Name : Sakshi Patil
Branch : SE Computer
Batch : C
UID : 2018130039

Lab 2

Basic Network Utilities

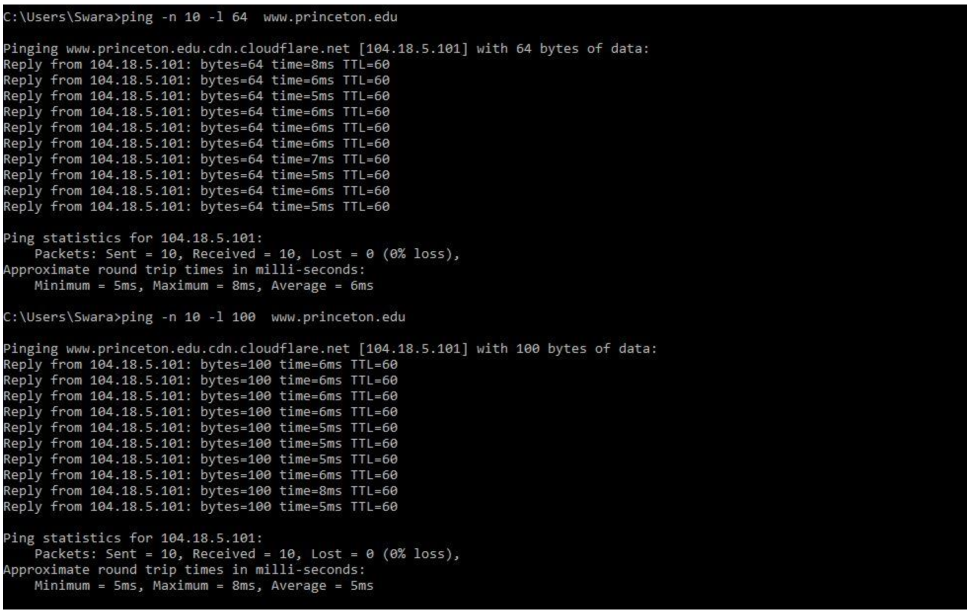
Aim: To study and understand some basic command line network utilities.

Command : ping

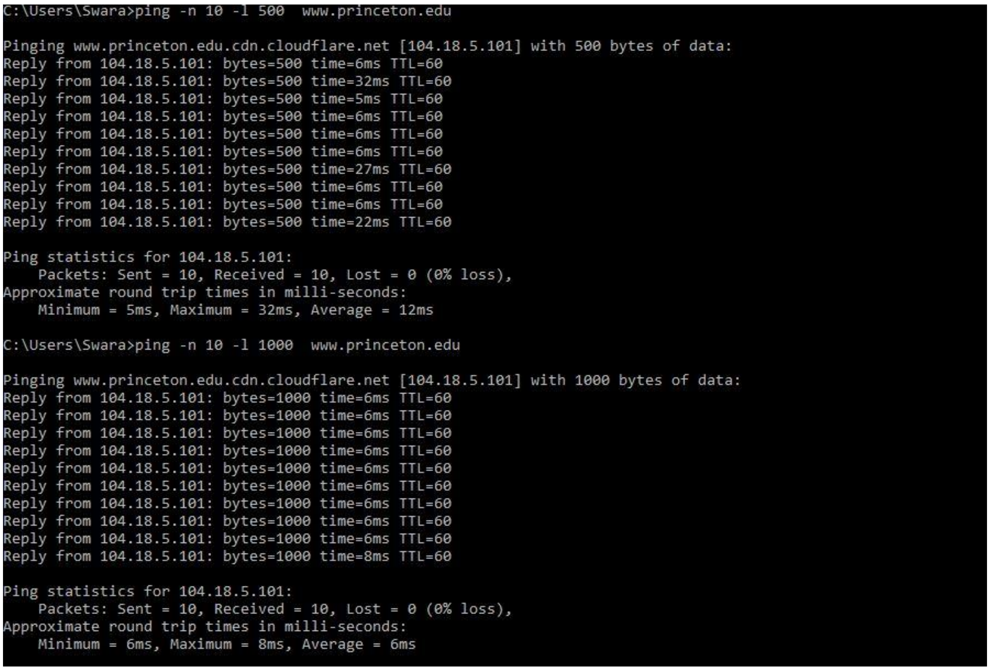
Description : PING (Packet Internet Groper) command is used to check the network connectivity between host and server/host. This command takes as input the IP address or the URL and sends a data packet to the specified address with the message "PING" and gets a response from the server/host this time is recorded which is called latency. Fast ping low latency means faster connection. Ping uses ICMP(Internet Control Message Protocol) to send an ICMP echo message to the specified host if that host is available then it sends an ICMP reply message. Ping is generally measured in millisecond every modern operating system has this ping pre-installed.

Experiments with Ping

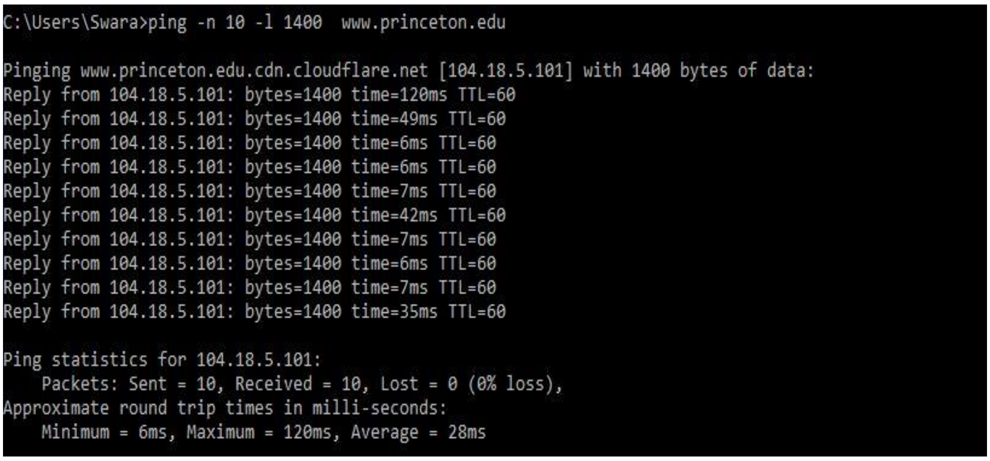
1. Ping the any hosts 10 times (i.e., packet count is 10) with a packet size of 64 bytes, 100 bytes, 500 bytes, 1000 bytes, 1400 bytes



```
C:\Users\Swara>ping -n 10 -l 64  www.princeton.edu

Pinging www.princeton.edu.cdn.cloudflare.net [104.18.5.101] with 64 bytes of data:
Reply from 104.18.5.101: bytes=64 time=8ms TTL=60
Reply from 104.18.5.101: bytes=64 time=6ms TTL=60
Reply from 104.18.5.101: bytes=64 time=5ms TTL=60
Reply from 104.18.5.101: bytes=64 time=6ms TTL=60
Reply from 104.18.5.101: bytes=64 time=6ms TTL=60
Reply from 104.18.5.101: bytes=64 time=6ms TTL=60
Reply from 104.18.5.101: bytes=64 time=7ms TTL=60
Reply from 104.18.5.101: bytes=64 time=5ms TTL=60
Reply from 104.18.5.101: bytes=64 time=6ms TTL=60
Reply from 104.18.5.101: bytes=64 time=5ms TTL=60

Ping statistics for 104.18.5.101:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 8ms, Average = 6ms

C:\Users\Swara>ping -n 10 -l 100  www.princeton.edu

Pinging www.princeton.edu.cdn.cloudflare.net [104.18.5.101] with 100 bytes of data:
Reply from 104.18.5.101: bytes=100 time=6ms TTL=60
Reply from 104.18.5.101: bytes=100 time=6ms TTL=60
Reply from 104.18.5.101: bytes=100 time=6ms TTL=60
Reply from 104.18.5.101: bytes=100 time=6ms TTL=60
Reply from 104.18.5.101: bytes=100 time=5ms TTL=60
Reply from 104.18.5.101: bytes=100 time=5ms TTL=60
Reply from 104.18.5.101: bytes=100 time=5ms TTL=60
Reply from 104.18.5.101: bytes=100 time=6ms TTL=60
Reply from 104.18.5.101: bytes=100 time=8ms TTL=60
Reply from 104.18.5.101: bytes=100 time=5ms TTL=60

Ping statistics for 104.18.5.101:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 8ms, Average = 5ms
```

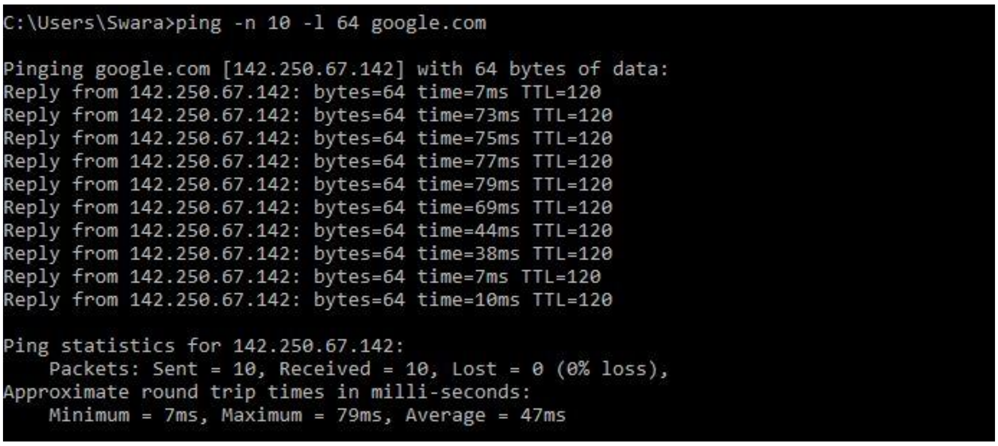


```
C:\Users\Swara>ping -n 10 -l 500  www.princeton.edu

Pinging www.princeton.edu.cdn.cloudflare.net [104.18.5.101] with 500 bytes of data:
Reply from 104.18.5.101: bytes=500 time=6ms TTL=60
Reply from 104.18.5.101: bytes=500 time=32ms TTL=60
Reply from 104.18.5.101: bytes=500 time=5ms TTL=60
Reply from 104.18.5.101: bytes=500 time=6ms TTL=60
Reply from 104.18.5.101: bytes=500 time=6ms TTL=60
Reply from 104.18.5.101: bytes=500 time=6ms TTL=60
Reply from 104.18.5.101: bytes=500 time=27ms TTL=60
Reply from 104.18.5.101: bytes=500 time=6ms TTL=60
Reply from 104.18.5.101: bytes=500 time=6ms TTL=60
Reply from 104.18.5.101: bytes=500 time=22ms TTL=60

Ping statistics for 104.18.5.101:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 32ms, Average = 12ms

C:\Users\Swara>ping -n 10 -l 1000  www.princeton.edu

Pinging www.princeton.edu.cdn.cloudflare.net [104.18.5.101] with 1000 bytes of data:
Reply from 104.18.5.101: bytes=1000 time=6ms TTL=60
Reply from 104.18.5.101: bytes=1000 time=6ms TTL=60
Reply from 104.18.5.101: bytes=1000 time=6ms TTL=60
Reply from 104.18.5.101: bytes=1000 time=6ms TTL=60
Reply from 104.18.5.101: bytes=1000 time=6ms TTL=60
Reply from 104.18.5.101: bytes=1000 time=6ms TTL=60
Reply from 104.18.5.101: bytes=1000 time=6ms TTL=60
Reply from 104.18.5.101: bytes=1000 time=6ms TTL=60
Reply from 104.18.5.101: bytes=1000 time=6ms TTL=60
Reply from 104.18.5.101: bytes=1000 time=8ms TTL=60

Ping statistics for 104.18.5.101:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 8ms, Average = 6ms
```



