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 receieve a response to eachpacket. 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 Linux or Mac OS is:

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

The syntax in Windows is:

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

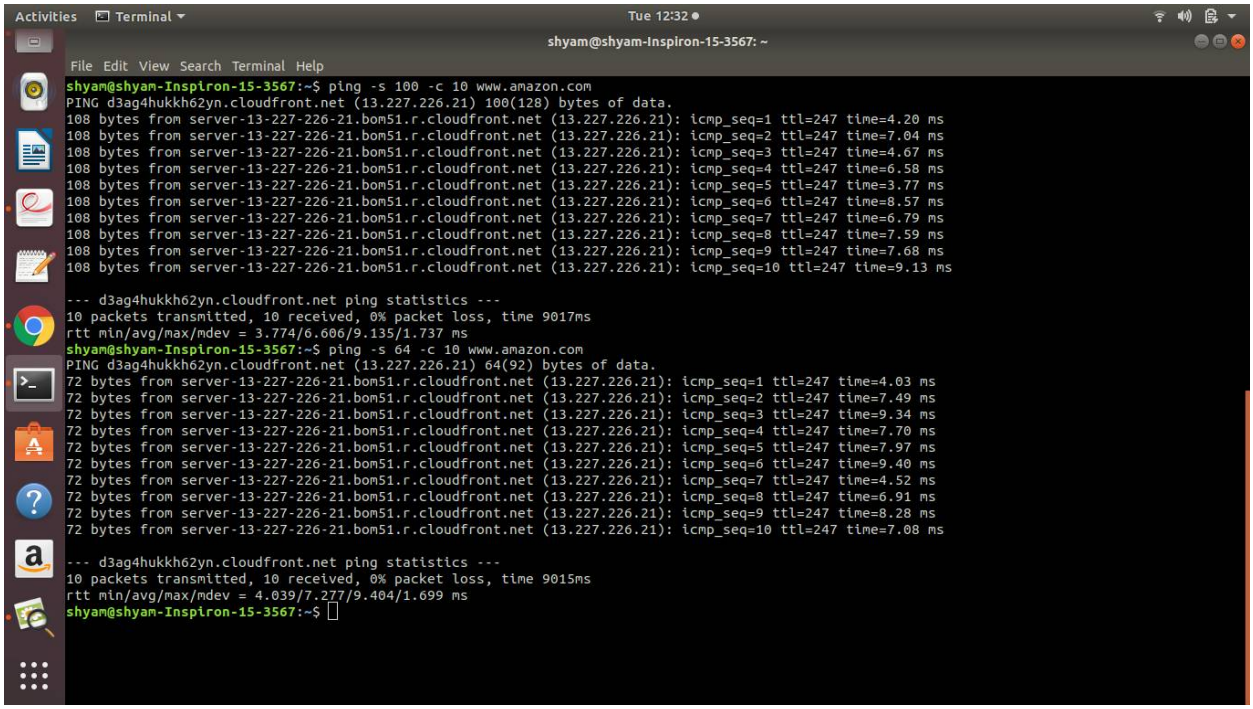
The default number of ICMP packets to send is either infinite (in Linux and Mac OS) or 4 (in Windows). The default packet size is either 64 bytes (in Linux) or 32 bytes (in Windows). You can specify either a hostname (e.g., `spit.ac.in`) or an IP address.

