Assignment – 1

Name: Abhishek Agrahari

Roll Number: 190123066

Ans. 1-

a) -c <u>count</u> => specifies the number of echo requests, as indicated by the count variable, to be sent.

b) -i <u>Wait</u> => Waits the number of seconds specified by the Wait variable between the sending of each packet. The default is to wait for one second between each packet.

c) -l <u>Preload</u> => Defines the number of packets to send without waiting for a reply. To specify a value higher than 3, you need superuser permissions.

d) -s <u>PacketSize</u> => Specifies the number of data bytes to be sent. If the payload size is set to 32 bytes, total packet size becomes 40 bytes when combined with the 8 bytes of <u>ICMP</u> header data.

Ans. 2-

IP 1 – www.google.com (172.217.166.196) USA

IP 2 – www.codeforces.com (213.248.110.126) Russia

**IP 3 –** www.lichess.org (37.187.205.99) France

IP 4 – www.flipkart.com (103.47.13.145) India

IP 5 – www.leetcode.com(104.26.9.101)USA

IP 6 - www.facebook.com(157.240.198.60) Germany

Time of execution	Average RTT					
	IP-1	IP-2	IP-3	IP-4	IP-5	IP-6
Aug 16 16:20	10.501	188.793	144.229	49.597	33.646	9.134
Aug 16 18:42	26.638	178.449	142.390	65.082	40.251	8.315
Aug 16 20:37	7.637	196.034	146.272	49.196	37.458	10.388

a) Yes, there is a positive correlation between distance and RTT. There are a number of reasons for this. For example, an increased hop count. The packets have to go through more routers, at each router there may be a delay.

b) Two times 4% packet loss in IP-2 and one time 4% packet loss in IP-5. Packet loss is either caused by errors in data transmission, typically across wireless networks, or network congestion.

c) I have chosen IP-6 and increased the packet size from 64 to 1024 in the power of 2. My further pings are rejected.
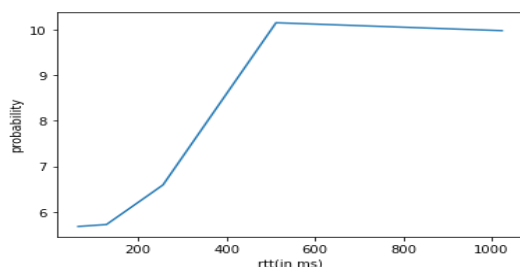
d) Yes, there is an increase in RTT with increasing packet size but it is not that significant. The main factor that impacts RTT is source internet connection which if unstable could lead to significant changes in the graph above. There are slight variations in RTT at different times of day due to variations in network congestion and traffic.
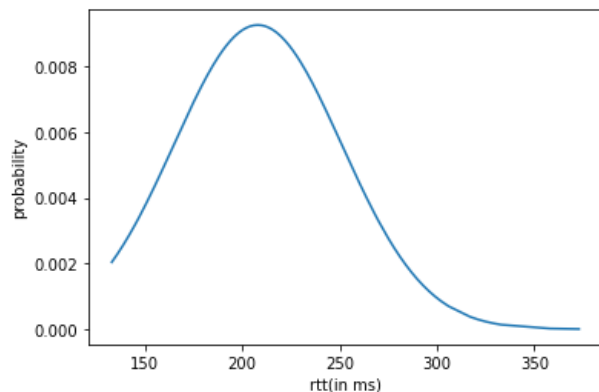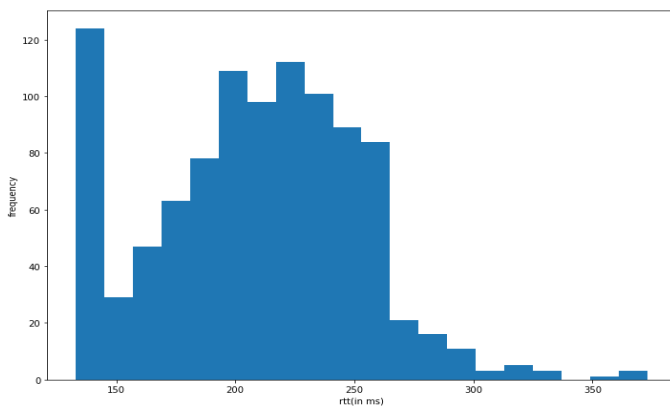
Ans. 3-

