CS315: Lab Assignment 1

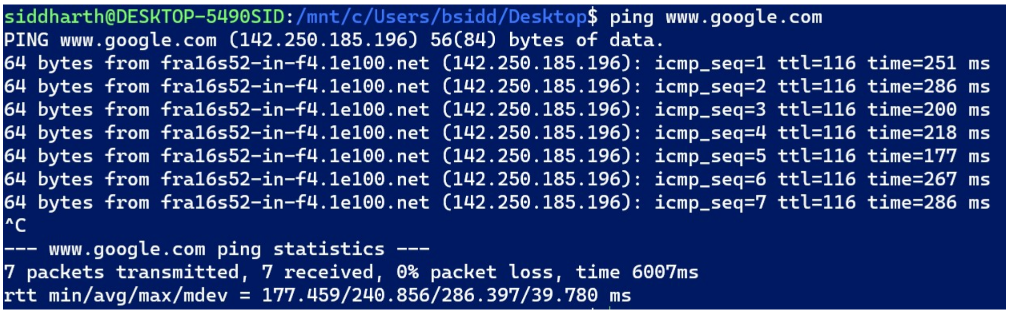
B Siddharth Prabhu
`200010003@iitdh.ac.in`

03 January 2023

1 Answers for Task 1: Background

1.1 ping

We use ping to check the connectivity between two computers. On running the command (here, in WSL) `ping www.google.com` , we get the round-trip time (RTT) for messages sent from the originating host to the destination computer (in this case, the web servers of google.com). On the linux terminal, such messages keep getting sent, and RTT values are displayed, until termination via Ctrl+C. On terminating this, we get statistics on the packets sent, received, and lost.

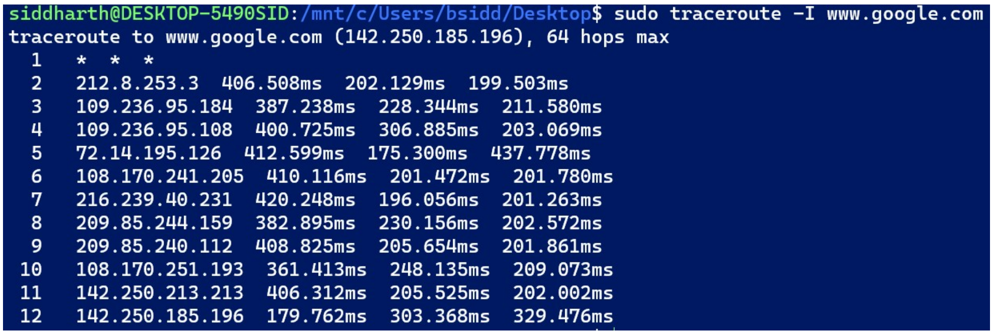


```
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop$ ping www.google.com
PING www.google.com (142.250.185.196) 56(84) bytes of data.
64 bytes from fra16s52-in-f4.1e100.net (142.250.185.196): icmp_seq=1 ttl=116 time=251 ms
64 bytes from fra16s52-in-f4.1e100.net (142.250.185.196): icmp_seq=2 ttl=116 time=286 ms
64 bytes from fra16s52-in-f4.1e100.net (142.250.185.196): icmp_seq=3 ttl=116 time=200 ms
64 bytes from fra16s52-in-f4.1e100.net (142.250.185.196): icmp_seq=4 ttl=116 time=218 ms
64 bytes from fra16s52-in-f4.1e100.net (142.250.185.196): icmp_seq=5 ttl=116 time=177 ms
64 bytes from fra16s52-in-f4.1e100.net (142.250.185.196): icmp_seq=6 ttl=116 time=267 ms
64 bytes from fra16s52-in-f4.1e100.net (142.250.185.196): icmp_seq=7 ttl=116 time=286 ms
^C
--- www.google.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6007ms
rtt min/avg/max/mdev = 177.459/240.856/286.397/39.780 ms
```

Figure 1: Output for ping

1.2 traceroute

We use traceroute to get the path taken to reach a host. On running `traceroute www.google.com` , we would get a report with five columns of information. The first column contains the hop number. The second column contains the IP address of the device at the given hop along the route. Then, the next three columns contain the RTT values for three signal packets that have been sent to that point (to display consistency). Note that here, the command has been adjusted according to our needs.