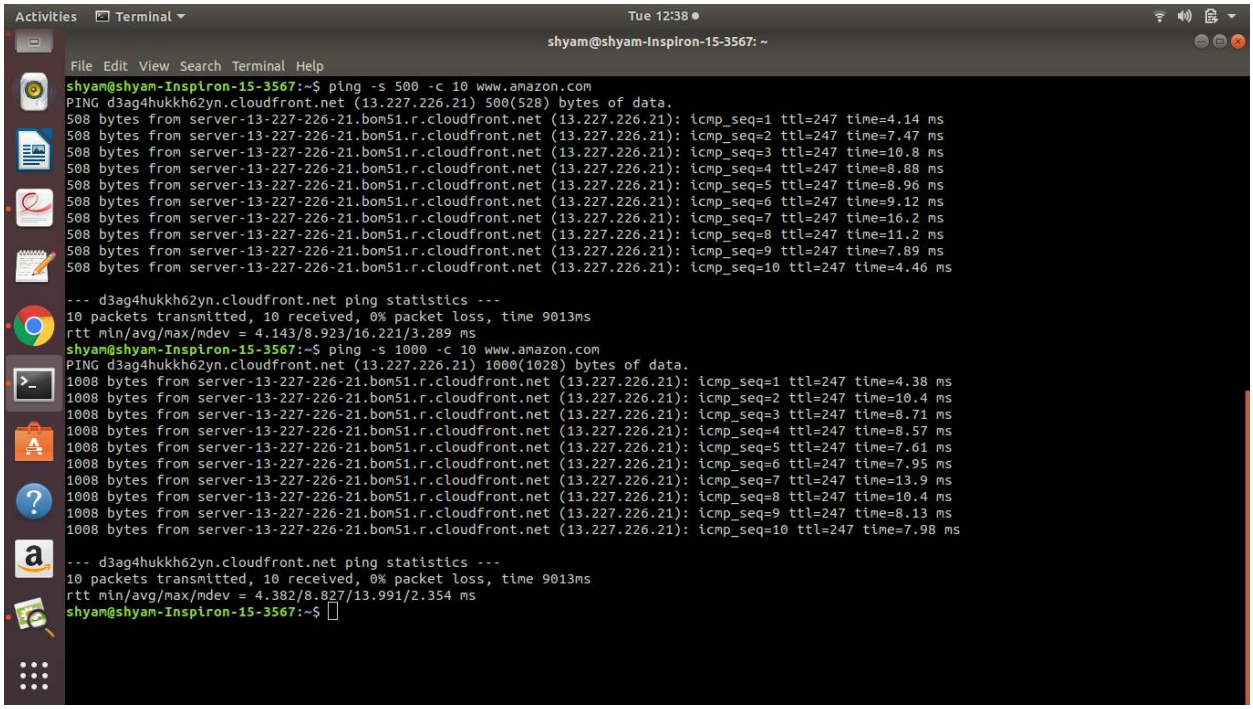
To save the output from `ping` to a file, include a greater than symbol and a file name at the end of the command. For example:

```
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





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`.

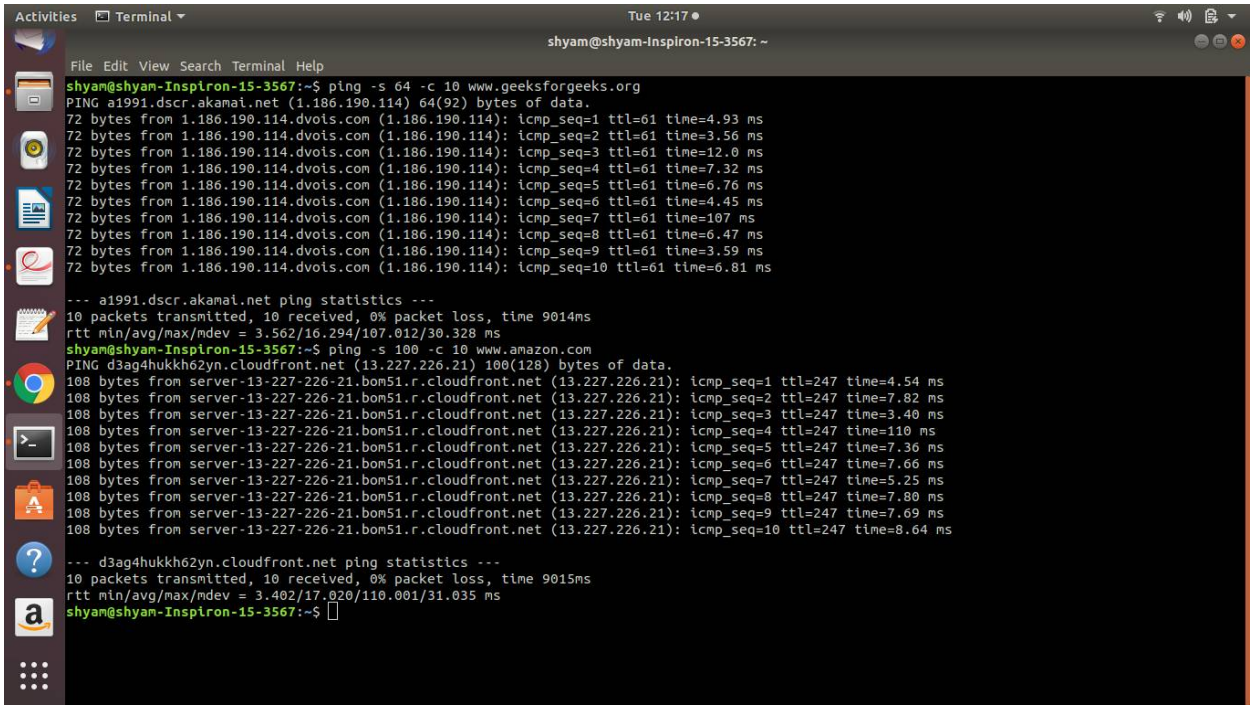
Does the average RTT vary between different hosts? What aspects of latency (transmit, propagation, and queueing delay) might impact this and why?

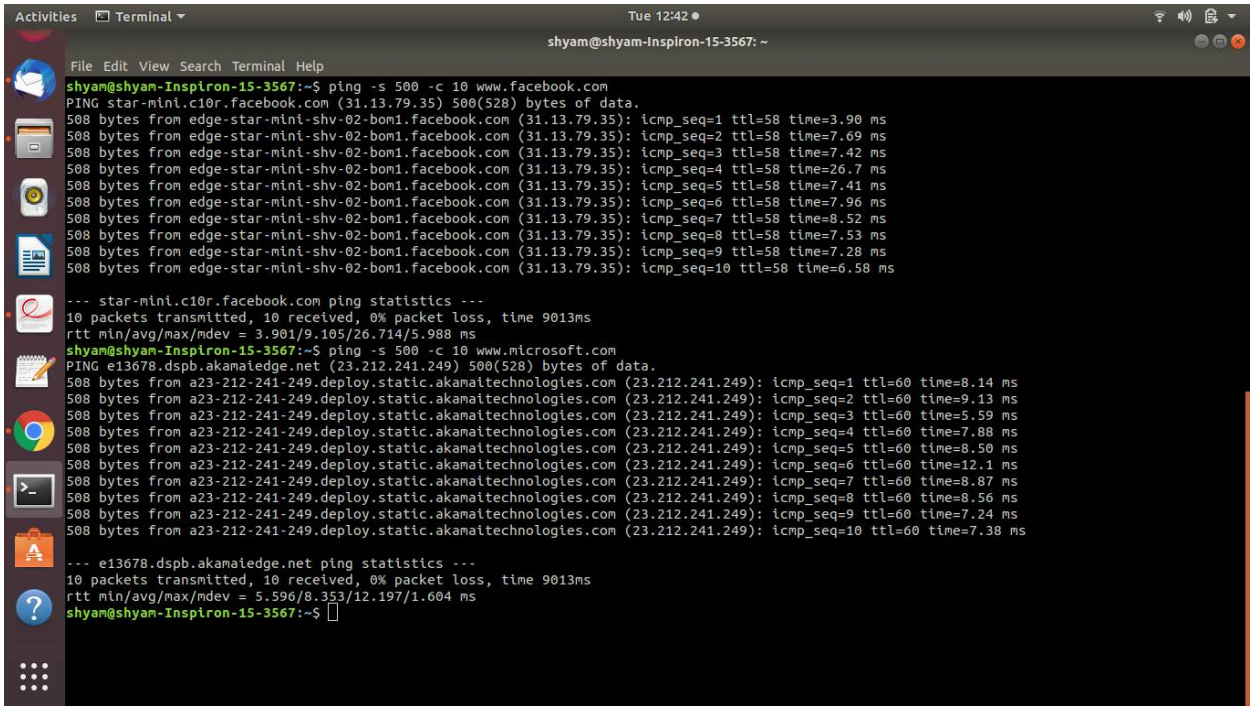
Ans : RTT varies between different hosts. RTT depends on the distance of host, the medium, number of network hops, traffic levels in the network and server response time of the host. Propogation delay depends on distance. Transmission delay depends on the efficiency of medium. Propogation and Transmission 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?

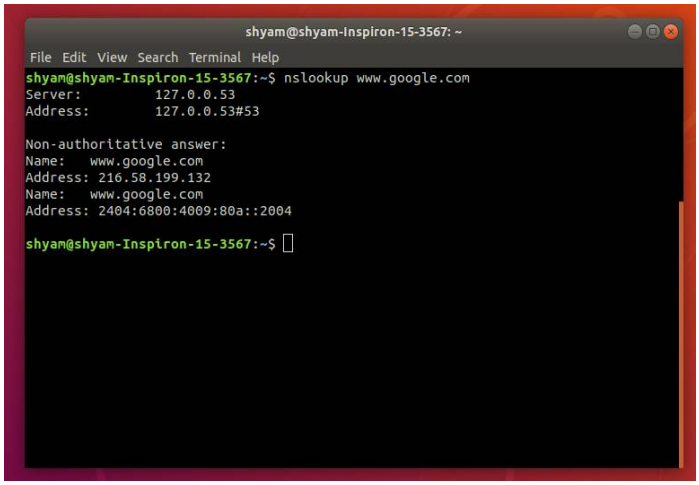
Ans : RTT varies with packet size. RTT increases as packet size increases. Transmission delay depends on size of packet.So, transmission delay might have an impact on this.

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).





nslookup — The command nslookup <host> will do a DNS query to find and report the IP address (oraddresses) 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 nslokup by adding the server name or IP address to the command: nslookup <host><server>



telnet — Telnet is an old program for remote login. It's not used so much for that any more, since it hasno 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 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>
```

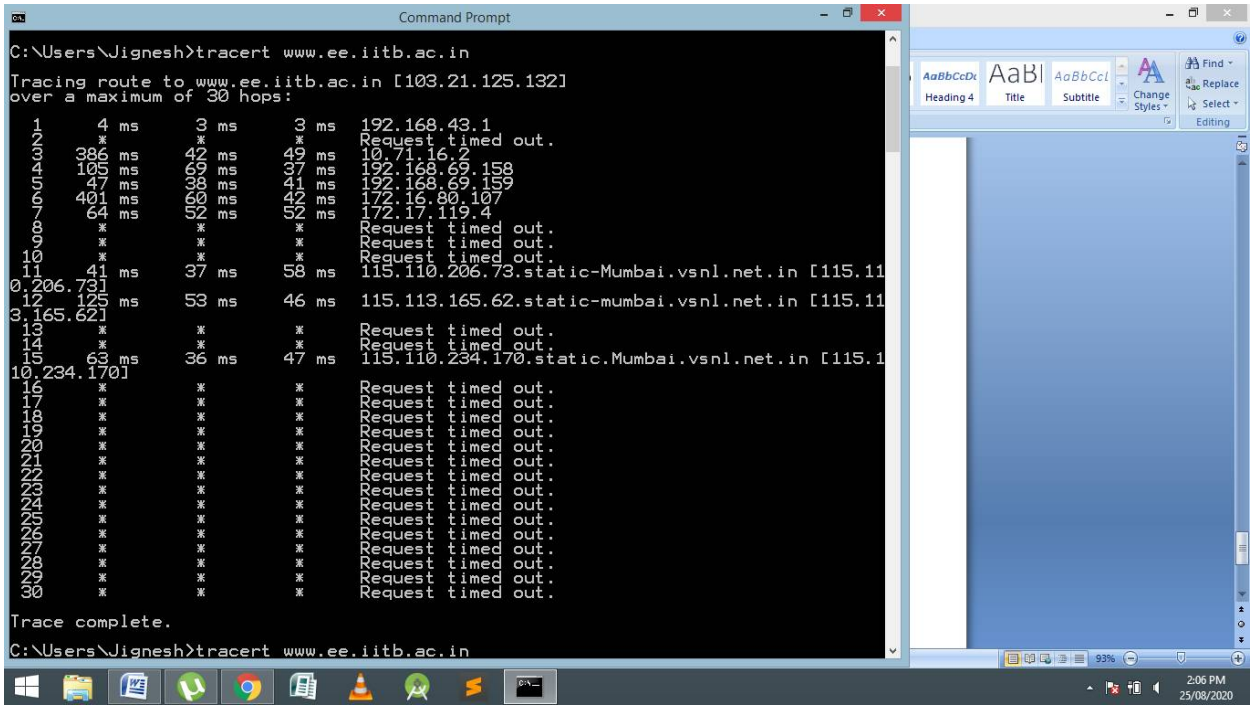
You can specify either a hostname (e.g., `cs.iitb.ac.in`) or an IP address (e.g., `128.105.2.6`).

