Name: apeksha chavan
TE COMPS
A Batch
Roll No.: 2
UID: 2017130013

CEL 51, DCCN, Monsoon 2020
Lab 2: Basic Network Utilities

This lab introduces some basic network monitoring/analysis tools. There are a few exercises along the way. You should write up answers to the ***ping*** and ***traceroute*** exercises and turn them in next lab. (You should try out each tool, whether it is needed for an exercise or not!).

Prerequisite: Basic understanding of command line utilities of Linux Operating system.

Some Basic command line Networking utilities

Start with a few of the most basic command line tools. These commands are available on Unix, including Linux (and the first two, at least, are also for Windows). Some parameters or options might differ on different operating systems. Remember that you can use man <command> to get information about a command and its options.

ping — The command ping <host> sends a series of packets and expects to receieve a response to each packet. When a return packet is received, ping reports the round trip time (the time between sending the packet and receiving the response). Some routers and firewalls block ping requests, so you might get no reponse at all. Ping can be used to check whether a computer is up and running, to measure network delay time, and to check for dropped packets indicating network congestion. Note that <host> can be either a domain name or an IP address. By default, ping will send a packet every second indefinitely; stop it with Control-C

Network latency, specifically round trip time (RTT), can be measured using ping, which sends ICMP packets. The syntax for the command in

The syntax in Windows is:

```
ping [-n <count>] [-l <packetsize>] <hostname>
```

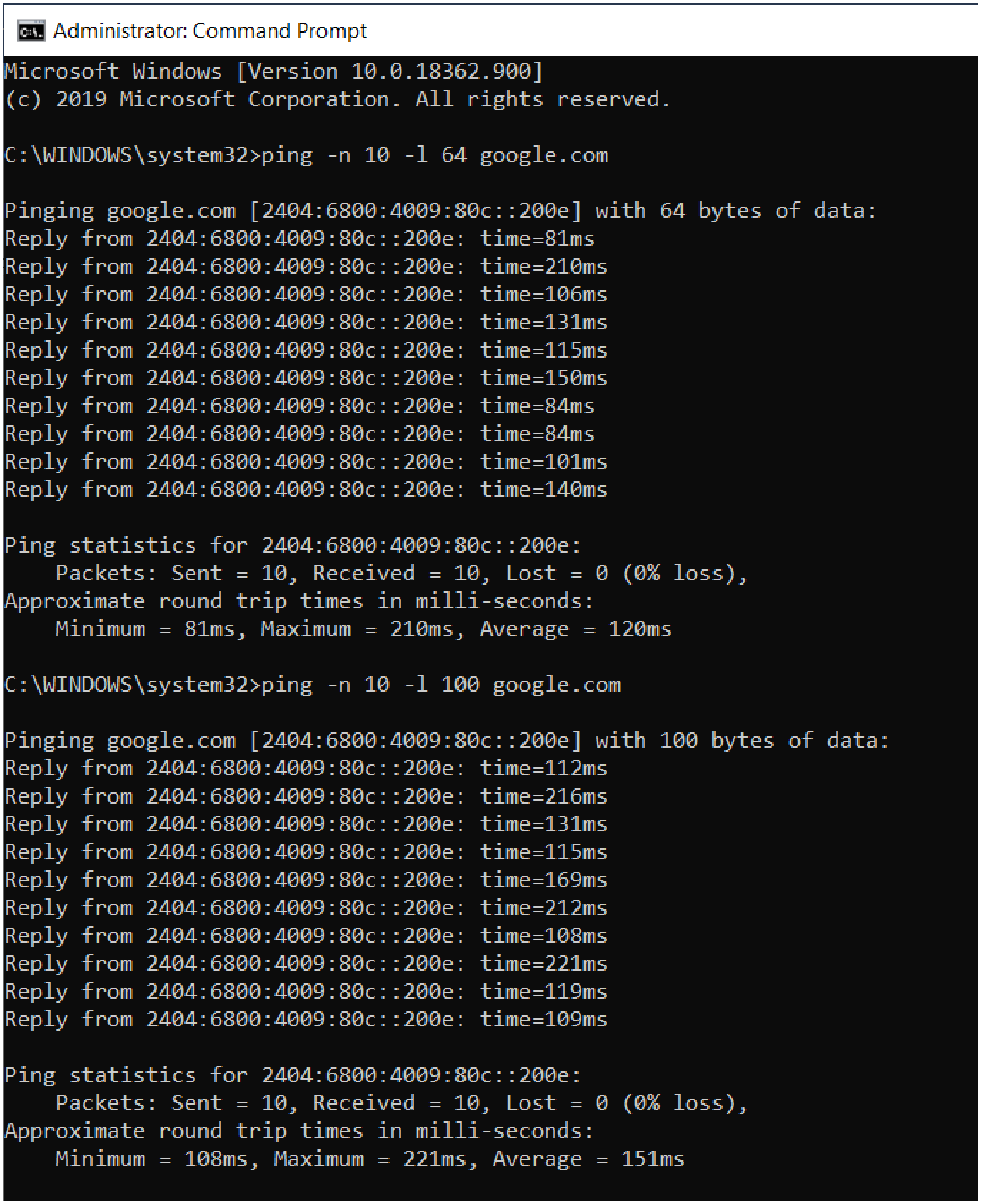
The default number of ICMP packets to send is either infinite (in Linux and Mac OS) or 4 (in Windows). The default packet size is either 64 bytes (in Linux) or 32 bytes (in Windows). You can specify either a hostname (e.g., spit.ac.in) or an IP address.

To save the output from ping to a file, include a greater than symbol and a file name at the end of the command. For example:

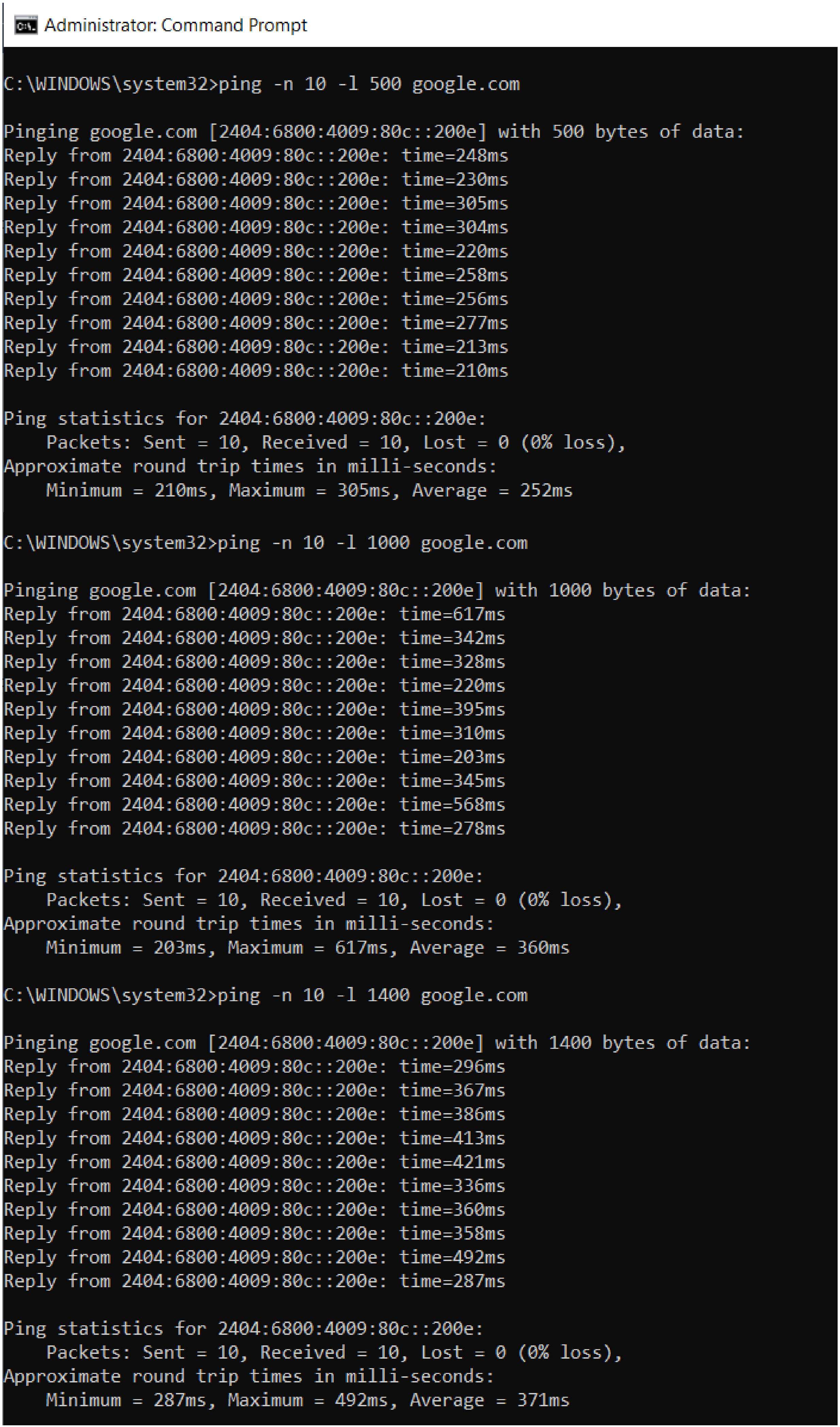
```
ping -c 10 google.com > ping_c10_s64_google.log
```

EXPERIMENTS WITH PING

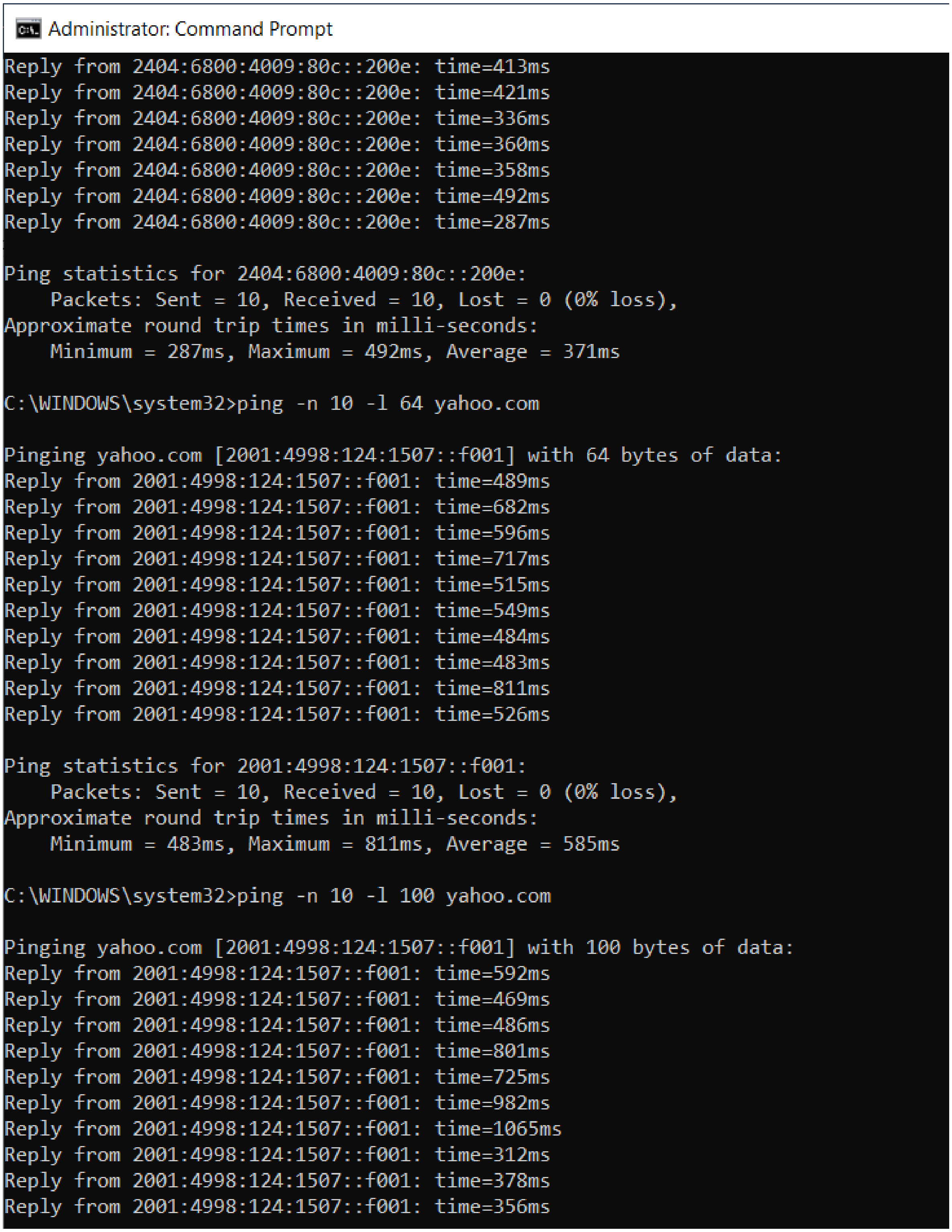
1. Ping the any hosts 10 times (i.e., packet count is 10) with a packet size of 64 bytes, 100 bytes, 500 bytes, 1000 bytes, 1400 bytes



```
Microsoft Windows [Version 10.0.18362.900]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping -n 10 -l 64 google.com

Pinging google.com [2404:6800:4009:80c::200e] with 64 bytes of data:
Reply from 2404:6800:4009:80c::200e: time=81ms
Reply from 2404:6800:4009:80c::200e: time=210ms
Reply from 2404:6800:4009:80c::200e: time=106ms
Reply from 2404:6800:4009:80c::200e: time=131ms
Reply from 2404:6800:4009:80c::200e: time=115ms
Reply from 2404:6800:4009:80c::200e: time=150ms
Reply from 2404:6800:4009:80c::200e: time=84ms
Reply from 2404:6800:4009:80c::200e: time=84ms
Reply from 2404:6800:4009:80c::200e: time=101ms
Reply from 2404:6800:4009:80c::200e: time=140ms

Ping statistics for 2404:6800:4009:80c::200e:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 81ms, Maximum = 210ms, Average = 120ms

C:\WINDOWS\system32>ping -n 10 -l 100 google.com

Pinging google.com [2404:6800:4009:80c::200e] with 100 bytes of data:
Reply from 2404:6800:4009:80c::200e: time=112ms
Reply from 2404:6800:4009:80c::200e: time=216ms
Reply from 2404:6800:4009:80c::200e: time=131ms
Reply from 2404:6800:4009:80c::200e: time=115ms
Reply from 2404:6800:4009:80c::200e: time=169ms
Reply from 2404:6800:4009:80c::200e: time=212ms
Reply from 2404:6800:4009:80c::200e: time=108ms
Reply from 2404:6800:4009:80c::200e: time=221ms
Reply from 2404:6800:4009:80c::200e: time=119ms
Reply from 2404:6800:4009:80c::200e: time=109ms

Ping statistics for 2404:6800:4009:80c::200e:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 108ms, Maximum = 221ms, Average = 151ms
```



```
C:\WINDOWS\system32>ping -n 10 -l 500 google.com

Pinging google.com [2404:6800:4009:80c::200e] with 500 bytes of data:
Reply from 2404:6800:4009:80c::200e: time=248ms
Reply from 2404:6800:4009:80c::200e: time=230ms
Reply from 2404:6800:4009:80c::200e: time=305ms
Reply from 2404:6800:4009:80c::200e: time=304ms
Reply from 2404:6800:4009:80c::200e: time=220ms
Reply from 2404:6800:4009:80c::200e: time=258ms
Reply from 2404:6800:4009:80c::200e: time=256ms
Reply from 2404:6800:4009:80c::200e: time=277ms
Reply from 2404:6800:4009:80c::200e: time=213ms
Reply from 2404:6800:4009:80c::200e: time=210ms

Ping statistics for 2404:6800:4009:80c::200e:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 210ms, Maximum = 305ms, Average = 252ms

C:\WINDOWS\system32>ping -n 10 -l 1000 google.com

Pinging google.com [2404:6800:4009:80c::200e] with 1000 bytes of data:
Reply from 2404:6800:4009:80c::200e: time=617ms
Reply from 2404:6800:4009:80c::200e: time=342ms
Reply from 2404:6800:4009:80c::200e: time=328ms
Reply from 2404:6800:4009:80c::200e: time=220ms
Reply from 2404:6800:4009:80c::200e: time=395ms
Reply from 2404:6800:4009:80c::200e: time=310ms
Reply from 2404:6800:4009:80c::200e: time=203ms
Reply from 2404:6800:4009:80c::200e: time=345ms
Reply from 2404:6800:4009:80c::200e: time=568ms
Reply from 2404:6800:4009:80c::200e: time=278ms

Ping statistics for 2404:6800:4009:80c::200e:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 203ms, Maximum = 617ms, Average = 360ms

C:\WINDOWS\system32>ping -n 10 -l 1400 google.com

Pinging google.com [2404:6800:4009:80c::200e] with 1400 bytes of data:
Reply from 2404:6800:4009:80c::200e: time=296ms
Reply from 2404:6800:4009:80c::200e: time=367ms
Reply from 2404:6800:4009:80c::200e: time=386ms
Reply from 2404:6800:4009:80c::200e: time=413ms
Reply from 2404:6800:4009:80c::200e: time=421ms
Reply from 2404:6800:4009:80c::200e: time=336ms
Reply from 2404:6800:4009:80c::200e: time=360ms
Reply from 2404:6800:4009:80c::200e: time=358ms
Reply from 2404:6800:4009:80c::200e: time=492ms
Reply from 2404:6800:4009:80c::200e: time=287ms

Ping statistics for 2404:6800:4009:80c::200e:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 287ms, Maximum = 492ms, Average = 371ms
```