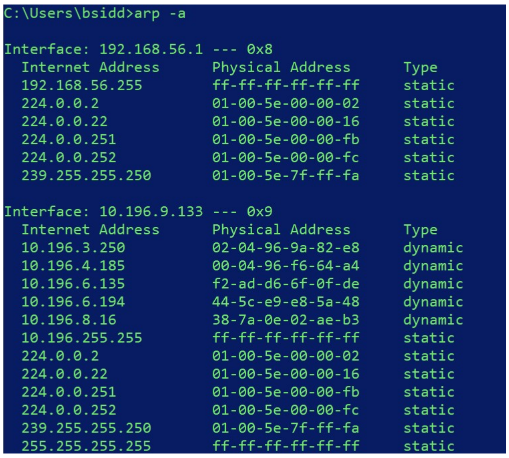


```
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop$ sudo traceroute -I www.google.com
traceroute to www.google.com (142.250.185.196), 64 hops max
  1   *  *  *
  2   212.8.253.3  406.508ms  202.129ms  199.503ms
  3   109.236.95.184  387.238ms  228.344ms  211.580ms
  4   109.236.95.108  400.725ms  306.885ms  203.069ms
  5   72.14.195.126  412.599ms  175.300ms  437.778ms
  6   108.170.241.205  410.116ms  201.472ms  201.780ms
  7   216.239.40.231  420.248ms  196.056ms  201.263ms
  8   209.85.244.159  382.895ms  230.156ms  202.572ms
  9   209.85.240.112  408.825ms  205.654ms  201.861ms
 10   108.170.251.193  361.413ms  248.135ms  209.073ms
 11   142.250.213.213  406.312ms  205.525ms  202.002ms
 12   142.250.185.196  179.762ms  303.368ms  329.476ms
```

Figure 2: Output for traceroute

1.3 arp

The `arp` command is used to view and modify the contents of the local ARP (Address Resolution Protocol Cache). On running the command with the `-a` flag on Windows, we can view the contents of the ARP Table, which contains details of the recently resolved MAC addresses of IP hosts on the network.



```
C:\Users\bsidd>arp -a

Interface: 192.168.56.1 --- 0x8
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 10.196.9.133 --- 0x9
  Internet Address      Physical Address      Type
  10.196.3.250          02-04-96-9a-82-e8     dynamic
  10.196.4.185          00-04-96-f6-64-a4     dynamic
  10.196.6.135          f2-ad-d6-6f-0f-de     dynamic
  10.196.6.194          44-5c-e9-e8-5a-48     dynamic
  10.196.8.16           38-7a-0e-02-ae-b3     dynamic
  10.196.255.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Figure 3: A section of the output for arp

1.4 ifconfig

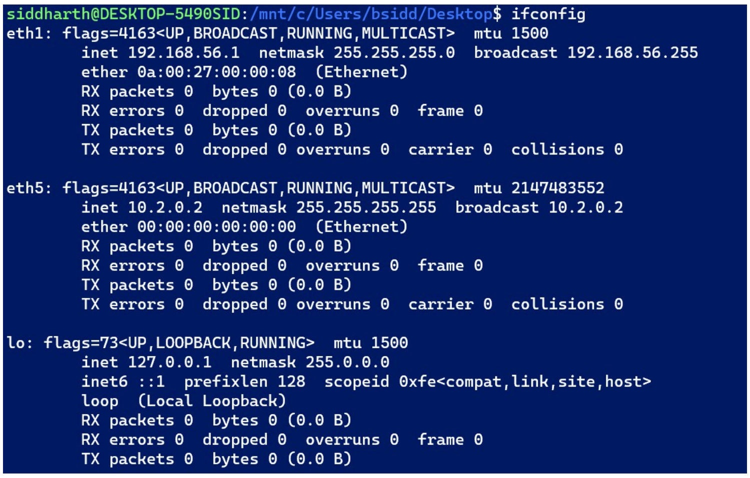
The `ifconfig` (interface configurator) utility is used for network interface configuration. Using this command, we can view the IP and MAC addresses of the different network interfaces in a system. The output from ifconfig has three main parts:

Status Line This line contains the interface name and status flags currently associated with the interface. Also, it includes MTU (Maximum Transmission Unit) and the index number of the interface. This line determines the current state of the interface.

IP address information line This line includes the IPv4/IPv6 address that is configured for the interface. For an IPv4 address, the configured netmask and broadcast address are also displayed.

MAC Address Line For an IPv4 address, the third line shows the MAC address (Ethernet layer address) that is assigned to the interface.

These lines are then followed by different interface statistics.

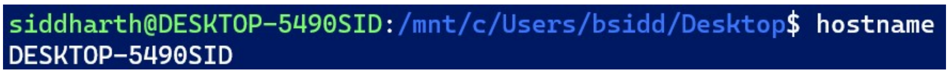


```
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop$ ifconfig
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.1  netmask 255.255.255.0  broadcast 192.168.56.255
        ether 0a:00:27:00:00:08  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 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

eth5: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 2147483552
        inet 10.2.0.2  netmask 255.255.255.255  broadcast 10.2.0.2
        ether 00:00:00:00:00:00  (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 1500
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0xfe<compat,link,site,host>
        loop  (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)
```

Figure 4: Output for ifconfig

1.5 hostname

The `hostname` command is used to retrieve the host name of a computer or network node in a network. Hostnames are specific names or character strings that refer to a host. It is usable for the network and people.