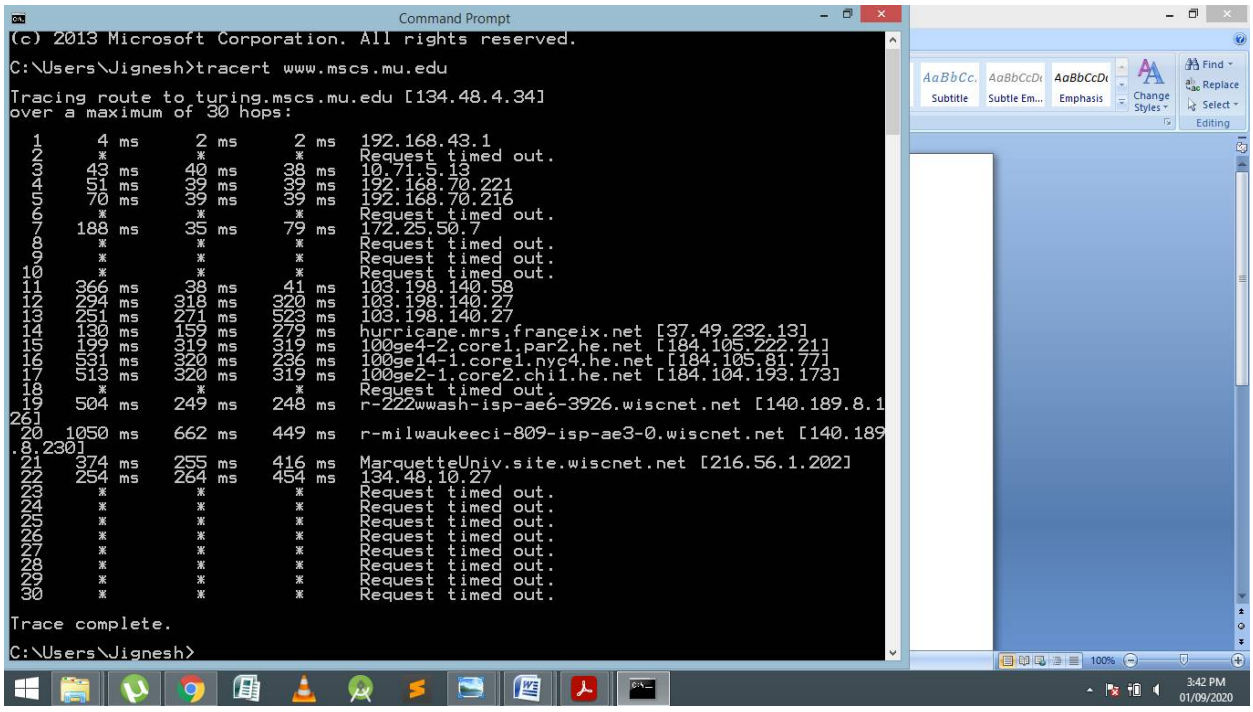
1.2.1 EXPERIMENTS WITH TRACEROUTE

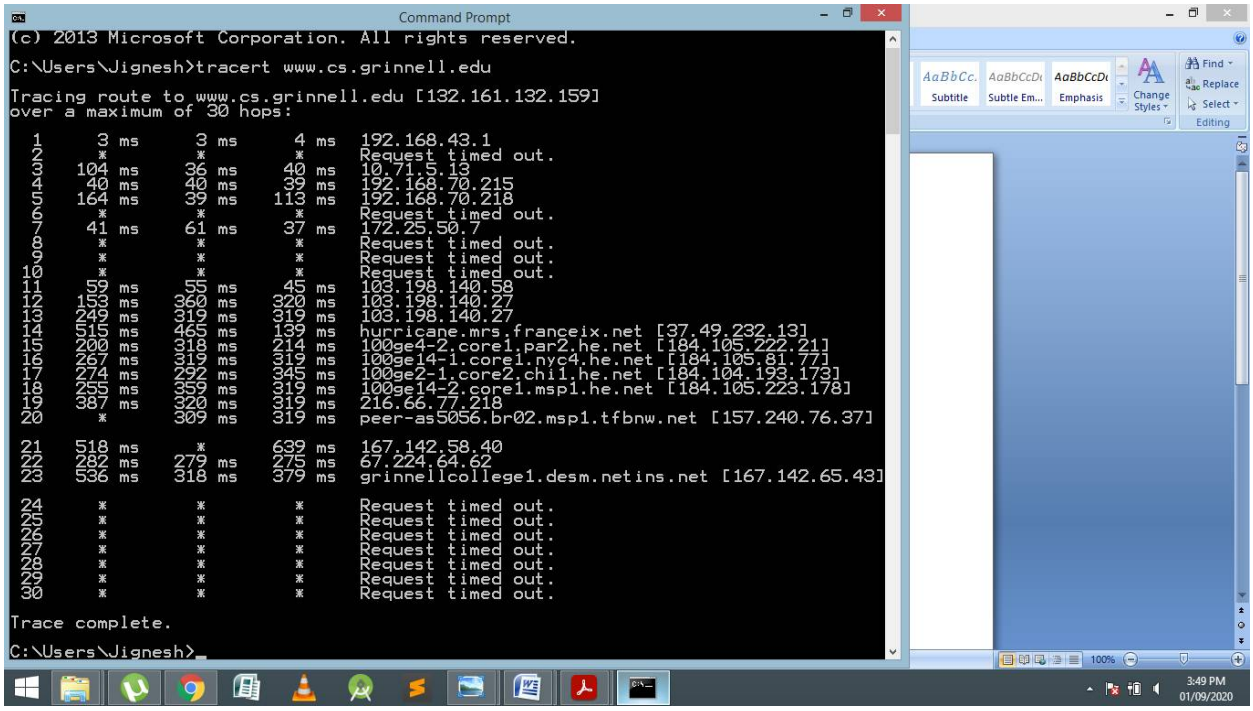
From **your machine** traceroute to the following hosts:

