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

Chaitya Shah 2018130046

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 the 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.

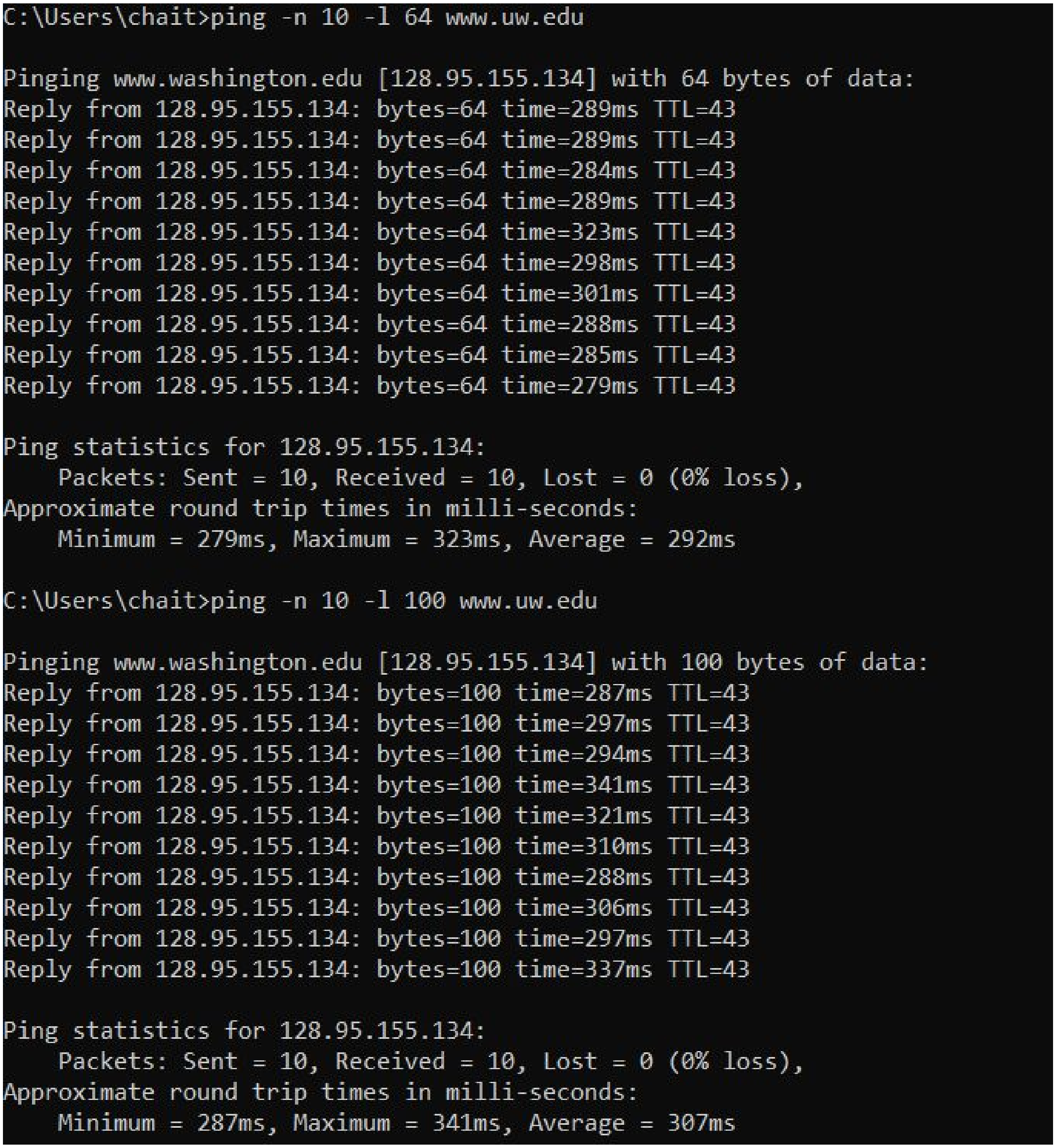
To save the output from `ping` to a file, include a greater than symbol and a file name at the end of the command. For example:

