

**NAME: SHYAM MEHTA**  
**UID: 2018130027**  
**BATCH: B**

## 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 receive 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 response 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 Linux or Mac OS is:

```
ping [-c <count>] [-s <packetsize>] <hostname>
```

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

```
Activities Terminal Tue 12:32 ● shyam@shyam-Inspiron-15-3567: ~
File Edit View Search Terminal Help
shyam@shyam-Inspiron-15-3567:~$ ping -s 100 -c 10 www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (13.227.226.21) 100(128) bytes of data.
100 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=1 ttl=247 time=4.20 ms
100 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=2 ttl=247 time=7.04 ms
100 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=3 ttl=247 time=4.67 ms
100 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=4 ttl=247 time=6.58 ms
100 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=5 ttl=247 time=3.77 ms
100 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=6 ttl=247 time=8.57 ms
100 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=7 ttl=247 time=6.79 ms
100 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=8 ttl=247 time=7.59 ms
100 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=9 ttl=247 time=7.68 ms
100 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=10 ttl=247 time=9.13 ms

--- d3ag4hukkh62yn.cloudfront.net ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9017ms
rtt min/avg/max/mdev = 3.774/6.606/9.135/1.737 ms
shyam@shyam-Inspiron-15-3567:~$ ping -s 64 -c 10 www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (13.227.226.21) 64(92) bytes of data.
72 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=1 ttl=247 time=4.03 ms
72 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=2 ttl=247 time=7.49 ms
72 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=3 ttl=247 time=9.34 ms
72 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=4 ttl=247 time=7.70 ms
72 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=5 ttl=247 time=7.97 ms
72 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=6 ttl=247 time=9.40 ms
72 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=7 ttl=247 time=4.52 ms
72 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=8 ttl=247 time=6.91 ms
72 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=9 ttl=247 time=8.28 ms
72 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=10 ttl=247 time=7.08 ms

--- d3ag4hukkh62yn.cloudfront.net ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9015ms
rtt min/avg/max/mdev = 4.039/7.277/9.404/1.699 ms
shyam@shyam-Inspiron-15-3567:~$
```

```
Activities Terminal Tue 12:38 ● shyam@shyam-Inspiron-15-3567: ~
File Edit View Search Terminal Help
shyam@shyam-Inspiron-15-3567:~$ ping -s 500 -c 10 www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (13.227.226.21) 500(528) bytes of data.
500 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=1 ttl=247 time=4.14 ms
500 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=2 ttl=247 time=7.47 ms
500 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=3 ttl=247 time=10.8 ms
500 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=4 ttl=247 time=8.88 ms
500 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=5 ttl=247 time=8.96 ms
500 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=6 ttl=247 time=9.12 ms
500 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=7 ttl=247 time=16.2 ms
500 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=8 ttl=247 time=11.2 ms
500 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=9 ttl=247 time=7.89 ms
500 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=10 ttl=247 time=4.46 ms

--- d3ag4hukkh62yn.cloudfront.net ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
rtt min/avg/max/mdev = 4.143/8.923/16.221/3.289 ms
shyam@shyam-Inspiron-15-3567:~$ ping -s 1000 -c 10 www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (13.227.226.21) 1000(1028) bytes of data.
1000 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=1 ttl=247 time=4.38 ms
1000 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=2 ttl=247 time=10.4 ms
1000 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=3 ttl=247 time=8.71 ms
1000 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=4 ttl=247 time=8.57 ms
1000 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=5 ttl=247 time=7.61 ms
1000 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=6 ttl=247 time=7.95 ms
1000 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=7 ttl=247 time=13.9 ms
1000 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=8 ttl=247 time=10.4 ms
1000 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=9 ttl=247 time=8.13 ms
1000 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=10 ttl=247 time=7.98 ms

--- d3ag4hukkh62yn.cloudfront.net ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
rtt min/avg/max/mdev = 4.382/8.827/13.991/2.354 ms
shyam@shyam-Inspiron-15-3567:~$
```

## 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`.

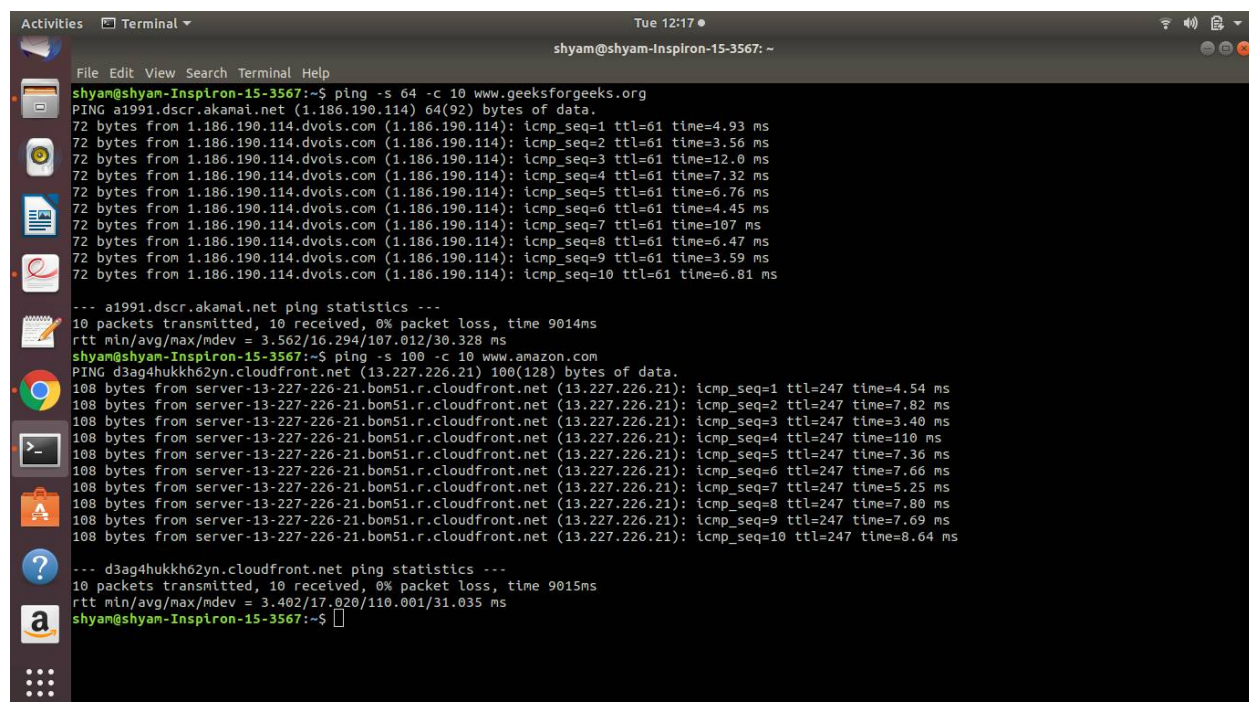
Does the average RTT vary between different hosts? What aspects of latency (transmit, propagation, and queueing delay) might impact this and why?