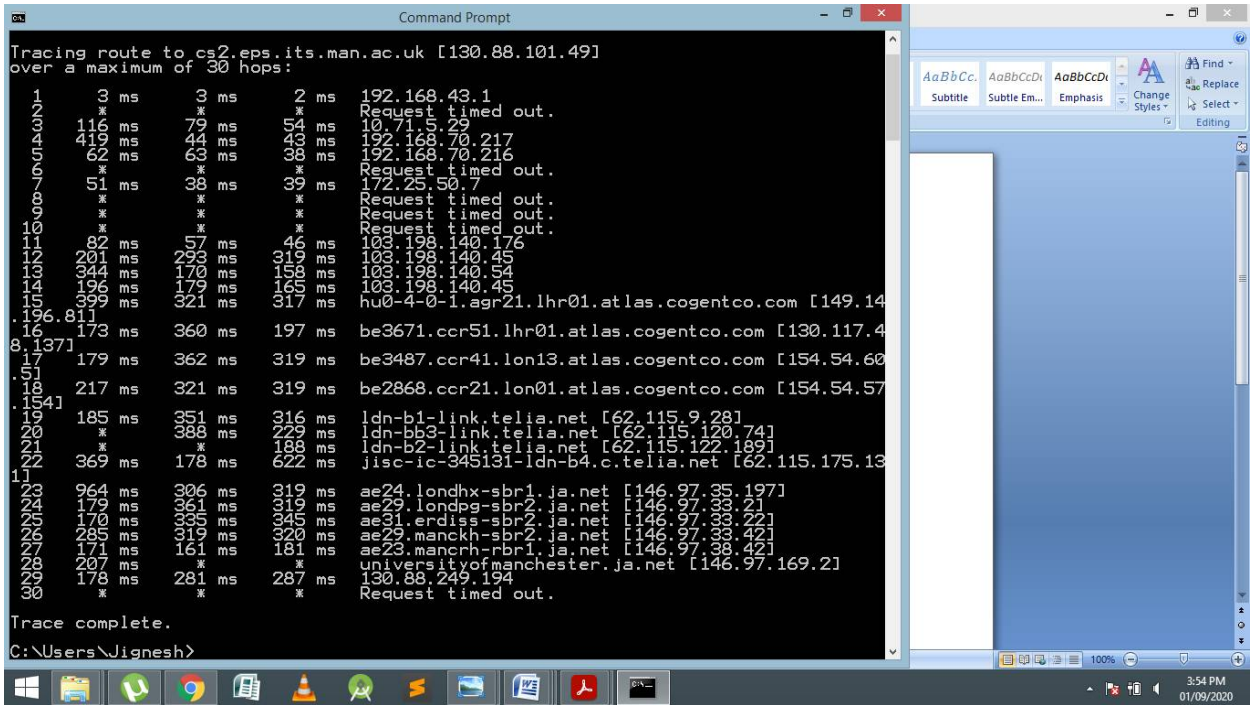
1. ee.iitb.ac.in
2. mscs.mu.edu
3. www.cs.grinnell.edu
4. csail.mit.edu
5. cs.stanford.edu
6. cs.manchester.ac.uk

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`).

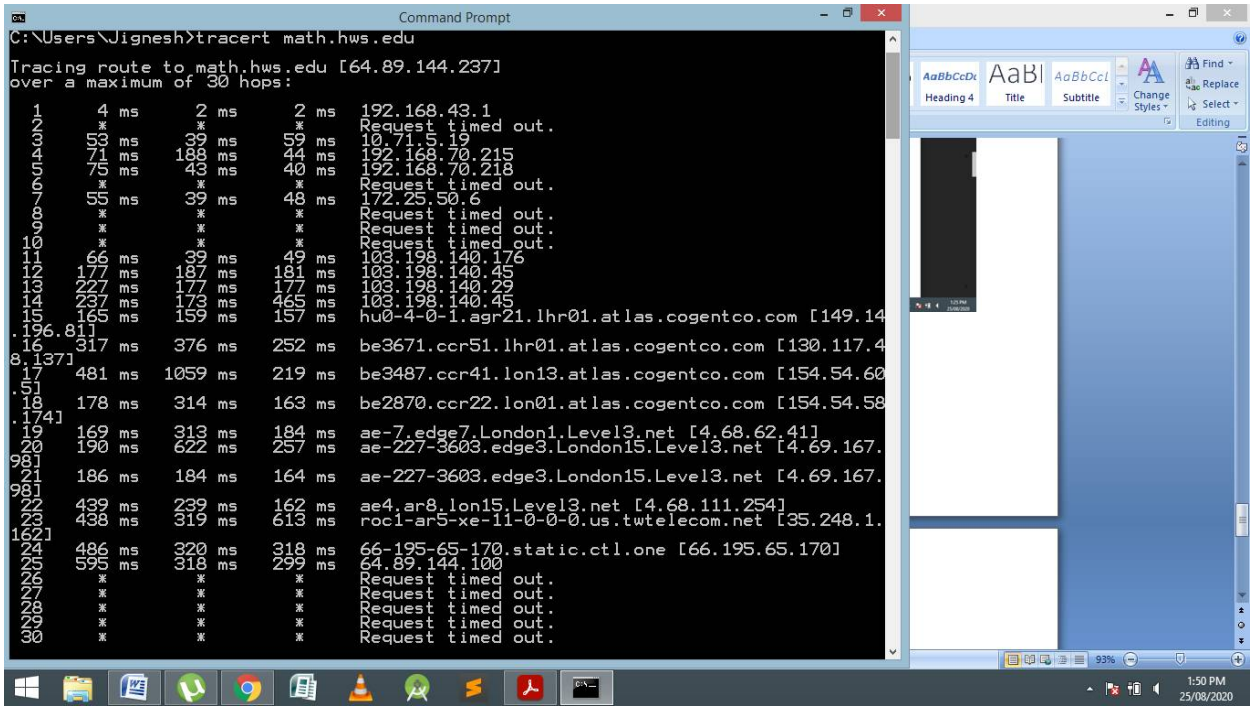

Command Prompt
C:\Users\Jignesh>tracert www.ee.iitb.ac.in
Tracing route to www.ee.iitb.ac.in [103.21.125.132]
over a maximum of 30 hops:
1 4 ms 3 ms 3 ms 192.168.43.1
2 * * * Request timed out.
3 386 ms 42 ms 49 ms 10.71.16.2
4 105 ms 69 ms 37 ms 192.168.69.158
5 47 ms 38 ms 41 ms 192.168.69.159
6 401 ms 60 ms 42 ms 172.16.80.107
7 64 ms 52 ms 52 ms 172.17.119.4
8 * * * Request timed out.
9 * * * Request timed out.
10 * * * Request timed out.
11 41 ms 37 ms 58 ms 115.110.206.73.static-Mumbai.vsnl.net.in [115.110.206.73]
12 125 ms 53 ms 46 ms 115.113.165.62.static-mumbai.vsnl.net.in [115.113.165.62]
13 * * * Request timed out.
14 * * * Request timed out.
15 63 ms 36 ms 47 ms 115.110.234.170.static.Mumbai.vsnl.net.in [115.110.234.170]
16 * * * Request timed out.
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
Heading 4
Title
Subtitle
Change Styles
Find
Replace
Select
Editing
93%
2:06 PM
25/08/2020