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

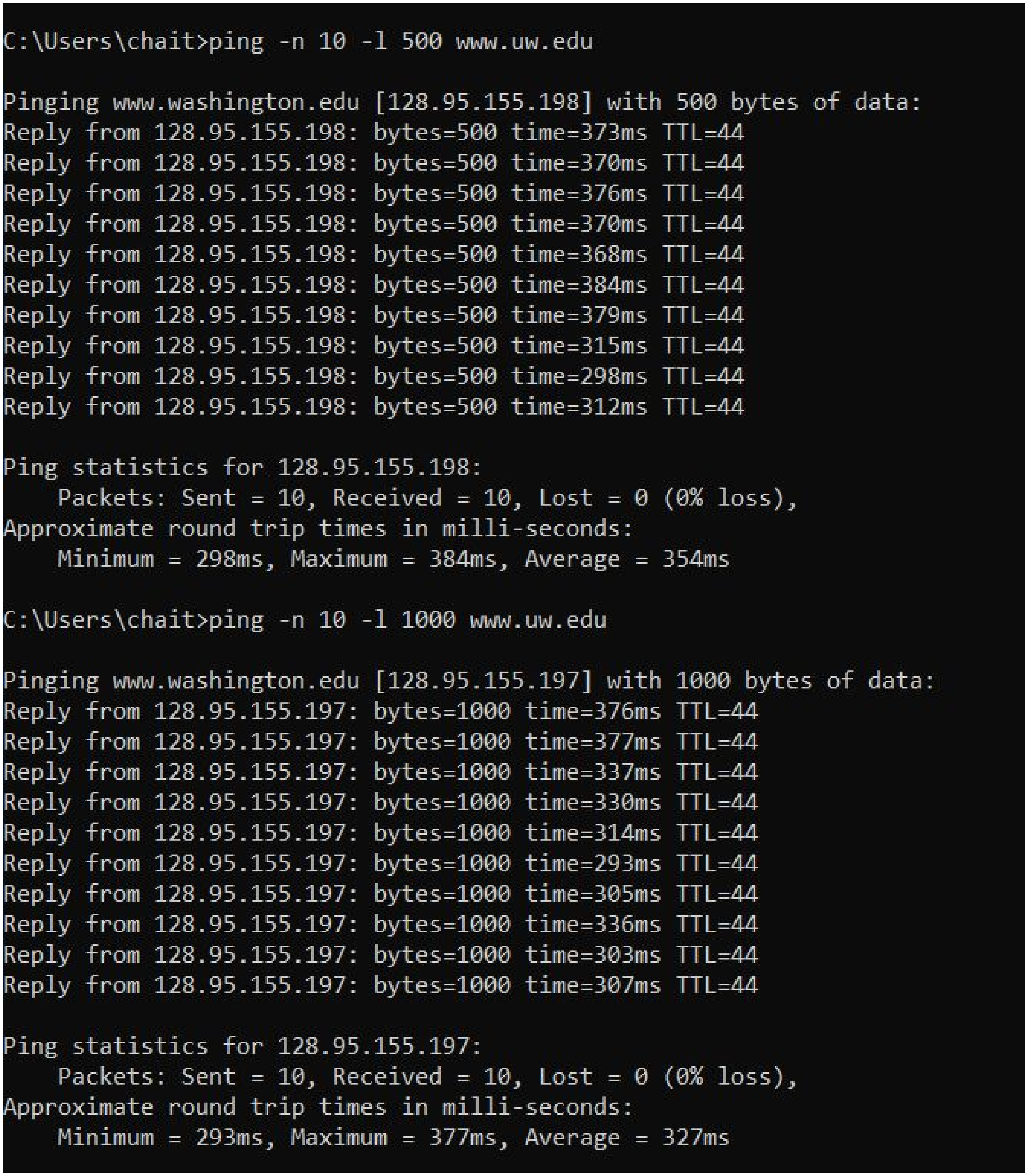
Experiments with Ping

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

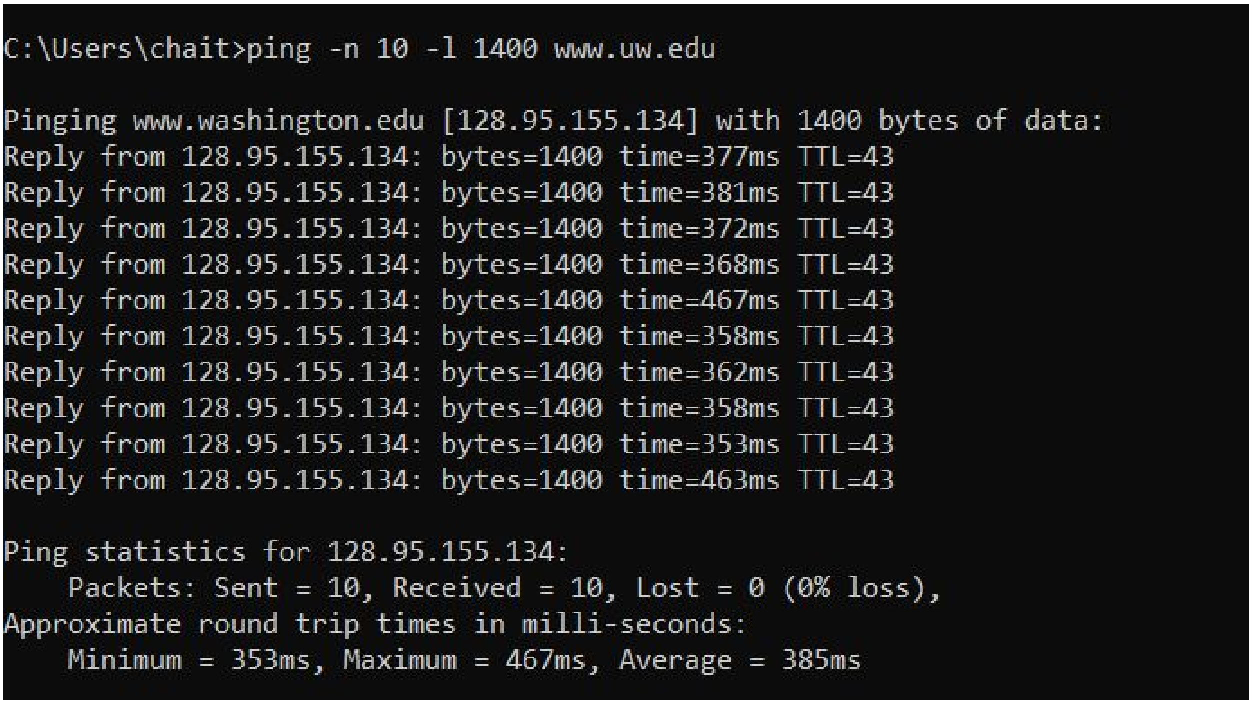
Result:



```
C:\Users\chait>ping -n 10 -l 64 www.uw.edu

Pinging www.washington.edu [128.95.155.134] with 64 bytes of data:
Reply from 128.95.155.134: bytes=64 time=289ms TTL=43
Reply from 128.95.155.134: bytes=64 time=289ms TTL=43
Reply from 128.95.155.134: bytes=64 time=284ms TTL=43
Reply from 128.95.155.134: bytes=64 time=289ms TTL=43
Reply from 128.95.155.134: bytes=64 time=323ms TTL=43
Reply from 128.95.155.134: bytes=64 time=298ms TTL=43
Reply from 128.95.155.134: bytes=64 time=301ms TTL=43
Reply from 128.95.155.134: bytes=64 time=288ms TTL=43
Reply from 128.95.155.134: bytes=64 time=285ms TTL=43
Reply from 128.95.155.134: bytes=64 time=279ms TTL=43

Ping statistics for 128.95.155.134:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 279ms, Maximum = 323ms, Average = 292ms

C:\Users\chait>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=287ms TTL=43
Reply from 128.95.155.134: bytes=100 time=297ms TTL=43
Reply from 128.95.155.134: bytes=100 time=294ms TTL=43
Reply from 128.95.155.134: bytes=100 time=341ms TTL=43
Reply from 128.95.155.134: bytes=100 time=321ms TTL=43
Reply from 128.95.155.134: bytes=100 time=310ms TTL=43
Reply from 128.95.155.134: bytes=100 time=288ms TTL=43
Reply from 128.95.155.134: bytes=100 time=306ms TTL=43
Reply from 128.95.155.134: bytes=100 time=297ms TTL=43
Reply from 128.95.155.134: bytes=100 time=337ms TTL=43

Ping statistics for 128.95.155.134:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 287ms, Maximum = 341ms, Average = 307ms
```



```
C:\Users\chait>ping -n 10 -l 500 www.uw.edu

Pinging www.washington.edu [128.95.155.198] with 500 bytes of data:
Reply from 128.95.155.198: bytes=500 time=373ms TTL=44
Reply from 128.95.155.198: bytes=500 time=370ms TTL=44
Reply from 128.95.155.198: bytes=500 time=376ms TTL=44
Reply from 128.95.155.198: bytes=500 time=370ms TTL=44