```
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop$ hostname
DESKTOP-5490SID
```

Figure 5: Output for hostname

1.6 Review of Configuration files

1.6.1 `/etc/hostname`

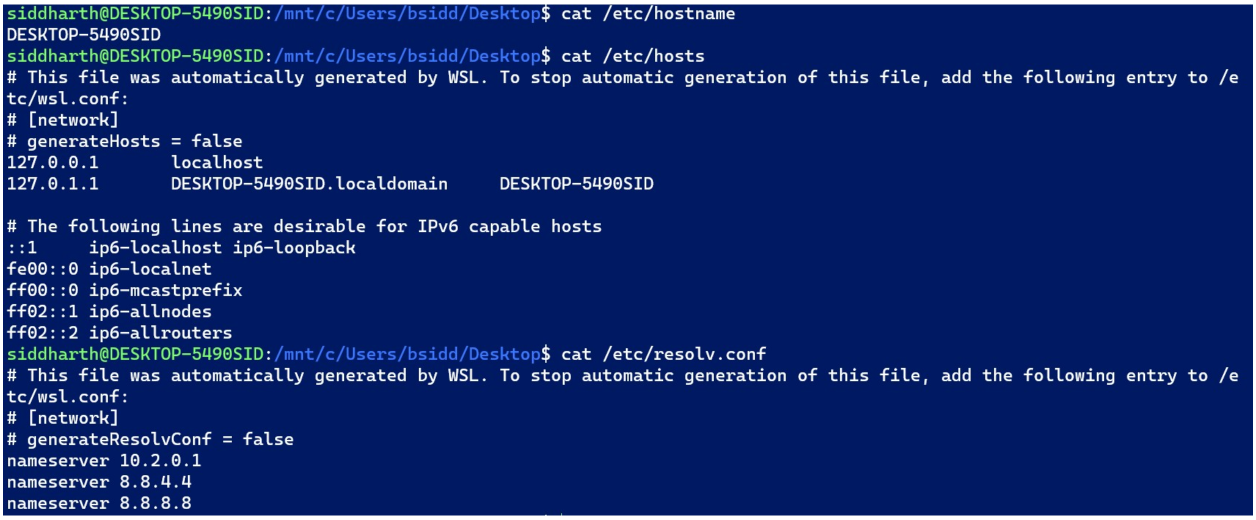
This file stores the system's host name, which is the FQDN (Fully Qualified Domain Name) of the system.

1.6.2 `/etc/hosts`

When a machine is started, it needs to know the mapping of some hostnames to IP addresses before DNS can be referenced. This mapping is kept in this particular file. In the absence of a name server, any network program on the system consults this file to determine the IP address that corresponds to a host name.

1.6.3 `/etc/resolv.conf`

This file a text file which is used by the resolver library that determines the IP address for a host name. This file contains the list of name servers used by the host for DNS resolution. When using DHCP (Dynamic Host Configuration Protocol), this file is populated automatically with the records issued by the DHCP Server.

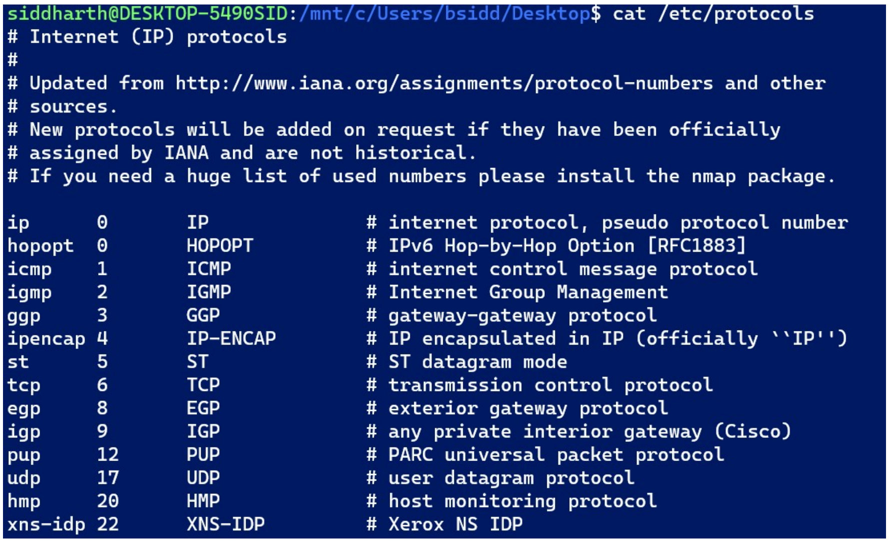