*Ans : RTT varies between different hosts. RTT depends on the distance of host, the medium, number of network hops, traffic levels in the network and server response time of the host. Propagation delay depends on distance. Transmission delay depends on the efficiency of medium. Propagation and Transmission delay might have an impact in this case.*

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

*Ans : RTT varies with packet size. RTT increases as packet size increases. Transmission delay depends on size of packet. So, transmission delay might have an impact on this.*

**Exercise 1:** 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), `www.u-tokyo.ac.jp` (Japan).



```
shyam@shyam-Inspiron-15-3567:~$ ping -s 64 -c 10 www.geeksforgeeks.org
PING a1991.dscr.akamai.net (1.186.190.114) 64(92) bytes of data:
72 bytes from 1.186.190.114.dvois.com (1.186.190.114): icmp_seq=1 ttl=61 time=4.93 ms
72 bytes from 1.186.190.114.dvois.com (1.186.190.114): icmp_seq=2 ttl=61 time=3.56 ms
72 bytes from 1.186.190.114.dvois.com (1.186.190.114): icmp_seq=3 ttl=61 time=12.0 ms
72 bytes from 1.186.190.114.dvois.com (1.186.190.114): icmp_seq=4 ttl=61 time=7.32 ms
72 bytes from 1.186.190.114.dvois.com (1.186.190.114): icmp_seq=5 ttl=61 time=6.76 ms
72 bytes from 1.186.190.114.dvois.com (1.186.190.114): icmp_seq=6 ttl=61 time=4.45 ms
72 bytes from 1.186.190.114.dvois.com (1.186.190.114): icmp_seq=7 ttl=61 time=107 ms
72 bytes from 1.186.190.114.dvois.com (1.186.190.114): icmp_seq=8 ttl=61 time=6.47 ms
72 bytes from 1.186.190.114.dvois.com (1.186.190.114): icmp_seq=9 ttl=61 time=3.59 ms
72 bytes from 1.186.190.114.dvois.com (1.186.190.114): icmp_seq=10 ttl=61 time=6.81 ms

--- a1991.dscr.akamai.net ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 3.562/16.294/107.012/30.328 ms
shyam@shyam-Inspiron-15-3567:~$ ping -s 100 -c 10 www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (13.227.226.21) 100(128) bytes of data:
108 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=1 ttl=247 time=4.54 ms
108 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=2 ttl=247 time=7.82 ms
108 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=3 ttl=247 time=3.40 ms
108 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=4 ttl=247 time=110 ms
108 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=5 ttl=247 time=7.36 ms
108 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=6 ttl=247 time=7.66 ms
108 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=7 ttl=247 time=5.25 ms
108 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=8 ttl=247 time=7.80 ms
108 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=9 ttl=247 time=7.69 ms
108 bytes from server-13-227-226-21.bom51.r.cloudfront.net (13.227.226.21): icmp_seq=10 ttl=247 time=8.64 ms

--- d3ag4hukkh62yn.cloudfront.net ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9015ms
rtt min/avg/max/mdev = 3.402/17.020/110.001/31.035 ms
shyam@shyam-Inspiron-15-3567:~$
```



```
Activities Terminal Tue 12:42 shyam@shyam-Inspiron-15-3567: ~
File Edit View Search Terminal Help
shyam@shyam-Inspiron-15-3567:~$ ping -s 500 -c 10 www.facebook.com
PING star-mini.c10r.facebook.com (31.13.79.35) 500(528) bytes of data.
508 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=1 ttl=58 time=3.90 ms
508 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=2 ttl=58 time=7.69 ms
508 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=3 ttl=58 time=7.42 ms
508 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=4 ttl=58 time=26.7 ms
508 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=5 ttl=58 time=7.41 ms
508 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=6 ttl=58 time=7.96 ms
508 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=7 ttl=58 time=8.52 ms
508 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=8 ttl=58 time=7.53 ms
508 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=9 ttl=58 time=7.28 ms
508 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=10 ttl=58 time=6.58 ms

--- star-mini.c10r.facebook.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
rtt min/avg/max/mdev = 3.901/9.105/26.714/5.988 ms
shyam@shyam-Inspiron-15-3567:~$ ping -s 500 -c 10 www.microsoft.com
PING e13678.dspb.akamaiedge.net (23.212.241.249) 500(528) bytes of data.
508 bytes from a23-212-241-249.deploy.static.akamaitechnologies.com (23.212.241.249): icmp_seq=1 ttl=60 time=8.14 ms
508 bytes from a23-212-241-249.deploy.static.akamaitechnologies.com (23.212.241.249): icmp_seq=2 ttl=60 time=9.13 ms
508 bytes from a23-212-241-249.deploy.static.akamaitechnologies.com (23.212.241.249): icmp_seq=3 ttl=60 time=5.59 ms
508 bytes from a23-212-241-249.deploy.static.akamaitechnologies.com (23.212.241.249): icmp_seq=4 ttl=60 time=7.88 ms
508 bytes from a23-212-241-249.deploy.static.akamaitechnologies.com (23.212.241.249): icmp_seq=5 ttl=60 time=8.50 ms
508 bytes from a23-212-241-249.deploy.static.akamaitechnologies.com (23.212.241.249): icmp_seq=6 ttl=60 time=12.1 ms
508 bytes from a23-212-241-249.deploy.static.akamaitechnologies.com (23.212.241.249): icmp_seq=7 ttl=60 time=8.87 ms
508 bytes from a23-212-241-249.deploy.static.akamaitechnologies.com (23.212.241.249): icmp_seq=8 ttl=60 time=8.56 ms
508 bytes from a23-212-241-249.deploy.static.akamaitechnologies.com (23.212.241.249): icmp_seq=9 ttl=60 time=7.24 ms
508 bytes from a23-212-241-249.deploy.static.akamaitechnologies.com (23.212.241.249): icmp_seq=10 ttl=60 time=7.38 ms

--- e13678.dspb.akamaiedge.net ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
rtt min/avg/max/mdev = 5.596/8.353/12.197/1.604 ms
shyam@shyam-Inspiron-15-3567:~$
```

**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>

```
shyam@shyam-Inspiron-15-3567: ~
File Edit View Search Terminal Help
shyam@shyam-Inspiron-15-3567:~$ nslookup www.google.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 216.58.199.132
Name:   www.google.com
Address: 2404:6800:4009:80a::2004
shyam@shyam-Inspiron-15-3567:~$
```

**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 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: `telnet <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  $n = 1, 2, 3, \dots$ , 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 it was not installed in your virtual server last week, but you can install it with the command `sudo apt-get install traceroute`

The path taken through a network, can be measured using `traceroute`. The syntax for the command in Linux is:

```
traceroute <hostname>
```

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`).