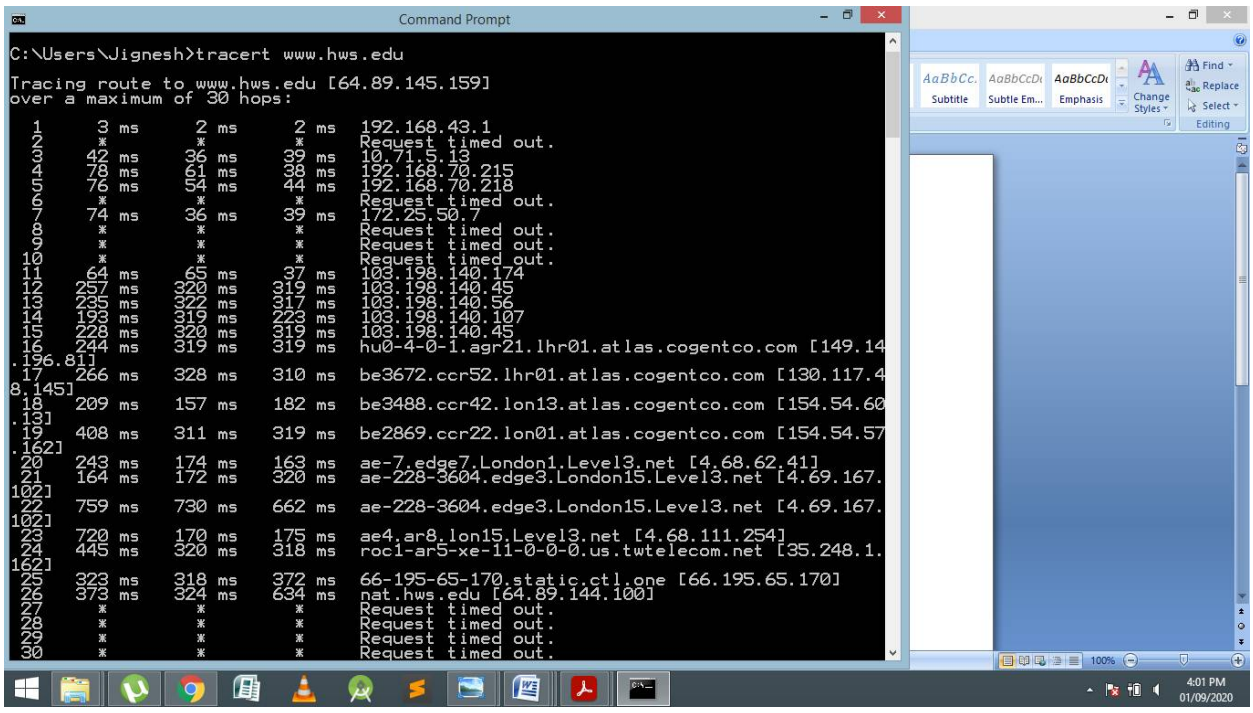

Command Prompt
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\Jignesh>tracert www.mscs.mu.edu
Tracing route to turing.mscs.mu.edu [134.48.4.34]
over a maximum of 30 hops:
1 4 ms 2 ms 2 ms 192.168.43.1
2 * * * Request timed out.
3 43 ms 40 ms 38 ms 10.71.5.13
4 51 ms 39 ms 39 ms 192.168.70.221
5 70 ms 39 ms 39 ms 192.168.70.216
6 * * * Request timed out.
7 188 ms 35 ms 79 ms 172.25.50.7
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.wiscnet.net [140.189.8.126]
20 1050 ms 662 ms 449 ms r-milwaukeeci-809-isp-ae3-0.wiscnet.net [140.189.8.230]
21 374 ms 255 ms 416 ms MarquetteUniv.site.wiscnet.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>
Subtitle
Subtle Em...
Emphasis
Change Styles
Find
Replace
Select
Editing
100%
3:42 PM
01/09/2020





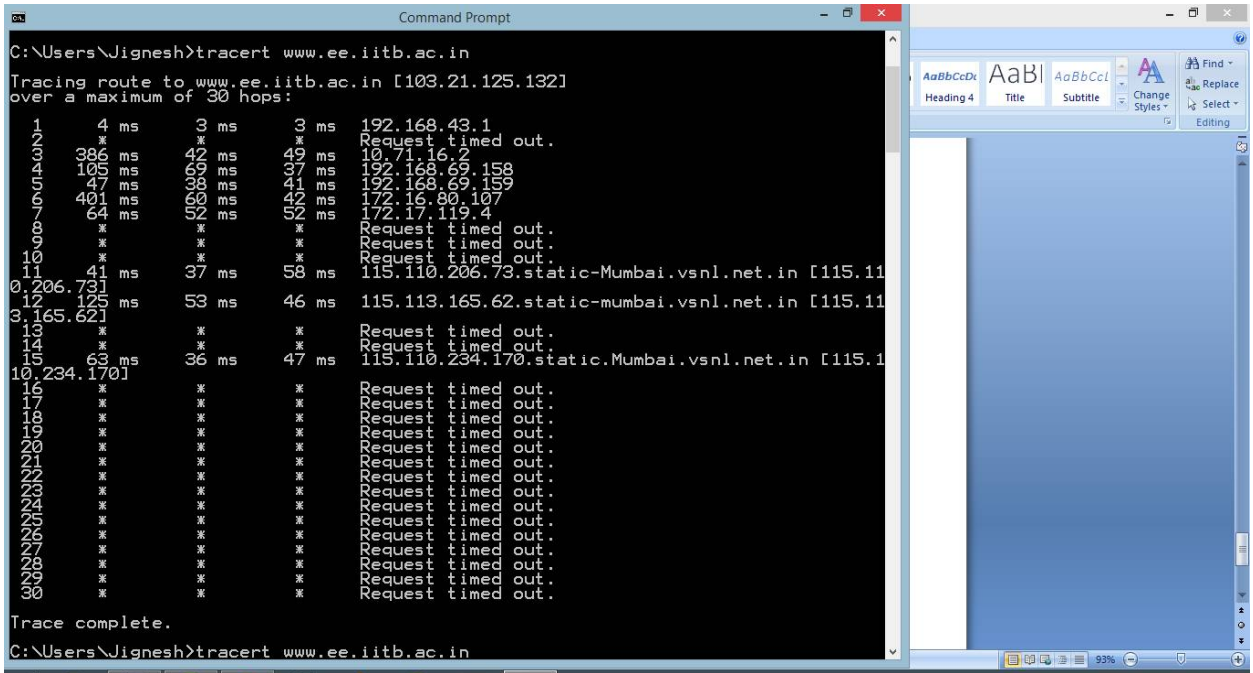
Exercise 2:(Very short.) Use traceroute to trace the route from your computer to math.hws.edu and towww.hws.edu. Explain the difference in the results.