```
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop$ cat /etc/hostname
DESKTOP-5490SID
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop$ cat /etc/hosts
# This file was automatically generated by WSL. To stop automatic generation of this file, add the following entry to /e
tc/wsl.conf:
# [network]
# generateHosts = false
127.0.0.1       localhost
127.0.1.1       DESKTOP-5490SID.localdomain     DESKTOP-5490SID

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop$ cat /etc/resolv.conf
# This file was automatically generated by WSL. To stop automatic generation of this file, add the following entry to /e
tc/wsl.conf:
# [network]
# generateResolvConf = false
nameserver 10.2.0.1
nameserver 8.8.4.4
nameserver 8.8.8.8
```

Figure 6: Contents of the hostname, hosts, and resolv.conf files

1.6.4 `/etc/protocols`

This file contains information regarding known protocols. For each protocol, a single line is present with information in the format: `official-protocol-name` `protocol-number` `aliases` . # is used for comments regarding the protocols.

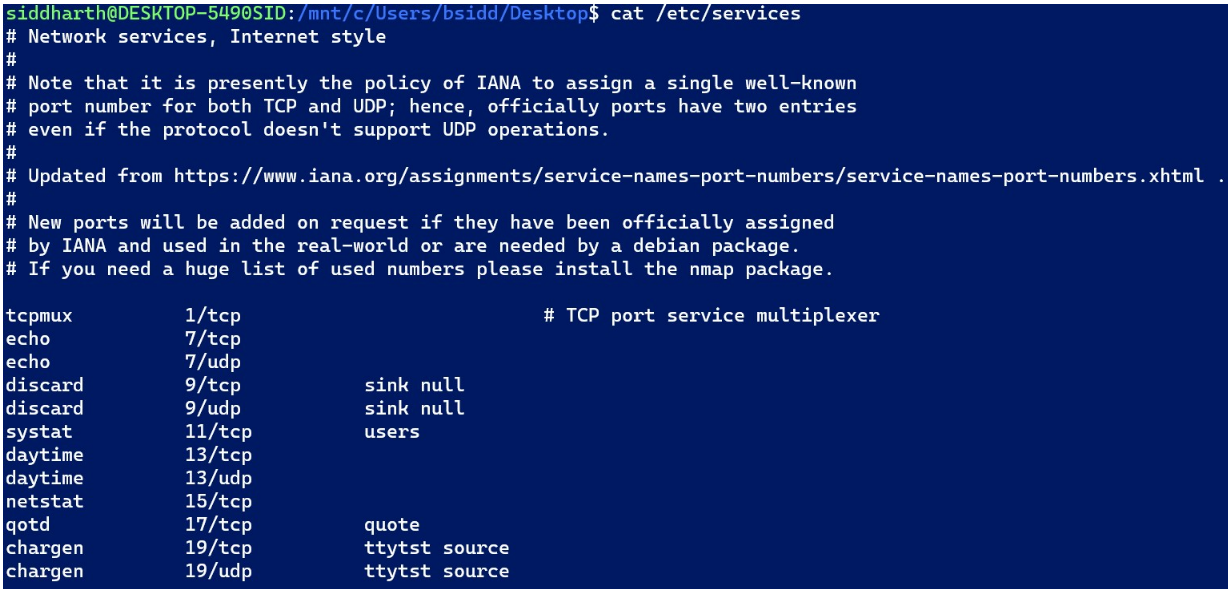


```
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop$ cat /etc/protocols
# Internet (IP) protocols
#
# Updated from http://www.iana.org/assignments/protocol-numbers and other
# sources.
# New protocols will be added on request if they have been officially
# assigned by IANA and are not historical.
# If you need a huge list of used numbers please install the nmap package.