Administrator: Command Prompt

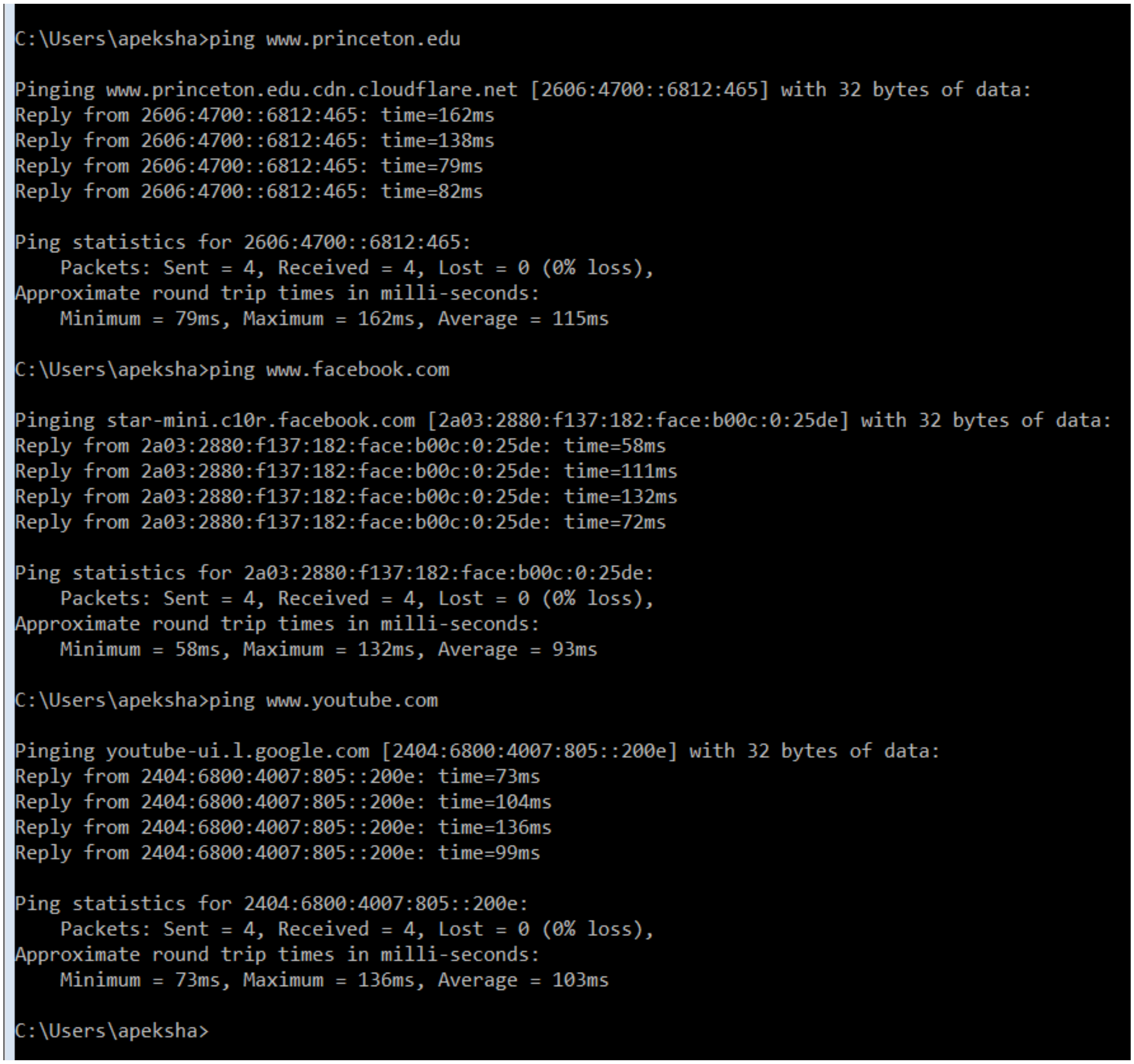
```
Reply from 2404:6800:4009:80c::200e: time=413ms
Reply from 2404:6800:4009:80c::200e: time=421ms
Reply from 2404:6800:4009:80c::200e: time=336ms
Reply from 2404:6800:4009:80c::200e: time=360ms
Reply from 2404:6800:4009:80c::200e: time=358ms
Reply from 2404:6800:4009:80c::200e: time=492ms
Reply from 2404:6800:4009:80c::200e: time=287ms

Ping statistics for 2404:6800:4009:80c::200e:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 287ms, Maximum = 492ms, Average = 371ms

C:\WINDOWS\system32>ping -n 10 -l 64 yahoo.com

Pinging yahoo.com [2001:4998:124:1507::f001] with 64 bytes of data:
Reply from 2001:4998:124:1507::f001: time=489ms
Reply from 2001:4998:124:1507::f001: time=682ms
Reply from 2001:4998:124:1507::f001: time=596ms
Reply from 2001:4998:124:1507::f001: time=717ms
Reply from 2001:4998:124:1507::f001: time=515ms
Reply from 2001:4998:124:1507::f001: time=549ms
Reply from 2001:4998:124:1507::f001: time=484ms
Reply from 2001:4998:124:1507::f001: time=483ms
Reply from 2001:4998:124:1507::f001: time=811ms
Reply from 2001:4998:124:1507::f001: time=526ms

Ping statistics for 2001:4998:124:1507::f001:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 483ms, Maximum = 811ms, Average = 585ms

C:\WINDOWS\system32>ping -n 10 -l 100 yahoo.com

Pinging yahoo.com [2001:4998:124:1507::f001] with 100 bytes of data:
Reply from 2001:4998:124:1507::f001: time=592ms
Reply from 2001:4998:124:1507::f001: time=469ms
Reply from 2001:4998:124:1507::f001: time=486ms
Reply from 2001:4998:124:1507::f001: time=801ms
Reply from 2001:4998:124:1507::f001: time=725ms
Reply from 2001:4998:124:1507::f001: time=982ms
Reply from 2001:4998:124:1507::f001: time=1065ms
Reply from 2001:4998:124:1507::f001: time=312ms
Reply from 2001:4998:124:1507::f001: time=378ms
Reply from 2001:4998:124:1507::f001: time=356ms
```

Questions About Latency

Now look at the results you gathered and answer the following questions about latency. Store your answers in a file named ping.txt.

1. Does the average RTT vary between different hosts? What aspects of latency (transmit, propagation, and queueing delay) might impact this and why?

Ans:



```
C:\Users\apeksha>ping www.princeton.edu

Pinging www.princeton.edu.cdn.cloudflare.net [2606:4700::6812:465] with 32 bytes of data:
Reply from 2606:4700::6812:465: time=162ms
Reply from 2606:4700::6812:465: time=138ms
Reply from 2606:4700::6812:465: time=79ms
Reply from 2606:4700::6812:465: time=82ms

Ping statistics for 2606:4700::6812:465:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 79ms, Maximum = 162ms, Average = 115ms

C:\Users\apeksha>ping www.facebook.com

Pinging star-mini.c10r.facebook.com [2a03:2880:f137:182:face:b00c:0:25de] with 32 bytes of data:
Reply from 2a03:2880:f137:182:face:b00c:0:25de: time=58ms
Reply from 2a03:2880:f137:182:face:b00c:0:25de: time=111ms
Reply from 2a03:2880:f137:182:face:b00c:0:25de: time=132ms
Reply from 2a03:2880:f137:182:face:b00c:0:25de: time=72ms

Ping statistics for 2a03:2880:f137:182:face:b00c:0:25de:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 58ms, Maximum = 132ms, Average = 93ms

C:\Users\apeksha>ping www.youtube.com

Pinging youtube-ui.l.google.com [2404:6800:4007:805::200e] with 32 bytes of data:
Reply from 2404:6800:4007:805::200e: time=73ms
Reply from 2404:6800:4007:805::200e: time=104ms
Reply from 2404:6800:4007:805::200e: time=136ms
Reply from 2404:6800:4007:805::200e: time=99ms

Ping statistics for 2404:6800:4007:805::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 73ms, Maximum = 136ms, Average = 103ms

C:\Users\apeksha>
```

Yes, the average RTT varies between different hosts.

Round Trip Time (RTT) is the length time it takes for a data packet to be sent to a destination plus the time it takes for an acknowledgment of that packet to be received back at the origin.
The RTT between a network and server can be determined by using the ping command.
Network delay is a design and performance characteristic of a telecommunications network. It specifies the latency for a bit of data to travel across the network from one communication endpoint to another. It is typically measured in multiples or fractions of a second. Delay may differ slightly, depending on the location of the specific pair of communicating endpoints. Engineers usually report both the maximum and average delay, and they divide the delay into several parts:

- Processing delay – time it takes a router to process the packet header
- Queuing delay – time the packet spends in routing queues
- Transmission delay – time it takes to push the packet's bits onto the link
- Propagation delay – time for a signal to reach its destination,

Propagation delay is usually the dominant component in RTT. It ranges from a few milliseconds to hundreds of milliseconds depending on whether the endpoints are separated by a few kilometers or by an entire ocean.

2. Does the average RTT vary with different packet sizes? What aspects of latency (transmit, propagation, and queueing delay) might impact this and why?

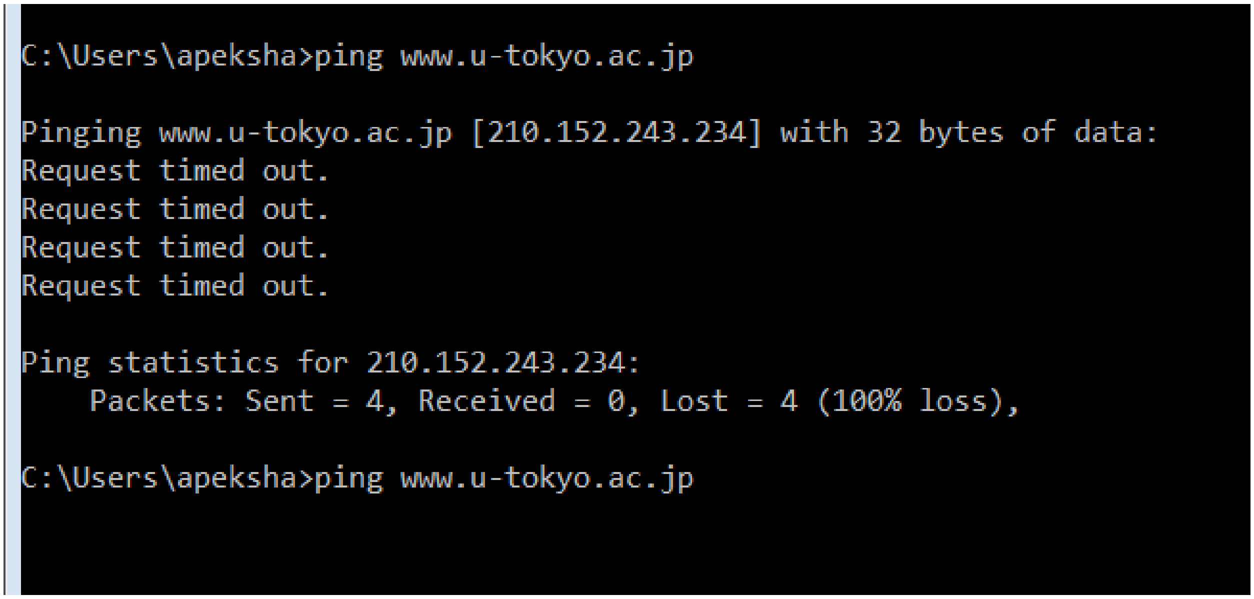
Ans.: The observational results match with theoretical results. There is an increase in latency with increase in packet size due to transmission delay and propagation delay.

RTT depends on the network infrastructure, the distance between nodes, network conditions, and packet size. Hence, RTT increases with increase in packet size. Packet size and payload compressibility have a significant impact on RTT for slower links.
Transmission delay depends on size of packet. So, transmission delay might have an impact on this.

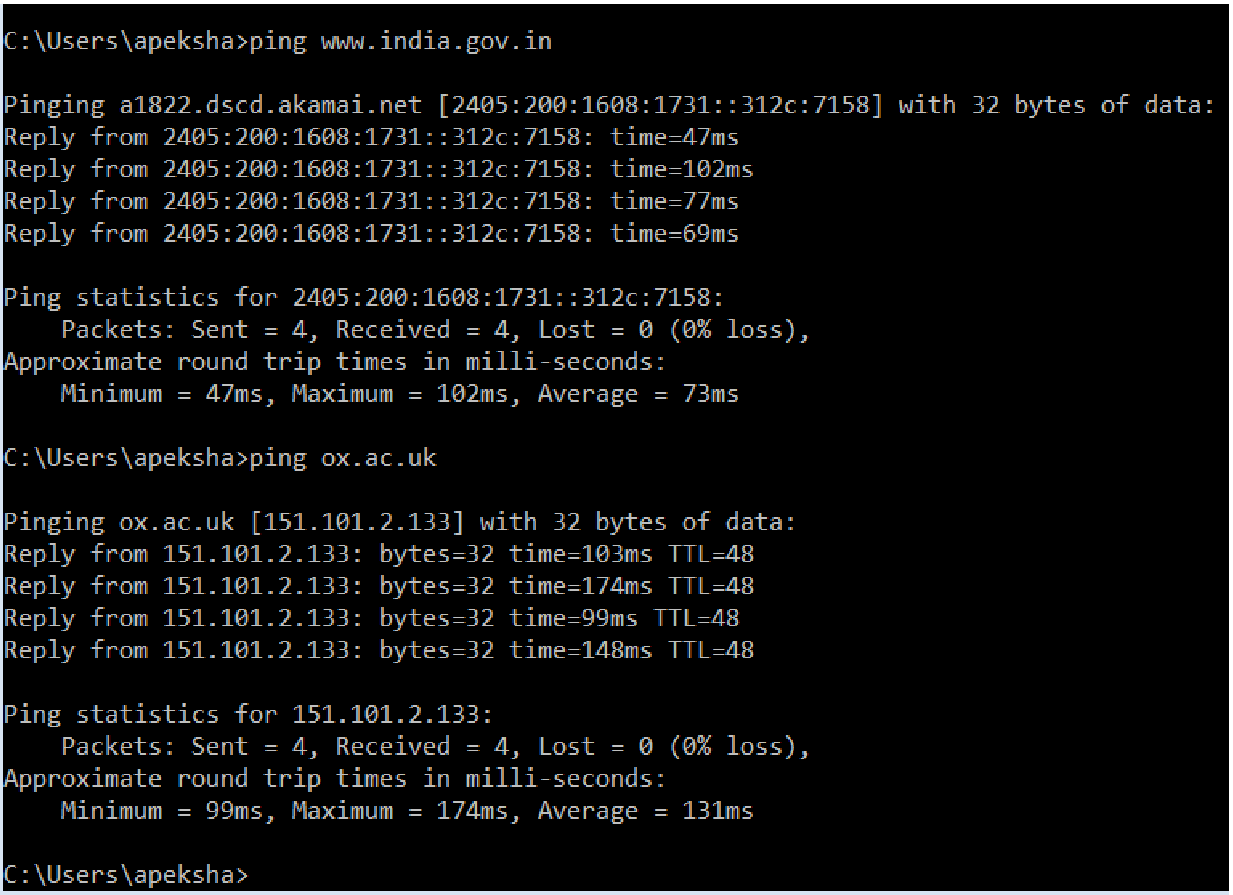
<u>Exercise 1</u>: Experiment with ping to find the round trip times to a variety of destinations. Write up any interesting observations, including in particular how the round trip time compares to the physical distance. Here are few places from who to get replies: www.uw.edu, www.cornell.edu, berkeley.edu, www.uchicago.edu, www.ox.ac.uk (England), (Japan).