Reply from 128.95.155.198: bytes=500 time=368ms TTL=44
Reply from 128.95.155.198: bytes=500 time=384ms TTL=44
Reply from 128.95.155.198: bytes=500 time=379ms TTL=44
Reply from 128.95.155.198: bytes=500 time=315ms TTL=44
Reply from 128.95.155.198: bytes=500 time=298ms TTL=44
Reply from 128.95.155.198: bytes=500 time=312ms TTL=44

Ping statistics for 128.95.155.198:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 298ms, Maximum = 384ms, Average = 354ms

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

Pinging www.washington.edu [128.95.155.197] with 1000 bytes of data:
Reply from 128.95.155.197: bytes=1000 time=376ms TTL=44
Reply from 128.95.155.197: bytes=1000 time=377ms TTL=44
Reply from 128.95.155.197: bytes=1000 time=337ms TTL=44
Reply from 128.95.155.197: bytes=1000 time=330ms TTL=44
Reply from 128.95.155.197: bytes=1000 time=314ms TTL=44
Reply from 128.95.155.197: bytes=1000 time=293ms TTL=44
Reply from 128.95.155.197: bytes=1000 time=305ms TTL=44
Reply from 128.95.155.197: bytes=1000 time=336ms TTL=44
Reply from 128.95.155.197: bytes=1000 time=303ms TTL=44
Reply from 128.95.155.197: bytes=1000 time=307ms TTL=44

Ping statistics for 128.95.155.197:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 293ms, Maximum = 377ms, Average = 327ms
```



```
C:\Users\chait>ping -n 10 -l 1400 www.uw.edu

Pinging www.washington.edu [128.95.155.134] with 1400 bytes of data:
Reply from 128.95.155.134: bytes=1400 time=377ms TTL=43
Reply from 128.95.155.134: bytes=1400 time=381ms TTL=43
Reply from 128.95.155.134: bytes=1400 time=372ms TTL=43
Reply from 128.95.155.134: bytes=1400 time=368ms TTL=43
Reply from 128.95.155.134: bytes=1400 time=467ms TTL=43
Reply from 128.95.155.134: bytes=1400 time=358ms TTL=43
Reply from 128.95.155.134: bytes=1400 time=362ms TTL=43
Reply from 128.95.155.134: bytes=1400 time=358ms TTL=43
Reply from 128.95.155.134: bytes=1400 time=353ms TTL=43
Reply from 128.95.155.134: bytes=1400 time=463ms TTL=43

Ping statistics for 128.95.155.134:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 353ms, Maximum = 467ms, Average = 385ms
```