ip      0       IP              # internet protocol, pseudo protocol number
hopopt  0       HOPOPT          # IPv6 Hop-by-Hop Option [RFC1883]
icmp    1       ICMP            # internet control message protocol
igmp    2       IGMP            # Internet Group Management
ggp     3       GGP             # gateway-gateway protocol
ipencap 4       IP-ENCAP        # IP encapsulated in IP (officially ``IP'')
st      5       ST              # ST datagram mode
tcp     6       TCP             # transmission control protocol
egp     8       EGP             # exterior gateway protocol
igp     9       IGP             # any private interior gateway (Cisco)
pup     12      PUP             # PARC universal packet protocol
udp     17      UDP             # user datagram protocol
hmp     20      HMP             # host monitoring protocol
xns-idp 22      XNS-IDP         # Xerox NS IDP
```

Figure 7: A section of the contents of the protocols file

1.6.5 `/etc/services`

This file contains a list of network services, with the ports mapped to each of them. Most Internet services are assigned a specific port for their use. When a client opens a connection across the network to a server, the client uses the port to specify which service it wishes to use. This file serves as a small local database to store this information. For each service, this file specifies the service's 'well-known port number', and notes whether the service is available as a TCP (connection-oriented) or UDP (connectionless) service.



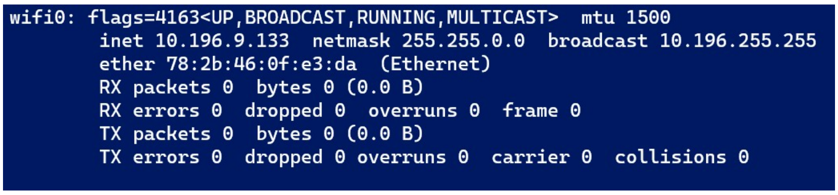
```
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop$ cat /etc/services
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, officially ports have two entries
# even if the protocol doesn't support UDP operations.
#
# Updated from https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml .
#
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.

tcpmux          1/tcp                           # TCP port service multiplexer
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
```

Figure 8: A section of the contents of the services file

2 Answers for Task 2: Warm-Up Questions

(i) What is your machine's hostname and IP address? How did you get this information?

My machine's hostname is `DESKTOP-5490SID` , and the IP address assigned to it is `10.196.9.133` . The hostname was obtained via the `hostname` command, as shown in Section (1.5). The IP Address was obtained using the `ifconfig` command, next to the wifi0 label.

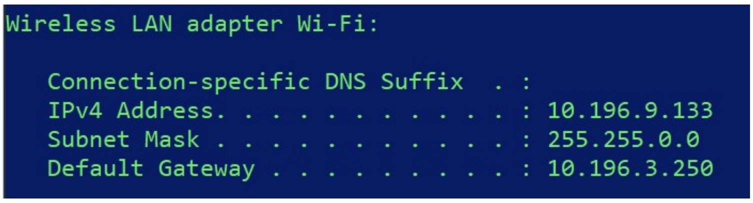


```
wifi0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.196.9.133  netmask 255.255.0.0  broadcast 10.196.255.255
        ether 78:2b:46:0f:e3:da  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 9: wifi0 section of ifconfig output

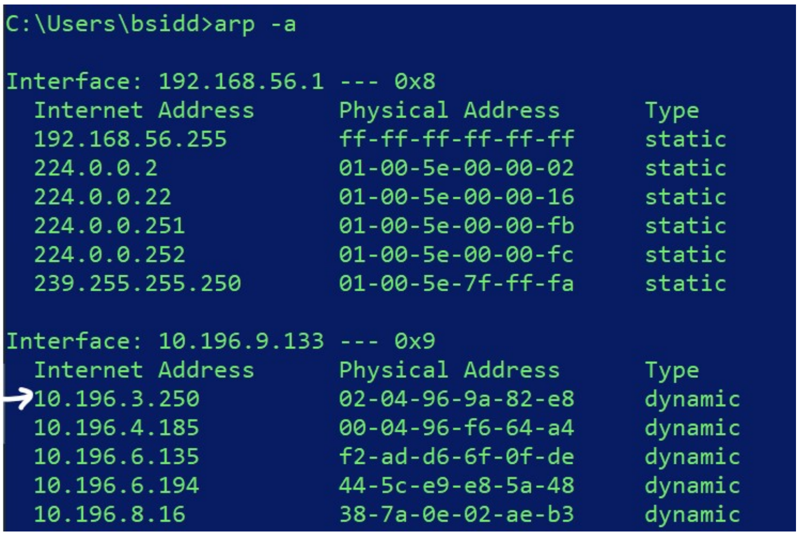
(ii) What is the next hop router's IP address and MAC address? How did you get this information?