Ans.:

The website based in India has an average RTT of 5ms while the one in the UK has an average RTT of 8ms. This demonstrates that with increase in physical distance the RTT increases.
Increase in physical distance causes an increase in propagation delay.

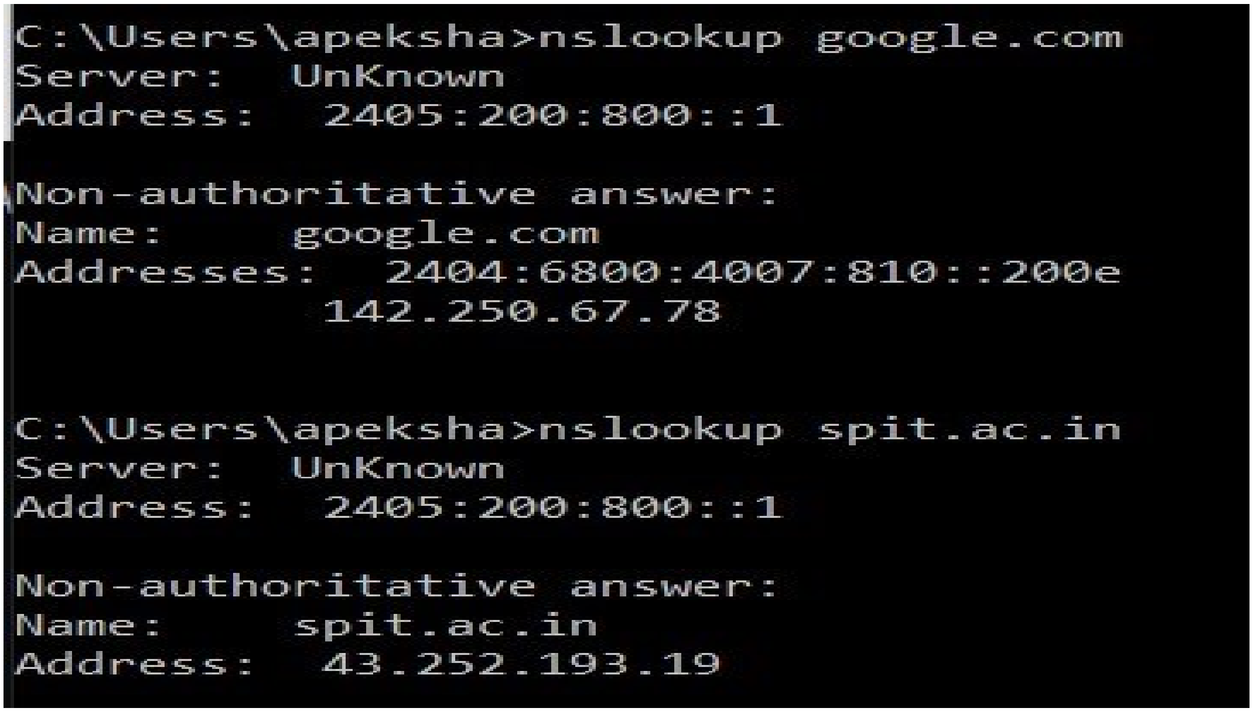


```
C:\Users\apeksha>ping www.u-tokyo.ac.jp

Pinging www.u-tokyo.ac.jp [210.152.243.234] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 210.152.243.234:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\apeksha>ping www.u-tokyo.ac.jp
```

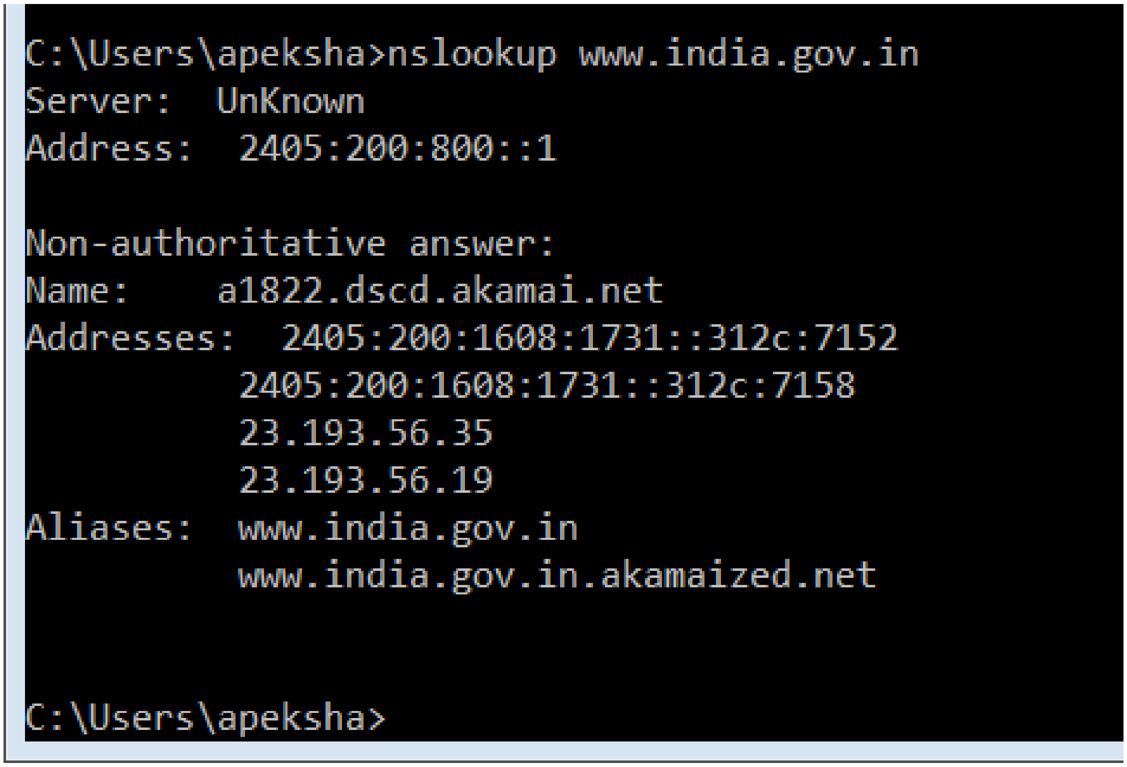


```
C:\Users\apeksha>ping www.india.gov.in

Pinging a1822.dscd.akamai.net [2405:200:1608:1731::312c:7158] with 32 bytes of data:
Reply from 2405:200:1608:1731::312c:7158: time=47ms
Reply from 2405:200:1608:1731::312c:7158: time=102ms
Reply from 2405:200:1608:1731::312c:7158: time=77ms
Reply from 2405:200:1608:1731::312c:7158: time=69ms

Ping statistics for 2405:200:1608:1731::312c:7158:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 47ms, Maximum = 102ms, Average = 73ms

C:\Users\apeksha>ping ox.ac.uk

Pinging ox.ac.uk [151.101.2.133] with 32 bytes of data:
Reply from 151.101.2.133: bytes=32 time=103ms TTL=48
Reply from 151.101.2.133: bytes=32 time=174ms TTL=48
Reply from 151.101.2.133: bytes=32 time=99ms TTL=48
Reply from 151.101.2.133: bytes=32 time=148ms TTL=48

Ping statistics for 151.101.2.133:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 99ms, Maximum = 174ms, Average = 131ms

C:\Users\apeksha>
```

nslookup — The command nslookup <host> will do a DNS query to find and report the IP address (or addresses) for a domain name or the domain name corresponding to an IP address. To do this, it contacts a "DNS server." Default DNS servers are part of a computer's network configuration. (For a static IP address in Linux, they are configured in the file /etc/network/interfaces that you encountered in the last lab.) You can specify a different DNS server to be used by nslookup by adding the server name or IP address to the command: nslookup <host> <server>

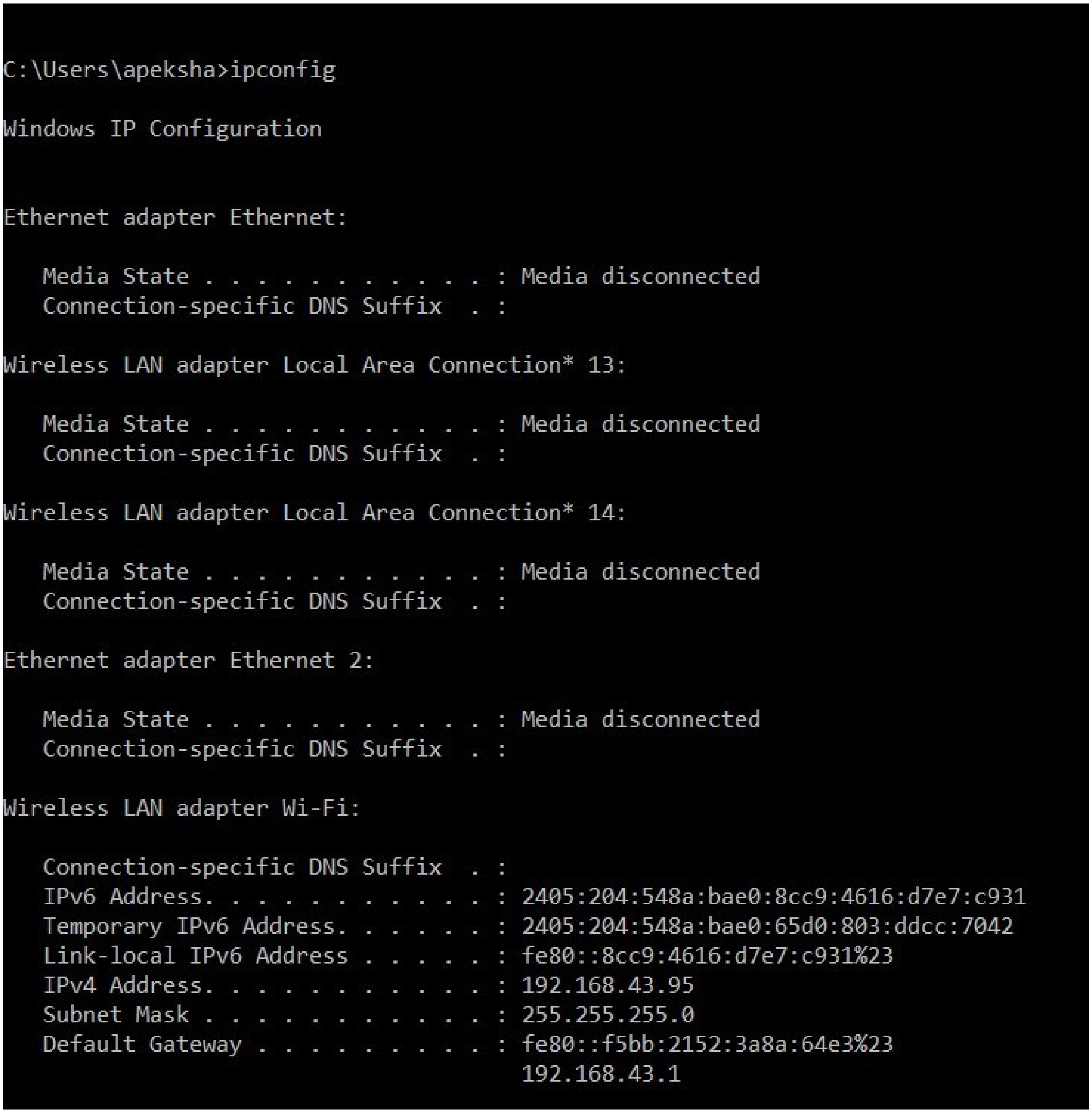


```
C:\Users\apeksha>nslookup google.com
Server:  UnKnown
Address:  2405:200:800::1

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4007:810::200e
          142.250.67.78


C:\Users\apeksha>nslookup spit.ac.in
Server:  UnKnown
Address:  2405:200:800::1

Non-authoritative answer:
Name:    spit.ac.in
Address:  43.252.193.19
```