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?

   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(difference of distance from India between the 2 is around 5000km). 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?

   We can say that the Round Trip Time is impacted due to the difference in the size of the packets. This is because of the Transmission delay and the Queueing delay which depend on the size of the packets.RTT increases with increase in packet size. There would be increased latency for increased packet size due to transmission delay and propagation delay.

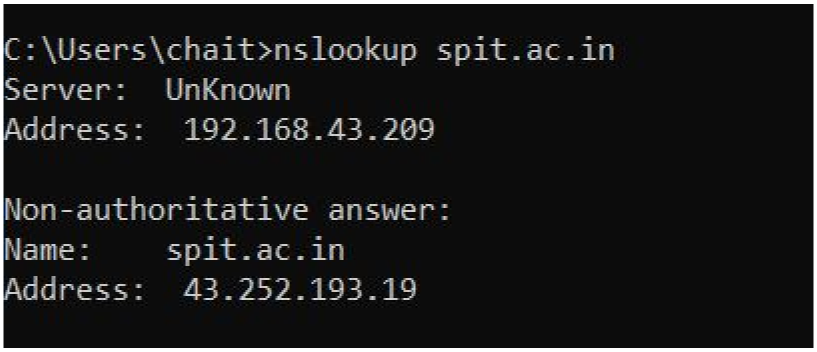
<u>**Exercise 1**</u>: Experiment with ping to find the round trip times to a variety of destinations. Write up any interesting observations, including in particular how the round trip time compares to the

physical distance. Here are a 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).