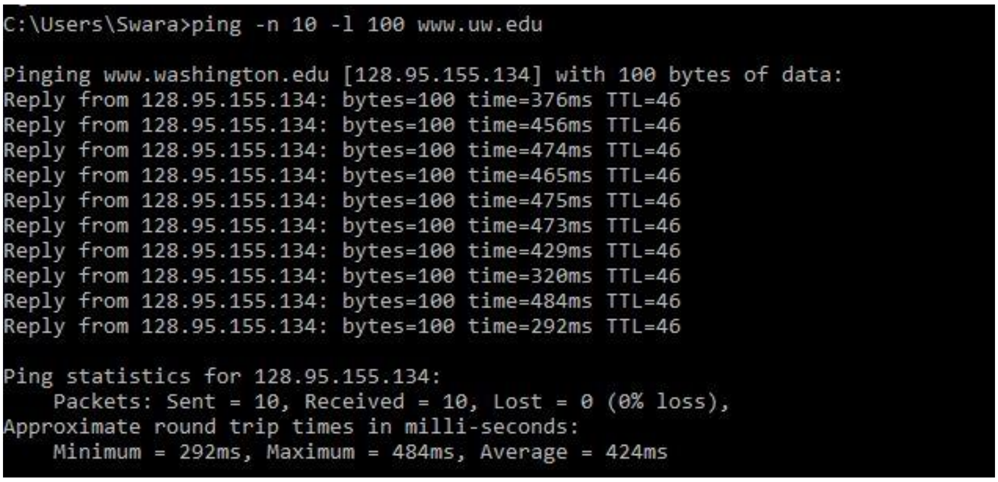
```
C:\Users\Swara>ping -n 10 -l 1400  www.princeton.edu

Pinging www.princeton.edu.cdn.cloudflare.net [104.18.5.101] with 1400 bytes of data:
Reply from 104.18.5.101: bytes=1400 time=120ms TTL=60
Reply from 104.18.5.101: bytes=1400 time=49ms TTL=60
Reply from 104.18.5.101: bytes=1400 time=6ms TTL=60
Reply from 104.18.5.101: bytes=1400 time=6ms TTL=60
Reply from 104.18.5.101: bytes=1400 time=7ms TTL=60
Reply from 104.18.5.101: bytes=1400 time=42ms TTL=60
Reply from 104.18.5.101: bytes=1400 time=7ms TTL=60
Reply from 104.18.5.101: bytes=1400 time=6ms TTL=60
Reply from 104.18.5.101: bytes=1400 time=7ms TTL=60
Reply from 104.18.5.101: bytes=1400 time=35ms TTL=60

Ping statistics for 104.18.5.101:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 120ms, Average = 28ms
```

- ping -n 10 -l 64 google.com



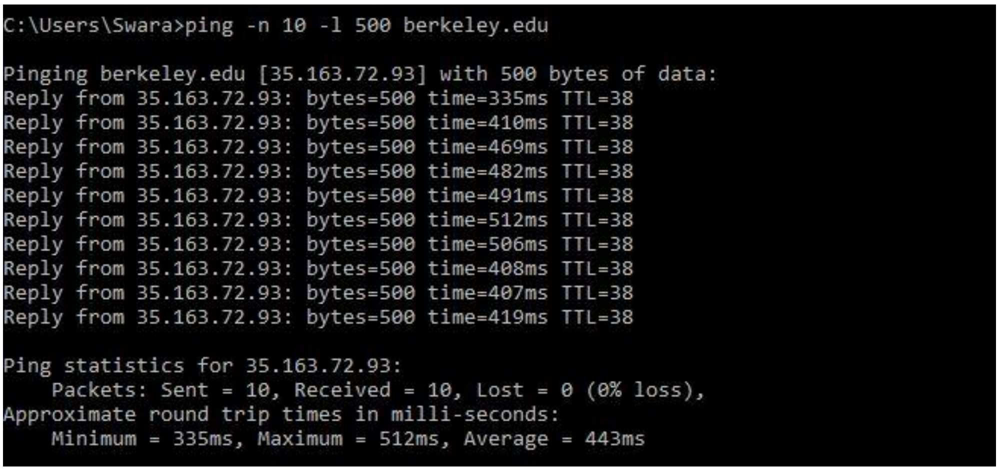
```
C:\Users\Swara>ping -n 10 -l 64 google.com

Pinging google.com [142.250.67.142] with 64 bytes of data:
Reply from 142.250.67.142: bytes=64 time=7ms TTL=120
Reply from 142.250.67.142: bytes=64 time=73ms TTL=120
Reply from 142.250.67.142: bytes=64 time=75ms TTL=120
Reply from 142.250.67.142: bytes=64 time=77ms TTL=120
Reply from 142.250.67.142: bytes=64 time=79ms TTL=120
Reply from 142.250.67.142: bytes=64 time=69ms TTL=120
Reply from 142.250.67.142: bytes=64 time=44ms TTL=120
Reply from 142.250.67.142: bytes=64 time=38ms TTL=120
Reply from 142.250.67.142: bytes=64 time=7ms TTL=120
Reply from 142.250.67.142: bytes=64 time=10ms TTL=120

Ping statistics for 142.250.67.142:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 79ms, Average = 47ms
```

- ping -n 10 -l 100 www.uw.edu



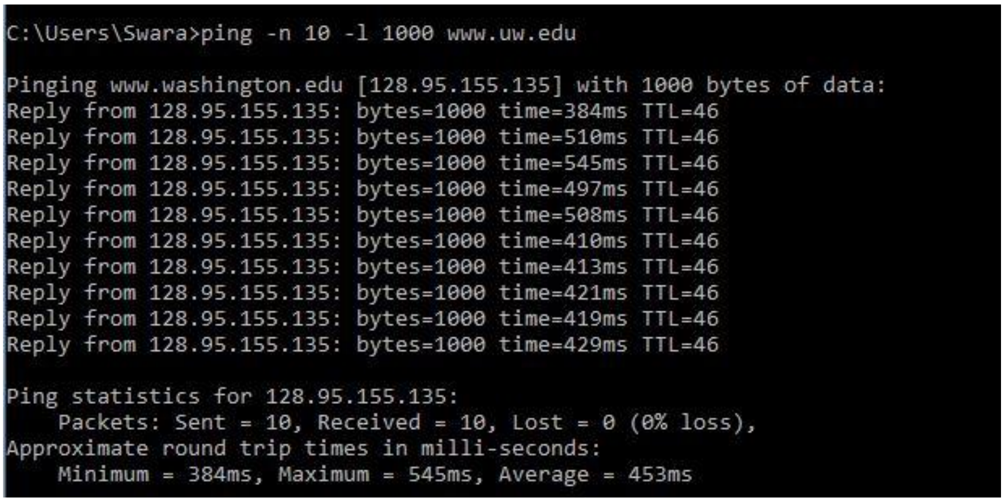
```
C:\Users\Swara>ping -n 10 -l 100 www.uw.edu

Pinging www.washington.edu [128.95.155.134] with 100 bytes of data:
Reply from 128.95.155.134: bytes=100 time=376ms TTL=46
Reply from 128.95.155.134: bytes=100 time=456ms TTL=46
Reply from 128.95.155.134: bytes=100 time=474ms TTL=46
Reply from 128.95.155.134: bytes=100 time=465ms TTL=46
Reply from 128.95.155.134: bytes=100 time=475ms TTL=46
Reply from 128.95.155.134: bytes=100 time=473ms TTL=46
Reply from 128.95.155.134: bytes=100 time=429ms TTL=46
Reply from 128.95.155.134: bytes=100 time=320ms TTL=46
Reply from 128.95.155.134: bytes=100 time=484ms TTL=46
Reply from 128.95.155.134: bytes=100 time=292ms TTL=46

Ping statistics for 128.95.155.134:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 292ms, Maximum = 484ms, Average = 424ms
```

- ping -n 10 -l 500 berkeley.edu



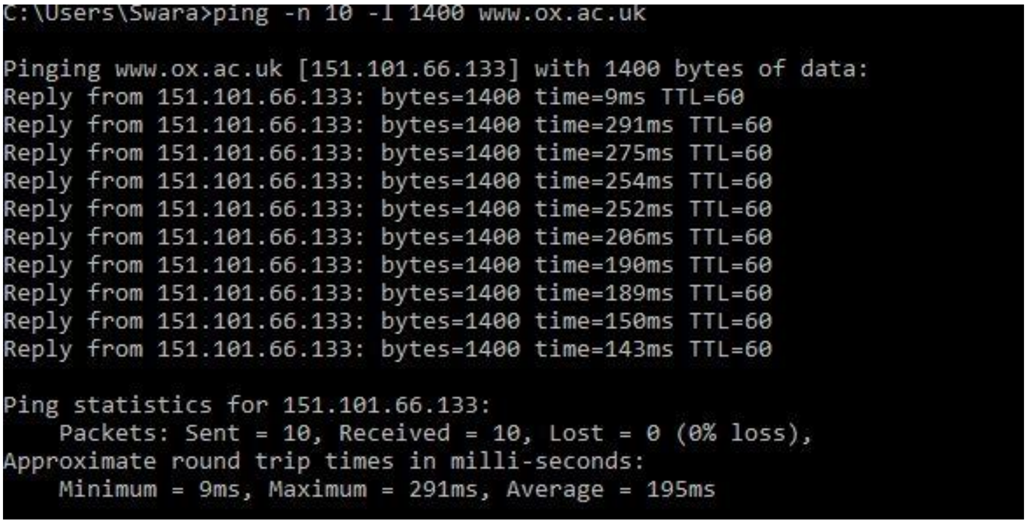
```
C:\Users\Swara>ping -n 10 -l 500 berkeley.edu

Pinging berkeley.edu [35.163.72.93] with 500 bytes of data:
Reply from 35.163.72.93: bytes=500 time=335ms TTL=38
Reply from 35.163.72.93: bytes=500 time=410ms TTL=38
Reply from 35.163.72.93: bytes=500 time=469ms TTL=38
Reply from 35.163.72.93: bytes=500 time=482ms TTL=38
Reply from 35.163.72.93: bytes=500 time=491ms TTL=38
Reply from 35.163.72.93: bytes=500 time=512ms TTL=38
Reply from 35.163.72.93: bytes=500 time=506ms TTL=38
Reply from 35.163.72.93: bytes=500 time=408ms TTL=38
Reply from 35.163.72.93: bytes=500 time=407ms TTL=38
Reply from 35.163.72.93: bytes=500 time=419ms TTL=38

Ping statistics for 35.163.72.93:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 335ms, Maximum = 512ms, Average = 443ms
```