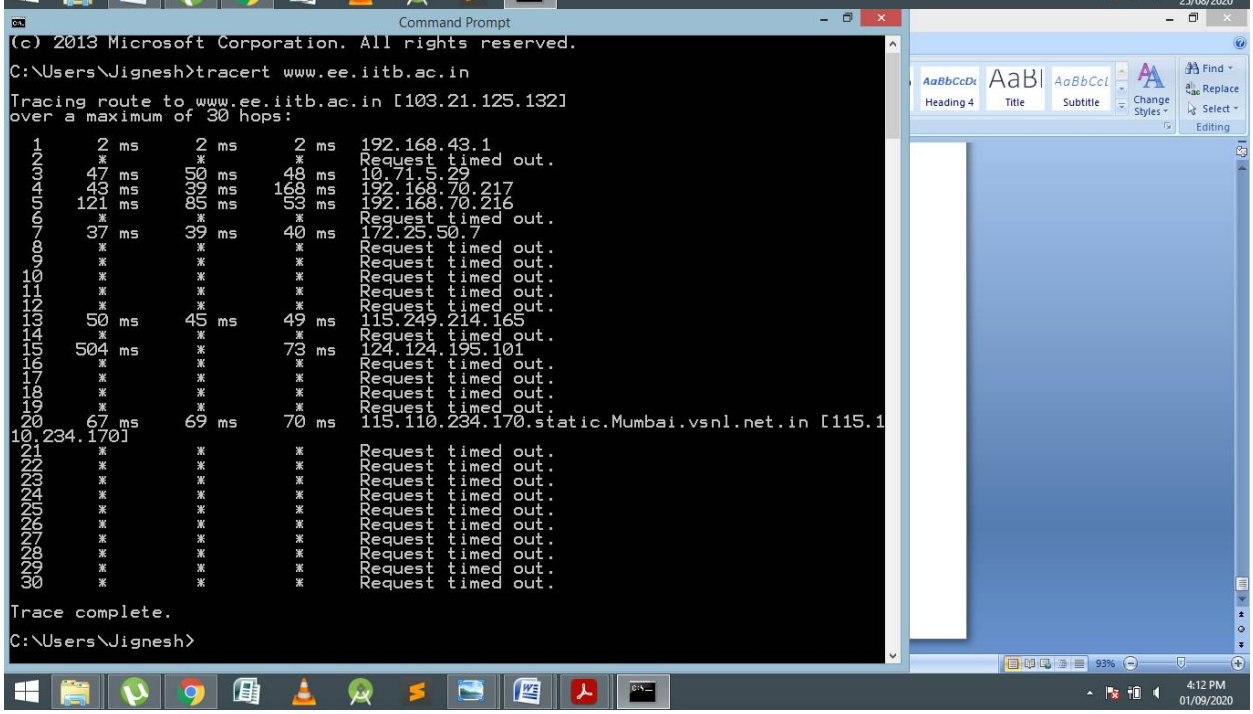




Ans : On using traceroute command for www.hws.edu and math.hws.edu, we observe that The ip address at hop 21 is different for both the websites. math.hws.edu goes at ae-7.edge7.London1.Level3.net [4.69.167.98] whereas hws.edu goes at lag-3.ear2.London2.Level3.net [4.69.167.102]

Exercise 3: Two packets sent from the same source to the same destination do not necessarily follow thesame 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.





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, he 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..

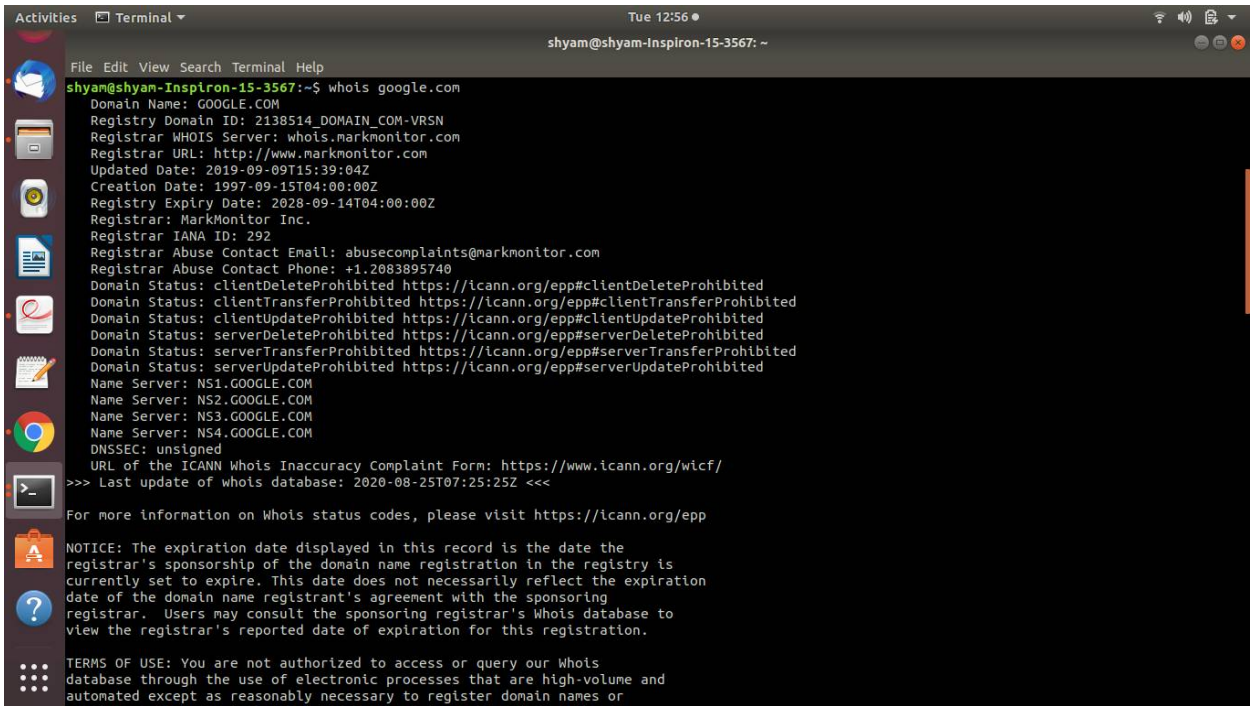
3. Is there a relationship between the number of nodes that show up in the traceroute and latency of the host (from your ping results above)? Does the same relationship hold for all hosts?

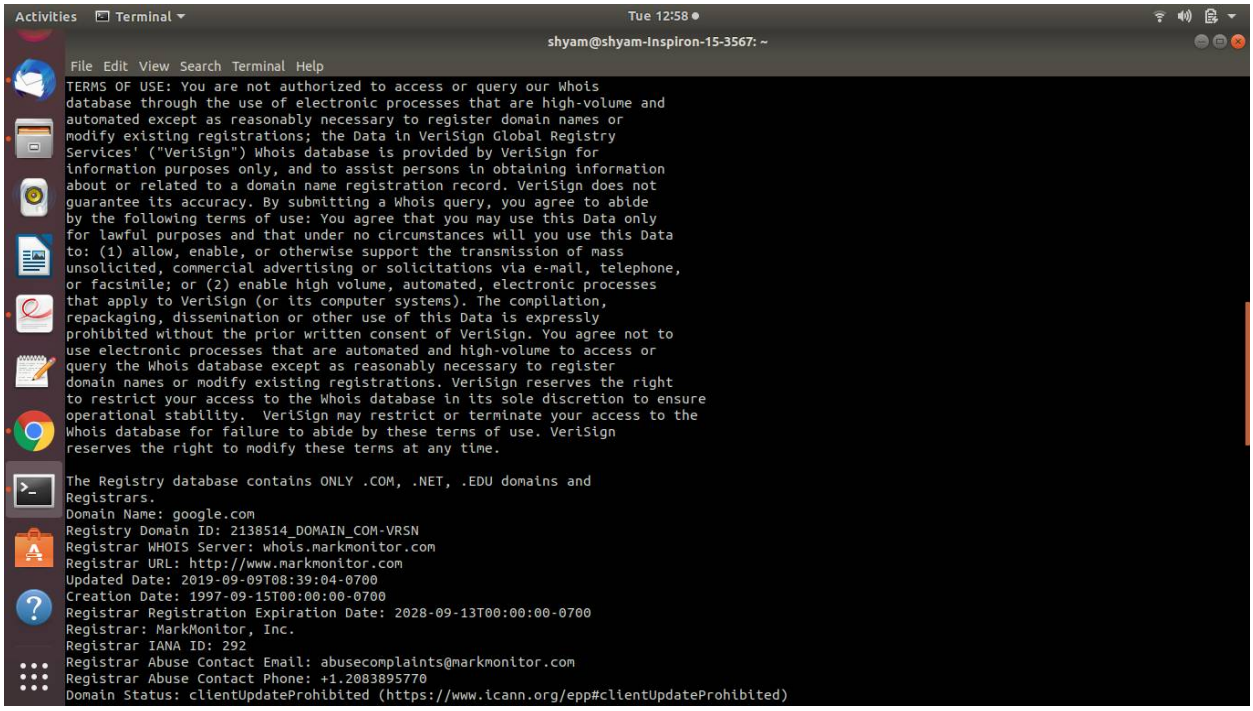
Ans : Since the two hosts were of the same institution there were certain nodes that were common on running the tracert command. If the location of the host is farther away then generally it means more hops (more nodes/steps).
The main difference between Ping and Traceroute is that Ping is a quick and 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).