### 1.2.1 EXPERIMENTS WITH TRACEROUTE

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

1. `ee.iitb.ac.in`
2. `mcs.mu.edu`
3. `www.cs.grinnell.edu`
4. `csail.mit.edu`
5. `cs.stanford.edu`
6. `cs.manchester.ac.uk`

Store the output of each traceroute command in a separate file named `traceroute_HOSTNAME.log`, replacing `HOSTNAME` with the hostname for end-host you pinged (e.g., `traceroute_ee.iitb.ac.in.log`).

```
Command Prompt
C:\Users\Jignesh>tracert www.ee.iitb.ac.in
Tracing route to www.ee.iitb.ac.in [103.21.125.132]
over a maximum of 30 hops:
  0  4 ms  3 ms  3 ms  192.168.43.1
  1  *      *      *      Request timed out.
  2  386 ms 42 ms 49 ms 10.71.16.2
  3  105 ms 69 ms 37 ms 192.168.69.158
  4  47 ms 38 ms 41 ms 192.168.69.159
  5  401 ms 60 ms 42 ms 172.16.80.107
  6  64 ms 52 ms 52 ms 172.17.119.4
  7  *      *      *      Request timed out.
  8  *      *      *      Request timed out.
  9  *      *      *      Request timed out.
 10  41 ms 37 ms 58 ms 115.110.206.73.static-Mumbai.vsnl.net.in [115.11
 11  125 ms 53 ms 46 ms 115.113.165.62.static-mumbai.vsnl.net.in [115.11
 12  165.62]
 13  *      *      *      Request timed out.
 14  *      *      *      Request timed out.
 15  63 ms 36 ms 47 ms 115.110.234.170.static.Mumbai.vsnl.net.in [115.1
 16  234.170]
 17  *      *      *      Request timed out.
 18  *      *      *      Request timed out.
 19  *      *      *      Request timed out.
 20  *      *      *      Request timed out.
 21  *      *      *      Request timed out.
 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.
C:\Users\Jignesh>tracert www.ee.iitb.ac.in
```

```
Command Prompt
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\Jignesh>tracert www.mscs.mu.edu
Tracing route to turing.mscs.mu.edu [134.48.4.34]
over a maximum of 30 hops:
  0  4 ms  2 ms  2 ms  192.168.43.1
  1  *      *      *      Request timed out.
  2  43 ms 40 ms 38 ms 10.71.5.13
  3  51 ms 39 ms 39 ms 192.168.70.221
  4  70 ms 39 ms 39 ms 192.168.70.216
  5  *      *      *      Request timed out.
  6  188 ms 35 ms 79 ms 172.25.50.7
  7  *      *      *      Request timed out.
  8  *      *      *      Request timed out.
  9  *      *      *      Request timed out.
 10  *      *      *      Request timed out.
 11  366 ms 38 ms 41 ms 103.198.140.58
 12  294 ms 318 ms 320 ms 103.198.140.27
 13  251 ms 271 ms 523 ms 103.198.140.27
 14  130 ms 159 ms 279 ms hurricane.mrs.franceix.net [37.49.232.13]
 15  199 ms 319 ms 319 ms 100ge4-2.core1.par2.he.net [184.105.222.21]
 16  531 ms 320 ms 236 ms 100ge14-1.core1.nyc4.he.net [184.105.81.77]
 17  513 ms 320 ms 319 ms 100ge2-1.core2.chi1.he.net [184.104.193.173]
 18  *      *      *      Request timed out.
 19  504 ms 249 ms 248 ms r-222wwash-isp-ae6-3926.wisnet.net [140.189.8.1
 20  1050 ms 662 ms 449 ms r-milwaukee-ci-809-isp-ae3-0.wisnet.net [140.189
 21  374 ms 255 ms 416 ms MarquetteUniv.site.wisnet.net [216.56.1.202]
 22  254 ms 264 ms 454 ms 134.48.10.27
 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.
C:\Users\Jignesh>
```

```
Command Prompt
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\Jignesh>tracert www.cs.grinnell.edu

Tracing route to www.cs.grinnell.edu [132.161.132.159]
over a maximum of 30 hops:
  0  3 ms  3 ms  4 ms  192.168.43.1
  1  *  *  *  Request timed out.
  2  104 ms  36 ms  40 ms  10.71.5.13
  3  40 ms  40 ms  39 ms  192.168.70.215
  4  164 ms  39 ms  113 ms  192.168.70.218
  5  *  *  *  Request timed out.
  6  41 ms  61 ms  37 ms  172.25.50.7
  7  *  *  *  Request timed out.
  8  *  *  *  Request timed out.
  9  *  *  *  Request timed out.
 10  *  *  *  Request timed out.
 11  59 ms  55 ms  45 ms  103.198.140.58
 12  153 ms  360 ms  320 ms  103.198.140.27
 13  249 ms  319 ms  319 ms  103.198.140.27
 14  515 ms  465 ms  139 ms  hurricane.mrs.franceix.net [37.49.232.13]
 15  200 ms  318 ms  214 ms  100ge4-2.core1.par2.he.net [184.105.222.21]
 16  267 ms  319 ms  345 ms  100ge4-1.core1.nyc4.he.net [184.105.81.77]
 17  274 ms  299 ms  345 ms  100ge2-1.core2.chi1.he.net [184.104.133.173]
 18  255 ms  359 ms  319 ms  100ge14-2.core1.msp1.he.net [184.105.223.178]
 19  387 ms  320 ms  319 ms  216.66.74.218
 20  *  *  *  peer-as5056.br02.msp1.tfbnw.net [157.240.76.37]
 21  518 ms  *  639 ms  167.142.58.40
 22  282 ms  279 ms  275 ms  67.224.64.62
 23  536 ms  318 ms  379 ms  grinnellcollege1.desm.netins.net [167.142.65.43]
 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.
C:\Users\Jignesh>
```

```
Command Prompt
Tracing route to cs2.eps.its.man.ac.uk [130.88.101.49]
over a maximum of 30 hops:
  0  3 ms  3 ms  2 ms  192.168.43.1
  1  *  *  *  Request timed out.
  2  116 ms  79 ms  54 ms  10.71.5.29
  3  419 ms  44 ms  43 ms  192.168.70.217
  4  62 ms  63 ms  38 ms  192.168.70.216
  5  *  *  *  Request timed out.
  6  51 ms  38 ms  39 ms  172.25.50.7
  7  *  *  *  Request timed out.
  8  *  *  *  Request timed out.
  9  *  *  *  Request timed out.
 10  *  *  *  Request timed out.
 11  82 ms  57 ms  46 ms  103.198.140.176
 12  201 ms  293 ms  319 ms  103.198.140.45
 13  344 ms  170 ms  158 ms  103.198.140.54
 14  196 ms  179 ms  165 ms  103.198.140.45
 15  399 ms  321 ms  317 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14
 16  196.811]
 17  173 ms  360 ms  197 ms  be3671.ccr51.lhr01.atlas.cogentco.com [130.117.4
 18  179 ms  362 ms  319 ms  be3487.ccr41.lon13.atlas.cogentco.com [154.54.60
 19  217 ms  321 ms  319 ms  be2868.ccr21.lon01.atlas.cogentco.com [154.54.57
 20  185 ms  351 ms  316 ms  ldn-b1-link.telvia.net [62.115.9.28]
 21  *  388 ms  229 ms  ldn-bb3-link.telvia.net [62.115.120.74]
 22  369 ms  178 ms  622 ms  ldn-b2-link.telvia.net [62.115.122.189]
 23  *  *  *  jisc-ic-345131-ldn-b4.c.telvia.net [62.115.175.13
 24  964 ms  306 ms  319 ms  ae24.londhx-sbr1.ja.net [146.97.35.197]
 25  179 ms  361 ms  345 ms  ae23.londpg-sbr2.ja.net [146.97.33.21]
 26  170 ms  335 ms  345 ms  ae31.erdisg-sbr2.ja.net [146.97.33.22]
 27  285 ms  319 ms  320 ms  ae23.mancrh-sbr2.ja.net [146.97.33.42]
 28  171 ms  161 ms  181 ms  ae23.mancrh-nbr1.ja.net [146.97.38.42]
 29  207 ms  *  *  universityofmanchester.ja.net [146.97.169.2]
 30  178 ms  281 ms  287 ms  130.88.249.194
 31  *  *  *  Request timed out.

Trace complete.
C:\Users\Jignesh>
```