- ping -n 10 -l 1000 www.uw.edu



```
C:\Users\Swara>ping -n 10 -l 1000 www.uw.edu

Pinging www.washington.edu [128.95.155.135] with 1000 bytes of data:
Reply from 128.95.155.135: bytes=1000 time=384ms TTL=46
Reply from 128.95.155.135: bytes=1000 time=510ms TTL=46
Reply from 128.95.155.135: bytes=1000 time=545ms TTL=46
Reply from 128.95.155.135: bytes=1000 time=497ms TTL=46
Reply from 128.95.155.135: bytes=1000 time=508ms TTL=46
Reply from 128.95.155.135: bytes=1000 time=410ms TTL=46
Reply from 128.95.155.135: bytes=1000 time=413ms TTL=46
Reply from 128.95.155.135: bytes=1000 time=421ms TTL=46
Reply from 128.95.155.135: bytes=1000 time=419ms TTL=46
Reply from 128.95.155.135: bytes=1000 time=429ms TTL=46

Ping statistics for 128.95.155.135:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 384ms, Maximum = 545ms, Average = 453ms
```

- ping -n 10 -l 1400 www.ox.ac.uk



```
C:\Users\Swara>ping -n 10 -l 1400 www.ox.ac.uk

Pinging www.ox.ac.uk [151.101.66.133] with 1400 bytes of data:
Reply from 151.101.66.133: bytes=1400 time=9ms TTL=60
Reply from 151.101.66.133: bytes=1400 time=291ms TTL=60
Reply from 151.101.66.133: bytes=1400 time=275ms TTL=60
Reply from 151.101.66.133: bytes=1400 time=254ms TTL=60
Reply from 151.101.66.133: bytes=1400 time=252ms TTL=60
Reply from 151.101.66.133: bytes=1400 time=206ms TTL=60
Reply from 151.101.66.133: bytes=1400 time=190ms TTL=60
Reply from 151.101.66.133: bytes=1400 time=189ms TTL=60
Reply from 151.101.66.133: bytes=1400 time=150ms TTL=60
Reply from 151.101.66.133: bytes=1400 time=143ms TTL=60

Ping statistics for 151.101.66.133:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 291ms, Average = 195ms
```

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: The RTT is dependent on the host on which the 'ping' command is used. Transmission delay is the time taken to put a packet onto a link or simply, the time required to put data bits on the wire/communication medium. It depends on the size of the packet and the bandwidth of the network. Since the hosts are the only parameters changed, there is no transmission delay in the two cases. Propagation delay is the time taken by the first bit to travel from sender to receiver end of the link or simply the time required for bits to reach the destination from the start point. Factors on which propagation delay depends are distance and propagation speed. So, there exists a propagation delay in the two cases. Queueing delay is the time difference between when the packet arrived at its destination and when the packet data was processed or executed. It depends on the number of packets, size of the packet and bandwidth of the network. Since all the parameters are non-varying in both cases, there is hardly any queueing delay.

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: RTT increases with increase in packet size. There would be increased latency for increased packet size due to transmission delay and propagation delay.

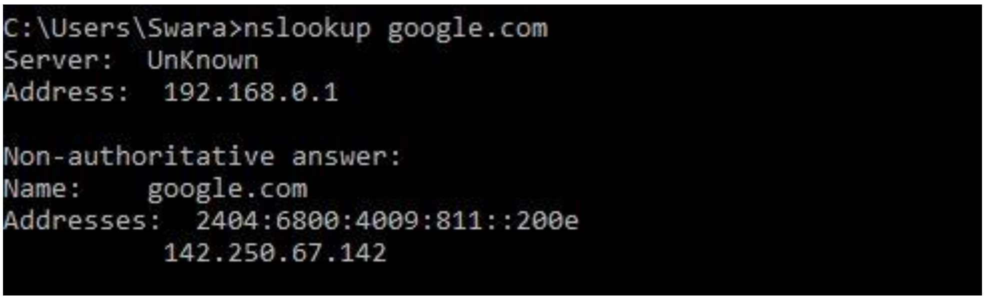
Exercise 1: Experiment with ping to find the round trip times to a variety of destinations. Write up any interesting observations, including in particular how the round trip time compares to the physical distance. Here are few places from who to get replies: www.uw.edu, www.cornell.edu, berkeley.edu,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

Ans : From the images shown above, the following observations can be made :

- The length a signal has to travel correlates with the time taken for a request to reach a server and a response to reach a browser.
- The medium used to route a signal (e.g., copper wire, fiber optic cables) can impact how quickly a request is received by a server and routed back to a user.
- Intermediate routers or servers take time to process a signal, increasing RTT. The more hops a signal has to travel through, the higher the RTT.

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 nslokup by adding the server name or IP address to the command: nslookup <host> <server>

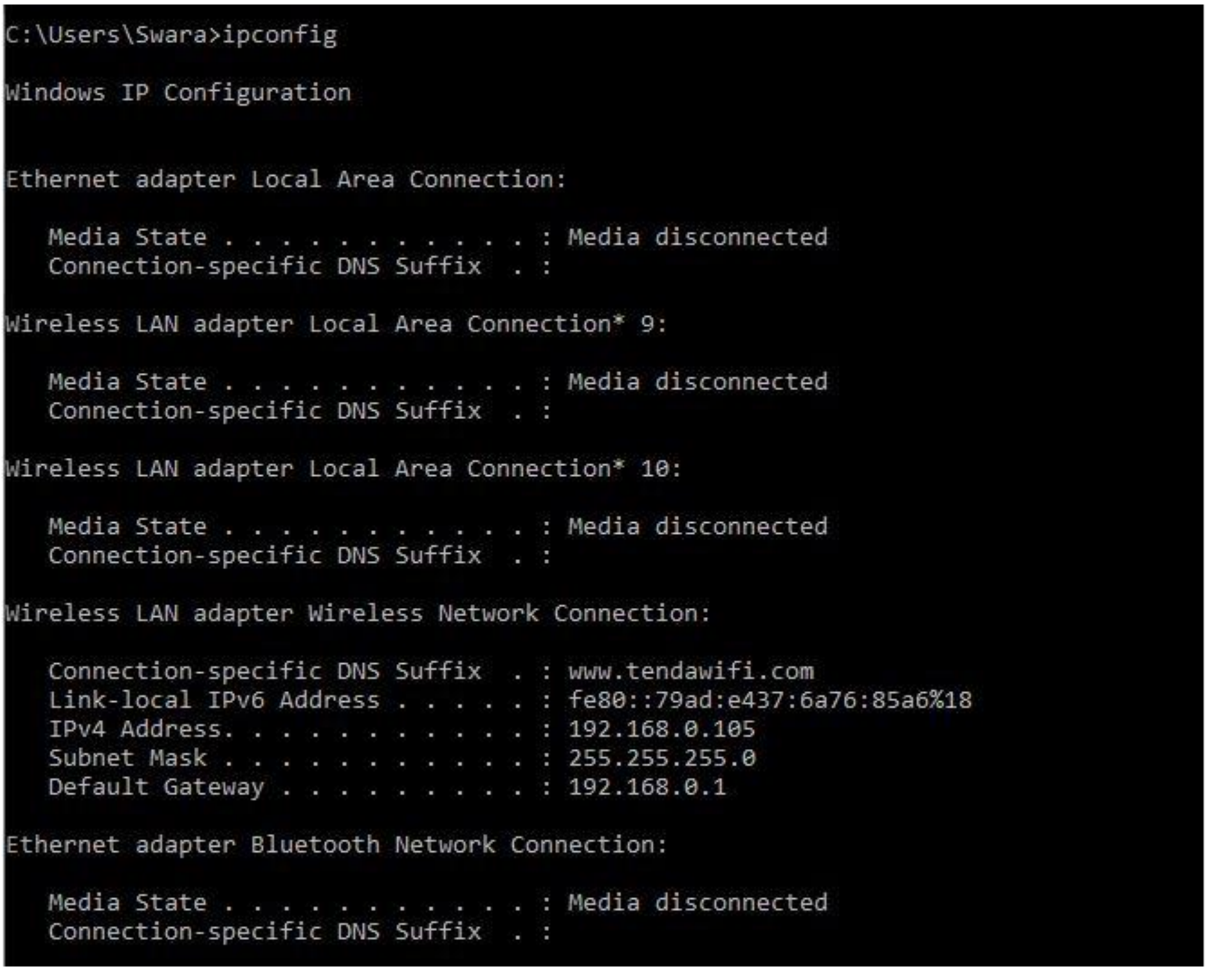
Screenshot:



```
C:\Users\Swara>nslookup google.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4009:811::200e
          142.250.67.142
```

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!!!.)

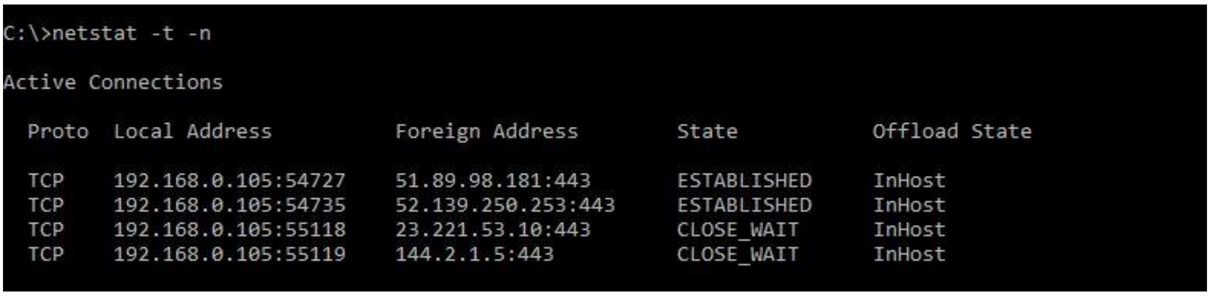
Screenshot:



```
C:\Users\Swara>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

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

Wireless LAN adapter Local Area Connection* 9:

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

Wireless LAN adapter Local Area Connection* 10:

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

Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : www.tendawifi.com
   Link-local IPv6 Address . . . . . : fe80::79ad:e437:6a76:85a6%18
   IPv4 Address. . . . . . . . . . . : 192.168.0.105
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

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

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.)

Screenshot:



```
C:\>netstat -t -n

Active Connections

  Proto  Local Address          Foreign Address        State           Offload State