Commands used to create output files-

  i.   **ping -c 1000 -n www.lichess.org >n.txt**
  ii. **ping -c 1000 -p ff00 www.lichess.org > ff00.txt**
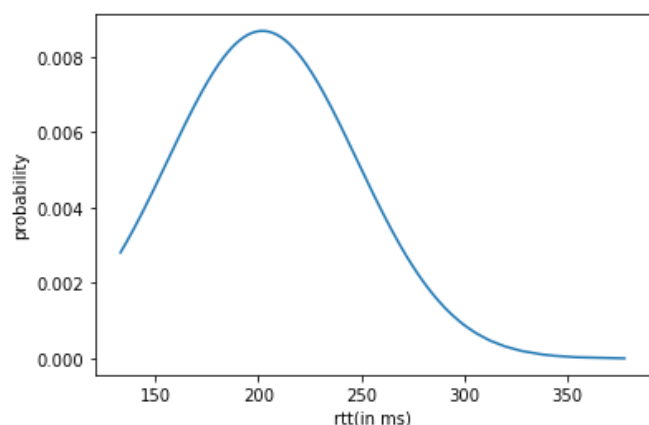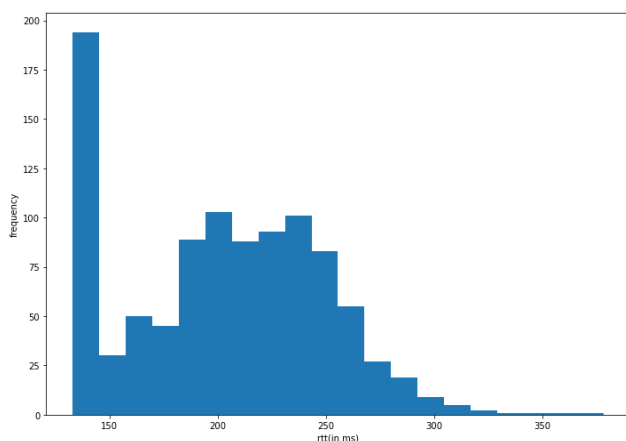
a) i. 0.1%   ii. 0.3%

b) i. min/max /mean /median = 133.309/373.032/208.109/210 ms

   ii. min/max /mean / median = 133.156/377.776/202.932/205 ms

c) i.

ii.

d) The mean and median of (i) is more than (ii).
-p <u>pattern</u>: is used to fill out the packet with upto 16 bytes. This is useful for diagnosing data-dependent problems in a network.
-n: is used for numeric output only. No attempt will be made to lookup symbolic names for host addresses
These variations are mild only and the distribution is nearly the same.

Ans. 4-

a) Important attributes of ifconfig command are as follows:

1. **Interface**: Specifies the network interface configuration. Abbreviation for the interfaces are used like lo for loopback, eth0 for ethernet etc.
2. **IP address** (inet addr), netmask and broadcast of the interface.
3. **RX**: number of packets received.
4. **TX**: number of packets transmitted.
5. **MTU**: A maximum transmission unit (MTU) is the largest packet or frame size, specified in octets (eight-bit bytes) that can be sent in a packet- or frame-based network such as the internet. The internet's transmission control protocol (TCP) uses the MTU to determine the maximum size of each packet in any transmission.

b) The "ifconfig" (interface configuration) command is used for
1. **Displaying current network configuration information**: The ifconfig command with no arguments will display all the active interfaces details.
2. **Creating an alias for the network interface:** The ifconfig utility allows you to configure additional network interfaces using the **alias** feature.
3. **Assigning a netmask to network interface**: Using the ifconfig command with the "netmask" argument and interface name as (**eth0**) allows you to define a netmask to a given interface.
4. **setting up hardware address**: MAC address can be changed by infonfig with "hw ether" argument.
c)

i) mtu <u>N</u>: This is used to set the Maximum Transfer Unit (MTU).