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



```
Command Prompt
C:\Users\Jignesh>tracert math.hws.edu
Tracing route to math.hws.edu [64.89.144.237]
over a maximum of 30 hops:
  0  4 ms    2 ms    2 ms  192.168.43.1
  1  *        *        *        Request timed out.
  2  53 ms   39 ms   59 ms  10.71.5.19
  3  71 ms   188 ms  44 ms  192.168.70.215
  4  75 ms   43 ms   40 ms  192.168.70.218
  5  *        *        *        Request timed out.
  6  55 ms   39 ms   48 ms  172.25.50.6
  7  *        *        *        Request timed out.
  8  *        *        *        Request timed out.
  9  *        *        *        Request timed out.
 10  *        *        *        Request timed out.
 11  66 ms   39 ms   49 ms  103.198.140.176
 12  177 ms  187 ms  181 ms  103.198.140.45
 13  227 ms  177 ms  177 ms  103.198.140.29
 14  237 ms  173 ms  465 ms  103.198.140.45
 15  165 ms  159 ms  157 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14
 16  317 ms  376 ms  252 ms  be3671.ccr51.lhr01.atlas.cogentco.com [130.117.4
 17  481 ms 1059 ms 219 ms  be3487.ccr41.lon13.atlas.cogentco.com [154.54.60
 18  178 ms  314 ms  163 ms  be2870.ccr22.lon01.atlas.cogentco.com [154.54.58
 19  169 ms  313 ms  184 ms  ae-7.edge7.London1.Level3.net [4.68.62.41]
 20  190 ms  622 ms  257 ms  ae-227-3603.edge3.London15.Level3.net [4.69.167.
 21  186 ms  184 ms  164 ms  ae-227-3603.edge3.London15.Level3.net [4.69.167.
 22  439 ms  239 ms  162 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 23  438 ms  319 ms  613 ms  roc1-ar5-xe-11-0-0-us.twtelecom.net [35.248.1.
 24  486 ms  320 ms  318 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 25  595 ms  318 ms  299 ms  64.89.144.100
 26  *        *        *        Request timed out.
 27  *        *        *        Request timed out.
 28  *        *        *        Request timed out.
 29  *        *        *        Request timed out.
 30  *        *        *        Request timed out.
```

```
Command Prompt
C:\Users\Jignesh>tracert www.hws.edu
Tracing route to www.hws.edu [64.89.145.159]
over a maximum of 30 hops:
  0  3 ms    2 ms    2 ms  192.168.43.1
  1  *        *        *        Request timed out.
  2  42 ms   36 ms   39 ms  10.71.5.13
  3  78 ms   61 ms   38 ms  192.168.70.215
  4  76 ms   54 ms   44 ms  192.168.70.218
  5  *        *        *        Request timed out.
  6  74 ms   36 ms   39 ms  172.25.50.7
  7  *        *        *        Request timed out.
  8  *        *        *        Request timed out.
  9  *        *        *        Request timed out.
 10  *        *        *        Request timed out.
 11  64 ms   65 ms   37 ms  103.198.140.174
 12  297 ms  320 ms  319 ms  103.198.140.45
 13  235 ms  322 ms  317 ms  103.198.140.56
 14  193 ms  319 ms  223 ms  103.198.140.107
 15  228 ms  320 ms  319 ms  103.198.140.45
 16  244 ms  319 ms  319 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14
 17  266 ms  328 ms  310 ms  be3672.ccr52.lhr01.atlas.cogentco.com [130.117.4
 18  209 ms  157 ms  182 ms  be3488.ccr42.lon13.atlas.cogentco.com [154.54.60
 19  408 ms  311 ms  319 ms  be2869.ccr22.lon01.atlas.cogentco.com [154.54.57
 20  243 ms  174 ms  163 ms  ae-7.edge7.London1.Level3.net [4.68.62.41]
 21  164 ms  172 ms  320 ms  ae-228-3604.edge3.London15.Level3.net [4.69.167.
 22  759 ms  730 ms  662 ms  ae-228-3604.edge3.London15.Level3.net [4.69.167.
 23  720 ms  170 ms  175 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 24  445 ms  320 ms  318 ms  roc1-ar5-xe-11-0-0-us.twtelecom.net [35.248.1.
 25  323 ms  318 ms  372 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 26  373 ms  324 ms  634 ms  nat.hws.edu [64.89.144.100]
 27  *        *        *        Request timed out.
 28  *        *        *        Request timed out.
 29  *        *        *        Request timed out.
 30  *        *        *        Request timed out.
```

Ans : On using traceroute command for [www.hws.edu](http://www.hws.edu) and [math.hws.edu](http://math.hws.edu), we observe that The ip address at hop 21 is different for both the websites. [math.hws.edu](http://math.hws.edu) goes at ae-7.edge7.London1.Level3.net [4.69.167.98] whereas [hws.edu](http://hws.edu) goes at lag-3.ear2.London2.Level3.net [4.69.167.102]



**Exercise 3:** 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.

The image displays two screenshots of a Windows Command Prompt window, showing the output of the `tracert` command for the destination `www.ee.iitb.ac.in` (IP: 103.21.125.132).