  TCP    192.168.0.105:54727    51.89.98.181:443       ESTABLISHED     InHost
  TCP    192.168.0.105:54735    52.139.250.253:443     ESTABLISHED     InHost
  TCP    192.168.0.105:55118    23.221.53.10:443       CLOSE_WAIT      InHost
  TCP    192.168.0.105:55119    144.2.1.5:443          CLOSE_WAIT      InHost
```

tracert-The tracert diagnostic utility determines the route to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination. In these packets, traceroute uses varying IP Time-To-Live (TTL) values. Because each router along the path is required to decrement the packet's TTL by at least 1 before forwarding the packet, the TTL is effectively a hop counter. When the TTL on a packet reaches zero (0), the router sends an ICMP "Time Exceeded" message back to the source computer

Experiments with Traceroute

From your machine traceroute to the following hosts:

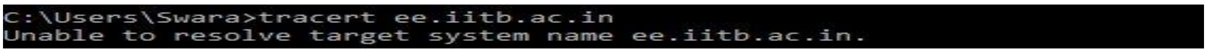
- ee.iitb.ac.in
- mscs.mu.edu
- www.cs.grinnell.edu
- csail.mit.edu
- cs.stanford.edu
- cs.manchester.ac.uk

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).

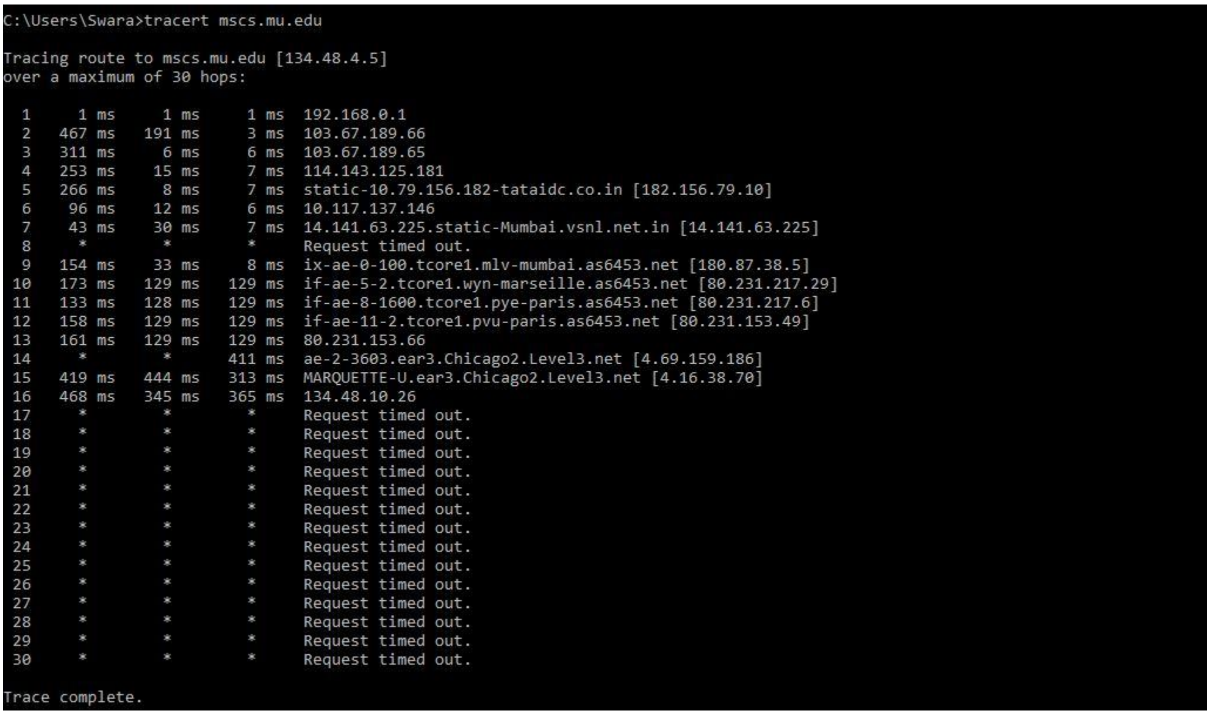
Screenshots :

1)ee.iitb.ac.in



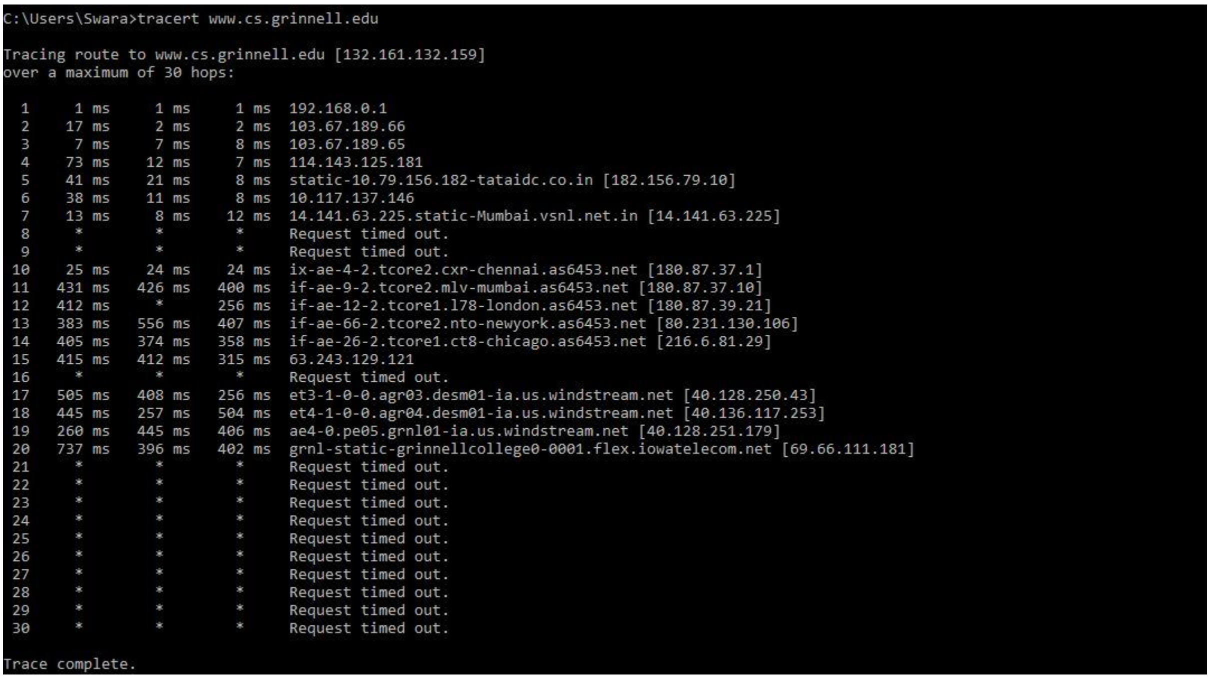
```
C:\Users\Swara>tracert ee.iitb.ac.in
Unable to resolve target system name ee.iitb.ac.in.
```

2) mscs.mu.edu



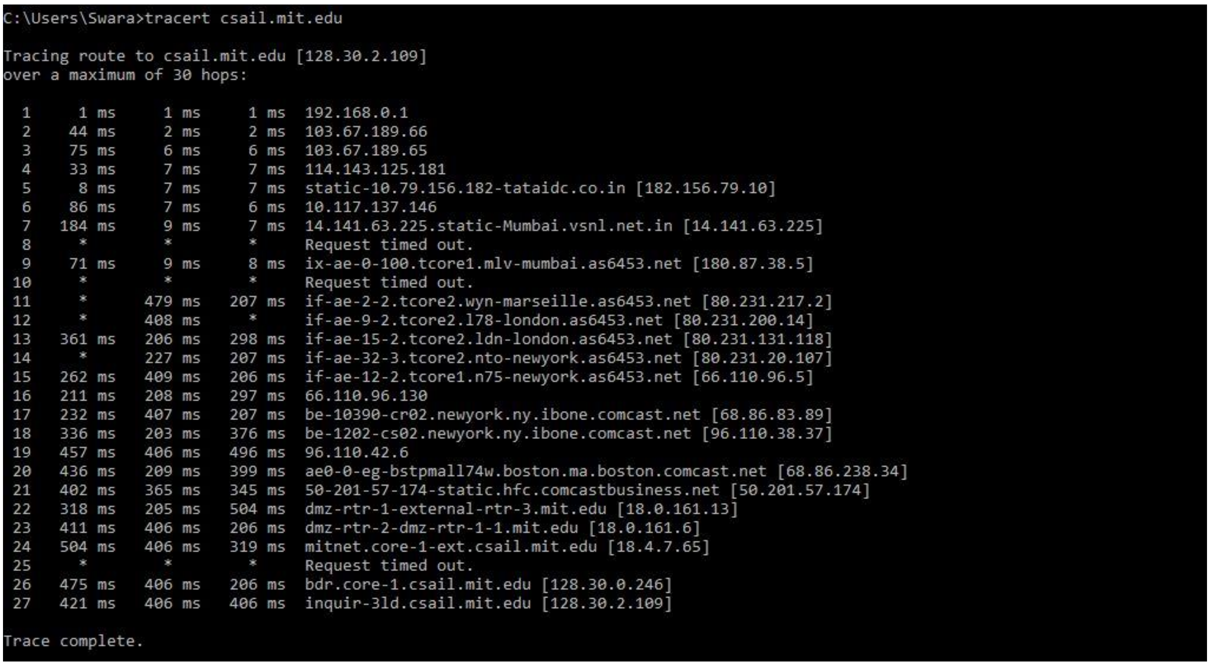
```
C:\Users\Swara>tracert mscs.mu.edu

