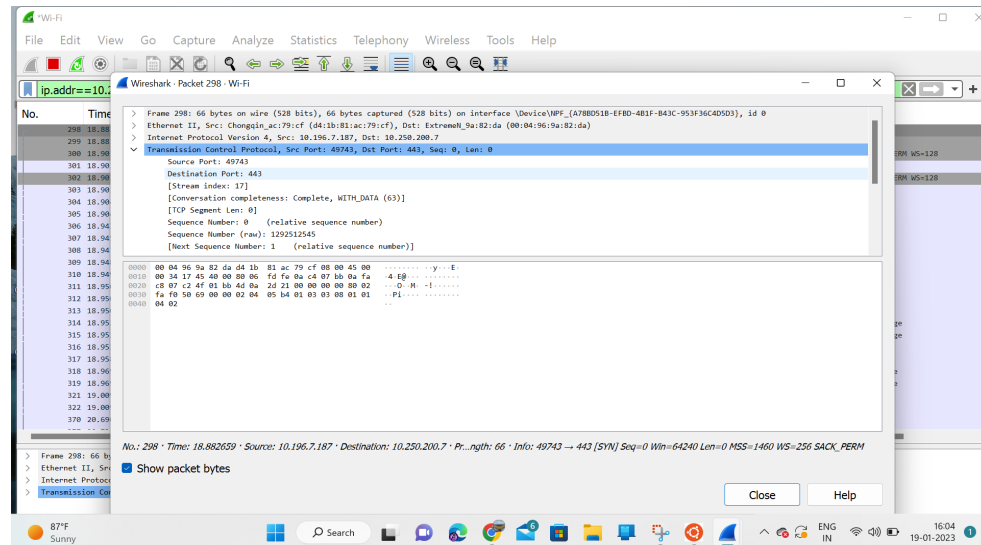
b) At the first syn packet, the layers are piled up as follows. Firstly, we can observe that there is an ethernet layer (Link layer) followed by internet protocol (Network layer) and at last there is transmission control protocol (Transport layer). The image is attached below.



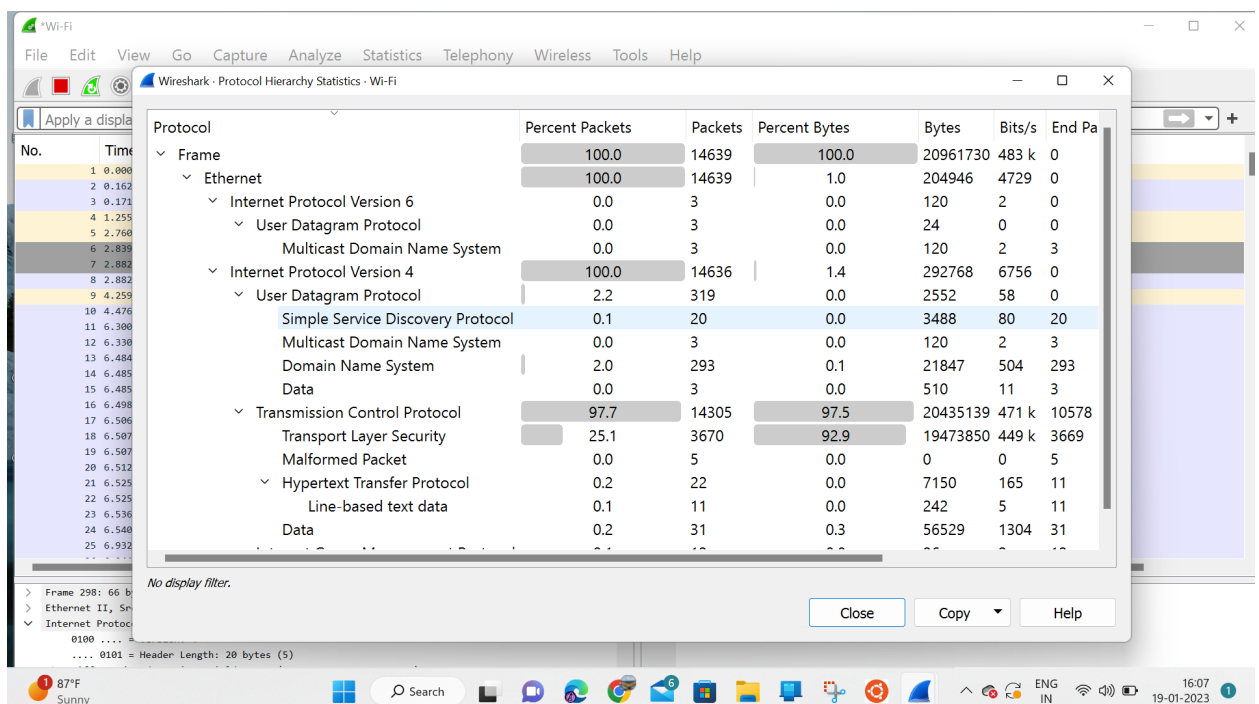
The source IP address is 10.196.7.187 and the destination IP address is 10.250.200.7. You can observe in the image below that the destination address matches with www.iitgoa.ac.in IP address.



c) The source and destination port numbers are 49743 and 443 respectively.



d) In the image below, you can observe that in protocol hierarchy statistics, 97.7 percent of packets follow TCP protocol whereas 2.2 percent follow UDP protocol. Therefore TCP packets take up a majority of the traffic on our computer network.