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

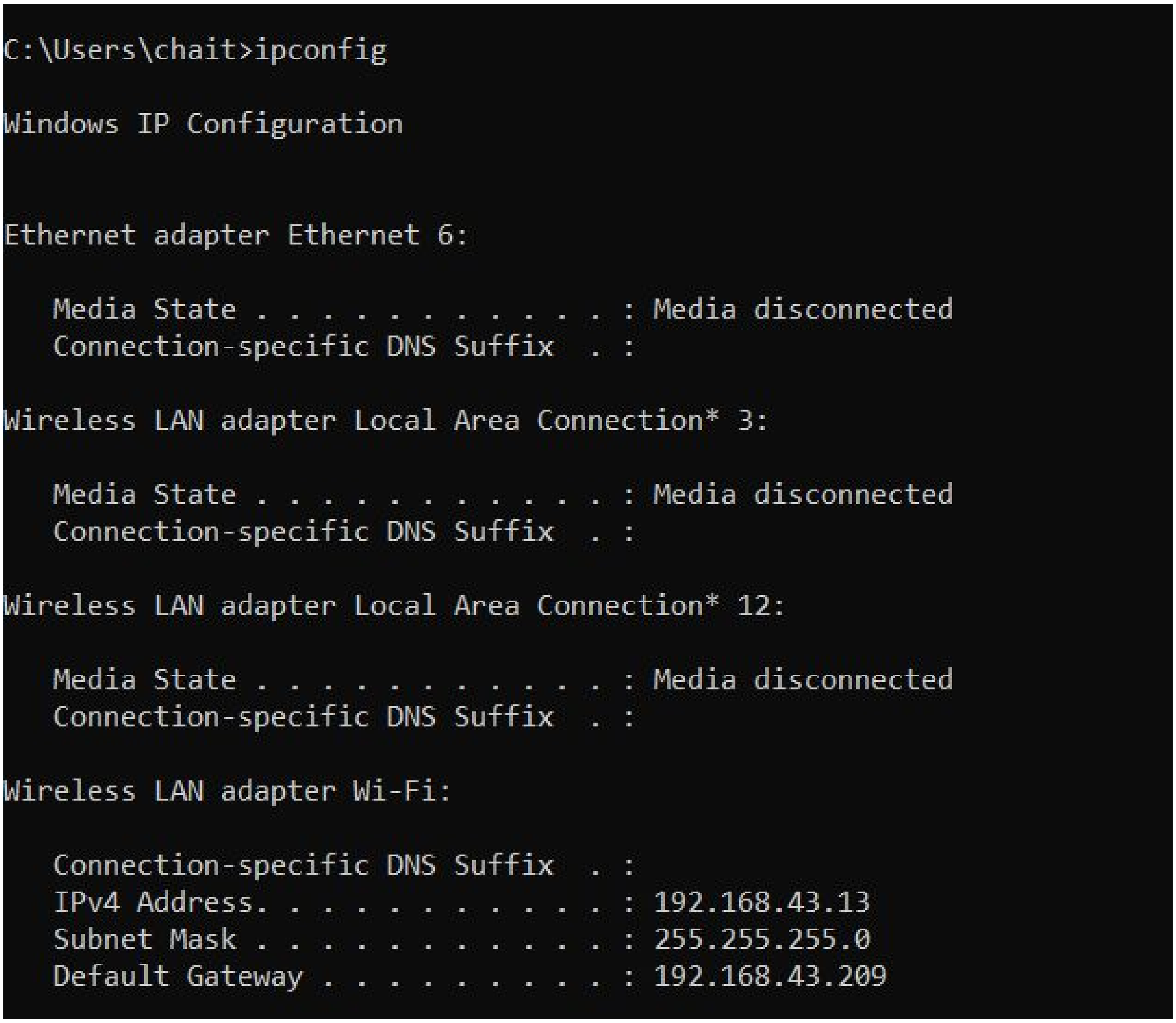
1. The length a signal has to travel correlates with the time taken for a request to reach a server and a response to reach a browser.
2. The medium used to route a signal (e.g., copper wire, fiber optic cables) can impact how quickly a request is received by a server and routed back to a user.
3. Intermediate routers or servers take time to process a signal, increasing RTT. The more hops a signal has to travel through, the higher the RTT.
4. RTT typically increases when a network is congested with high levels of traffic. Conversely, low traffic times can result in decreased RTT.
5. The time taken for a target server to respond to a request depends on its processing capacity, the number of requests being handled and the nature of the request (i.e., how much server-side work is required). A longer server response time increases 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 nslookup by adding the server name or IP address to the command: nslookup <host> <server>