Tracing route to mscs.mu.edu [134.48.4.5]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.0.1
  2   467 ms   191 ms     3 ms  103.67.189.66
  3   311 ms     6 ms     6 ms  103.67.189.65
  4   253 ms    15 ms     7 ms  114.143.125.181
  5   266 ms     8 ms     7 ms  static-10.79.156.182-tataidc.co.in [182.156.79.10]
  6    96 ms    12 ms     6 ms  10.117.137.146
  7    43 ms    30 ms     7 ms  14.141.63.225.static-Mumbai.vsnl.net.in [14.141.63.225]
  8     *        *        *     Request timed out.
  9   154 ms    33 ms     8 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
 10   173 ms   129 ms   129 ms  if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
 11   133 ms   128 ms   129 ms  if-ae-8-1600.tcore1.pye-paris.as6453.net [80.231.217.6]
 12   158 ms   129 ms   129 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 13   161 ms   129 ms   129 ms  80.231.153.66
 14     *        *      411 ms  ae-2-3603.ear3.Chicago2.Level3.net [4.69.159.186]
 15   419 ms   444 ms   313 ms  MARQUETTE-U.ear3.Chicago2.Level3.net [4.16.38.70]
 16   468 ms   345 ms   365 ms  134.48.10.26
 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.
```

3) www.cs.grinnell.edu



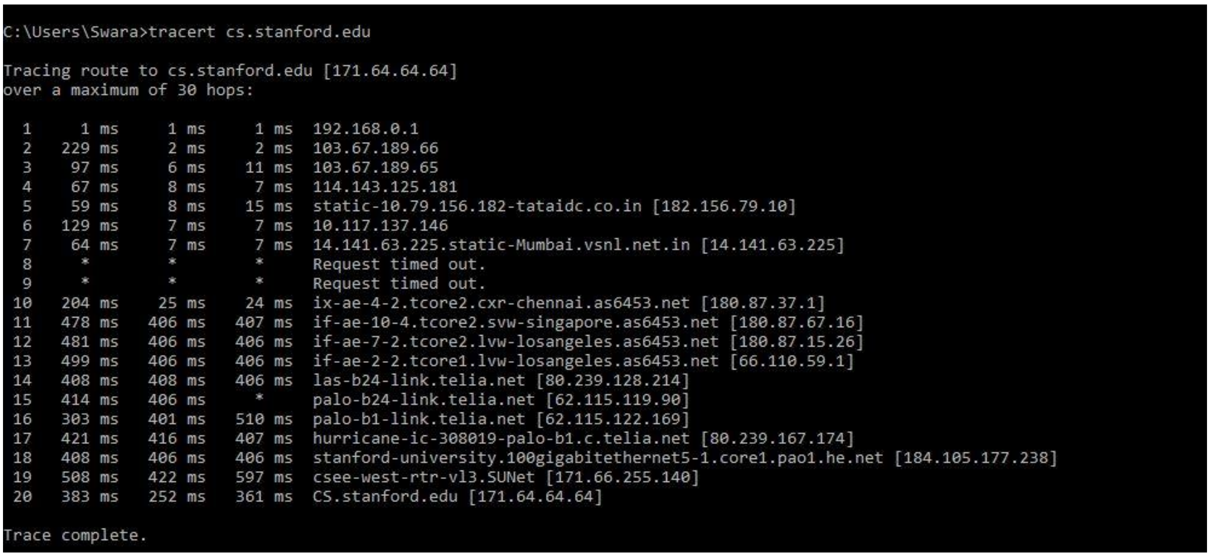
```
C:\Users\Swara>tracert www.cs.grinnell.edu

Tracing route to www.cs.grinnell.edu [132.161.132.159]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.0.1
  2    17 ms     2 ms     2 ms  103.67.189.66
  3     7 ms     7 ms     8 ms  103.67.189.65
  4    73 ms    12 ms     7 ms  114.143.125.181
  5    41 ms    21 ms     8 ms  static-10.79.156.182-tataidc.co.in [182.156.79.10]
  6    38 ms    11 ms     8 ms  10.117.137.146
  7    13 ms     8 ms    12 ms  14.141.63.225.static-Mumbai.vsnl.net.in [14.141.63.225]
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10    25 ms    24 ms    24 ms  ix-ae-4-2.tcore2.cxr-chennai.as6453.net [180.87.37.1]
 11   431 ms   426 ms   400 ms  if-ae-9-2.tcore2.mlv-mumbai.as6453.net [180.87.37.10]
 12   412 ms     *      256 ms  if-ae-12-2.tcore1.178-london.as6453.net [180.87.39.21]
 13   383 ms   556 ms   407 ms  if-ae-66-2.tcore2.nto-newyork.as6453.net [80.231.130.106]
 14   405 ms   374 ms   358 ms  if-ae-26-2.tcore1.ct8-chicago.as6453.net [216.6.81.29]
 15   415 ms   412 ms   315 ms  63.243.129.121
 16     *        *        *     Request timed out.
 17   505 ms   408 ms   256 ms  et3-1-0-0.agr03.desm01-ia.us.windstream.net [40.128.250.43]
 18   445 ms   257 ms   504 ms  et4-1-0-0.agr04.desm01-ia.us.windstream.net [40.136.117.253]
 19   260 ms   445 ms   406 ms  ae4-0.pe05.grnl01-ia.us.windstream.net [40.128.251.179]
 20   737 ms   396 ms   402 ms  grnl-static-grinnellcollege0-0001.flex.iowatelecom.net [69.66.111.181]
 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.
```

4)csail.mit.edu



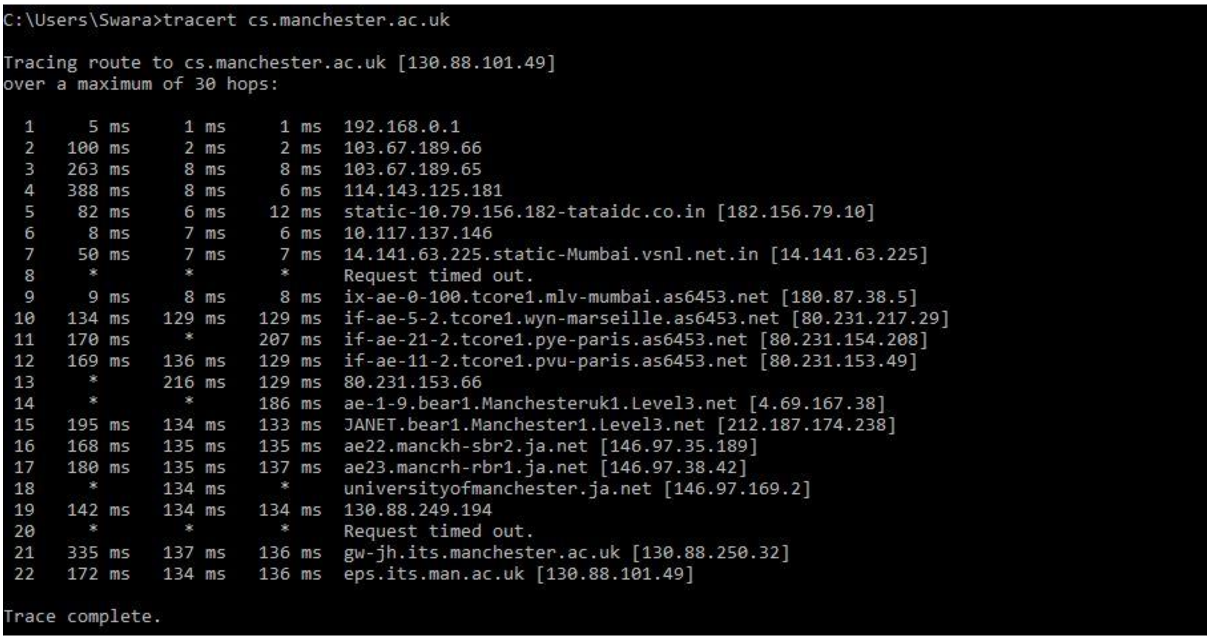
```
C:\Users\Swara>tracert csail.mit.edu

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

  1     1 ms     1 ms     1 ms  192.168.0.1
  2    44 ms     2 ms     2 ms  103.67.189.66
  3    75 ms     6 ms     6 ms  103.67.189.65
  4    33 ms     7 ms     7 ms  114.143.125.181
  5     8 ms     7 ms     7 ms  static-10.79.156.182-tataidc.co.in [182.156.79.10]
  6    86 ms     7 ms     6 ms  10.117.137.146
  7   184 ms     9 ms     7 ms  14.141.63.225.static-Mumbai.vsnl.net.in [14.141.63.225]
  8     *        *        *     Request timed out.
  9    71 ms     9 ms     8 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
 10     *        *        *     Request timed out.
 11     *      479 ms   207 ms  if-ae-2-2.tcore2.wyn-marseille.as6453.net [80.231.217.2]
 12     *      408 ms     *     if-ae-9-2.tcore2.178-london.as6453.net [80.231.200.14]
 13   361 ms   206 ms   298 ms  if-ae-15-2.tcore2.ldn-london.as6453.net [80.231.131.118]
 14     *      227 ms   207 ms  if-ae-32-3.tcore2.nto-newyork.as6453.net [80.231.20.107]
 15   262 ms   409 ms   206 ms  if-ae-12-2.tcore1.n75-newyork.as6453.net [66.110.96.5]
 16   211 ms   208 ms   297 ms  66.110.96.130
 17   232 ms   407 ms   207 ms  be-10390-cr02.newyork.ny.ibone.comcast.net [68.86.83.89]
 18   336 ms   203 ms   376 ms  be-1202-cs02.newyork.ny.ibone.comcast.net [96.110.38.37]
 19   457 ms   406 ms   496 ms  96.110.42.6
 20   436 ms   209 ms   399 ms  ae0-0-eg-bstpmall74w.boston.ma.boston.comcast.net [68.86.238.34]
 21   402 ms   365 ms   345 ms  50-201-57-174-static.hfc.comcastbusiness.net [50.201.57.174]
 22   318 ms   205 ms   504 ms  dmz-rtr-1-external-rtr-3.mit.edu [18.0.161.13]
 23   411 ms   406 ms   206 ms  dmz-rtr-2-dmz-rtr-1-1.mit.edu [18.0.161.6]
 24   504 ms   406 ms   319 ms  mitnet.core-1-ext.csail.mit.edu [18.4.7.65]
 25     *        *        *     Request timed out.
 26   475 ms   406 ms   206 ms  bdr.core-1.csail.mit.edu [128.30.0.246]
 27   421 ms   406 ms   406 ms  inquir-3ld.csail.mit.edu [128.30.2.109]

Trace complete.
```

5)cs.stanford.edu



```
C:\Users\Swara>tracert cs.stanford.edu

Tracing route to cs.stanford.edu [171.64.64.64]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.0.1
  2   229 ms     2 ms     2 ms  103.67.189.66
  3    97 ms     6 ms    11 ms  103.67.189.65
  4    67 ms     8 ms     7 ms  114.143.125.181
  5    59 ms     8 ms    15 ms  static-10.79.156.182-tataidc.co.in [182.156.79.10]
  6   129 ms     7 ms     7 ms  10.117.137.146
  7    64 ms     7 ms     7 ms  14.141.63.225.static-Mumbai.vsnl.net.in [14.141.63.225]
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10   204 ms    25 ms    24 ms  ix-ae-4-2.tcore2.cxr-chennai.as6453.net [180.87.37.1]
 11   478 ms   406 ms   407 ms  if-ae-10-4.tcore2.svw-singapore.as6453.net [180.87.67.16]
 12   481 ms   406 ms   406 ms  if-ae-7-2.tcore2.lvw-losangeles.as6453.net [180.87.15.26]
 13   499 ms   406 ms   406 ms  if-ae-2-2.tcore1.lvw-losangeles.as6453.net [66.110.59.1]
 14   408 ms   408 ms   406 ms  las-b24-link.telia.net [80.239.128.214]
 15   414 ms   406 ms     *     palo-b24-link.telia.net [62.115.119.90]
 16   303 ms   401 ms   510 ms  palo-b1-link.telia.net [62.115.122.169]
 17   421 ms   416 ms   407 ms  hurricane-ic-308019-palo-b1.c.telia.net [80.239.167.174]
 18   408 ms   406 ms   406 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 19   508 ms   422 ms   597 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 20   383 ms   252 ms   361 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