ii) -a: This option is used to display all the interfaces available, even if they are down
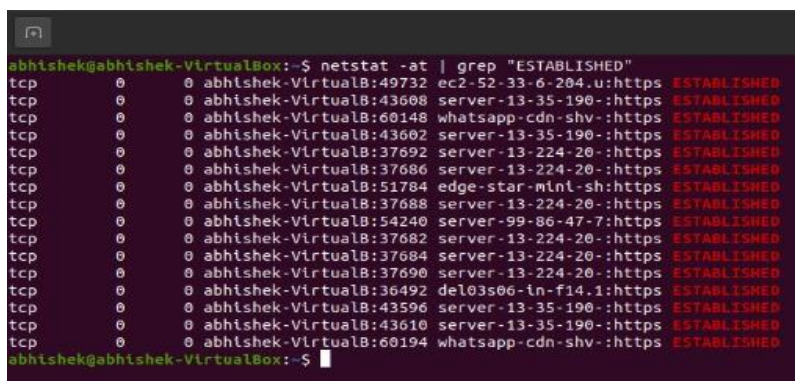
iii) <u>interface</u> up: This option is used to activate the driver for the given interface.

iv) <u>interface</u> down: This option is used to deactivate the driver for the given interface.

Ans. 5-

a) The network statistics (netstat) command is a networking tool used for troubleshooting and configuration, that can also serve as a monitoring tool for connections over the network. Both incoming and outgoing connections, routing tables, port listening, and usage statistics are common uses for this command.

b) netstat -at | grep "ESTABLISHED"

c) netstat -r shows the kernels routing table. It has following fields in the output
  1- Destination: destination ip address
  2- Gateway: next router where to hop

3-Genmask: network mask of the destination
4- Flags: It indicates
      i. U-Up (The route is up)
      ii. G-Gateway (The is via a remote router/gateway)
      iii. H - Host (The destination of the route is a specific host)
5- MSS: maximum segment size for the TCP connections
6- Window: default window size of TCP connection over this route
7- irtt: initial round trip time.
8- Iface: interface of the network

d) netstat -ai => it shows all network interfaces
    netstat -ai | tail -n +3 | wc -l => it finds no of interfaces in computer. It is 2 in my case.
e) netstat -aus

```
abhishek@abhishek-VirtualBox:~$ netstat -aus
IcmpMsg:
    InType3: 40
    OutType3: 40
Udp:
    1481 packets received
    40 packets to unknown port received
    0 packet receive errors
    1533 packets sent
    0 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 11
UdpLite:
IpExt:
    InMcastPkts: 126
    OutMcastPkts: 128
    InBcastPkts: 11
    OutBcastPkts: 11
    InOctets: 58674109
    OutOctets: 2243041
    InMcastOctets: 15678
    OutMcastOctets: 15758
    InBcastOctets: 854
    OutBcastOctets: 854
    InNoECTPkts: 49082
MPTcpExt:
abhishek@abhishek-VirtualBox:~$
```

f) The loopback device is a special, virtual network interface that your computer uses to communicate with itself. It is used mainly for diagnostics and troubleshooting, and to connect to servers running on the local machine.
Ans 6.
a) Traceroute is a network diagnostic tool used to track in real-time the pathway taken by a packet on an IP network from source to destination, reporting the IP addresses of all the routers it pinged in between.
Command: sudo traceroute -I IP Address
IP 1 – www.google.com (172.217.166.196) USA

IP 2 – www.codeforces.com (213.248.110.126) Russia

IP 3 – www.lichess.org (37.187.205.99) France

IP 4 – www.flipkart.com(103.47.13.145) India

IP 5 – www.leetcode.com(104.26.9.101) USA

IP 6 - www.facebook.com(157.240.198.60) Germany

TIME OF EXECUTION	IP-1	IP-2	IP-3	IP-4	IP-5	IP-6
Sep 16 16:38	8	19	23	12	9	8
Sep 16 18:49	8	19	23	12	9	8
Sep 16 20:43	8	19	23	12	9	8

b) _gateway (10.0.2.2), 192.168.0.1, 10.118.20.1 are common among to all hosts.