The next hop router's IP address is `10.196.3.250` . Its MAC Address is `02:04:96:9a:82:e8` . This information is found using the `arp` command. On my Windows system, the same is done using `ipconfig` and `arp -a` .



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.196.9.133
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.196.3.250
```

Figure 10: Default Gateway IP address obtained by ifconfig

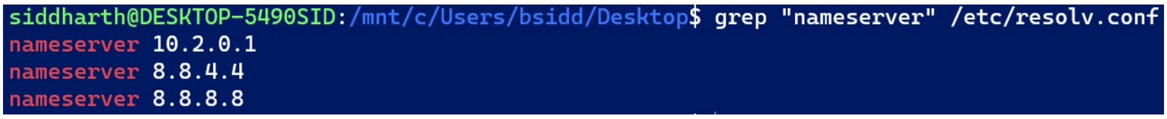


```
C:\Users\bsidd>arp -a

Interface: 192.168.56.1 --- 0x8
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 10.196.9.133 --- 0x9
  Internet Address      Physical Address      Type
  10.196.3.250          02-04-96-9a-82-e8     dynamic
  10.196.4.185          00-04-96-f6-64-a4     dynamic
  10.196.6.135          f2-ad-d6-6f-0f-de     dynamic
  10.196.6.194          44-5c-e9-e8-5a-48     dynamic
  10.196.8.16           38-7a-0e-02-ae-b3     dynamic
```

Figure 11: MAC address of the router found using arp -a

(iii) What is the local DNS server's IP address? How did you get this information?

The local DNS server's IP address is `10.2.0.1`. This was obtained by looking at the contents of `/etc/resolv.conf`.



```
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop$ grep "nameserver" /etc/resolv.conf
nameserver 10.2.0.1
nameserver 8.8.4.4
nameserver 8.8.8.8
```

Figure 12: Name Server IP Address

(iv) What do the numbers in the file /etc/protocols represent?

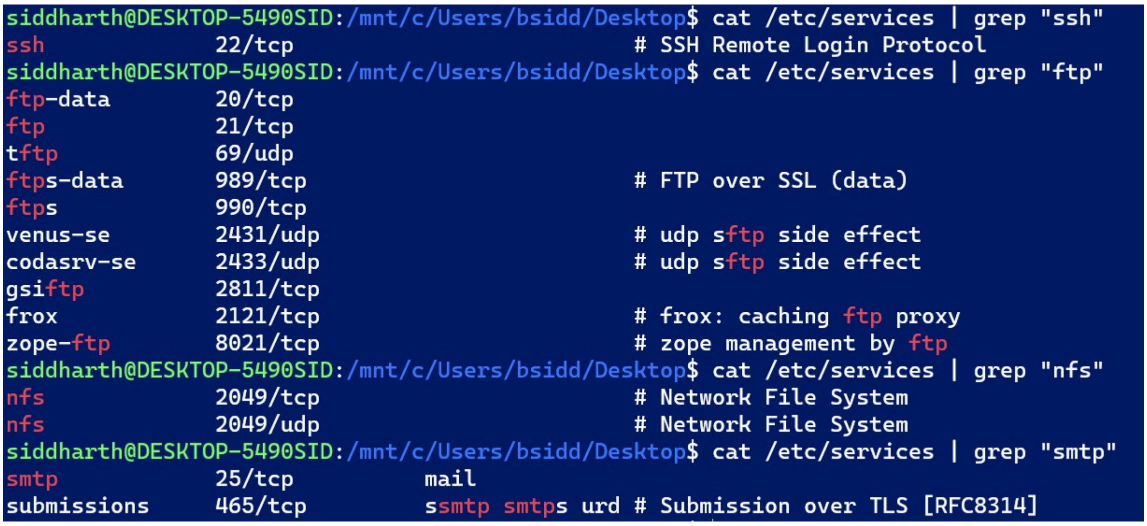
The (1-byte) numbers in the file `/etc/protocols` represents the protocol number, which is used to identify the protocol.

(v) What is the port number associated with applications: ssh, ftp, nfs, smtp (email)? How did you get this information?

The port numbers for the applications given are as follows:

- ssh: port 22
- ftp: port 21
- nfs: port 2049
- smtp: 25

This is obtained using the `/etc/services` file, in combination with the grep tool.