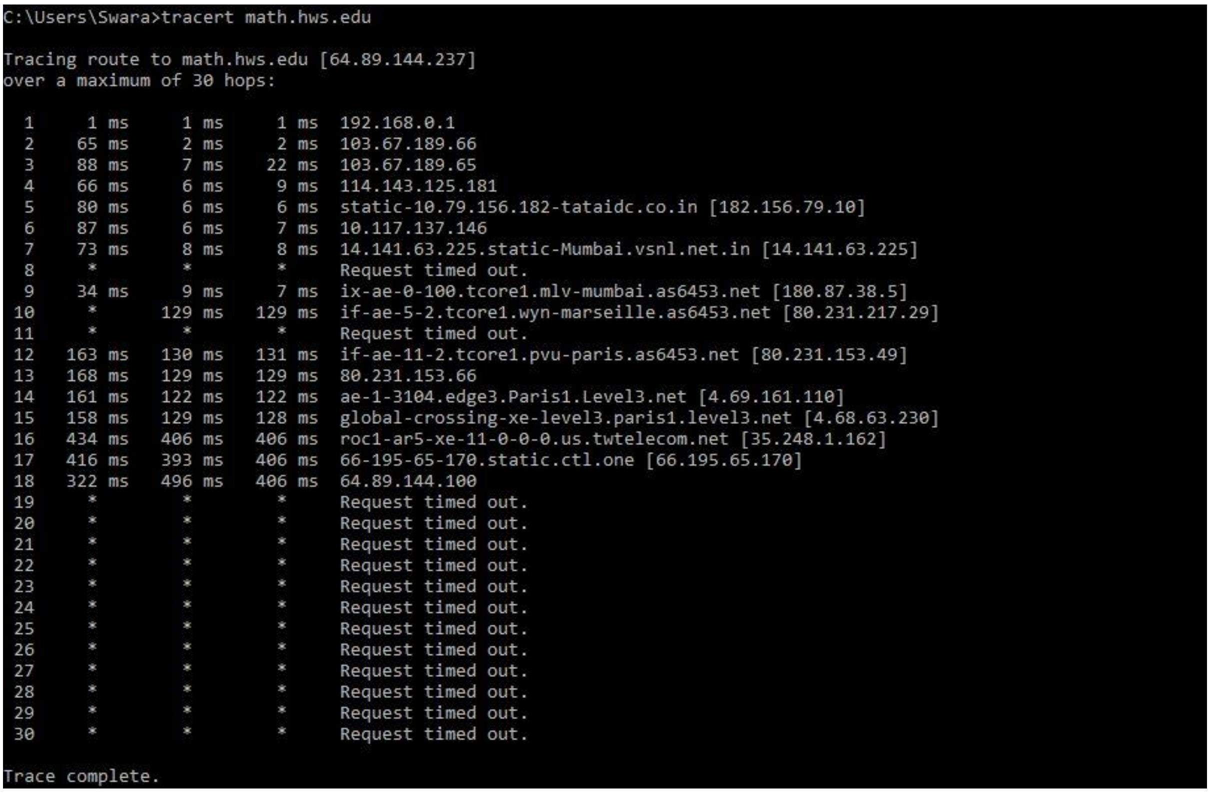
6) cs.manchester.ac.uk



```
C:\Users\Swara>tracert cs.manchester.ac.uk

Tracing route to cs.manchester.ac.uk [130.88.101.49]
over a maximum of 30 hops:

  1     5 ms     1 ms     1 ms  192.168.0.1
  2   100 ms     2 ms     2 ms  103.67.189.66
  3   263 ms     8 ms     8 ms  103.67.189.65
  4   388 ms     8 ms     6 ms  114.143.125.181
  5    82 ms     6 ms    12 ms  static-10.79.156.182-tataidc.co.in [182.156.79.10]
  6     8 ms     7 ms     6 ms  10.117.137.146
  7    50 ms     7 ms     7 ms  14.141.63.225.static-Mumbai.vsnl.net.in [14.141.63.225]
  8     *        *        *     Request timed out.
  9     9 ms     8 ms     8 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
 10   134 ms   129 ms   129 ms  if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
 11   170 ms     *      207 ms  if-ae-21-2.tcore1.pye-paris.as6453.net [80.231.154.208]
 12   169 ms   136 ms   129 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 13     *      216 ms   129 ms  80.231.153.66
 14     *        *      186 ms  ae-1-9.bear1.Manchesteruk1.Level3.net [4.69.167.38]
 15   195 ms   134 ms   133 ms  JANET.bear1.Manchester1.Level3.net [212.187.174.238]
 16   168 ms   135 ms   135 ms  ae22.manckh-sbr2.ja.net [146.97.35.189]
 17   180 ms   135 ms   137 ms  ae23.mancrh-rbr1.ja.net [146.97.38.42]
 18     *      134 ms     *     universityofmanchester.ja.net [146.97.169.2]
 19   142 ms   134 ms   134 ms  130.88.249.194
 20     *        *        *     Request timed out.
 21   335 ms   137 ms   136 ms  gw-jh.its.manchester.ac.uk [130.88.250.32]
 22   172 ms   134 ms   136 ms  eps.its.man.ac.uk [130.88.101.49]

Trace complete.
```

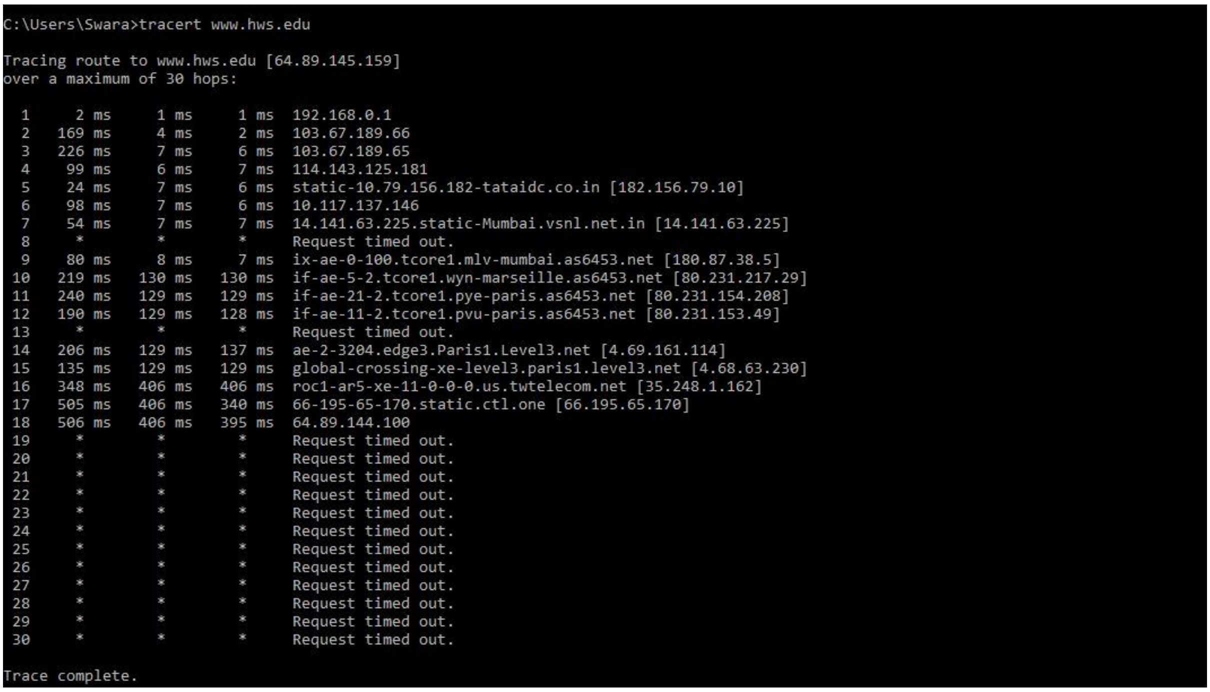
<u>Exercise 2:</u> (Very short.) Use traceroute to trace the route from your computer to math.hws.edu and to www.hws.edu. Explain the difference in the results.

maths.hws.edu



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

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

  1     1 ms     1 ms     1 ms  192.168.0.1
  2    65 ms     2 ms     2 ms  103.67.189.66
  3    88 ms     7 ms    22 ms  103.67.189.65
  4    66 ms     6 ms     9 ms  114.143.125.181
  5    80 ms     6 ms     6 ms  static-10.79.156.182-tataidc.co.in [182.156.79.10]
  6    87 ms     6 ms     7 ms  10.117.137.146
  7    73 ms     8 ms     8 ms  14.141.63.225.static-Mumbai.vsnl.net.in [14.141.63.225]
  8     *        *        *     Request timed out.
  9    34 ms     9 ms     7 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
 10     *      129 ms   129 ms  if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
 11     *        *        *     Request timed out.
 12   163 ms   130 ms   131 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 13   168 ms   129 ms   129 ms  80.231.153.66
 14   161 ms   122 ms   122 ms  ae-1-3104.edge3.Paris1.Level3.net [4.69.161.110]
 15   158 ms   129 ms   128 ms  global-crossing-xe-level3.paris1.level3.net [4.68.63.230]
 16   434 ms   406 ms   406 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 17   416 ms   393 ms   406 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 18   322 ms   496 ms   406 ms  64.89.144.100
 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.
```

www.hws.edu

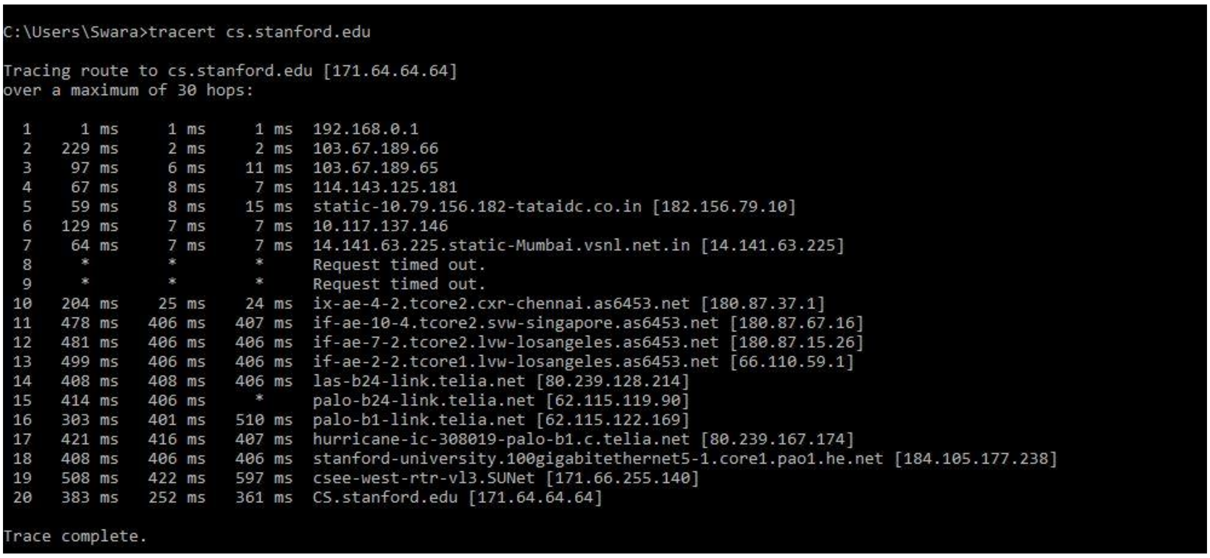