**Top Screenshot:**

```

C:\Users\Jignesh>tracert www.ee.iitb.ac.in

Tracing route to www.ee.iitb.ac.in [103.21.125.132]
over a maximum of 30 hops:
  0  4 ms  3 ms  3 ms  192.168.43.1
  1  *  *  *  Request timed out.
  2  386 ms  42 ms  49 ms  10.71.16.2
  3  105 ms  69 ms  37 ms  192.168.69.158
  4  47 ms  38 ms  41 ms  192.168.69.159
  5  401 ms  60 ms  42 ms  172.16.80.107
  6  64 ms  52 ms  52 ms  172.17.119.4
  7  *  *  *  Request timed out.
  8  *  *  *  Request timed out.
  9  *  *  *  Request timed out.
 10  41 ms  37 ms  58 ms  115.110.206.73.static-Mumbai.vsnl.net.in [115.11
 11  206.731
 12  25 ms  53 ms  46 ms  115.113.165.62.static-mumbai.vsnl.net.in [115.11
 13  165.621
 14  *  *  *  Request timed out.
 15  63 ms  36 ms  47 ms  115.110.234.170.static.Mumbai.vsnl.net.in [115.1
 16  234.1701
 17  *  *  *  Request timed out.
 18  *  *  *  Request timed out.
 19  *  *  *  Request timed out.
 20  *  *  *  Request timed out.
 21  *  *  *  Request timed out.
 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.
C:\Users\Jignesh>tracert www.ee.iitb.ac.in

```

**Bottom Screenshot:**

```

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Jignesh>tracert www.ee.iitb.ac.in

Tracing route to www.ee.iitb.ac.in [103.21.125.132]
over a maximum of 30 hops:
  0  2 ms  2 ms  2 ms  192.168.43.1
  1  *  *  *  Request timed out.
  2  47 ms  50 ms  48 ms  10.71.5.29
  3  43 ms  39 ms  168 ms  192.168.70.217
  4  121 ms  85 ms  53 ms  192.168.70.216
  5  *  *  *  Request timed out.
  6  37 ms  39 ms  40 ms  172.25.50.7
  7  *  *  *  Request timed out.
  8  *  *  *  Request timed out.
  9  *  *  *  Request timed out.
 10  *  *  *  Request timed out.
 11  *  *  *  Request timed out.
 12  *  *  *  Request timed out.
 13  50 ms  45 ms  49 ms  115.249.214.165
 14  *  *  *  Request timed out.
 15  504 ms  *  73 ms  124.124.195.101
 16  *  *  *  Request timed out.
 17  *  *  *  Request timed out.
 18  *  *  *  Request timed out.
 19  *  *  *  Request timed out.
 20  67 ms  69 ms  70 ms  115.110.234.170.static.Mumbai.vsnl.net.in [115.1
 21  234.1701
 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.
C:\Users\Jignesh>

```

*ANS : Traceroute command was executed for the website ee.iitb.ac.in first on 25 – 08 – 20 and for the second time on 1 – 09– 20 . The path followed was the same on both occasions. The RTT was different as seen in the images.*

#### **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 tracerouting follows a particular path from the user's IP address through the IP addresses of the ISP and then the path depends on which access point is ready to respond and which access points or routers have firewalls configured for blocking the requests and accordingly, the destination can be reached through different paths at different times.*

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 : there is, larger the distance larger is the number of nodes, which will require more hops in order to reach the destination as more number of access points will be used for routing..*

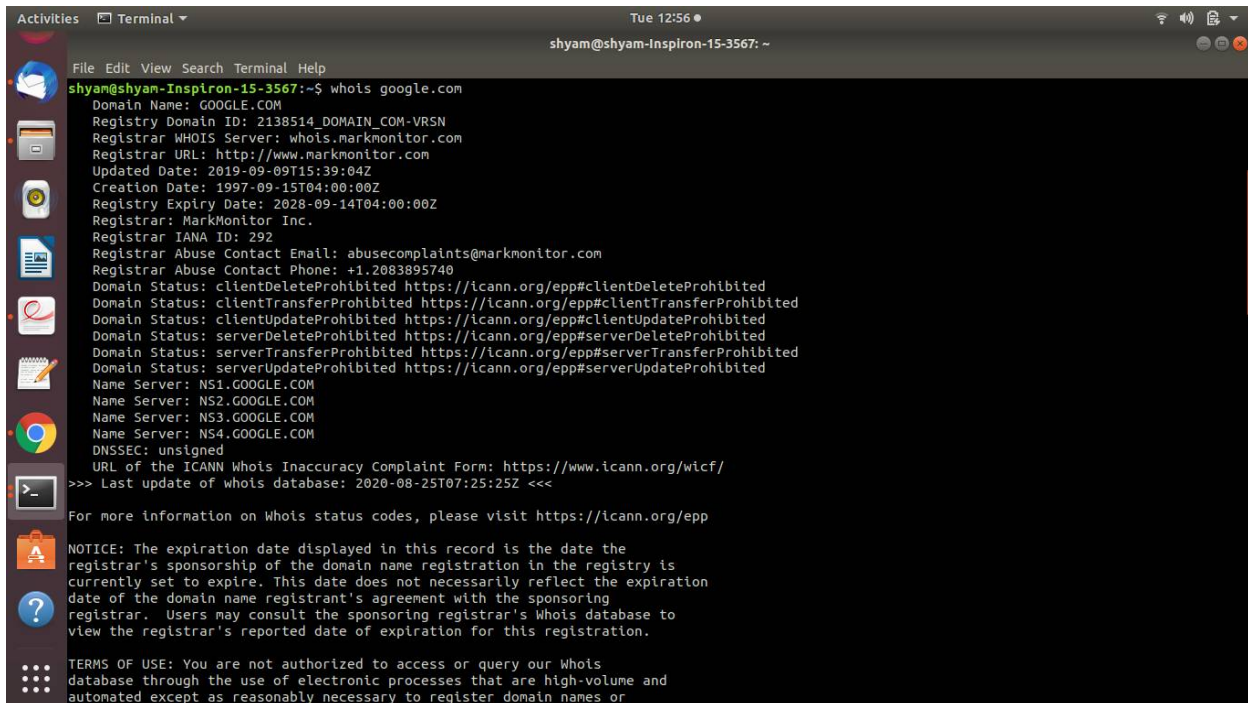
3. Is there a relationship between the number of nodes that show up in the traceroute and latency of the host (from your ping results above)? Does the same relationship hold for all hosts?

*Ans : Since the two hosts were of the same institution there were certain nodes that were common on running the tracert command. If the location of the host is farther away then generally it means more hops (more nodes/steps). The main difference between Ping and Traceroute is that Ping is a quick and easy utility to tell if the specified server is reachable and how long will it take to send and receive data from the server whereas Traceroute finds the exact route taken to reach the server and time taken by each step (hop).*