```
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop$ cat /etc/services | grep "ssh"
ssh             22/tcp                          # SSH Remote Login Protocol
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop$ cat /etc/services | grep "ftp"
ftp-data        20/tcp
ftp             21/tcp
tftp            69/udp
ftps-data       989/tcp                         # FTP over SSL (data)
ftps            990/tcp
venus-se        2431/udp                        # udp sftp side effect
codasrv-se      2433/udp                        # udp sftp side effect
gsiftp          2811/tcp
frox            2121/tcp                        # frox: caching ftp proxy
zope-ftp        8021/tcp                        # zope management by ftp
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop$ cat /etc/services | grep "nfs"
nfs             2049/tcp                        # Network File System
nfs             2049/udp                        # Network File System
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop$ cat /etc/services | grep "smtp"
smtp            25/tcp          mail
submissions     465/tcp         ssmtp smtps urd # Submission over TLS [RFC8314]
```

Figure 13: Applications Port Numbers

(vi) How many of these questions can you answer for the phone running on android/iOS?

In theory, we should be able to obtain all of the required answers for a phone as well. The only thing is that we would need some kind of terminal-like setup to find these things. We'd have to use some application that gets such details!

3 Answers for Task 3

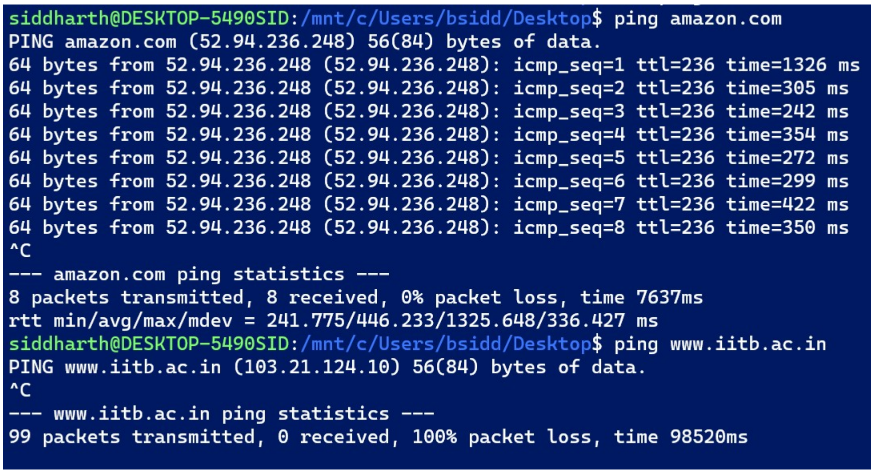
(i) Using ping

(a) Explain the results that you obtain; For example, the success and failure of the Ping

We have obtained results of values for www.amazon.com, while not for www.iitb.ac.in, since the website may have blocked ping requests. This shows that we are able to form a connection to www.amazon.com, but not with www.iitb.ac.in.

(b) What are the reasons for the values of RTTs that you see?

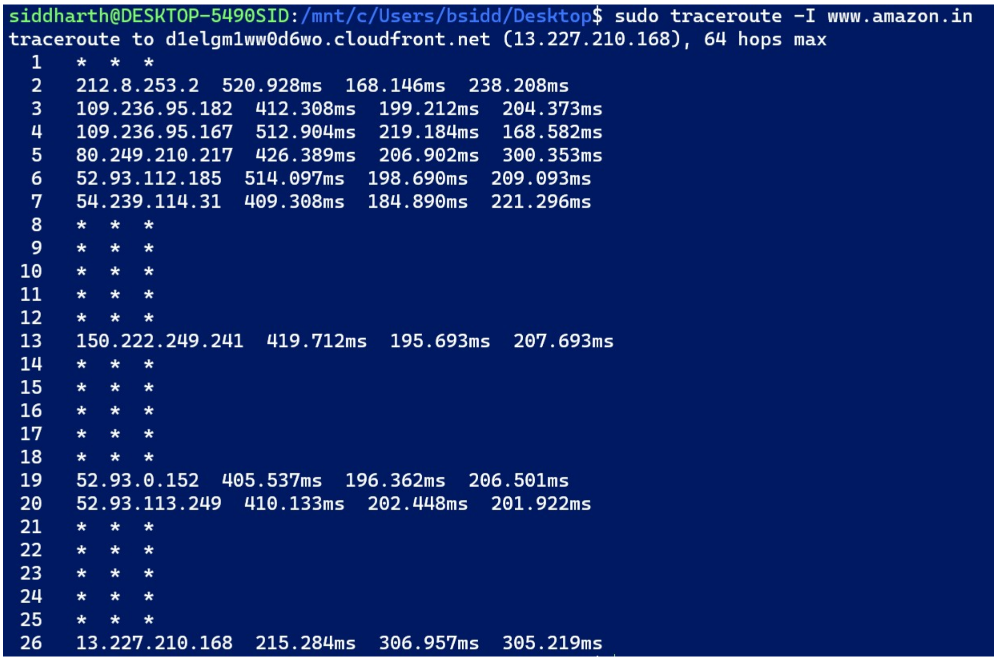
The initial value is quite high since it tries to find the path to locate the destination. The later RTT values fluctuate due to traffic and other factors. Multiple Ping requests are sent, to check consistency along the connection.