```
C:\Users\Swara>tracert www.hws.edu

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

  1     2 ms     1 ms     1 ms  192.168.0.1
  2   169 ms     4 ms     2 ms  103.67.189.66
  3   226 ms     7 ms     6 ms  103.67.189.65
  4    99 ms     6 ms     7 ms  114.143.125.181
  5    24 ms     7 ms     6 ms  static-10.79.156.182-tataidc.co.in [182.156.79.10]
  6    98 ms     7 ms     6 ms  10.117.137.146
  7    54 ms     7 ms     7 ms  14.141.63.225.static-Mumbai.vsnl.net.in [14.141.63.225]
  8     *        *        *     Request timed out.
  9    80 ms     8 ms     7 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
 10   219 ms   130 ms   130 ms  if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
 11   240 ms   129 ms   129 ms  if-ae-21-2.tcore1.pye-paris.as6453.net [80.231.154.208]
 12   190 ms   129 ms   128 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 13     *        *        *     Request timed out.
 14   206 ms   129 ms   137 ms  ae-2-3204.edge3.Paris1.Level3.net [4.69.161.114]
 15   135 ms   129 ms   129 ms  global-crossing-xe-level3.paris1.level3.net [4.68.63.230]
 16   348 ms   406 ms   406 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 17   505 ms   406 ms   340 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 18   506 ms   406 ms   395 ms  64.89.144.100
 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.
```

The first row shows that the process of route tracing has started as the last column shows the Default Gateway of the user. The next three rows in both the cases are similar as the route is being traced starting from the ISP (Internet service provider) of the user. The next few rows, after which the tracing reaches the common IP address of 66.195.65.170 and then math.hws.edu [64.89.144.100], clearly show that the route is completely different after crossing the ISP for both the cases. A domain name might have multiple IP addresses associated. If this is the case, multiple traces may access two or more IP addresses. This will yield trace paths that differ from one another, even if the origin and destinations are the same. Domains may also use multiple servers for its subdomains. Tracing the path to the base domain might result in a completely different path when tracing to the subdomain. A URL with the **www** prefix is technically a subdomain, so it's possible that traces to **example.com** and **www.example.com** follow two very different paths.

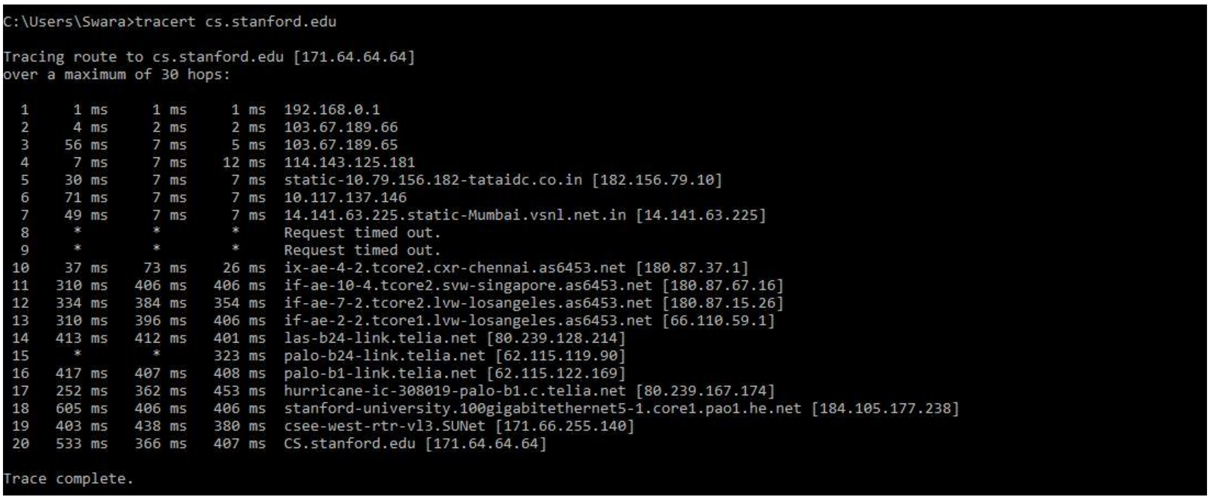
Exercise 3: Two packets sent from the same source to the same destination do not necessarily follow the same path through the net. Experiment with some sources that are fairly far away. Can you find cases where packets sent to the same destination follow different paths? How likely does it seem to be? 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.

1)



```
C:\Users\Swara>tracert cs.stanford.edu

Tracing route to cs.stanford.edu [171.64.64.64]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.0.1
  2   229 ms     2 ms     2 ms  103.67.189.66
  3    97 ms     6 ms    11 ms  103.67.189.65
  4    67 ms     8 ms     7 ms  114.143.125.181
  5    59 ms     8 ms    15 ms  static-10.79.156.182-tataidc.co.in [182.156.79.10]
  6   129 ms     7 ms     7 ms  10.117.137.146
  7    64 ms     7 ms     7 ms  14.141.63.225.static-Mumbai.vsnl.net.in [14.141.63.225]
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10   204 ms    25 ms    24 ms  ix-ae-4-2.tcore2.cxr-chennai.as6453.net [180.87.37.1]
 11   478 ms   406 ms   407 ms  if-ae-10-4.tcore2.svw-singapore.as6453.net [180.87.67.16]
 12   481 ms   406 ms   406 ms  if-ae-7-2.tcore2.lvw-losangeles.as6453.net [180.87.15.26]
 13   499 ms   406 ms   406 ms  if-ae-2-2.tcore1.lvw-losangeles.as6453.net [66.110.59.1]
 14   408 ms   408 ms   406 ms  las-b24-link.telia.net [80.239.128.214]
 15   414 ms   406 ms     *     palo-b24-link.telia.net [62.115.119.90]
 16   303 ms   401 ms   510 ms  palo-b1-link.telia.net [62.115.122.169]
 17   421 ms   416 ms   407 ms  hurricane-ic-308019-palo-b1.c.telia.net [80.239.167.174]
 18   408 ms   406 ms   406 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 19   508 ms   422 ms   597 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 20   383 ms   252 ms   361 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