8. In wireshark, you can apply a filter that displays packets only belonging to a certain protocol (such as TCP or UDP) as follows:

Two or more conditions can be combined using and/or to create more complex filters.

For example:

a) Now, you wish to find out whether YouTube operates over the TCP protocol or the UDP protocol. Open YouTube in Firefox browser and filter out its traffic in Wireshark using the appropriate IP address in the filter. Observe the packets. Does YouTube use TCP or UDP?

b) Does your conclusion change if you open YouTube in Google Chrome, instead of Firefox? List your observations. Check if your conclusion is correct, using a web search about what protocol YouTube actually uses.

A)

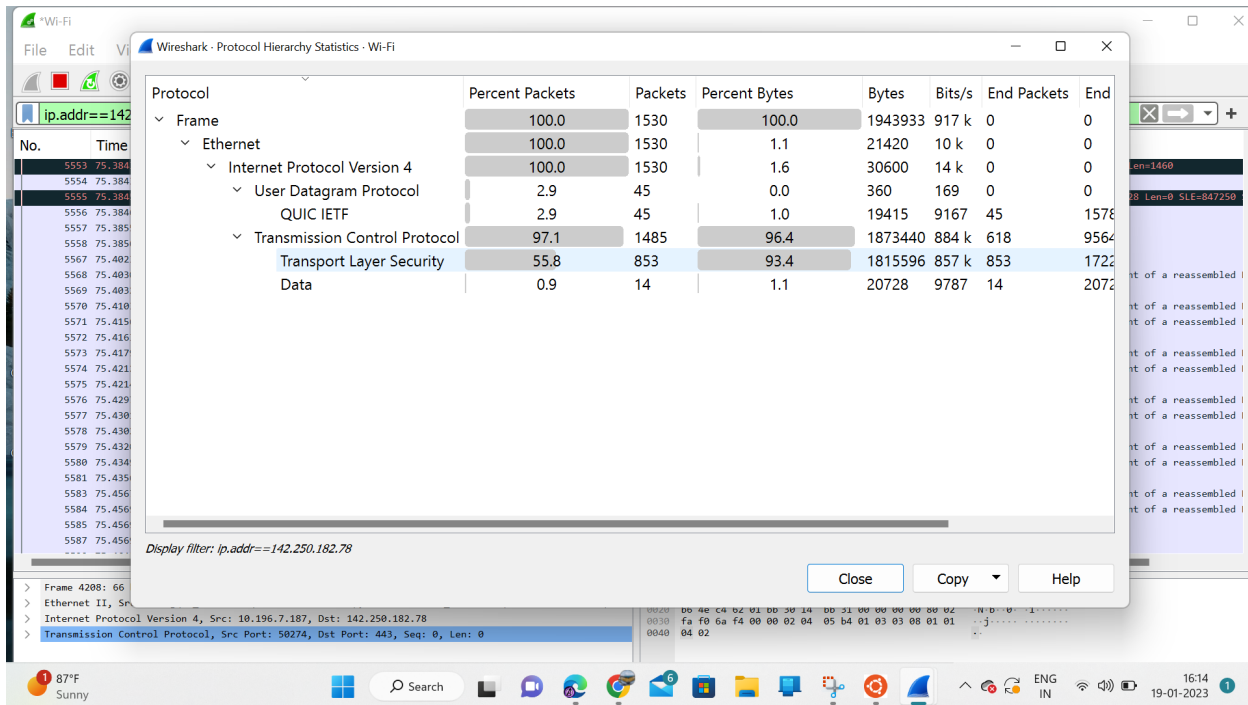
```
;; QUESTION SECTION:
;www.youtube.com.                IN      A

;; ANSWER SECTION:
www.youtube.com. 0      IN      CNAME   youtube-ui.l.google.com.
youtube-ui.l.google.com. 0      IN      A       142.250.182.78
youtube-ui.l.google.com. 0      IN      A       142.250.182.110
youtube-ui.l.google.com. 0      IN      A       142.250.182.142
youtube-ui.l.google.com. 0      IN      A       142.250.183.238
youtube-ui.l.google.com. 0      IN      A       142.250.193.110
youtube-ui.l.google.com. 0      IN      A       142.250.193.142
youtube-ui.l.google.com. 0      IN      A       142.250.193.174
youtube-ui.l.google.com. 0      IN      A       142.250.205.238
youtube-ui.l.google.com. 0      IN      A       172.217.160.142
youtube-ui.l.google.com. 0      IN      A       216.58.196.174
youtube-ui.l.google.com. 0      IN      A       142.250.71.14
youtube-ui.l.google.com. 0      IN      A       142.250.71.46