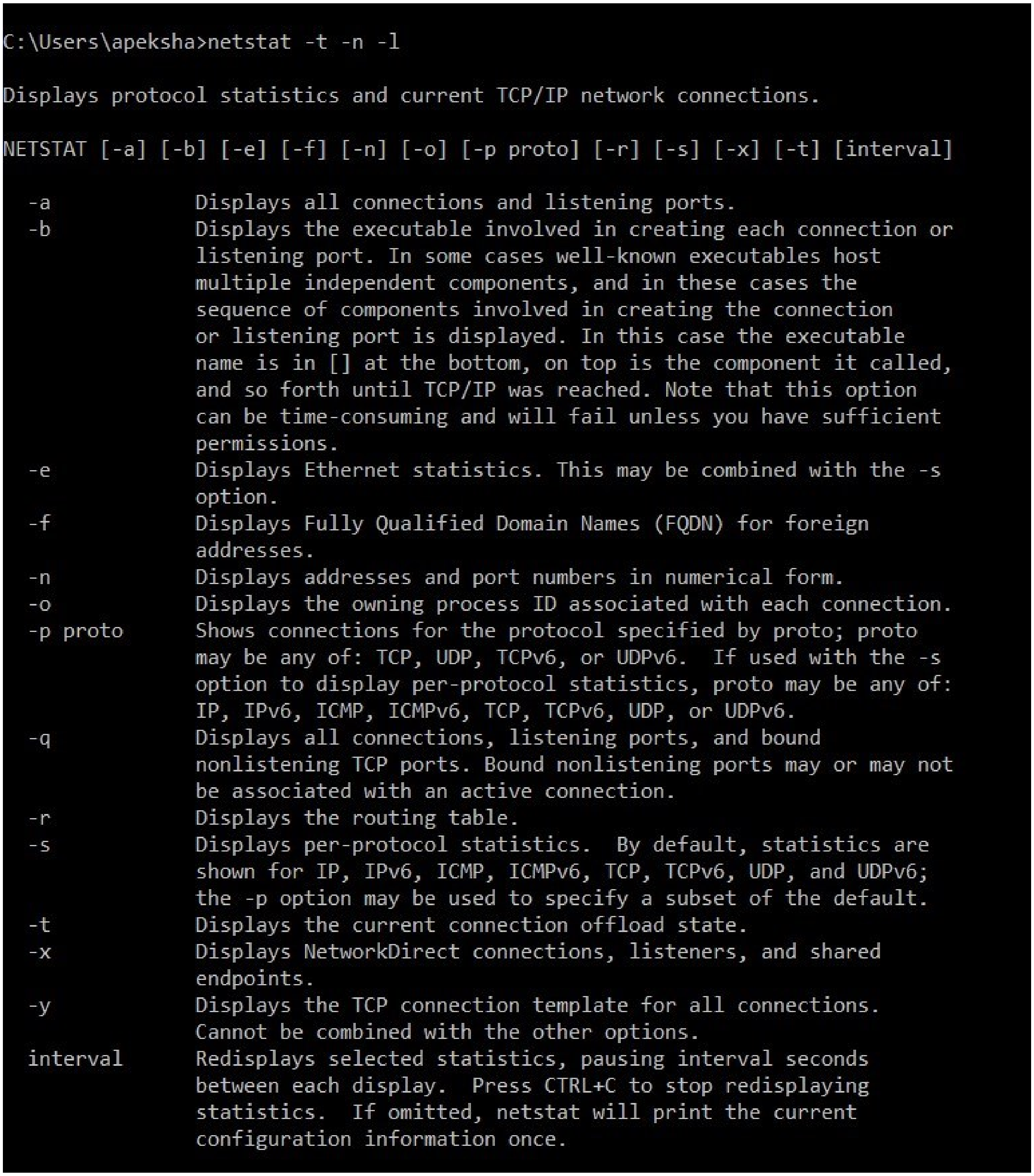
```
C:\Users\apeksha>nslookup www.india.gov.in
Server:  UnKnown
Address:  2405:200:800::1

Non-authoritative answer:
Name:    a1822.dscd.akamai.net
Addresses:  2405:200:1608:1731::312c:7152
          2405:200:1608:1731::312c:7158
          23.193.56.35
          23.193.56.19
Aliases:  www.india.gov.in
          www.india.gov.in.akamaized.net


C:\Users\apeksha>
```

ifconfig — You used ifconfig in the previous lab. When used with no parameters, ifconfig reports some information about the computer's network interfaces. This usually includes lo which stands for localhost; it can be used for communication between programs running on the same computer. Linux often has an interface named eth0, which is the first ethernet card. The information is different on Mac OS and Linux, but includes the IP or "inet" address and ethernet or "hardware" address for an ethernet card. On Linux, you get the number of packets received (RX) and sent (TX), as well as the number of bytes transmitted and received. (A better place to monitor network bytes on our Linux computers is in the GUI program System Monitor, if it is installed!!!.)



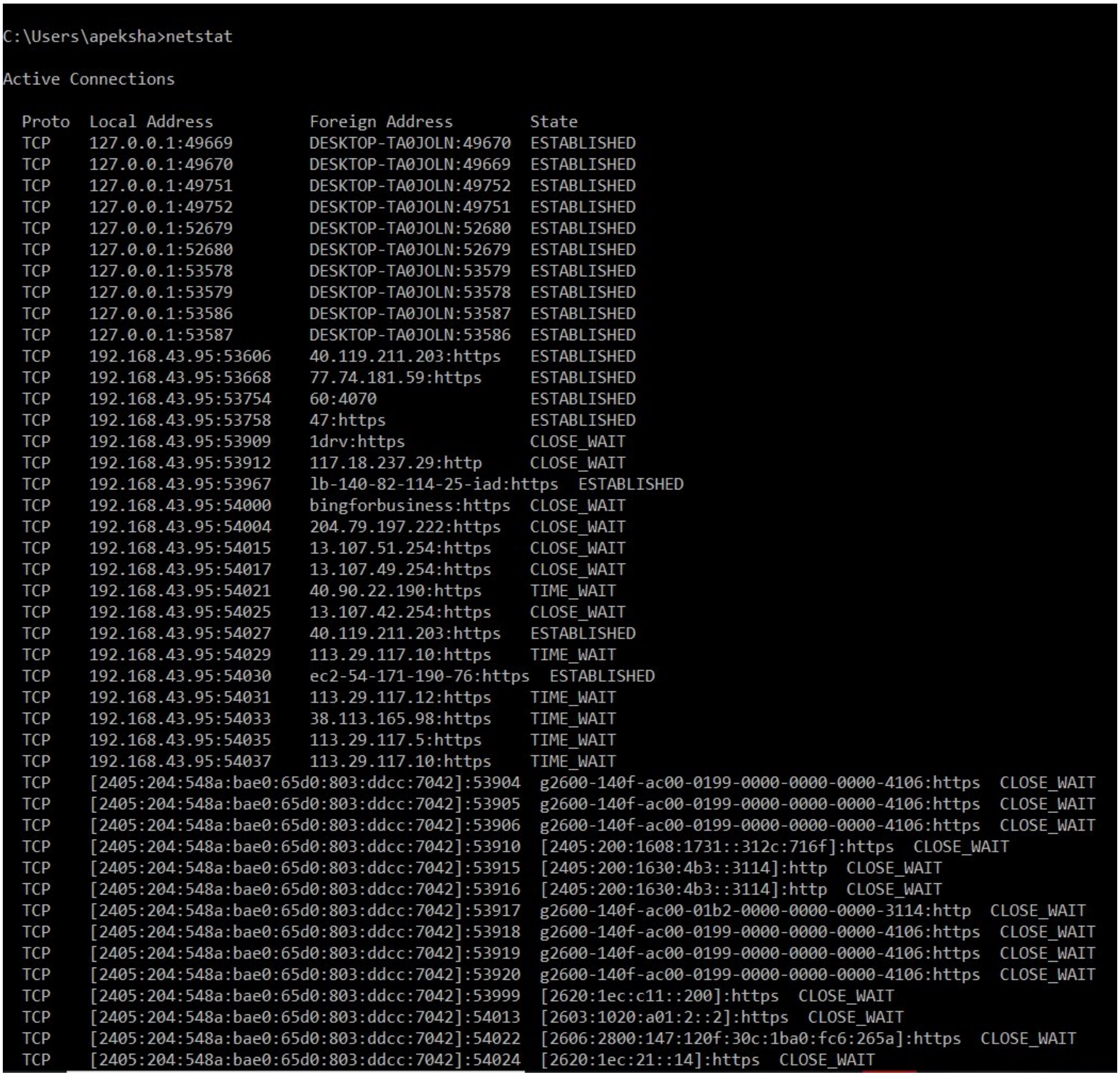
```
C:\Users\apeksha>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 13:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 14:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2405:204:548a:bae0:8cc9:4616:d7e7:c931
   Temporary IPv6 Address. . . . . . : 2405:204:548a:bae0:65d0:803:ddcc:7042
   Link-local IPv6 Address . . . . . : fe80::8cc9:4616:d7e7:c931%23
   IPv4 Address. . . . . . . . . . . : 192.168.43.95
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::f5bb:2152:3a8a:64e3%23
                                       192.168.43.1
```

netstat — The netstat command gives information about network connections. I often use netstat -t -n which lists currently open TCP connections (that's the "-t" option) by IP address rather than domain name (that's the "-n" option). Add the option "-l" (lower case ell) to list listening sockets, that is sockets that have been opened by server programs to wait for connection requests from clients: netstat -t -n -l. (On Mac, use netstat -p tcp to list tcp connections, and add "-a" to include listening sockets in the list.)

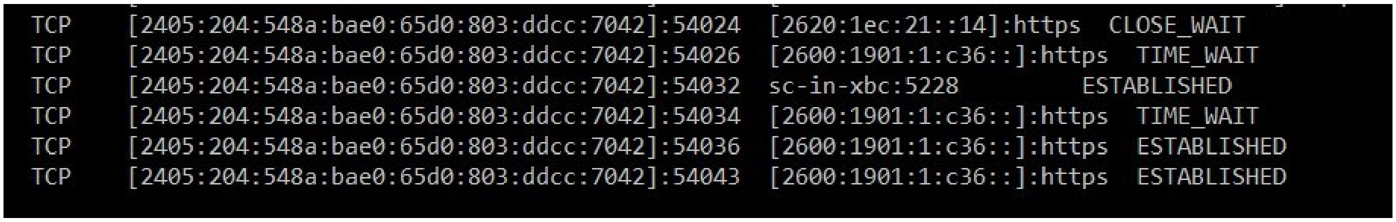


```
C:\Users\apeksha>netstat -t -n -l

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]

  -a            Displays all connections and listening ports.
  -b            Displays the executable involved in creating each connection or
                listening port. In some cases well-known executables host
                multiple independent components, and in these cases the
                sequence of components involved in creating the connection
                or listening port is displayed. In this case the executable
                name is in [] at the bottom, on top is the component it called,
                and so forth until TCP/IP was reached. Note that this option
                can be time-consuming and will fail unless you have sufficient
                permissions.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -f            Displays Fully Qualified Domain Names (FQDN) for foreign
                addresses.
  -n            Displays addresses and port numbers in numerical form.
  -o            Displays the owning process ID associated with each connection.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                option to display per-protocol statistics, proto may be any of:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -q            Displays all connections, listening ports, and bound
                nonlistening TCP ports. Bound nonlistening ports may or may not
                be associated with an active connection.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                the -p option may be used to specify a subset of the default.
  -t            Displays the current connection offload state.
  -x            Displays NetworkDirect connections, listeners, and shared
                endpoints.
  -y            Displays the TCP connection template for all connections.
                Cannot be combined with the other options.
  interval      Redisplays selected statistics, pausing interval seconds
                between each display.  Press CTRL+C to stop redisplaying
                statistics.  If omitted, netstat will print the current
                configuration information once.
```

The **netstat command** displays that what is the network status and protocol statistics.

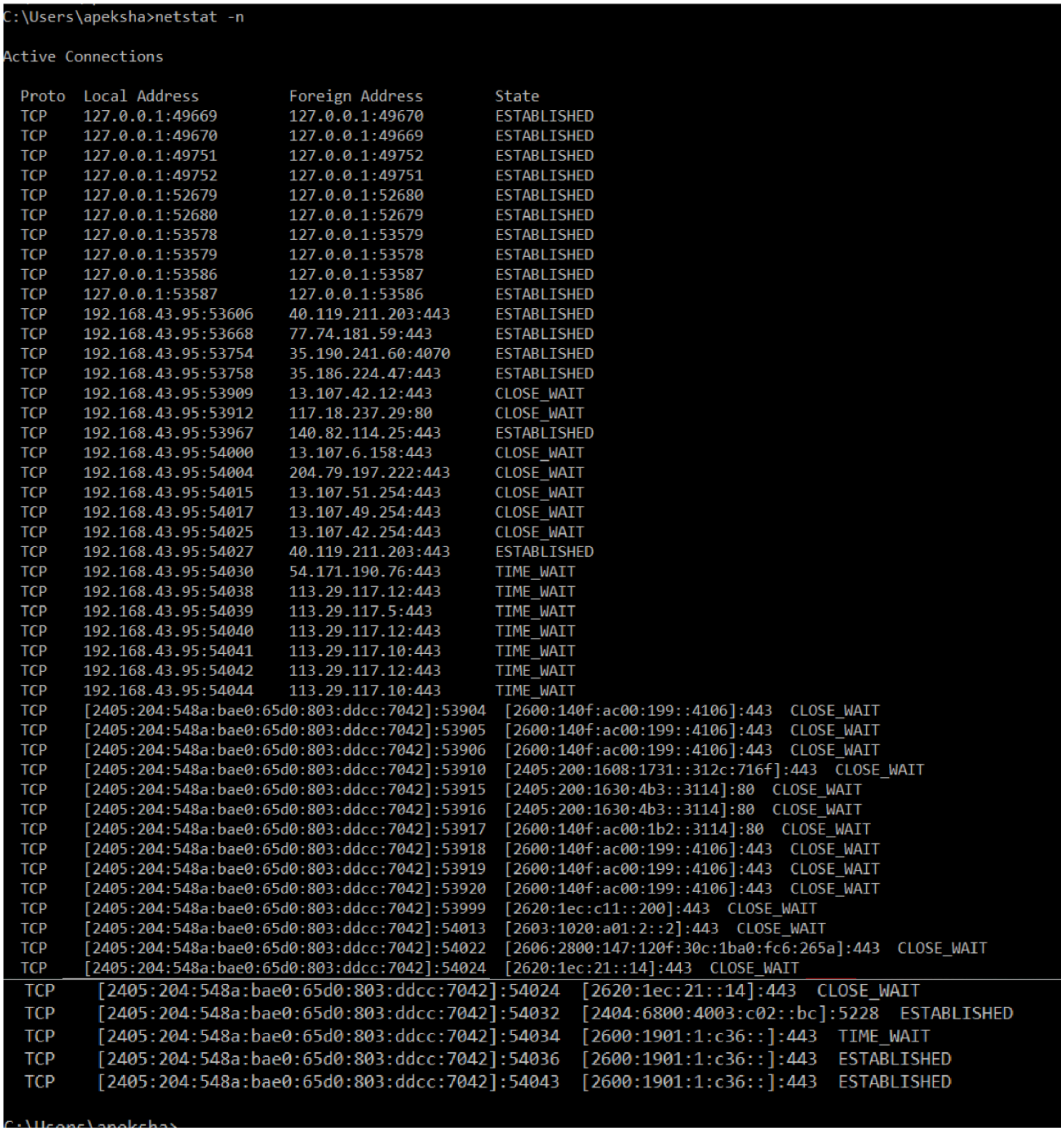


```
C:\Users\apeksha>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49669        DESKTOP-TA0JOLN:49670  ESTABLISHED
  TCP    127.0.0.1:49670        DESKTOP-TA0JOLN:49669  ESTABLISHED
  TCP    127.0.0.1:49751        DESKTOP-TA0JOLN:49752  ESTABLISHED
  TCP    127.0.0.1:49752        DESKTOP-TA0JOLN:49751  ESTABLISHED
  TCP    127.0.0.1:52679        DESKTOP-TA0JOLN:52680  ESTABLISHED
  TCP    127.0.0.1:52680        DESKTOP-TA0JOLN:52679  ESTABLISHED
  TCP    127.0.0.1:53578        DESKTOP-TA0JOLN:53579  ESTABLISHED
  TCP    127.0.0.1:53579        DESKTOP-TA0JOLN:53578  ESTABLISHED
  TCP    127.0.0.1:53586        DESKTOP-TA0JOLN:53587  ESTABLISHED
  TCP    127.0.0.1:53587        DESKTOP-TA0JOLN:53586  ESTABLISHED
  TCP    192.168.43.95:53606    40.119.211.203:https   ESTABLISHED
  TCP    192.168.43.95:53668    77.74.181.59:https     ESTABLISHED
  TCP    192.168.43.95:53754    60:4070                ESTABLISHED
  TCP    192.168.43.95:53758    47:https               ESTABLISHED
  TCP    192.168.43.95:53909    1drv:https             CLOSE_WAIT
  TCP    192.168.43.95:53912    117.18.237.29:http     CLOSE_WAIT
  TCP    192.168.43.95:53967    lb-140-82-114-25-iad:https  ESTABLISHED
  TCP    192.168.43.95:54000    bingforbusiness:https  CLOSE_WAIT
  TCP    192.168.43.95:54004    204.79.197.222:https   CLOSE_WAIT
  TCP    192.168.43.95:54015    13.107.51.254:https    CLOSE_WAIT
  TCP    192.168.43.95:54017    13.107.49.254:https    CLOSE_WAIT
  TCP    192.168.43.95:54021    40.90.22.190:https     TIME_WAIT
  TCP    192.168.43.95:54025    13.107.42.254:https    CLOSE_WAIT
  TCP    192.168.43.95:54027    40.119.211.203:https   ESTABLISHED
  TCP    192.168.43.95:54029    113.29.117.10:https    TIME_WAIT
  TCP    192.168.43.95:54030    ec2-54-171-190-76:https  ESTABLISHED
  TCP    192.168.43.95:54031    113.29.117.12:https    TIME_WAIT
  TCP    192.168.43.95:54033    38.113.165.98:https    TIME_WAIT
  TCP    192.168.43.95:54035    113.29.117.5:https     TIME_WAIT
  TCP    192.168.43.95:54037    113.29.117.10:https    TIME_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53904  g2600-140f-ac00-0199-0000-0000-0000-4106:https  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53905  g2600-140f-ac00-0199-0000-0000-0000-4106:https  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53906  g2600-140f-ac00-0199-0000-0000-0000-4106:https  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53910  [2405:200:1608:1731::312c:716f]:https  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53915  [2405:200:1630:4b3::3114]:http  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53916  [2405:200:1630:4b3::3114]:http  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53917  g2600-140f-ac00-01b2-0000-0000-0000-3114:http  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53918  g2600-140f-ac00-0199-0000-0000-0000-4106:https  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53919  g2600-140f-ac00-0199-0000-0000-0000-4106:https  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53920  g2600-140f-ac00-0199-0000-0000-0000-4106:https  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53999  [2620:1ec:c11::200]:https  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:54013  [2603:1020:a01:2::2]:https  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:54022  [2606:2800:147:120f:30c:1ba0:fc6:265a]:https  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:54024  [2620:1ec:21::14]:https  CLOSE_WAIT
```



```
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:54024  [2620:1ec:21::14]:https  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:54026  [2600:1901:1:c36::]:https  TIME_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:54032  sc-in-xbc:5228         ESTABLISHED
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:54034  [2600:1901:1:c36::]:https  TIME_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:54036  [2600:1901:1:c36::]:https  ESTABLISHED
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:54043  [2600:1901:1:c36::]:https  ESTABLISHED
```

Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names.



```
C:\Users\apeksha>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49669        127.0.0.1:49670        ESTABLISHED
  TCP    127.0.0.1:49670        127.0.0.1:49669        ESTABLISHED
  TCP    127.0.0.1:49751        127.0.0.1:49752        ESTABLISHED
  TCP    127.0.0.1:49752        127.0.0.1:49751        ESTABLISHED
  TCP    127.0.0.1:52679        127.0.0.1:52680        ESTABLISHED
  TCP    127.0.0.1:52680        127.0.0.1:52679        ESTABLISHED
  TCP    127.0.0.1:53578        127.0.0.1:53579        ESTABLISHED
  TCP    127.0.0.1:53579        127.0.0.1:53578        ESTABLISHED
  TCP    127.0.0.1:53586        127.0.0.1:53587        ESTABLISHED
  TCP    127.0.0.1:53587        127.0.0.1:53586        ESTABLISHED
  TCP    192.168.43.95:53606    40.119.211.203:443     ESTABLISHED
  TCP    192.168.43.95:53668    77.74.181.59:443       ESTABLISHED
  TCP    192.168.43.95:53754    35.190.241.60:4070     ESTABLISHED
  TCP    192.168.43.95:53758    35.186.224.47:443      ESTABLISHED
  TCP    192.168.43.95:53909    13.107.42.12:443       CLOSE_WAIT
  TCP    192.168.43.95:53912    117.18.237.29:80       CLOSE_WAIT
  TCP    192.168.43.95:53967    140.82.114.25:443      ESTABLISHED
  TCP    192.168.43.95:54000    13.107.6.158:443       CLOSE_WAIT
  TCP    192.168.43.95:54004    204.79.197.222:443     CLOSE_WAIT
  TCP    192.168.43.95:54015    13.107.51.254:443      CLOSE_WAIT
  TCP    192.168.43.95:54017    13.107.49.254:443      CLOSE_WAIT
  TCP    192.168.43.95:54025    13.107.42.254:443      CLOSE_WAIT
  TCP    192.168.43.95:54027    40.119.211.203:443     ESTABLISHED
  TCP    192.168.43.95:54030    54.171.190.76:443      TIME_WAIT
  TCP    192.168.43.95:54038    113.29.117.12:443      TIME_WAIT
  TCP    192.168.43.95:54039    113.29.117.5:443       TIME_WAIT
  TCP    192.168.43.95:54040    113.29.117.12:443      TIME_WAIT
  TCP    192.168.43.95:54041    113.29.117.10:443      TIME_WAIT
  TCP    192.168.43.95:54042    113.29.117.12:443      TIME_WAIT
  TCP    192.168.43.95:54044    113.29.117.10:443      TIME_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53904  [2600:140f:ac00:199::4106]:443  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53905  [2600:140f:ac00:199::4106]:443  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53906  [2600:140f:ac00:199::4106]:443  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53910  [2405:200:1608:1731::312c:716f]:443  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53915  [2405:200:1630:4b3::3114]:80  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53916  [2405:200:1630:4b3::3114]:80  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53917  [2600:140f:ac00:1b2::3114]:80  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53918  [2600:140f:ac00:199::4106]:443  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53919  [2600:140f:ac00:199::4106]:443  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53920  [2600:140f:ac00:199::4106]:443  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:53999  [2620:1ec:c11::200]:443  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:54013  [2603:1020:a01:2::2]:443  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:54022  [2606:2800:147:120f:30c:1ba0:fc6:265a]:443  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:54024  [2620:1ec:21::14]:443  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:54024  [2620:1ec:21::14]:443  CLOSE_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:54032  [2404:6800:4003:c02::bc]:5228  ESTABLISHED
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:54034  [2600:1901:1:c36::]:443  TIME_WAIT
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:54036  [2600:1901:1:c36::]:443  ESTABLISHED
  TCP    [2405:204:548a:bae0:65d0:803:ddcc:7042]:54043  [2600:1901:1:c36::]:443  ESTABLISHED

C:\Users\apeksha>
```

telnet — Telnet is an old program for remote login. It's not used so much for that any more, since it has no security features. But basically, all it does is open a connection to a server and allow server and client to send lines of plain text to each other. It can be used to check that it's possible to connect to a server and, if the server communicates in plain text, even to interact with the server by hand. Since the Web uses a plain text protocol, you can use telnet to connect to a web client and play the part of the web browser. I will suggest that you to do this with your own web server when you write it, but you might want to try it now. When you use telnet in this way, you need to specify both the host and the port number to which you want to connect: telent <host> <port>. For example, to connect to the web server on www.spit.ac.in: telnet spit.ac.in 80

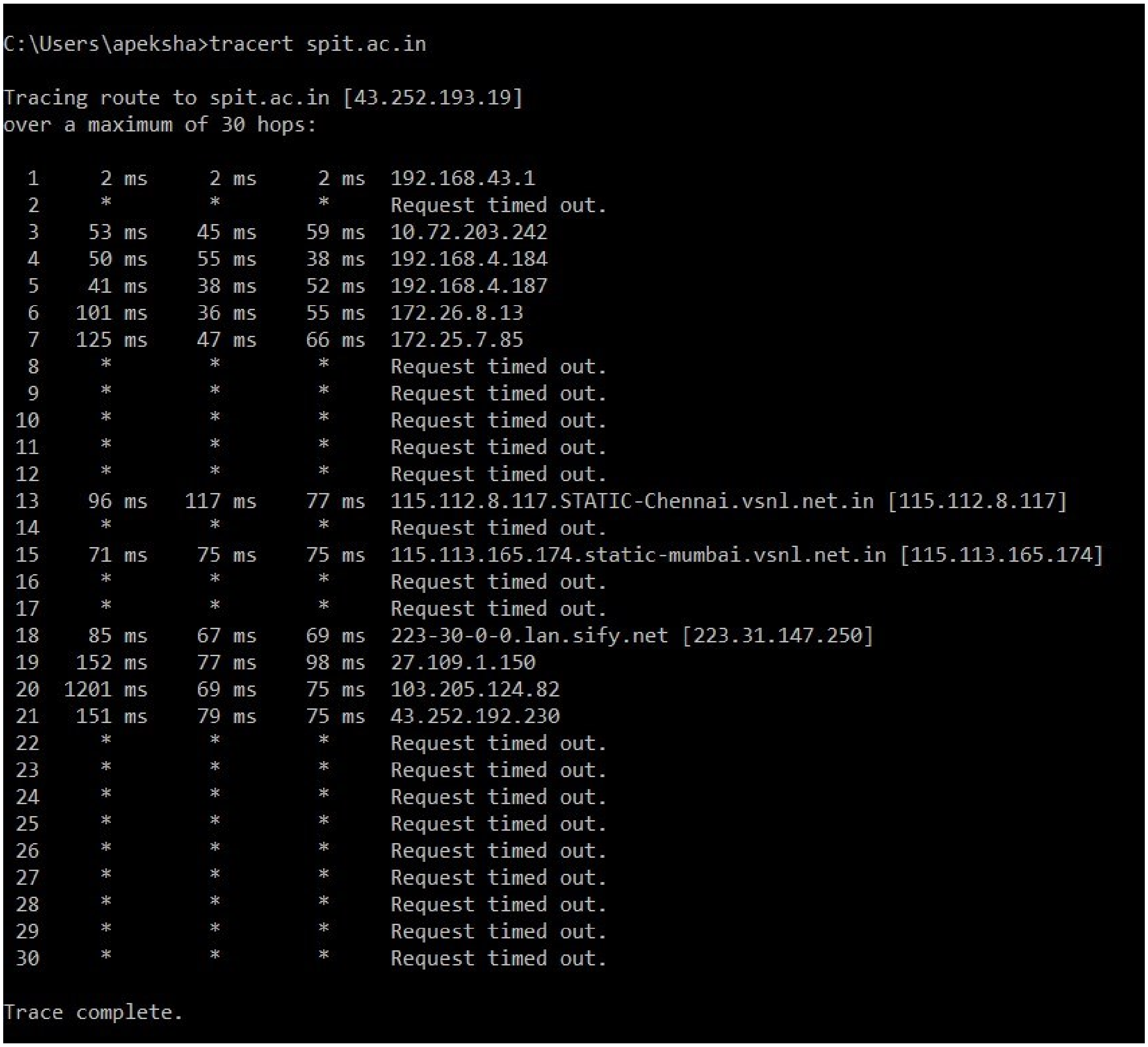
traceroute — Traceroute is discussed in man utility. The command traceroute <host> will show routers encountered by packets on their way from your computer to a specified <host>. For each n = 1, 2, 3,..., traceroute sends a packet with "time-to-live" (ttl) equal to n. Every time a router forwards a packet, it decreases the ttl of the packet by one. If the ttl drops to zero, the router discards the packet and sends an error message back to the sender of the packet. (Again, as with ping, the packets might be blocked or might not even be sent, so that the error messages will never be received.) The sender gets the identity of the router from the source of the error message. Traceroute will send packets until n reaches some set upper bound or until a packet actually gets through to the destination. It actually does this three times for each n. In this way, it identifies routers that are one step, two steps, three steps, ... away from the source computer. A packet for which no response is received is indicated in the output as a *.

Traceroute is installed on the computers. If was not installed in your virtual server last week, but you can install it with the command sudo apt-get install traceroute.

The syntax in Windows is:

```
tracert <hostname>
```

You can specify either a hostname (e.g., cs.iitb.ac.in) or an IP address (e.g., 128.105.2.6).

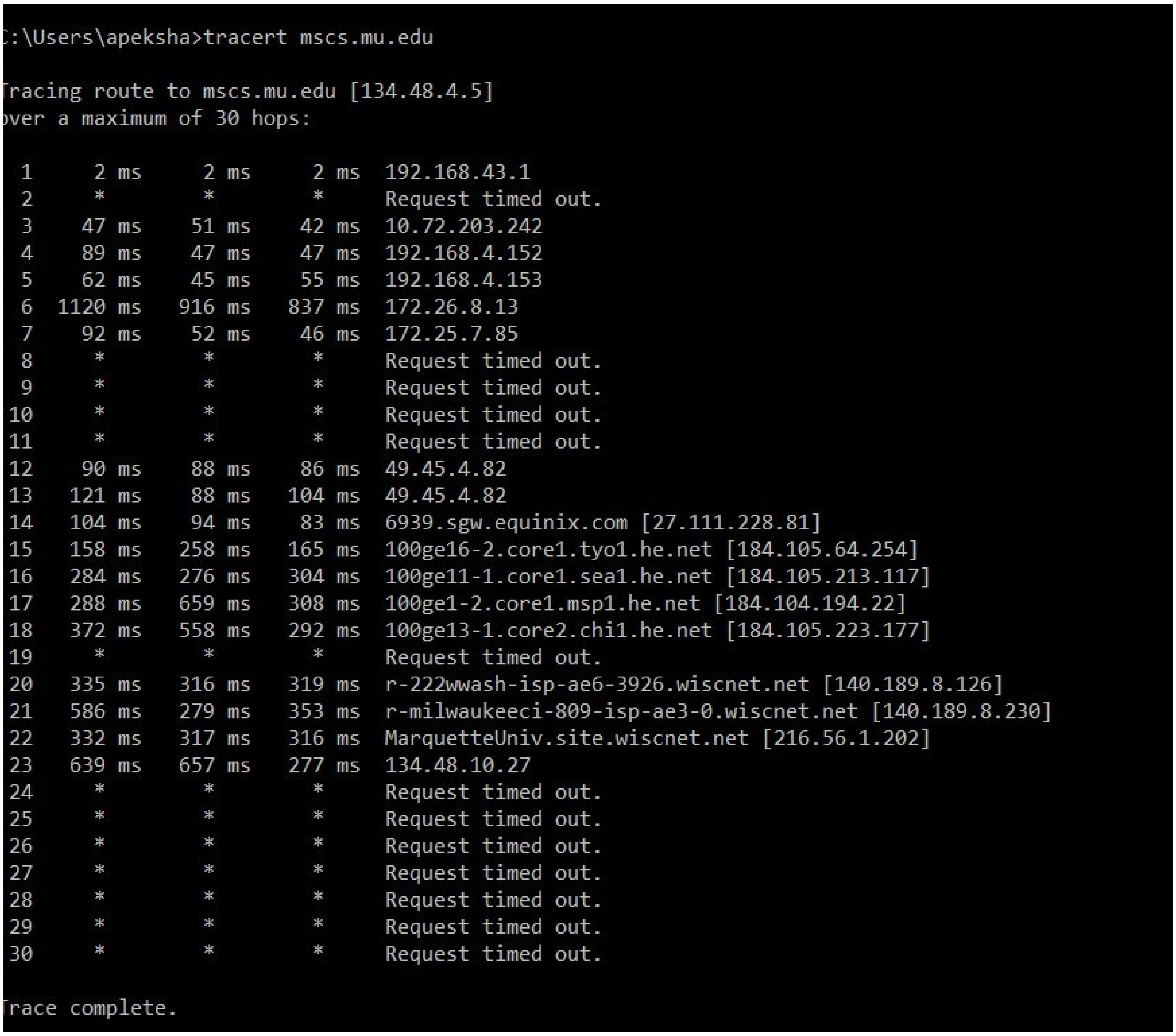


```
C:\Users\apeksha>tracert spit.ac.in

Tracing route to spit.ac.in [43.252.193.19]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3    53 ms    45 ms    59 ms  10.72.203.242
  4    50 ms    55 ms    38 ms  192.168.4.184
  5    41 ms    38 ms    52 ms  192.168.4.187
  6   101 ms    36 ms    55 ms  172.26.8.13
  7   125 ms    47 ms    66 ms  172.25.7.85
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13    96 ms   117 ms    77 ms  115.112.8.117.STATIC-Chennai.vsnl.net.in [115.112.8.117]
 14     *        *        *     Request timed out.
 15    71 ms    75 ms    75 ms  115.113.165.174.static-mumbai.vsnl.net.in [115.113.165.174]
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18    85 ms    67 ms    69 ms  223-30-0-0.lan.sify.net [223.31.147.250]
 19   152 ms    77 ms    98 ms  27.109.1.150
 20  1201 ms    69 ms    75 ms  103.205.124.82
 21   151 ms    79 ms    75 ms  43.252.192.230
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

1.2.1 EXPERIMENTS WITH TRACEROUTE

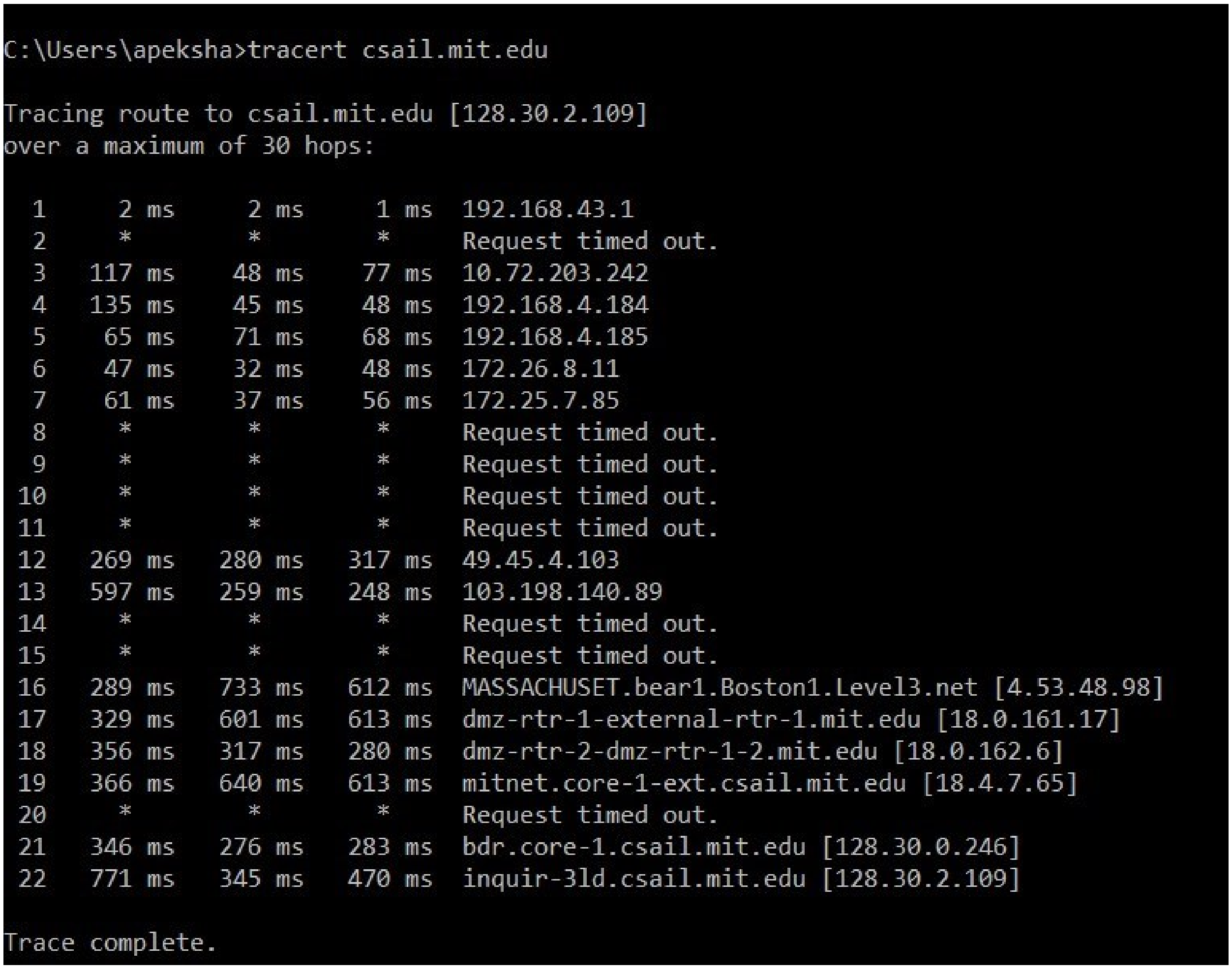
From **your machine** traceroute to the following hosts:

1. mscs.mu.edu