```
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop$ ping amazon.com
PING amazon.com (52.94.236.248) 56(84) bytes of data.
64 bytes from 52.94.236.248 (52.94.236.248): icmp_seq=1 ttl=236 time=1326 ms
64 bytes from 52.94.236.248 (52.94.236.248): icmp_seq=2 ttl=236 time=305 ms
64 bytes from 52.94.236.248 (52.94.236.248): icmp_seq=3 ttl=236 time=242 ms
64 bytes from 52.94.236.248 (52.94.236.248): icmp_seq=4 ttl=236 time=354 ms
64 bytes from 52.94.236.248 (52.94.236.248): icmp_seq=5 ttl=236 time=272 ms
64 bytes from 52.94.236.248 (52.94.236.248): icmp_seq=6 ttl=236 time=299 ms
64 bytes from 52.94.236.248 (52.94.236.248): icmp_seq=7 ttl=236 time=422 ms
64 bytes from 52.94.236.248 (52.94.236.248): icmp_seq=8 ttl=236 time=350 ms
^C
--- amazon.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7637ms
rtt min/avg/max/mdev = 241.775/446.233/1325.648/336.427 ms
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop$ ping www.iitb.ac.in
PING www.iitb.ac.in (103.21.124.10) 56(84) bytes of data.
^C
--- www.iitb.ac.in ping statistics ---
99 packets transmitted, 0 received, 100% packet loss, time 98520ms
```

Figure 14: Output of ping

(ii) Using traceroute



```
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop$ sudo traceroute -I www.amazon.in
traceroute to d1elgm1ww0d6wo.cloudfront.net (13.227.210.168), 64 hops max
  1   *  *  *
  2   212.8.253.2  520.928ms  168.146ms  238.208ms
  3   109.236.95.182  412.308ms  199.212ms  204.373ms
  4   109.236.95.167  512.904ms  219.184ms  168.582ms
  5   80.249.210.217  426.389ms  206.902ms  300.353ms
  6   52.93.112.185  514.097ms  198.690ms  209.093ms
  7   54.239.114.31  409.308ms  184.890ms  221.296ms
  8   *  *  *
  9   *  *  *
 10   *  *  *
 11   *  *  *
 12   *  *  *
 13   150.222.249.241  419.712ms  195.693ms  207.693ms
 14   *  *  *
 15   *  *  *
 16   *  *  *
 17   *  *  *
 18   *  *  *
 19   52.93.0.152  405.537ms  196.362ms  206.501ms
 20   52.93.113.249  410.133ms  202.448ms  201.922ms
 21   *  *  *
 22   *  *  *
 23   *  *  *
 24   *  *  *
 25   *  *  *
 26   13.227.210.168  215.284ms  306.957ms  305.219ms
```

Figure 15: Output of traceroute

(a) Explain what you see. Whenever successful, draw a network map from your machine to the destination, which includes the hop addresses obtained from Traceroute.

We observe that it took 26 hops for the packet to reach www.amazon.in. A network map would look like: 10.196.9.133 (Device) → 10.196.3.250 (Next-Hop Router) → 212.8.253.2 → 109.236.95.182 → 109.236.95.167 → 80.249.210.217 → 52.93.112.185 → 54.239.114.31 → 150.222.249.241 → 52.93.0.152 → 52.93.113.249 → 13.227.210.168 (Destination IP)

(b) How can you change the maximum hop number?

To do this, we can use the traceroute command along with flags `-m` , `--max-hop=num` , where num is the max hop number that we set (default is 64).

(c) What do the three timestamps signify in the result of Traceroute?

The three timestamps signify the RTT (Round-Trip Time) values (in milliseconds) for 3 signal packets that reach a certain point in the list of hops (and return back).

(d) What is the use of TTL (Time To Live) field in ICMP packets?

TTL field is a counter that decreases in value after each hop of the packet. It is a time limit imposed on the data packet to be in-network before being discarded. It is an 8-bit binary value set in the Internet Protocol (IP) Header by the sending host. The purpose of a TTL is to prevent data packets from being circulated forever in the network.