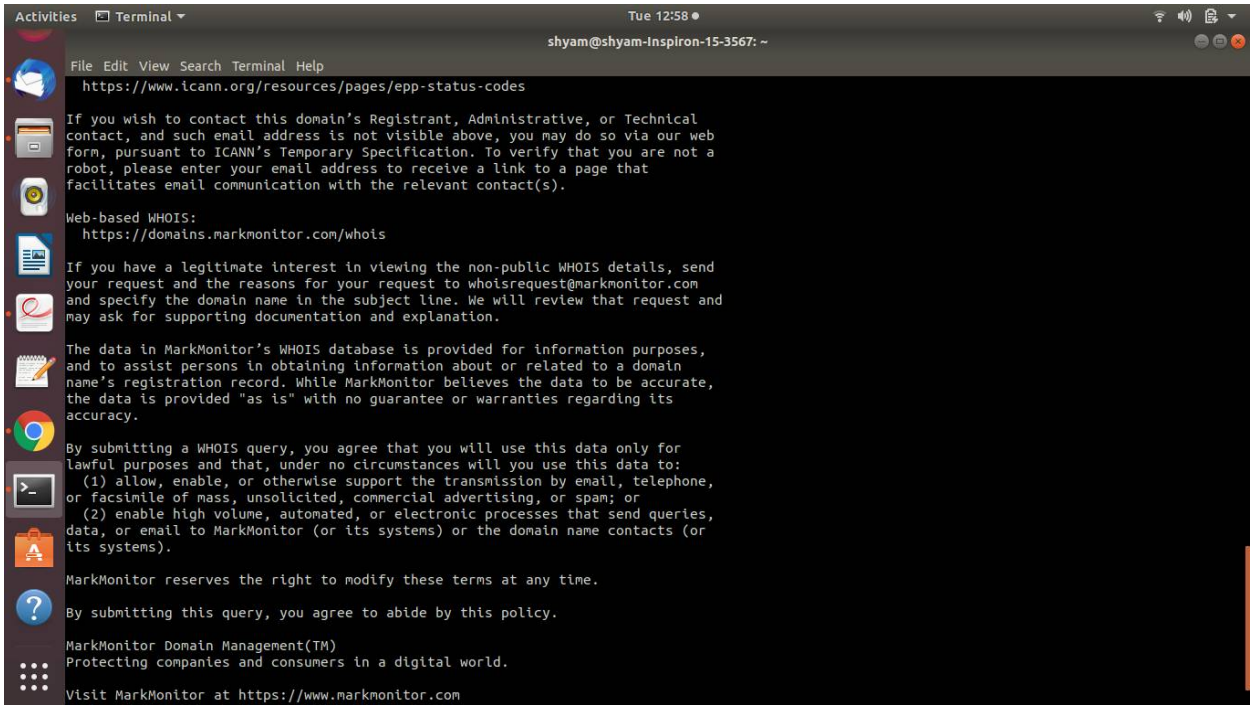
Whois — The *whois* command can give detailed information about domain names and IP addresses. If it is not installed on the computers then install it with command sudo apt-get

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*).







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*

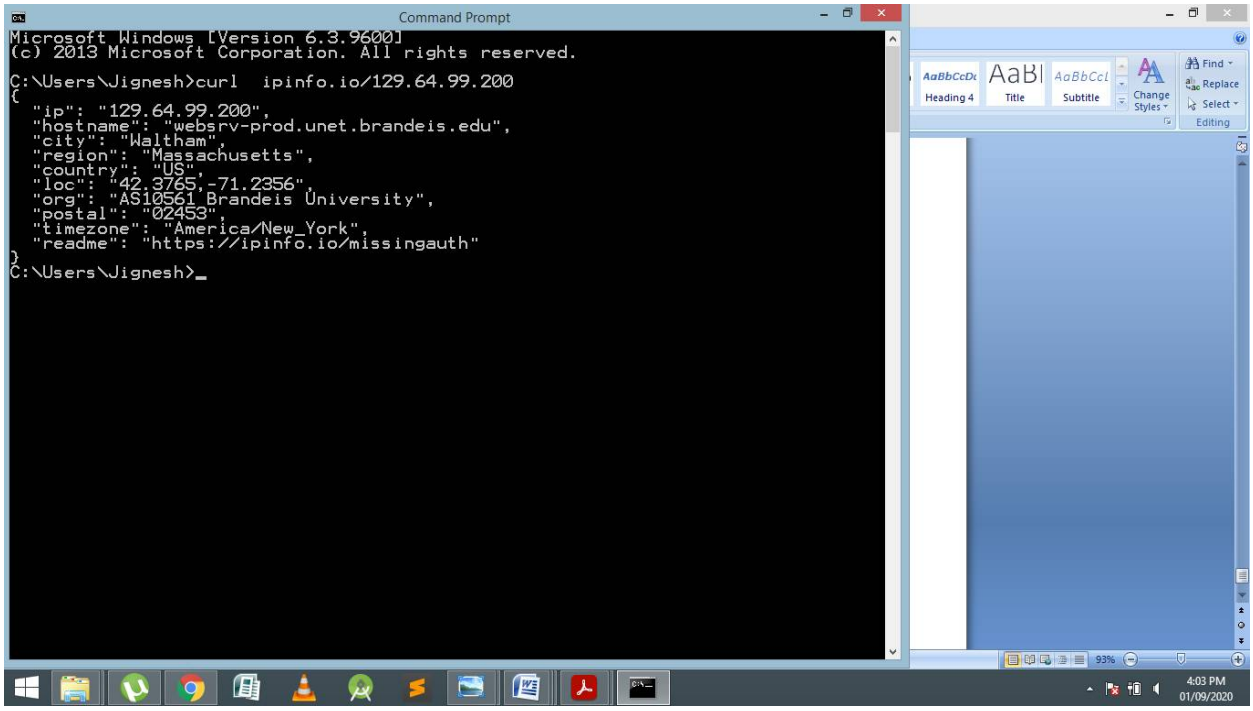
Exercise 5:(Should be short.) Because of NAT, the domain name*spit.ac.in*has a different IP addressoutside of SPIT than it does on campus. Using information in this lab and working on a home computer, find the outside IP address for spit.ac.in. Explain how you did it.

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.

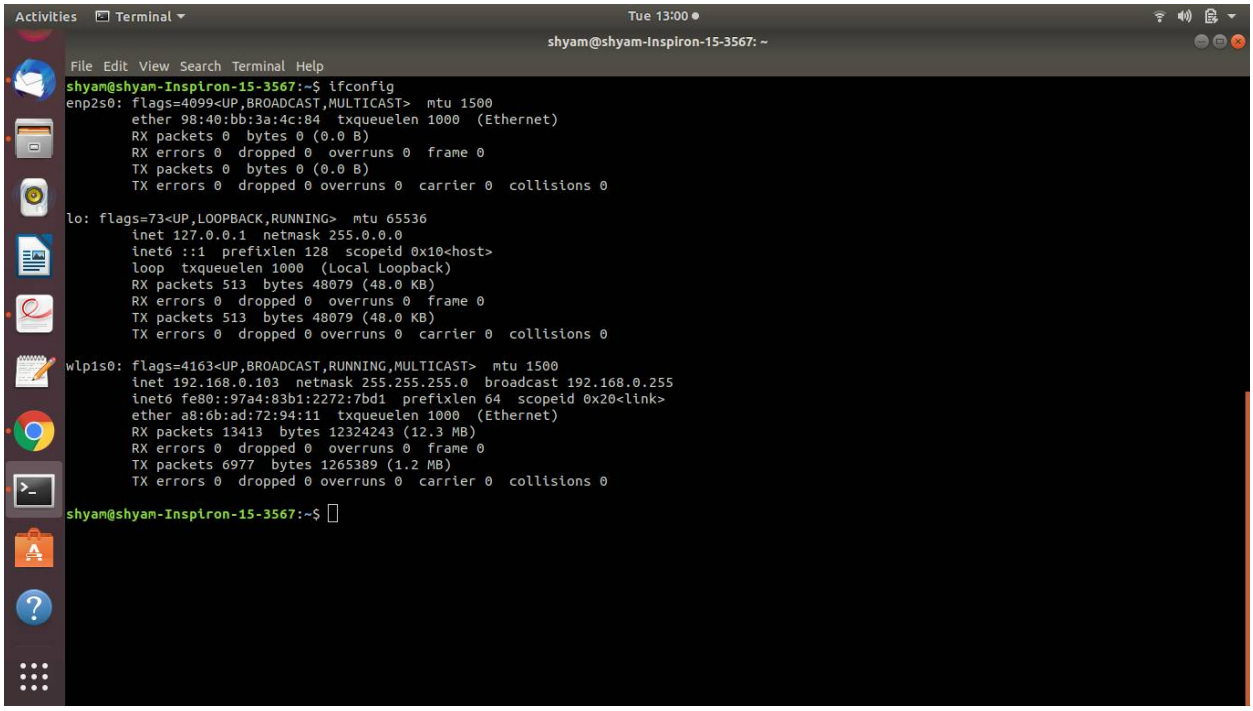
This geolocation program is not installed on our computers, but you can access one on the command line using the *curl* command, which can send HTTP requests and display the response. The following command uses *curl* to contact a public web service that will look up an IP address for you: curl ipinfo.io/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