```
:\Users\apeksha>tracert mscs.mu.edu

racing route to mscs.mu.edu [134.48.4.5]
ver a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3    47 ms    51 ms    42 ms  10.72.203.242
  4    89 ms    47 ms    47 ms  192.168.4.152
  5    62 ms    45 ms    55 ms  192.168.4.153
  6  1120 ms   916 ms   837 ms  172.26.8.13
  7    92 ms    52 ms    46 ms  172.25.7.85
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12    90 ms    88 ms    86 ms  49.45.4.82
 13   121 ms    88 ms   104 ms  49.45.4.82
 14   104 ms    94 ms    83 ms  6939.sgw.equinix.com [27.111.228.81]
 15   158 ms   258 ms   165 ms  100ge16-2.core1.tyo1.he.net [184.105.64.254]
 16   284 ms   276 ms   304 ms  100ge11-1.core1.sea1.he.net [184.105.213.117]
 17   288 ms   659 ms   308 ms  100ge1-2.core1.msp1.he.net [184.104.194.22]
 18   372 ms   558 ms   292 ms  100ge13-1.core2.chi1.he.net [184.105.223.177]
 19     *        *        *     Request timed out.
 20   335 ms   316 ms   319 ms  r-222wwash-isp-ae6-3926.wiscnet.net [140.189.8.126]
 21   586 ms   279 ms   353 ms  r-milwaukeeci-809-isp-ae3-0.wiscnet.net [140.189.8.230]
 22   332 ms   317 ms   316 ms  MarquetteUniv.site.wiscnet.net [216.56.1.202]
 23   639 ms   657 ms   277 ms  134.48.10.27
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

race complete.
```

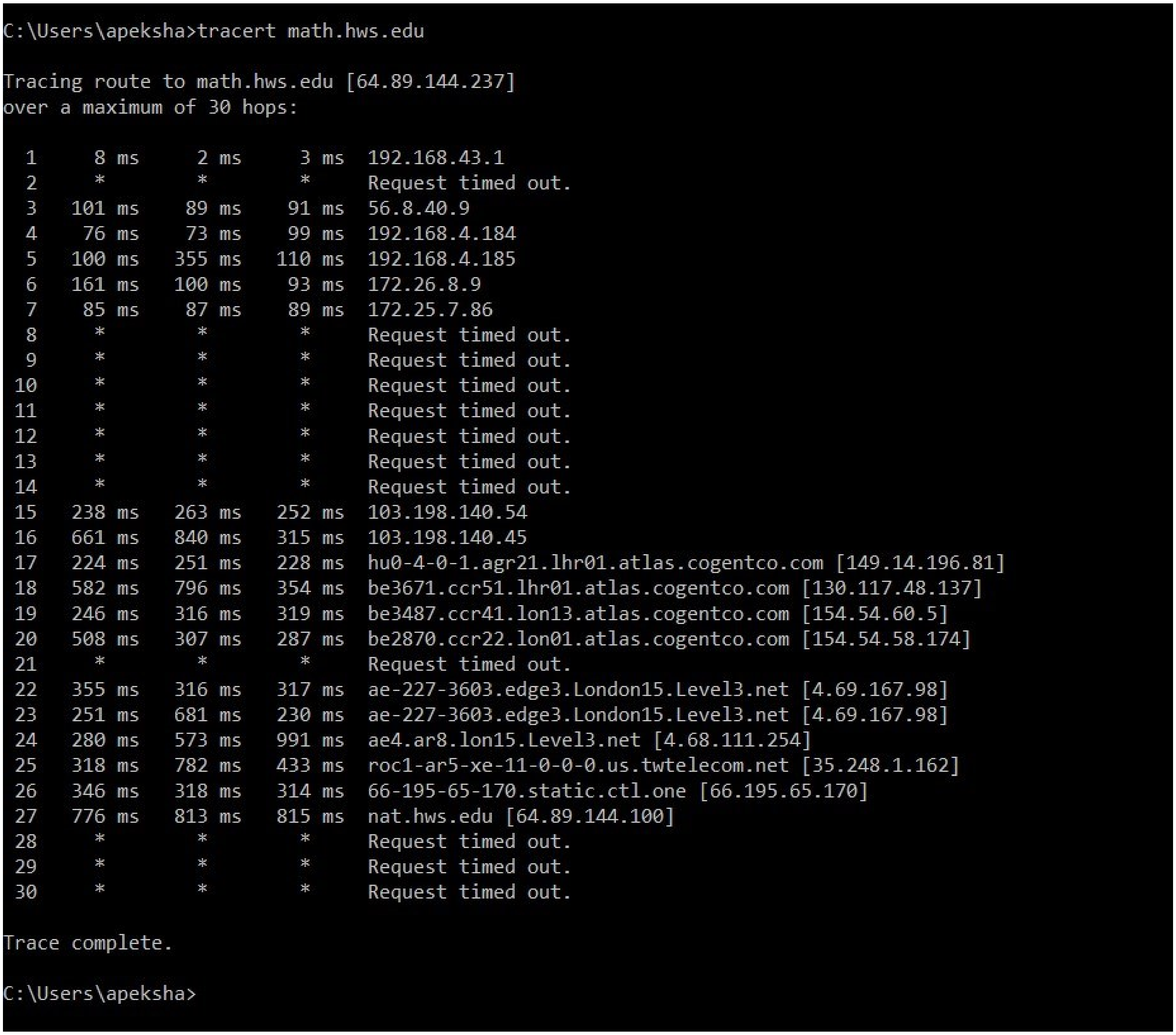
2. csail.mit.edu



```
C:\Users\apeksha>tracert csail.mit.edu

Tracing route to csail.mit.edu [128.30.2.109]
over a maximum of 30 hops:

  1     2 ms     2 ms     1 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   117 ms    48 ms    77 ms  10.72.203.242
  4   135 ms    45 ms    48 ms  192.168.4.184
  5    65 ms    71 ms    68 ms  192.168.4.185
  6    47 ms    32 ms    48 ms  172.26.8.11
  7    61 ms    37 ms    56 ms  172.25.7.85
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12   269 ms   280 ms   317 ms  49.45.4.103
 13   597 ms   259 ms   248 ms  103.198.140.89
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16   289 ms   733 ms   612 ms  MASSACHUSET.bear1.Boston1.Level3.net [4.53.48.98]
 17   329 ms   601 ms   613 ms  dmz-rtr-1-external-rtr-1.mit.edu [18.0.161.17]
 18   356 ms   317 ms   280 ms  dmz-rtr-2-dmz-rtr-1-2.mit.edu [18.0.162.6]
 19   366 ms   640 ms   613 ms  mitnet.core-1-ext.csail.mit.edu [18.4.7.65]
 20     *        *        *     Request timed out.
 21   346 ms   276 ms   283 ms  bdr.core-1.csail.mit.edu [128.30.0.246]
 22   771 ms   345 ms   470 ms  inquir-3ld.csail.mit.edu [128.30.2.109]

Trace complete.
```

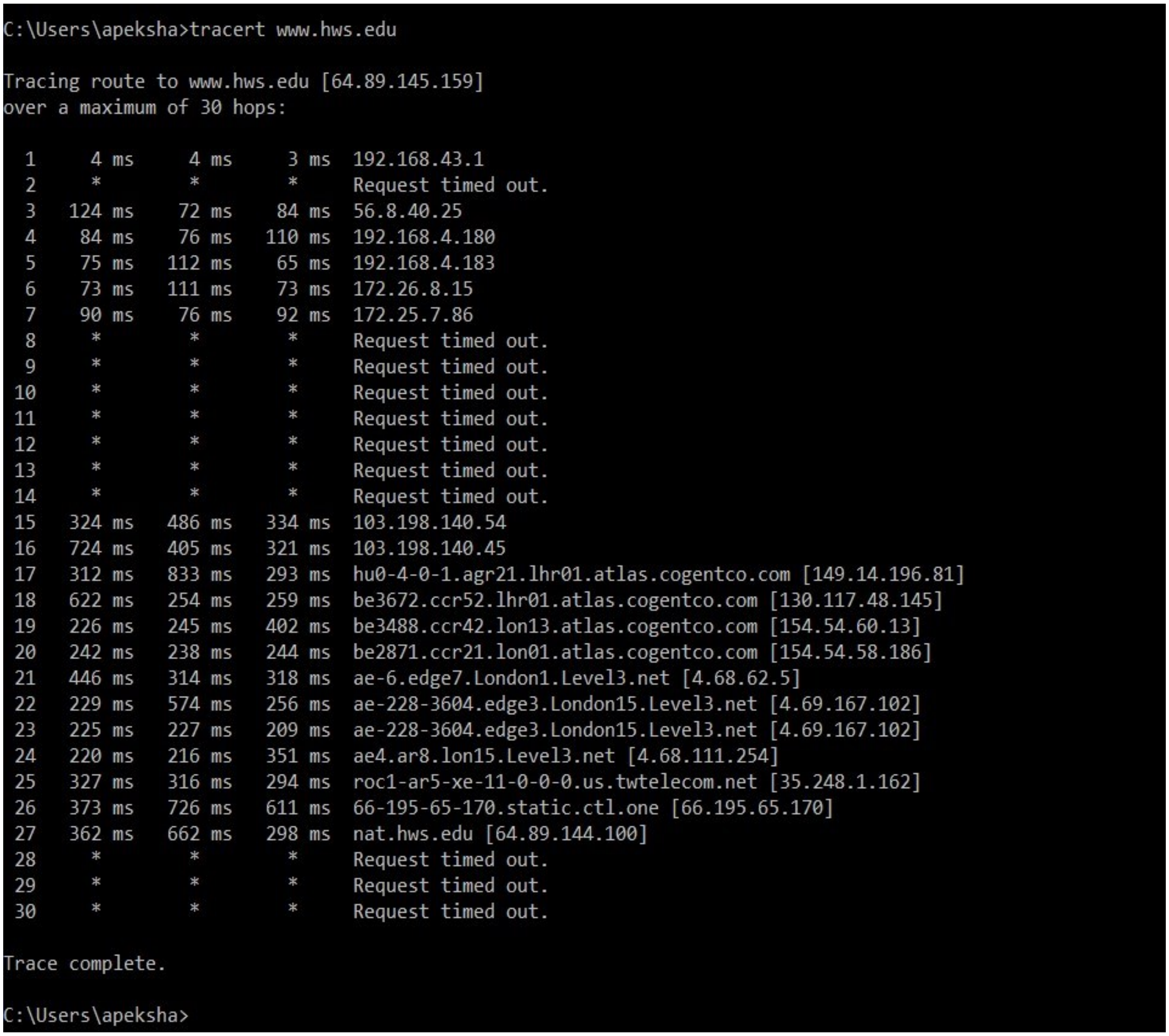
Exercise 2: (Very short.) Use traceroute to trace the route from your computer to math.hws.edu and to www.hws.edu. Explain the difference in the results.

1. math.hsw.edu



```
C:\Users\apeksha>tracert math.hws.edu

Tracing route to math.hws.edu [64.89.144.237]
over a maximum of 30 hops:

  1     8 ms     2 ms     3 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   101 ms    89 ms    91 ms  56.8.40.9
  4    76 ms    73 ms    99 ms  192.168.4.184
  5   100 ms   355 ms   110 ms  192.168.4.185
  6   161 ms   100 ms    93 ms  172.26.8.9
  7    85 ms    87 ms    89 ms  172.25.7.86
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15   238 ms   263 ms   252 ms  103.198.140.54
 16   661 ms   840 ms   315 ms  103.198.140.45
 17   224 ms   251 ms   228 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 18   582 ms   796 ms   354 ms  be3671.ccr51.lhr01.atlas.cogentco.com [130.117.48.137]
 19   246 ms   316 ms   319 ms  be3487.ccr41.lon13.atlas.cogentco.com [154.54.60.5]
 20   508 ms   307 ms   287 ms  be2870.ccr22.lon01.atlas.cogentco.com [154.54.58.174]
 21     *        *        *     Request timed out.
 22   355 ms   316 ms   317 ms  ae-227-3603.edge3.London15.Level3.net [4.69.167.98]
 23   251 ms   681 ms   230 ms  ae-227-3603.edge3.London15.Level3.net [4.69.167.98]
 24   280 ms   573 ms   991 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 25   318 ms   782 ms   433 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 26   346 ms   318 ms   314 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 27   776 ms   813 ms   815 ms  nat.hws.edu [64.89.144.100]
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.