2)



```
C:\Users\Swara>tracert cs.stanford.edu

Tracing route to cs.stanford.edu [171.64.64.64]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.0.1
  2     4 ms     2 ms     2 ms  103.67.189.66
  3    56 ms     7 ms     5 ms  103.67.189.65
  4     7 ms     7 ms    12 ms  114.143.125.181
  5    30 ms     7 ms     7 ms  static-10.79.156.182-tataidc.co.in [182.156.79.10]
  6    71 ms     7 ms     7 ms  10.117.137.146
  7    49 ms     7 ms     7 ms  14.141.63.225.static-Mumbai.vsnl.net.in [14.141.63.225]
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10    37 ms    73 ms    26 ms  ix-ae-4-2.tcore2.cxr-chennai.as6453.net [180.87.37.1]
 11   310 ms   406 ms   406 ms  if-ae-10-4.tcore2.svw-singapore.as6453.net [180.87.67.16]
 12   334 ms   384 ms   354 ms  if-ae-7-2.tcore2.lvw-losangeles.as6453.net [180.87.15.26]
 13   310 ms   396 ms   406 ms  if-ae-2-2.tcore1.lvw-losangeles.as6453.net [66.110.59.1]
 14   413 ms   412 ms   401 ms  las-b24-link.telia.net [80.239.128.214]
 15     *        *      323 ms  palo-b24-link.telia.net [62.115.119.90]
 16   417 ms   407 ms   408 ms  palo-b1-link.telia.net [62.115.122.169]
 17   252 ms   362 ms   453 ms  hurricane-ic-308019-palo-b1.c.telia.net [80.239.167.174]
 18   605 ms   406 ms   406 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 19   403 ms   438 ms   380 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 20   533 ms   366 ms   407 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

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?

   Yes, the tracerouting follows a particular path from the user's IP address through the IP addresses of the ISP and then the path really 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?

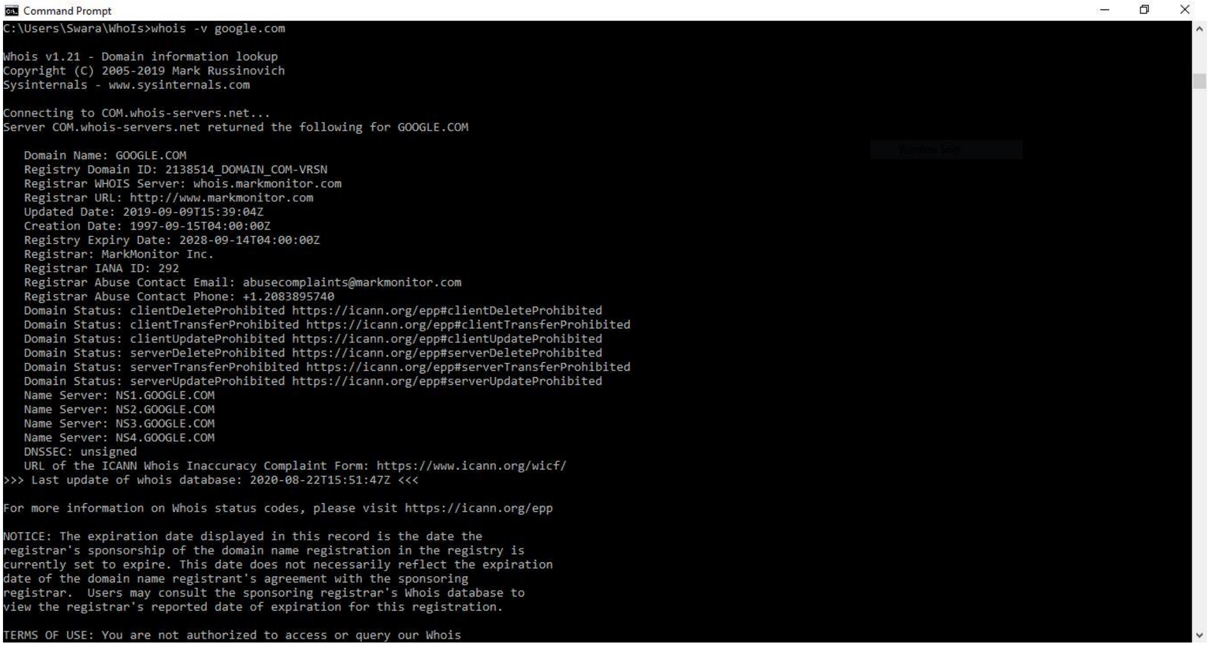
   Yes, the number of nodes(number of hops subtract 1) is directly proportional to the distance between the source and destination.

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?

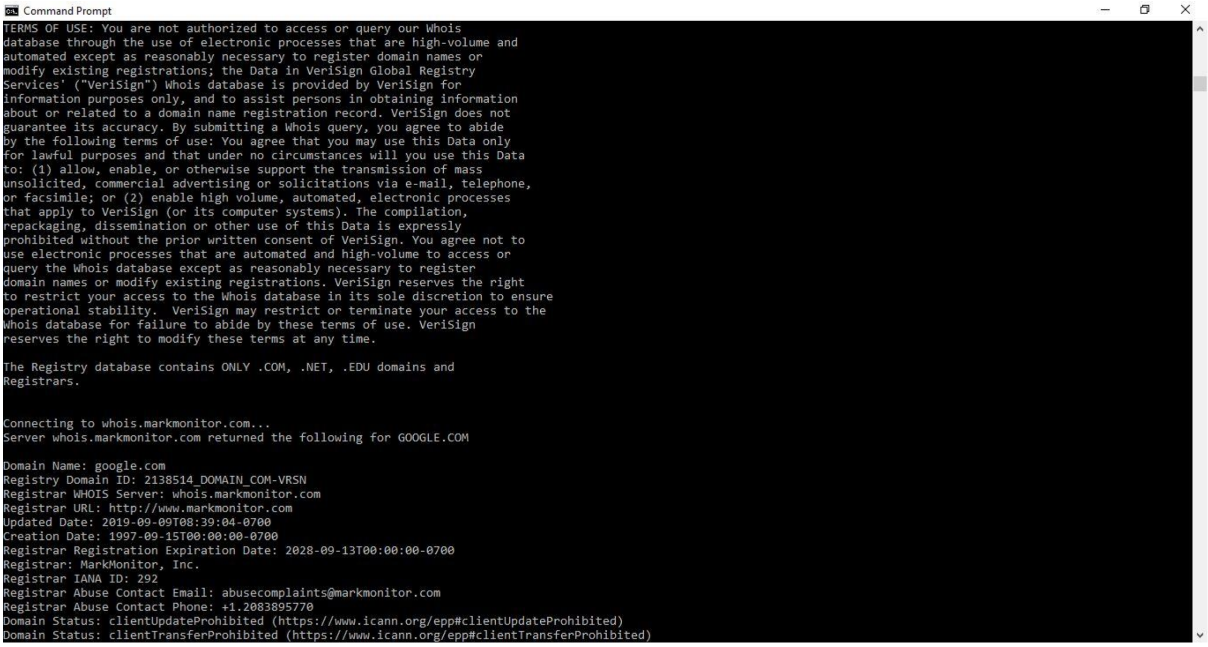
   There is a direct relationship between the number of nodes and the latency of the host. It also depends on the packet size. The amount of latency is largely dependent on how far the visitor is from the server location and how many nodes the signal has to travel through.

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*).

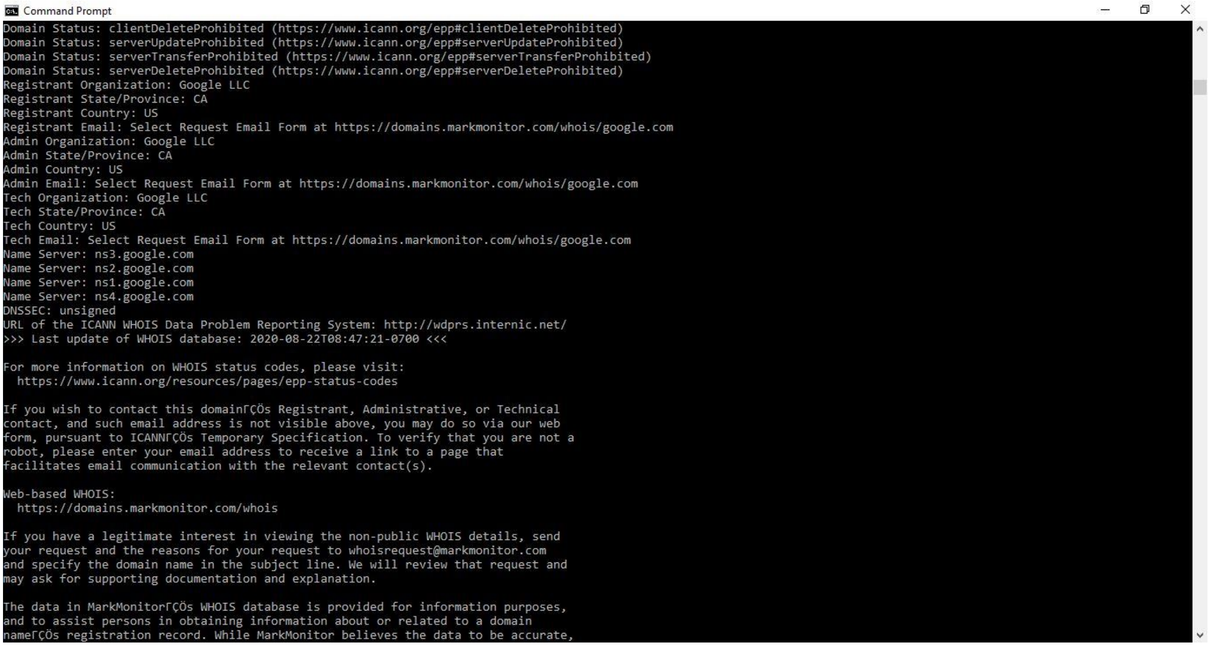
<u>Exercise 4:</u> (Short.) Use *whois* to investigate a well-known web site such as google.com or amazon.com, and write a couple of sentences about what you find out.



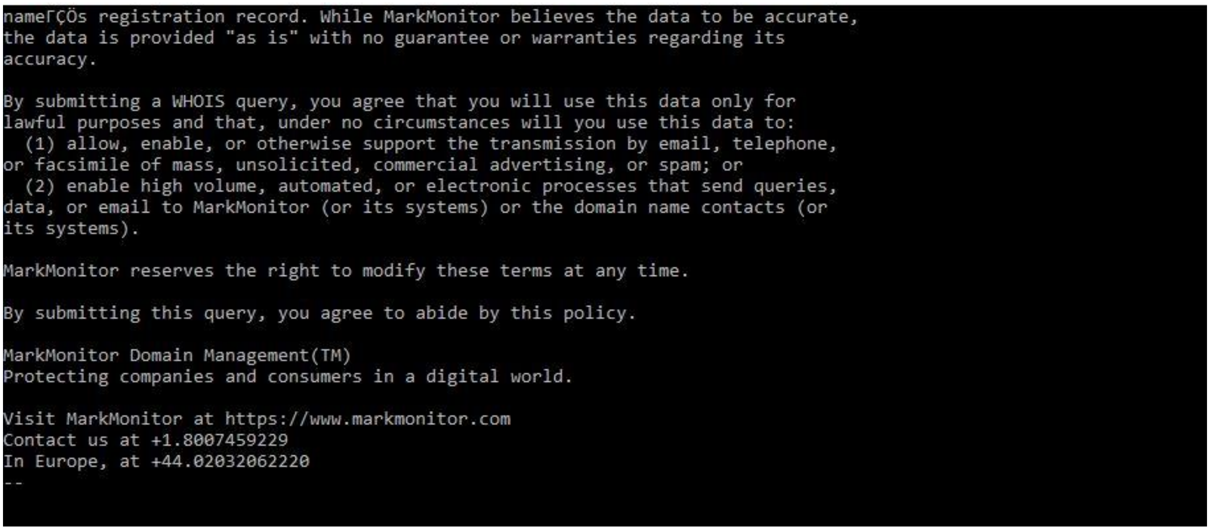
```
C:\Users\Swara\WhoIs>whois -v google.com

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

Connecting to COM.whois-servers.net...
Server COM.whois-servers.net returned the following for 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: 2020-08-22T15:51:47Z <<<

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
```



```
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.


Connecting to whois.markmonitor.com...
Server whois.markmonitor.com returned the following for 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: 2019-09-09T08:39:04-0700
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)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
```



```
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Google LLC
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Admin Organization: Google LLC
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Tech Organization: Google LLC
Tech State/Province: CA
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Name Server: ns3.google.com
Name Server: ns2.google.com
Name Server: ns1.google.com
Name Server: ns4.google.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-08-22T08:47:21-0700 <<<

For more information on WHOIS status codes, please visit:
  https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domainΓÇÖs Registrant, Administrative, or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANNΓÇÖs 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 MarkMonitorΓÇÖs WHOIS database is provided for information purposes,
and to assist persons in obtaining information about or related to a domain
nameΓÇÖs registration record. While MarkMonitor believes the data to be accurate,
```



```
nameΓÇÖs 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
Contact us at +1.8007459229
In Europe, at +44.02032062220
--
```

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 google.com (domain name), the Registrant Organization is Google LLC, the Registrant State/Province is California and the Registrant Country is the United States. It also provides the domain expiry date.

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.

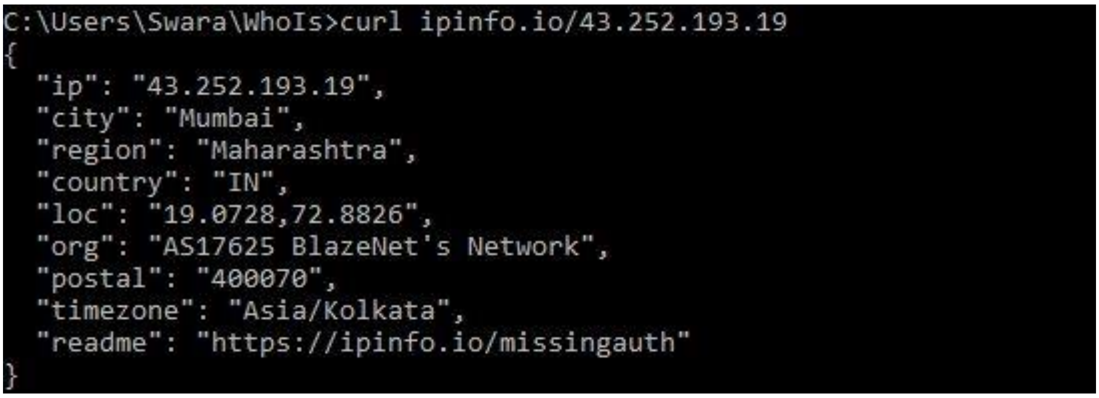
Geolocation — A geolocation service tries to tell, approximately, where a given IP address is located physically. They can't be completely accurate—but they probably get at least the country right most of the time.

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

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

Screenshot:



```
C:\Users\Swara\WhoIs>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"
}
```

Conclusion:

1. Learnt about some basic command line network utilities.
2. Learnt about Network Latency, RTT and the factors impacting RTT.