youtube-ui.l.google.com. 0      IN      A       142.250.195.46
youtube-ui.l.google.com. 0      IN      A       142.250.195.78
youtube-ui.l.google.com. 0      IN      A       142.250.195.110
youtube-ui.l.google.com. 0      IN      A       142.250.195.142

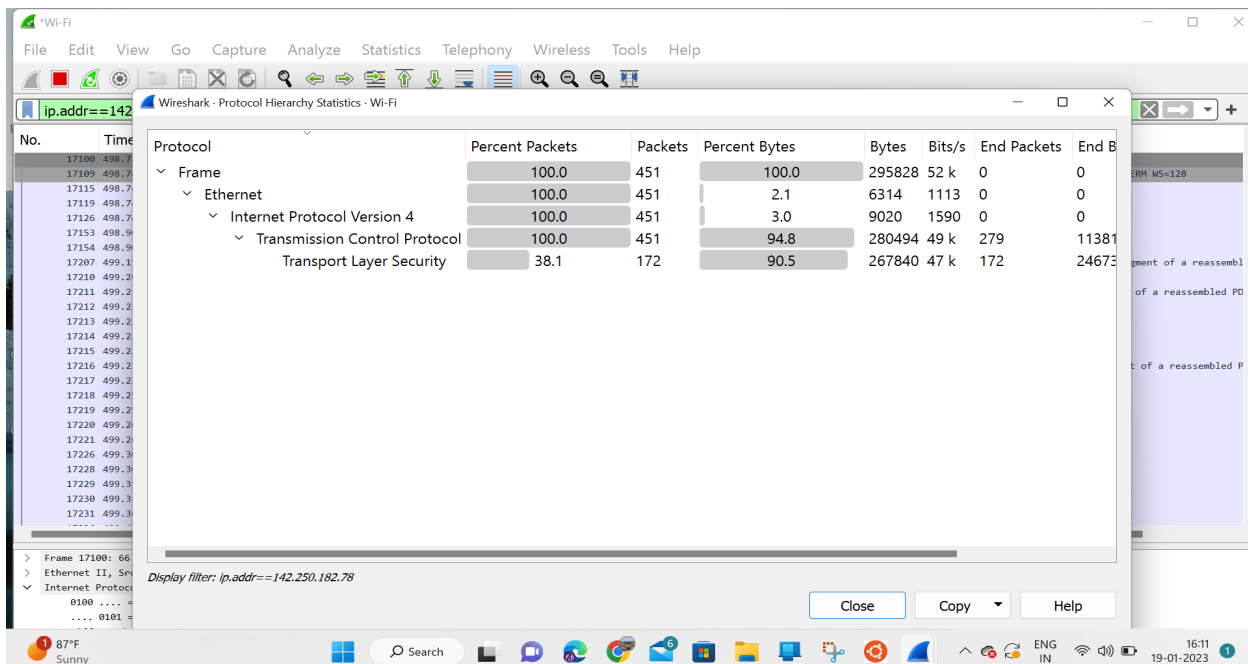
;; Query time: 119 msec
;; SERVER: 172.19.80.1#53(172.19.80.1)
;; WHEN: Thu Jan 19 16:09:26 IST 2023
;; MSG SIZE rcvd: 364
```

We have used 142.250.182.78 as the IP address of youtube for finding the traffic used in our computer network.

a) If we use Firefox browser, 97.7% of the traffic is controlled by TCP and 2.2 percent of the traffic is controlled by UDP. Therefore, youtube uses TCP protocol. The statistics of this are as follows.



b) If we use chrome instead of firefox, then all (100%) of the traffic is controlled by TCP. The statistics are as follows:



Even if we checked on google browser regarding this, it says that Youtube actually uses TCP protocol to control the traffic in the computer networks.

9. [Bonus question] Try connecting two different devices in the same network. For example, connect your mobile phone on the same network as your laptop. Apply the filter `ip.addr=<other device's IP addr>`. Check if you can sniff packets meant for another device on the same local network.

A) We have connected a Samsung phone mobile network with one of our laptops. What we observed was that our mobile network can actually sniff packets but our laptop cannot know this information because our operating system hides this information to avoid spying of other's data. The image is attached below for reference.