C:\Users\apeksha>
```

2. www.hws.edu



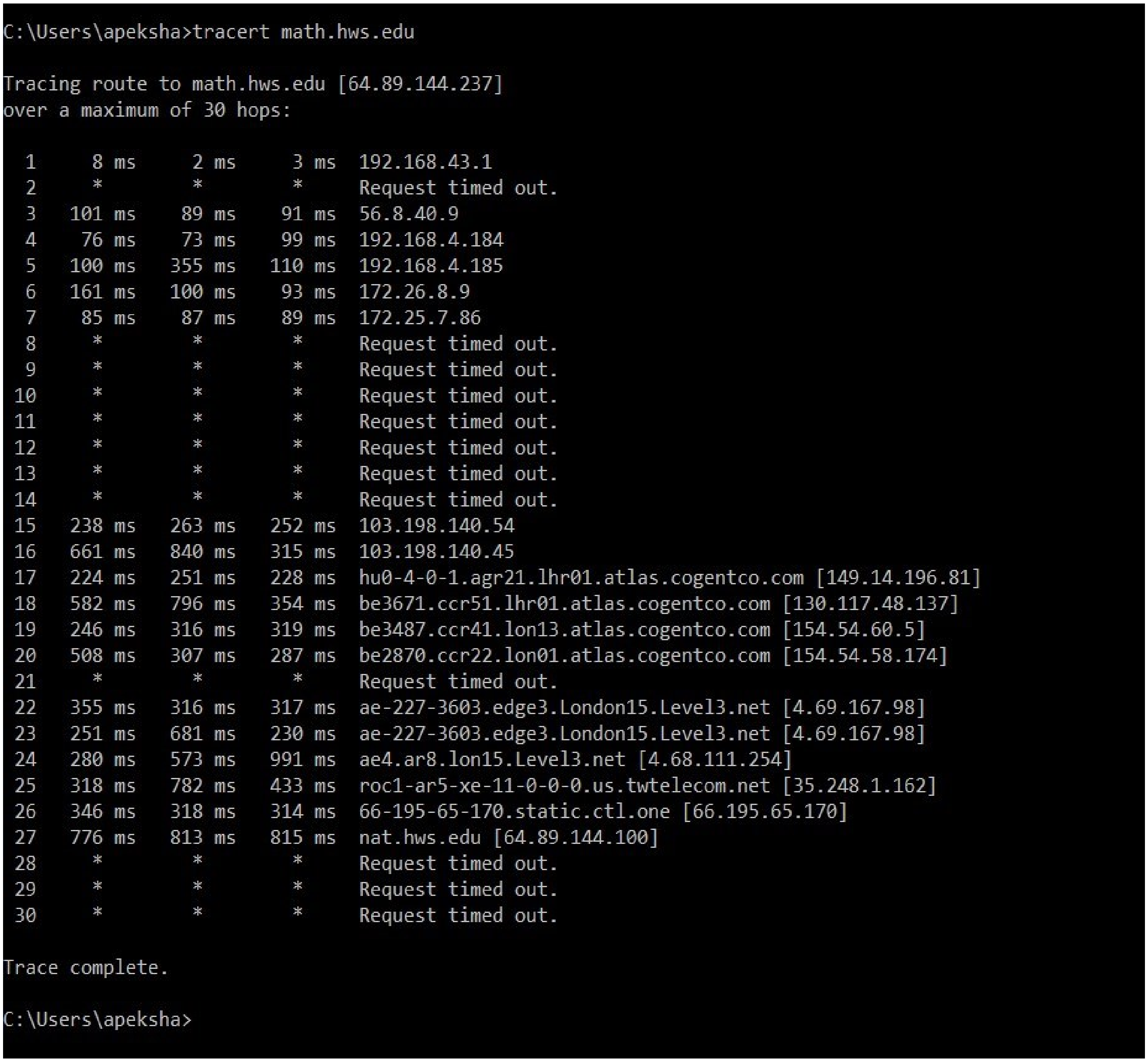
```
C:\Users\apeksha>tracert www.hws.edu

Tracing route to www.hws.edu [64.89.145.159]
over a maximum of 30 hops:

  1     4 ms     4 ms     3 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   124 ms    72 ms    84 ms  56.8.40.25
  4    84 ms    76 ms   110 ms  192.168.4.180
  5    75 ms   112 ms    65 ms  192.168.4.183
  6    73 ms   111 ms    73 ms  172.26.8.15
  7    90 ms    76 ms    92 ms  172.25.7.86
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15   324 ms   486 ms   334 ms  103.198.140.54
 16   724 ms   405 ms   321 ms  103.198.140.45
 17   312 ms   833 ms   293 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 18   622 ms   254 ms   259 ms  be3672.ccr52.lhr01.atlas.cogentco.com [130.117.48.145]
 19   226 ms   245 ms   402 ms  be3488.ccr42.lon13.atlas.cogentco.com [154.54.60.13]
 20   242 ms   238 ms   244 ms  be2871.ccr21.lon01.atlas.cogentco.com [154.54.58.186]
 21   446 ms   314 ms   318 ms  ae-6.edge7.London1.Level3.net [4.68.62.5]
 22   229 ms   574 ms   256 ms  ae-228-3604.edge3.London15.Level3.net [4.69.167.102]
 23   225 ms   227 ms   209 ms  ae-228-3604.edge3.London15.Level3.net [4.69.167.102]
 24   220 ms   216 ms   351 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 25   327 ms   316 ms   294 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 26   373 ms   726 ms   611 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 27   362 ms   662 ms   298 ms  nat.hws.edu [64.89.144.100]
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.

C:\Users\apeksha>
```

Observation –

1) From the above results, we can see that the path followed in 17th to 23rd hop, vary.
2) The IP address at hop 21 is different for both the websites. www.hws.edu goes at ae-6.edge7.London1.Level3.net [4.68.62.5] whereas math.hws.edu gets the request timed out.

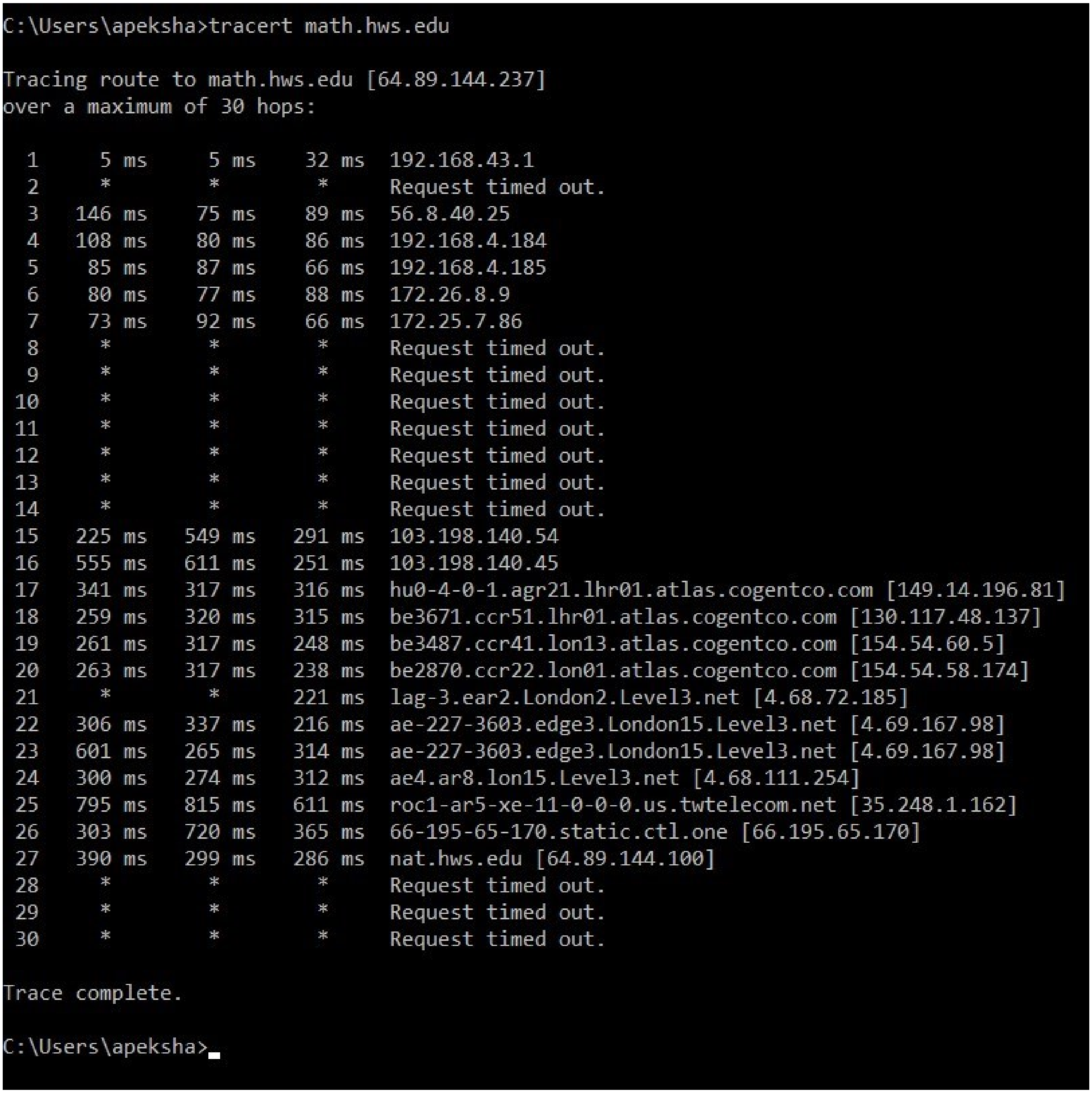
<u>Exercise 3:</u> Two packets sent from the same source to the same destination do not necessarily follow the same path through the net. Experiment with some sources that are fairly far away. Can you find cases where packets sent to the same destination follow different paths? How likely does it seem to be? What about when the packets are sent at very different times? Save some of the outputs from traceroute. (You can copy them from the Terminal window by highlighting and right-clicking, then paste into a text editor.) Come back sometime next week, try the same destinations again, and compare the results with the results from today. Report your observations.

Original Path –



```
C:\Users\apeksha>tracert math.hws.edu

Tracing route to math.hws.edu [64.89.144.237]
over a maximum of 30 hops:

  1     8 ms     2 ms     3 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   101 ms    89 ms    91 ms  56.8.40.9
  4    76 ms    73 ms    99 ms  192.168.4.184
  5   100 ms   355 ms   110 ms  192.168.4.185
  6   161 ms   100 ms    93 ms  172.26.8.9
  7    85 ms    87 ms    89 ms  172.25.7.86
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15   238 ms   263 ms   252 ms  103.198.140.54
 16   661 ms   840 ms   315 ms  103.198.140.45
 17   224 ms   251 ms   228 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 18   582 ms   796 ms   354 ms  be3671.ccr51.lhr01.atlas.cogentco.com [130.117.48.137]
 19   246 ms   316 ms   319 ms  be3487.ccr41.lon13.atlas.cogentco.com [154.54.60.5]
 20   508 ms   307 ms   287 ms  be2870.ccr22.lon01.atlas.cogentco.com [154.54.58.174]
 21     *        *        *     Request timed out.
 22   355 ms   316 ms   317 ms  ae-227-3603.edge3.London15.Level3.net [4.69.167.98]
 23   251 ms   681 ms   230 ms  ae-227-3603.edge3.London15.Level3.net [4.69.167.98]
 24   280 ms   573 ms   991 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 25   318 ms   782 ms   433 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 26   346 ms   318 ms   314 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 27   776 ms   813 ms   815 ms  nat.hws.edu [64.89.144.100]
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.

C:\Users\apeksha>
```

New Path –



```
C:\Users\apeksha>tracert math.hws.edu

Tracing route to math.hws.edu [64.89.144.237]
over a maximum of 30 hops:

  1     5 ms     5 ms    32 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   146 ms    75 ms    89 ms  56.8.40.25
  4   108 ms    80 ms    86 ms  192.168.4.184
  5    85 ms    87 ms    66 ms  192.168.4.185
  6    80 ms    77 ms    88 ms  172.26.8.9
  7    73 ms    92 ms    66 ms  172.25.7.86
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15   225 ms   549 ms   291 ms  103.198.140.54
 16   555 ms   611 ms   251 ms  103.198.140.45
 17   341 ms   317 ms   316 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 18   259 ms   320 ms   315 ms  be3671.ccr51.lhr01.atlas.cogentco.com [130.117.48.137]
 19   261 ms   317 ms   248 ms  be3487.ccr41.lon13.atlas.cogentco.com [154.54.60.5]
 20   263 ms   317 ms   238 ms  be2870.ccr22.lon01.atlas.cogentco.com [154.54.58.174]
 21     *        *      221 ms  lag-3.ear2.London2.Level3.net [4.68.72.185]
 22   306 ms   337 ms   216 ms  ae-227-3603.edge3.London15.Level3.net [4.69.167.98]
 23   601 ms   265 ms   314 ms  ae-227-3603.edge3.London15.Level3.net [4.69.167.98]
 24   300 ms   274 ms   312 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 25   795 ms   815 ms   611 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 26   303 ms   720 ms   365 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 27   390 ms   299 ms   286 ms  nat.hws.edu [64.89.144.100]
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.