**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*).



```
Activities  Terminal  Tue 12:56 ● shyam@shyam-Inspiron-15-3567: ~  
File Edit View Search Terminal Help  
shyam@shyam-Inspiron-15-3567:~$ whois google.com  
Domain Name: GOOGLE.COM  
Registry Domain ID: 2138514 DOMAIN_COM-VRSN  
Registrar WHOIS Server: whois.markmonitor.com  
Registrar URL: http://www.markmonitor.com  
Updated Date: 2019-09-09T15:39:04Z  
Creation Date: 1997-09-15T04:00:00Z  
Registry Expiry Date: 2028-09-14T04:00:00Z  
Registrar: MarkMonitor Inc.  
Registrar IANA ID: 292  
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com  
Registrar Abuse Contact Phone: +1.2083895740  
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited  
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited  
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited  
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited  
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited  
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited  
Name Server: NS1.GOOGLE.COM  
Name Server: NS2.GOOGLE.COM  
Name Server: NS3.GOOGLE.COM  
Name Server: NS4.GOOGLE.COM  
DNSSEC: unsigned  
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/  
>>> Last update of whois database: 2020-08-25T07:25:25Z <<<  
  
For more information on Whois status codes, please visit https://icann.org/epp  
  
NOTICE: The expiration date displayed in this record is the date the  
registrar's sponsorship of the domain name registration in the registry is  
currently set to expire. This date does not necessarily reflect the expiration  
date of the domain name registrant's agreement with the sponsoring  
registrar. Users may consult the sponsoring registrar's Whois database to  
view the registrar's reported date of expiration for this registration.  
  
TERMS OF USE: You are not authorized to access or query our Whois  
database through the use of electronic processes that are high-volume and  
automated except as reasonably necessary to register domain names or
```



```
Activities Terminal Tue 12:58 shyam@shyam-Inspiron-15-3567: ~
File Edit View Search Terminal Help
TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T08:39:04-0700
Creation Date: 1997-09-15T00:00:00-0700
Registrar Registration Expiration Date: 2028-09-13T00:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
```

```
Activities Terminal Tue 12:58 shyam@shyam-Inspiron-15-3567: ~
File Edit View Search Terminal Help
https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domain's Registrant, Administrative, or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANN's Temporary Specification. To verify that you are not a
robot, please enter your email address to receive a link to a page that
facilitates email communication with the relevant contact(s).

Web-based WHOIS:
https://domains.markmonitor.com/whois

If you have a legitimate interest in viewing the non-public WHOIS details, send
your request and the reasons for your request to whoisrequest@markmonitor.com
and specify the domain name in the subject line. We will review that request and
may ask for supporting documentation and explanation.

The data in MarkMonitor's WHOIS database is provided for information purposes,
and to assist persons in obtaining information about or related to a domain
name's registration record. While MarkMonitor believes the data to be accurate,
the data is provided "as is" with no guarantee or warranties regarding its
accuracy.

By submitting a WHOIS query, you agree that you will use this data only for
lawful purposes and that, under no circumstances will you use this data to:
(1) allow, enable, or otherwise support the transmission by email, telephone,
or facsimile of mass, unsolicited, commercial advertising, or spam; or
(2) enable high volume, automated, or electronic processes that send queries,
data, or email to MarkMonitor (or its systems) or the domain name contacts (or
its systems).

MarkMonitor reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

MarkMonitor Domain Management(TM)
Protecting companies and consumers in a digital world.

Visit MarkMonitor at https://www.markmonitor.com
```

**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.

ANSWER :

? **Domain:** This field will give you the domain name which we are querying the WHOIS details. Here domain name is google.com  
 ? **Registrar Name :** The registrar is an (ICANN) accredited organization, that sells domain names to the public. Here is MarkMonitor, Inc.  
 ? **Creation Date:** This is the date when the domain name was first registered. Here it is 1997-09-15  
 ? **Expiration Date:** This is the date when the domain will expire. Here it is 2028 – 09-13.  
 ? **Updated Date:** This is the date when the WHOIS details last updated. Here it is 2019-09-09  
 ? **Status:** This is the registrar status of the domain. clientDeleteProhibited: Tells domain's registry to reject requests to delete the domain. clientUpdateProhibited:- Tells domain's registry to reject requests to update the domain. clientTransferProhibited:- tells domain's registry to reject requests to transfer the domain from your current registrar to another. serverDeleteProhibited:- Prevents domain from being deleted. serverUpdateProhibited:- locks domain preventing it from being updated. serverTransferProhibited:- Prevents domain from being transferred from your current registrar to another.  
**Nameservers:** Nameservers essentially tell you where a domain's DNS records are stored. Here it is ns4.google.com, ns3.google.com, ns2.google.com, ns1.google.com  
 ? **Registrant Contact Details:** A registrant is the person or organization or company who registers a domain name. This area provides you with details of the registrant of a domain. Here organization is Google LLC

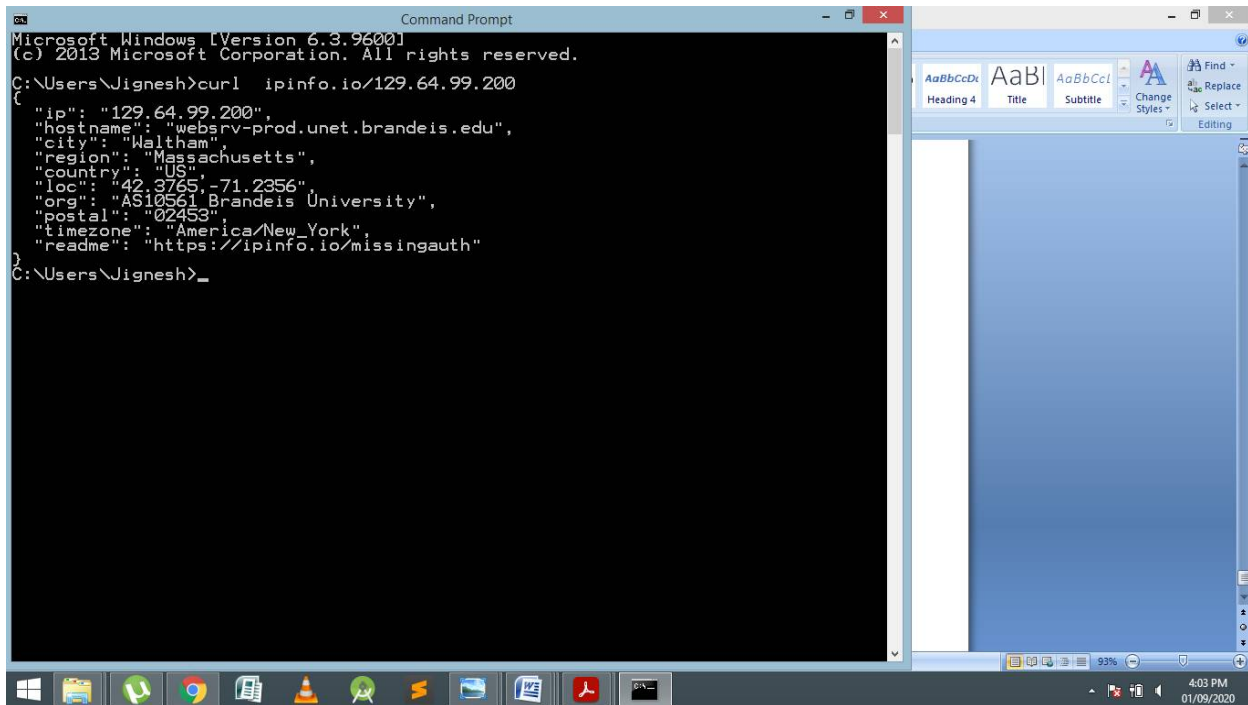
**Exercise 5:** (Should be short.) Because of NAT, the domain namespit.ac.in has a different IP address outside of SPIT than it does on campus. Using information in this lab and working on a home computer, find the outside IP address for spit.ac.in. Explain how you did it.