curl ipinfo.io/129.64.99.200

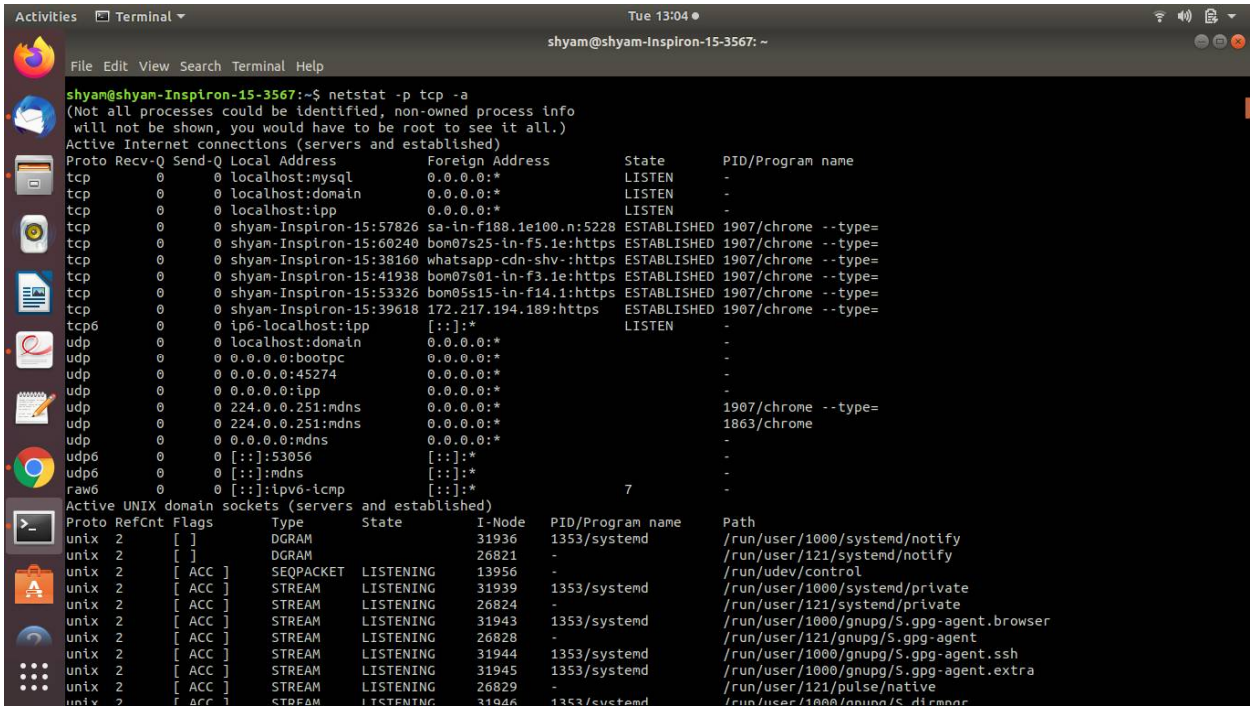
(As you can see, you get back more than just the location.)

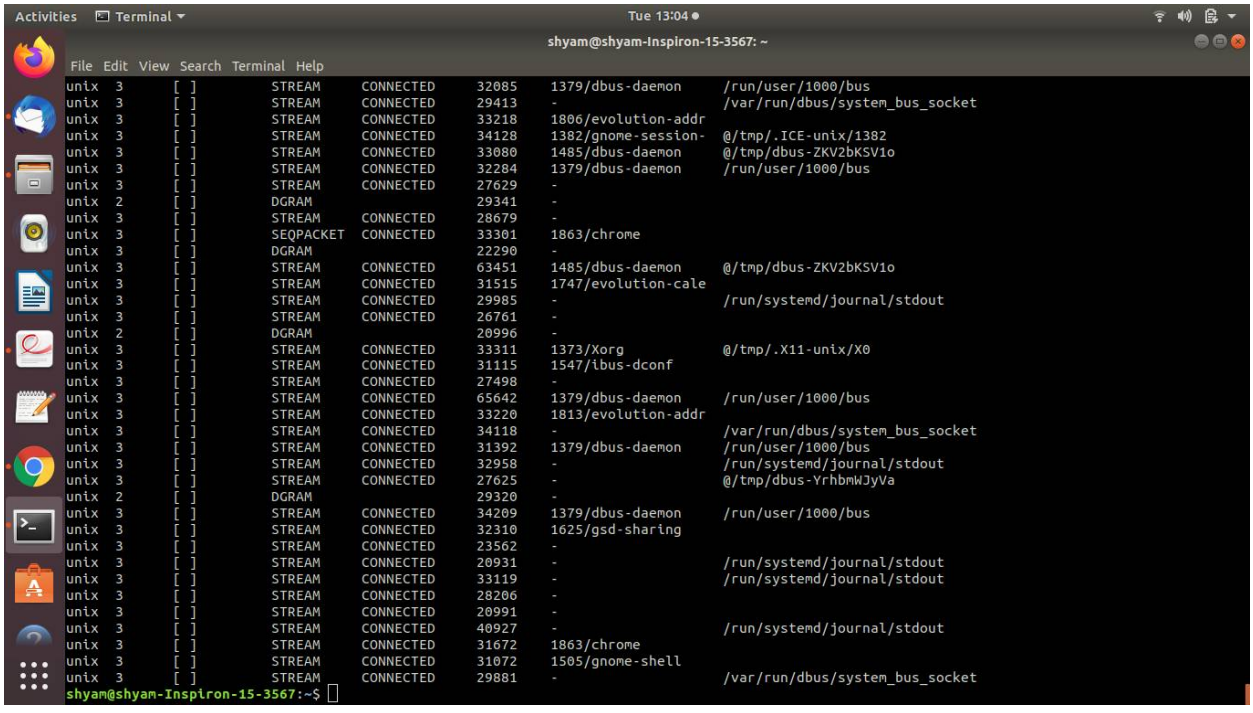


ifconfig — You used ifconfig in the previous lab. When used with no parameters, ifconfig reports someinformation about the computer's network interfaces. This usually includes lo which stands for localhost; it can be used for communication between programs running on the same computer. Linux often has 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!!!.)



netstat — The netstat command gives information about network connections. I often use netstat -t -nwhich 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.)





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.