C:\Users\apeksha>
```

1) From the above experiments I can conclude that for the same website, when the packets are sent at different times, the RTT taken is different.

2) Tracert command was executed for the website math.hws.edu first on 24 – 08 – 20 and for the second time on 25 – 08 – 20 . The path followed was the same on both occasions.

QUESTIONS ABOUT PATHS

Now look at the results you gathered and answer the following questions about the paths taken by your packets. Store your answers in a file named traceroute.txt.

1. Is any part of the path common for all hosts you tracerouted?

Ans.: Yes, the path to my ISP is always the same.

2. Is there a relationship between the number of nodes that show up in the traceroute and the location of the host? If so, what is this relationship?

Ans.: A hop depends on the location of the host. If the distance between the location of the user and that of the destination URL is more, then more hops will be required in order to reach the destination as more number of access points will be used for routing and the greater the number of access points involved, the greater are the chances of access points failing to respond and similarly for searching the alternative optimal path towards the destination.

3. Is there a relationship between the number of nodes that show up in the traceroute and latency of the host (from your ping results above)? Does the same relationship hold for all hosts?

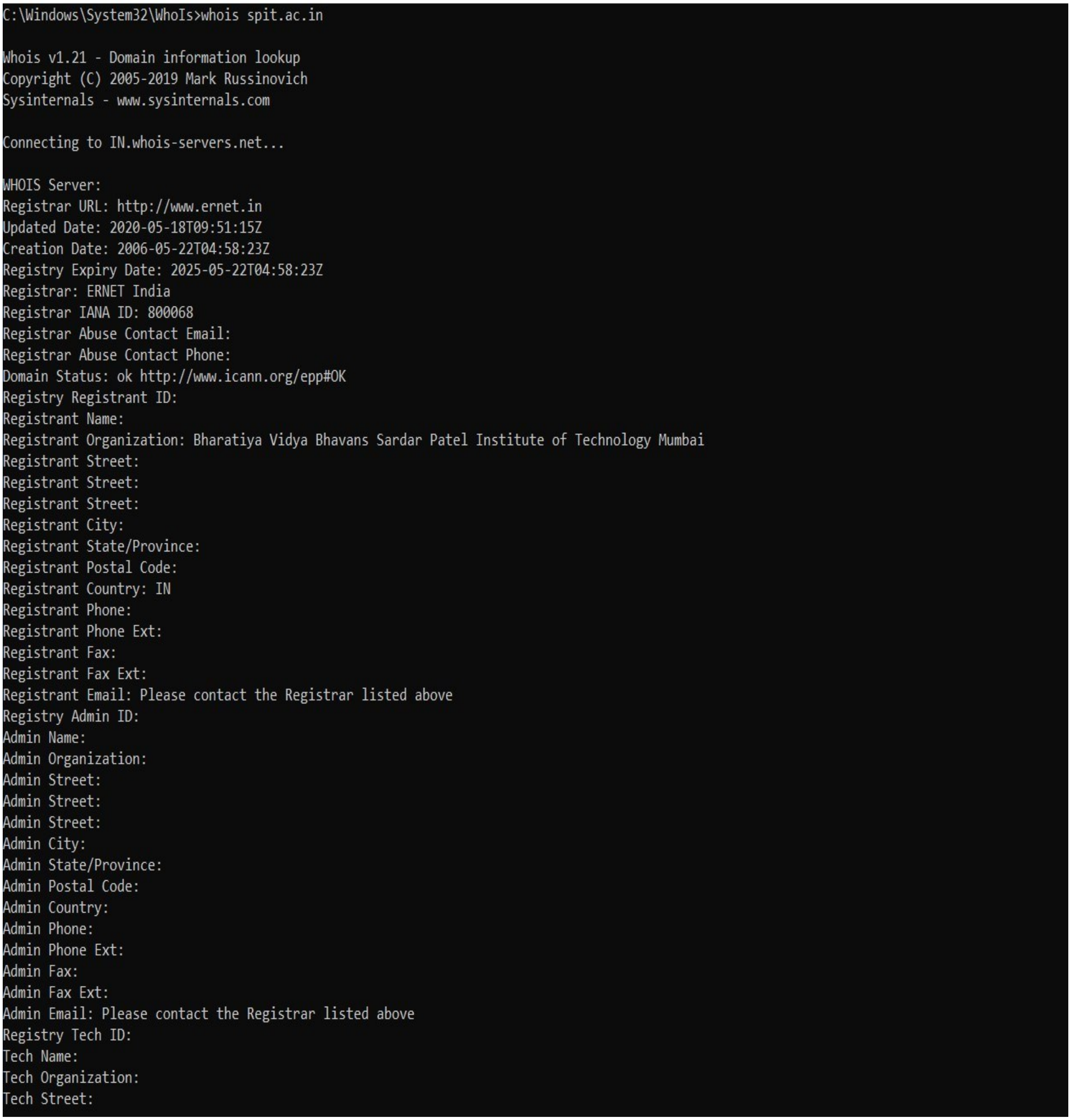
Ans.: If the latency of the host causes the traceroute request to get timed out even after the conventional three tries, then it keeps on sending the data packets until the host responds or up to a certain maximum hop. The same relationship may not hold for each host as it really depends on the time which the host takes to respond. If the host responds in the first request itself, the tracerouting stops with a success message.

It also depends on the packet size. The amount of latency is largely dependent on how far the visitor is from the server location and how many nodes the signal has to travel through.

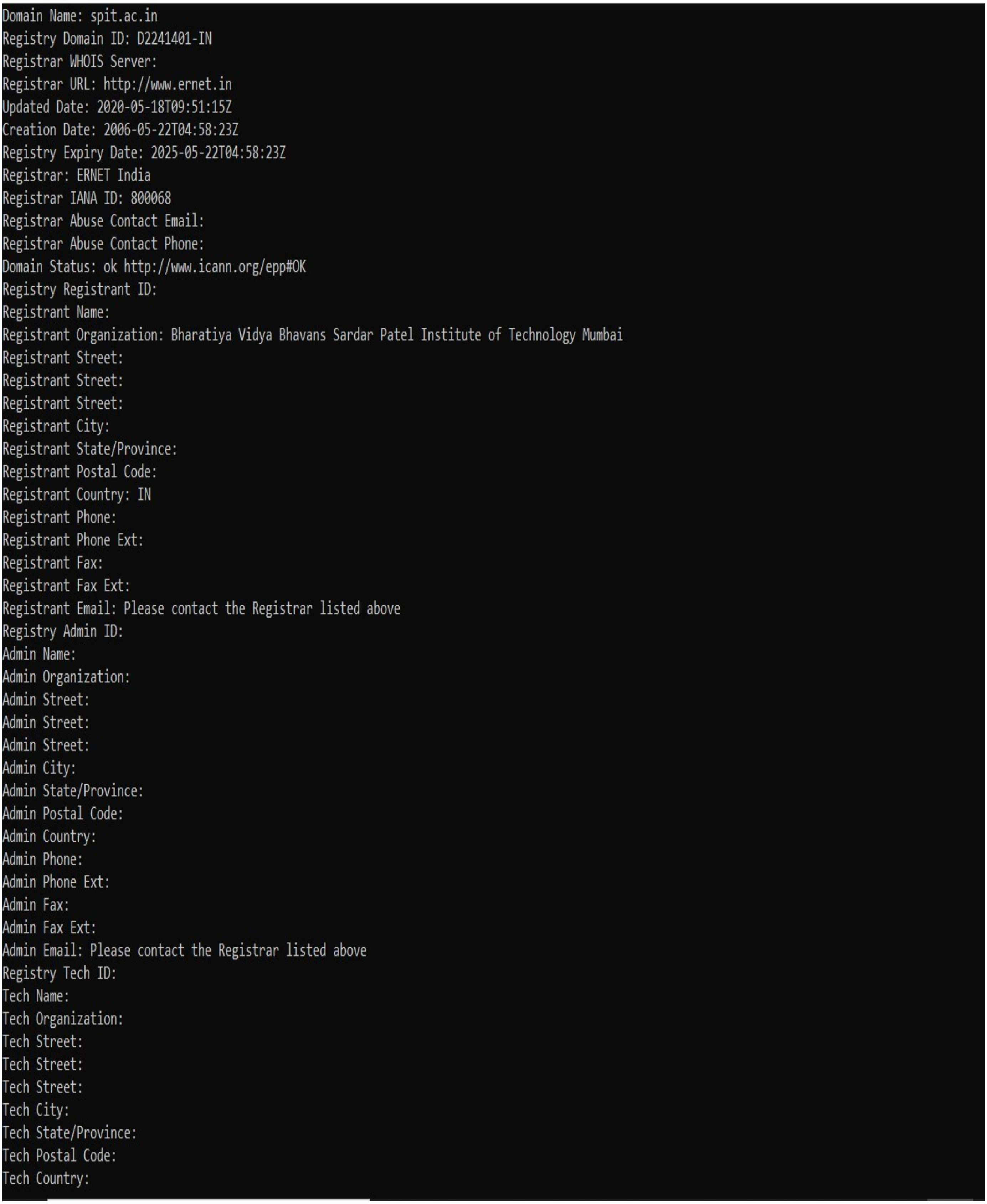
> The further apart two nodes are the more latency there is as latency is dependent on the distance between the two communicating nodes. Theoretically, latency of a packet going on a round trip across the world is 133ms. In actuality, such a round trip takes longer, though latency is decreased when direct connections through network backbones are achieved. When the source and destination are far apart, the hops increase. Due to high number of nodes, the latency adds up due to increase in queuing delay and increases the RTT.

Whois — The *whois* command can give detailed information about domain names and IP addresses. If it is not installed on the computers then install it with command sudo apt-get install whois in. *Whois* can tell you what organization owns or is responsible for the name or address and where to contact them. It often includes a list of domain name servers for the organization.

When using *whois* to look up a domain name, use the simple two-part network name, not an individual computer name (for example, *whois spit.ac.in*).



```
C:\Windows\System32\WhoIs>whois spit.ac.in

Whois v1.21 - Domain information lookup
Copyright (C) 2005-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to IN.whois-servers.net...

WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2020-05-18T09:51:15Z
Creation Date: 2006-05-22T04:58:23Z
Registry Expiry Date: 2025-05-22T04:58:23Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID:
Registrant Name:
Registrant Organization: Bharatiya Vidya Bhavans Sardar Patel Institute of Technology Mumbai
Registrant Street:
Registrant Street:
Registrant Street:
Registrant City:
Registrant State/Province:
Registrant Postal Code:
Registrant Country: IN
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Please contact the Registrar listed above
Registry Admin ID:
Admin Name:
Admin Organization:
Admin Street:
Admin Street:
Admin Street:
Admin City:
Admin State/Province:
Admin Postal Code:
Admin Country:
Admin Phone:
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: Please contact the Registrar listed above
Registry Tech ID:
Tech Name:
Tech Organization:
Tech Street:
```



```
Domain Name: spit.ac.in
Registry Domain ID: D2241401-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2020-05-18T09:51:15Z
Creation Date: 2006-05-22T04:58:23Z
Registry Expiry Date: 2025-05-22T04:58:23Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID:
Registrant Name:
Registrant Organization: Bharatiya Vidya Bhavans Sardar Patel Institute of Technology Mumbai
Registrant Street:
Registrant Street:
Registrant Street:
Registrant City:
Registrant State/Province:
Registrant Postal Code:
Registrant Country: IN
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Please contact the Registrar listed above
Registry Admin ID:
Admin Name:
Admin Organization:
Admin Street:
Admin Street:
Admin Street:
Admin City:
Admin State/Province:
Admin Postal Code:
Admin Country:
Admin Phone:
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: Please contact the Registrar listed above
Registry Tech ID:
Tech Name:
Tech Organization:
Tech Street:
Tech Street:
Tech Street:
Tech City:
Tech State/Province:
Tech Postal Code:
Tech Country:
```

Exercise 4: (Short.) Use *whois* to investigate a well-known web site such as google.com or amazon.com, and write a couple of sentences about what you find out.

The whois command gives information about the domain name, the Registry Domain ID and some other details such as the details of the Registrar and the Registrant. For example, in case of spit.ac.in (domain name), the Registrant Organization is Bharatiya Vidya Bhavans Sardar Patel Institute of Technology Mumbai, the Registrant Country is IN-India. It also provides the Registry expiry date.
We also can find information like Domain Name, Domain ID, Registrar URL, Updated Date, Creation and Expiry Date, Registrar Contact details, IANA ID, Name Server and Domain Status. Using whois we can get information about a specific ip address or we can get information regarding a registered domain.

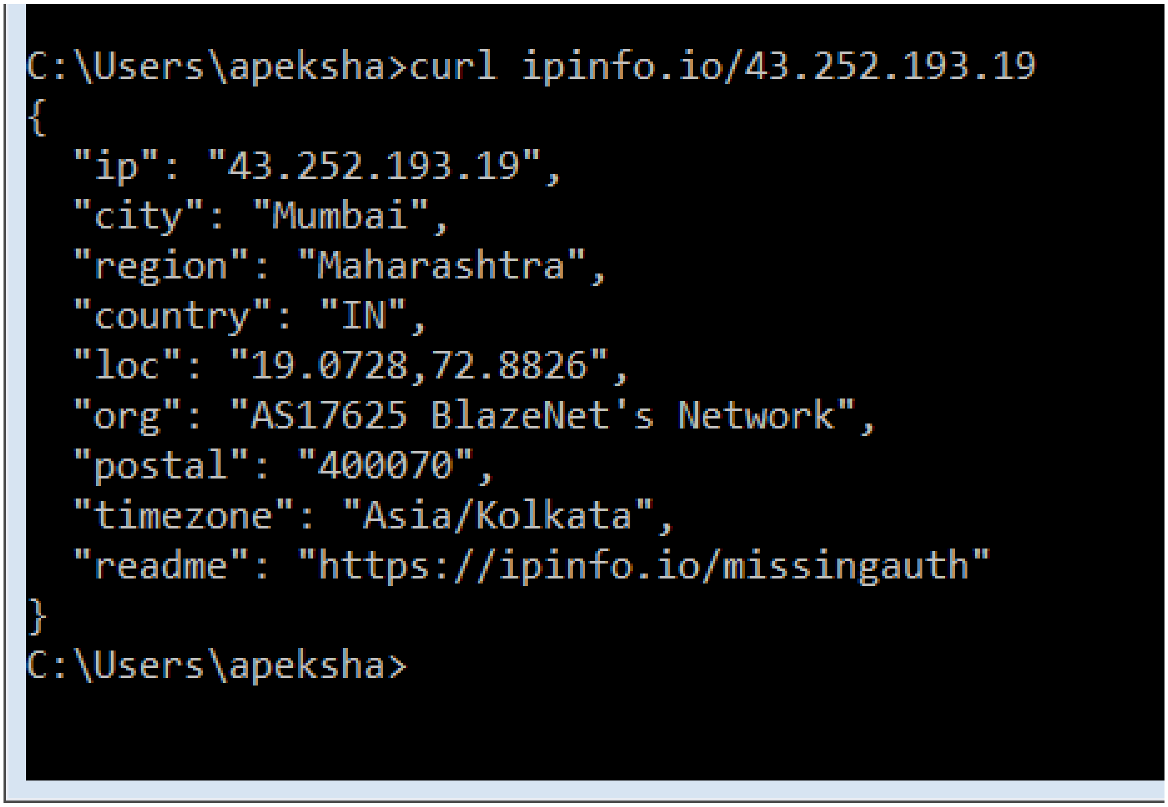
Exercise 5: (Should be short.) Because of NAT, the domain name *spit.ac.in* has a different IP address outside of SPIT than it does on campus. Using information in this lab and working on a home computer, find the outside IP address for spit.ac.in. Explain how you did it.

Geolocation — A geolocation service tries to tell, approximately, where a given IP address is located physically. They can't be completely accurate—but they probably get at least the country right most of the time.

This geolocation program is not installed on our computers, but you can access one on the command line using the *curl* command, which can send HTTP requests and display the response. The following command uses *curl* to contact a public web service that will look up an IP address for you: curl ipinfo.io/<IP-address>. For a specific example:

curl ipinfo.io/129.64.99.200

I have found the location of spit with the help of I.P. address
that I got by "tracert spit.ac.in" command



```
C:\Users\apeksha>curl ipinfo.io/43.252.193.19
{
  "ip": "43.252.193.19",
  "city": "Mumbai",
  "region": "Maharashtra",
  "country": "IN",
  "loc": "19.0728,72.8826",
  "org": "AS17625 BlazeNet's Network",
  "postal": "400070",
  "timezone": "Asia/Kolkata",
  "readme": "https://ipinfo.io/missingauth"
}
C:\Users\apeksha>
```

(As you can see, you get back more than just the location.)

Exercise 6: Find a few IP addresses that are connected to the web server on spit.ac.in right now, and determine where those IP addresses are located. (I'm expecting that there will be several; if not, try again in a few minutes or sometime later.) Find one that is far from Geneva, NY. Explain how you did it.

CONCLUSION:

In this experiment, I have learnt about some basic command line networking utilities like ping, tracert and ifconfig.
Learnt about Network Latency, RTT and the factors impacting RTT.
Learnt that network depends a lot on the time when the experiment is performed and on the host.

References:

https://en.wikipedia.org/wiki/Network_delay#:~:text=Processing%20delay%20%E2%80%93%20time%20it%20takes,signal%20to%20reach%20its%20destination

https://www.imperva.com/learn/performance/round-trip-time-rtt/
https://blog.stackpath.com/latency/#:~:text=Propagation%3A%20The%20further%20apart%20two,between%20the%20two%20communicating%20nodes.&text=In%20actuality%2C%20such%20a%20round,through%20network%20backbones%20are%20achieved

https://network-tools.com/trace/

https://www.2daygeek.com/linux-command-find-check-domain-ip-address/