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
```

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



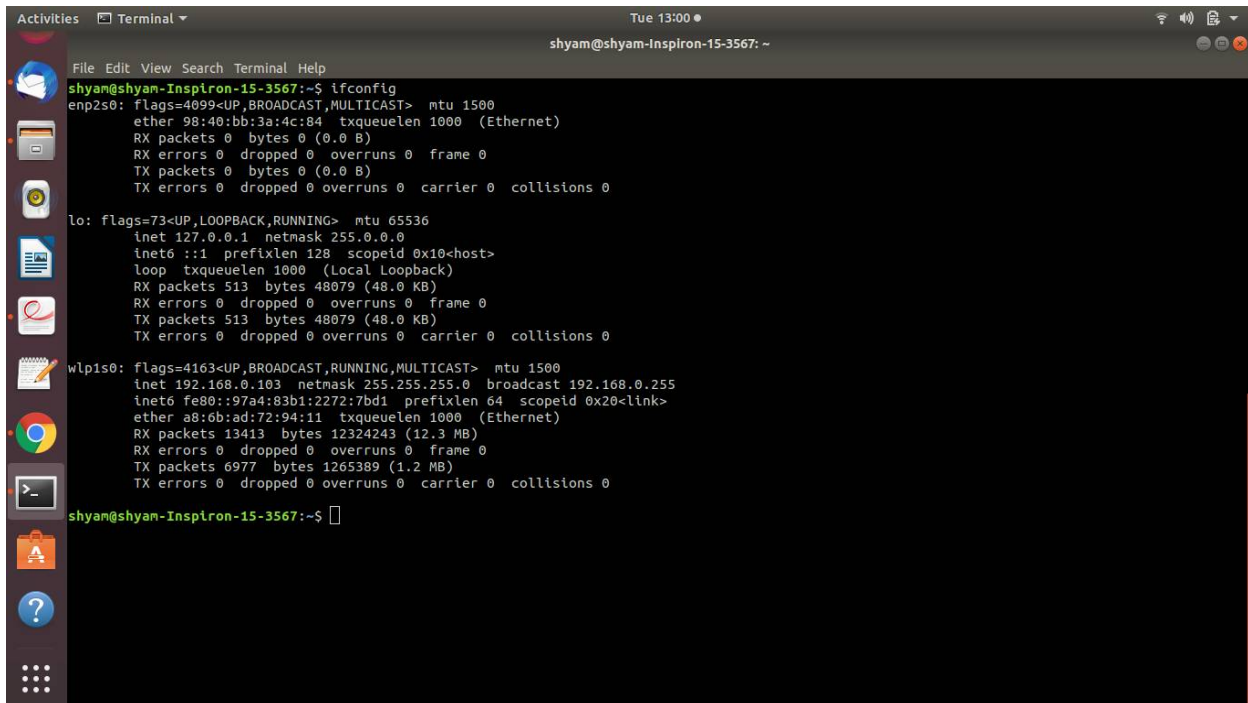
The screenshot shows a Windows 10 desktop environment. On the left, a Command Prompt window is open, displaying the output of a `curl` command. The output is a JSON object containing location and organization data for the IP address 129.64.99.200. On the right, a Microsoft Word document is open, showing a blank page with a blue header and footer area. The taskbar at the bottom includes icons for the Start menu, File Explorer, Google Chrome, and several other applications. The system clock in the bottom right corner indicates the time is 4:03 PM on 01/09/2020.

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Jignesh>curl ipinfo.io/129.64.99.200
{
  "ip": "129.64.99.200",
  "hostname": "websrv-prod.unet.brandeis.edu",
  "city": "Waltham",
  "region": "Massachusetts",
  "country": "US",
  "loc": "42.3765,-71.2356",
  "org": "AS10561 Brandeis University",
  "postal": "02453",
  "timezone": "America/New_York",
  "readme": "https://ipinfo.io/missingauth"
}
C:\Users\Jignesh>
```

**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!!!.)



A terminal window titled "shyam@shyam-Inspiron-15-3567: ~" showing the output of the "ifconfig" command. The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". On the left is a vertical dock with icons for various applications. The terminal output shows details for three network interfaces: enp2s0 (Ethernet), lo (Local Loopback), and wlp1s0 (Ethernet). Each interface listing includes flags, MTU, IP address, netmask, broadcast address, ether address, and statistics for RX and TX packets, bytes, errors, dropped, overruns, carrier, and collisions.

```
shyam@shyam-Inspiron-15-3567:~$ ifconfig
enp2s0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
        ether 98:40:bb:3a:4c:84 txqueuelen 1000 (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 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 513 bytes 48079 (48.0 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 513 bytes 48079 (48.0 KB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.0.103 netmask 255.255.255.0 broadcast 192.168.0.255
        inet6 fe80::97a4:83b1:2272:7bd1 prefixlen 64 scopeid 0x20<link>
        ether a8:6b:ad:72:94:11 txqueuelen 1000 (Ethernet)
        RX packets 13413 bytes 12324243 (12.3 MB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 6977 bytes 1265389 (1.2 MB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

shyam@shyam-Inspiron-15-3567:~$
```

**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.)

```

shyam@shyam-Inspiron-15-3567:~$ netstat -p tcp -a
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost:mysql        0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:domain       0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      -
tcp        0      0 shyam-Inspiron-15:57826 sa-in-f188.1e100.n:5228 ESTABLISHED 1907/chrome --type=
tcp        0      0 shyam-Inspiron-15:60240 bom07s25-ln-f5.1e:https ESTABLISHED 1907/chrome --type=
tcp        0      0 shyam-Inspiron-15:38160 whatsapp-cdn-shv-.:https ESTABLISHED 1907/chrome --type=
tcp        0      0 shyam-Inspiron-15:41938 bom07s01-ln-f3.1e:https ESTABLISHED 1907/chrome --type=
tcp        0      0 shyam-Inspiron-15:53326 bom05s15-ln-f14.1:https ESTABLISHED 1907/chrome --type=
tcp        0      0 shyam-Inspiron-15:39618 172.217.194.189:https ESTABLISHED 1907/chrome --type=
tcp6       0      0 ip6-localhost:ipp      [::]:*                 LISTEN      -
udp        0      0 localhost:domain       0.0.0.0:*               -
udp        0      0 0.0.0.0:bootpc         0.0.0.0:*               -
udp        0      0 0.0.0.0:45274          0.0.0.0:*               -
udp        0      0 0.0.0.0:ipp            0.0.0.0:*               -
udp        0      0 224.0.0.251:mdns       0.0.0.0:*               1907/chrome --type=
udp        0      0 224.0.0.251:mdns       0.0.0.0:*               1863/chrome
udp        0      0 0.0.0.0:mdns           0.0.0.0:*               -
udp6       0      0 [::]:53056             [::]:*                  -
udp6       0      0 [::]:mdns               [::]:*                  -
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags               Type               State         I-Node  PID/Program name  Path
unix    2      [ ]                 DGRAM             -              31936  1353/systemd      /run/user/1000/systemd/notify
unix    2      [ ]                 DGRAM             -              26821  -                  /run/user/121/systemd/notify
unix    2      [ ACC ]            SEQPACKET         LISTENING      13956  -                  /run/udev/control
unix    2      [ ACC ]            STREAM            LISTENING      31939  1353/systemd      /run/user/1000/systemd/private
unix    2      [ ACC ]            STREAM            LISTENING      26824  -                  /run/user/121/systemd/private
unix    2      [ ACC ]            STREAM            LISTENING      31943  1353/systemd      /run/user/1000/gnupg/S.gpg-agent.browser
unix    2      [ ACC ]            STREAM            LISTENING      26828  -                  /run/user/121/gnupg/S.gpg-agent
unix    2      [ ACC ]            STREAM            LISTENING      31944  1353/systemd      /run/user/1000/gnupg/S.gpg-agent.ssh
unix    2      [ ACC ]            STREAM            LISTENING      31945  1353/systemd      /run/user/1000/gnupg/S.gpg-agent.extra
unix    2      [ ACC ]            STREAM            LISTENING      26829  -                  /run/user/121/pulse/native
unix    2      [ ACC ]            STREAM            LISTENING      31946  1353/systemd      /run/user/1000/gnupg/S.gpg-agent