c) Yes, route to IP-1 and IP-5 changes at different times of the day probably due to change in traffic and congestion at different times.

d) In some cases, traceroute does not find complete paths to some. Most likely the device that was hit was not configured to reply to ICMP/UDP traffic. This result does not mean that the traffic wasn't passed. The second possibility is that the packets were dropped due to an issue on the network.

e) Yes, we can find a route to a host if ping isn't working. Ping is straight ICMP from point A to point B, that traverses networks via routing rules. Traceroute works very different, even though it uses ICMP. Traceroute works by targeting the final hop, but limiting the TTL and waiting for a time exceeded message, and then increasing it by one for the next iteration. Therefore, the response it gets is not an ICMP echo reply to the ICMP echo request from the host along the way, but a time exceeded message from that host - so even though it is using ICMP, it is using it in a very different way.
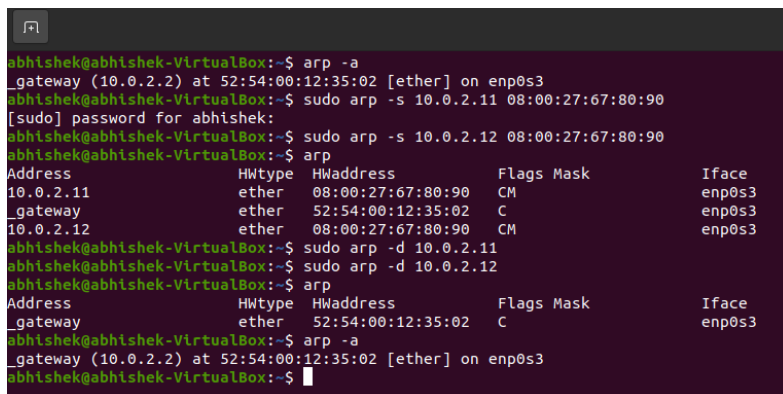
Ans 7.

a) Yes, we can see the full ARP table.

ARP Table is used to keep the record of the IP address and MAC address of the devices (source and destination device). For the communication between two devices, it is necessary that the IP address and the MAC address of the source and the destination device should be stored in an ARP table. If there is no record in the table, an ARP broadcast is sent by the source to all the devices in a network.

'Address' and **'Hwaddr'** shows the IP address and MAC address respectively. **Flags Mask** such as C for complete and M for permanent entries**.** The **'Iface'** col shows the interface name whose IP and MAC address are mapped.

b) To add and entry into the ARP table: arp -s address hw_addr

To delete an entry from the ARP table: arp -d address

```
abhishek@abhishek-VirtualBox:~$ arp -a
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
abhishek@abhishek-VirtualBox:~$ sudo arp -s 10.0.2.11 08:00:27:67:80:90
[sudo] password for abhishek:
abhishek@abhishek-VirtualBox:~$ sudo arp -s 10.0.2.12 08:00:27:67:80:90
abhishek@abhishek-VirtualBox:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.11                ether   08:00:27:67:80:90   CM                    enp0s3
_gateway                 ether   52:54:00:12:35:02   C                     enp0s3
10.0.2.12                ether   08:00:27:67:80:90   CM                    enp0s3
abhishek@abhishek-VirtualBox:~$ sudo arp -d 10.0.2.11
abhishek@abhishek-VirtualBox:~$ sudo arp -d 10.0.2.12
abhishek@abhishek-VirtualBox:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   52:54:00:12:35:02   C                     enp0s3
abhishek@abhishek-VirtualBox:~$ arp -a
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
abhishek@abhishek-VirtualBox:~$
```

c) No if the subnet is not connected, it will result in Network is unreachable error. ARP only works between devices in the same IP subnet.