```

```

shyam@shyam-Inspiron-15-3567:~$ netstat -p tcp -a
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost:mysql        0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:domain       0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      -
tcp        0      0 shyam-Inspiron-15:57826 sa-in-f188.1e100.n:5228 ESTABLISHED 1907/chrome --type=
tcp        0      0 shyam-Inspiron-15:60240 bom07s25-ln-f5.1e:https ESTABLISHED 1907/chrome --type=
tcp        0      0 shyam-Inspiron-15:38160 whatsapp-cdn-shv-.:https ESTABLISHED 1907/chrome --type=
tcp        0      0 shyam-Inspiron-15:41938 bom07s01-ln-f3.1e:https ESTABLISHED 1907/chrome --type=
tcp        0      0 shyam-Inspiron-15:53326 bom05s15-ln-f14.1:https ESTABLISHED 1907/chrome --type=
tcp        0      0 shyam-Inspiron-15:39618 172.217.194.189:https ESTABLISHED 1907/chrome --type=
tcp6       0      0 ip6-localhost:ipp      [::]:*                 LISTEN      -
udp        0      0 localhost:domain       0.0.0.0:*               -
udp        0      0 0.0.0.0:bootpc         0.0.0.0:*               -
udp        0      0 0.0.0.0:45274          0.0.0.0:*               -
udp        0      0 0.0.0.0:ipp            0.0.0.0:*               -
udp        0      0 224.0.0.251:mdns       0.0.0.0:*               1907/chrome --type=
udp        0      0 224.0.0.251:mdns       0.0.0.0:*               1863/chrome
udp        0      0 0.0.0.0:mdns           0.0.0.0:*               -
udp6       0      0 [::]:53056             [::]:*                  -
udp6       0      0 [::]:mdns               [::]:*                  -
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags               Type               State         I-Node  PID/Program name  Path
unix    3      [ ]                 STREAM            CONNECTED      32085  1379/dbus-daemon  /run/user/1000/bus
unix    3      [ ]                 STREAM            CONNECTED      29413  -                  /var/run/dbus/system_bus_socket
unix    3      [ ]                 STREAM            CONNECTED      33218  1806/evolution-addr
unix    3      [ ]                 STREAM            CONNECTED      34128  1382/gnome-session-@/tmp/.ICE-unix/1382
unix    3      [ ]                 STREAM            CONNECTED      33080  1485/dbus-daemon  @/tmp/dbus-ZKV2bKSV1o
unix    3      [ ]                 STREAM            CONNECTED      32284  1379/dbus-daemon  /run/user/1000/bus
unix    3      [ ]                 STREAM            CONNECTED      27629  -
unix    2      [ ]                 DGRAM             -              29341  -
unix    3      [ ]                 STREAM            CONNECTED      28679  -
unix    3      [ ]                 SEQPACKET         CONNECTED      33301  1863/chrome
unix    3      [ ]                 DGRAM             -              22290  -
unix    3      [ ]                 STREAM            CONNECTED      63451  1485/dbus-daemon  @/tmp/dbus-ZKV2bKSV1o
unix    3      [ ]                 STREAM            CONNECTED      31515  1747/evolution-cale
unix    3      [ ]                 STREAM            CONNECTED      29985  -                  /run/systemd/journal/stdout
unix    3      [ ]                 STREAM            CONNECTED      26761  -
unix    2      [ ]                 DGRAM             -              20996  -
unix    3      [ ]                 STREAM            CONNECTED      33311  1373/Xorg          @/tmp/.X11-unix/X0
unix    3      [ ]                 STREAM            CONNECTED      31115  1547/libus-dconf
unix    3      [ ]                 STREAM            CONNECTED      27498  -
unix    3      [ ]                 STREAM            CONNECTED      65642  1379/dbus-daemon  /run/user/1000/bus
unix    3      [ ]                 STREAM            CONNECTED      33220  1813/evolution-addr
unix    3      [ ]                 STREAM            CONNECTED      34118  -                  /var/run/dbus/system_bus_socket
unix    3      [ ]                 STREAM            CONNECTED      31392  1379/dbus-daemon  /run/user/1000/bus
unix    3      [ ]                 STREAM            CONNECTED      32958  -                  /run/systemd/journal/stdout
unix    3      [ ]                 STREAM            CONNECTED      27625  -                  @/tmp/dbus-YrhbmWjyVa
unix    2      [ ]                 DGRAM             -              29320  -
unix    3      [ ]                 STREAM            CONNECTED      34209  1379/dbus-daemon  /run/user/1000/bus
unix    3      [ ]                 STREAM            CONNECTED      32310  1625/gsd-sharing
unix    3      [ ]                 STREAM            CONNECTED      23562  -
unix    3      [ ]                 STREAM            CONNECTED      20931  -                  /run/systemd/journal/stdout
unix    3      [ ]                 STREAM            CONNECTED      33119  -                  /run/systemd/journal/stdout
unix    3      [ ]                 STREAM            CONNECTED      28206  -
unix    3      [ ]                 STREAM            CONNECTED      20991  -
unix    3      [ ]                 STREAM            CONNECTED      40927  -                  /run/systemd/journal/stdout
unix    3      [ ]                 STREAM            CONNECTED      31672  1863/chrome
unix    3      [ ]                 STREAM            CONNECTED      31072  1505/gnome-shell
unix    3      [ ]                 STREAM            CONNECTED      29881  -                  /var/run/dbus/system_bus_socket
shyam@shyam-Inspiron-15-3567:~$

```

**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.