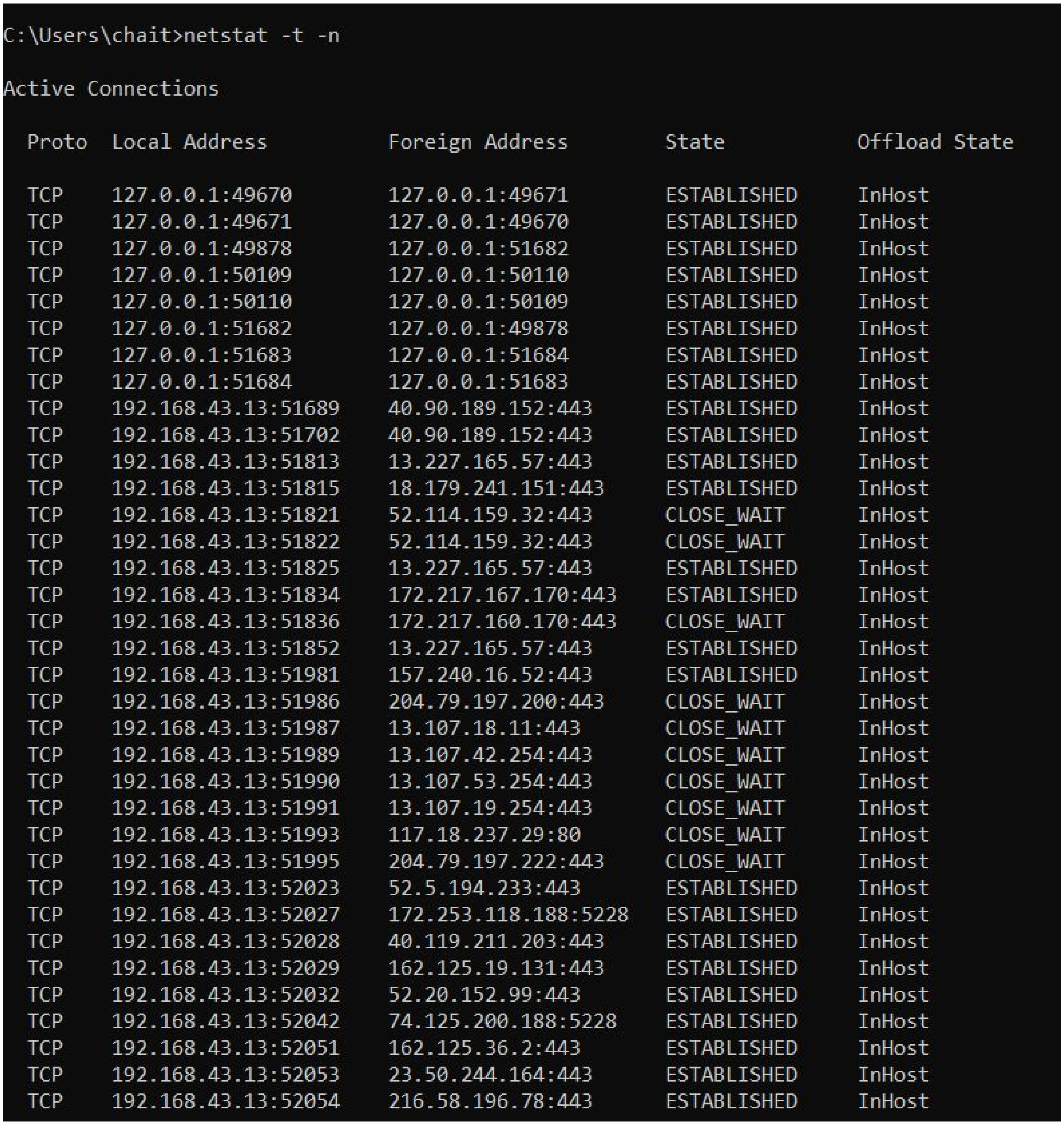
```
C:\Users\chait>nslookup spit.ac.in
Server:  UnKnown
Address:  192.168.43.209

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

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



```
C:\Users\chait>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 6:

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

Wireless LAN adapter Local Area Connection* 3:

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

Wireless LAN adapter Local Area Connection* 12:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.43.13
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.43.209
```

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



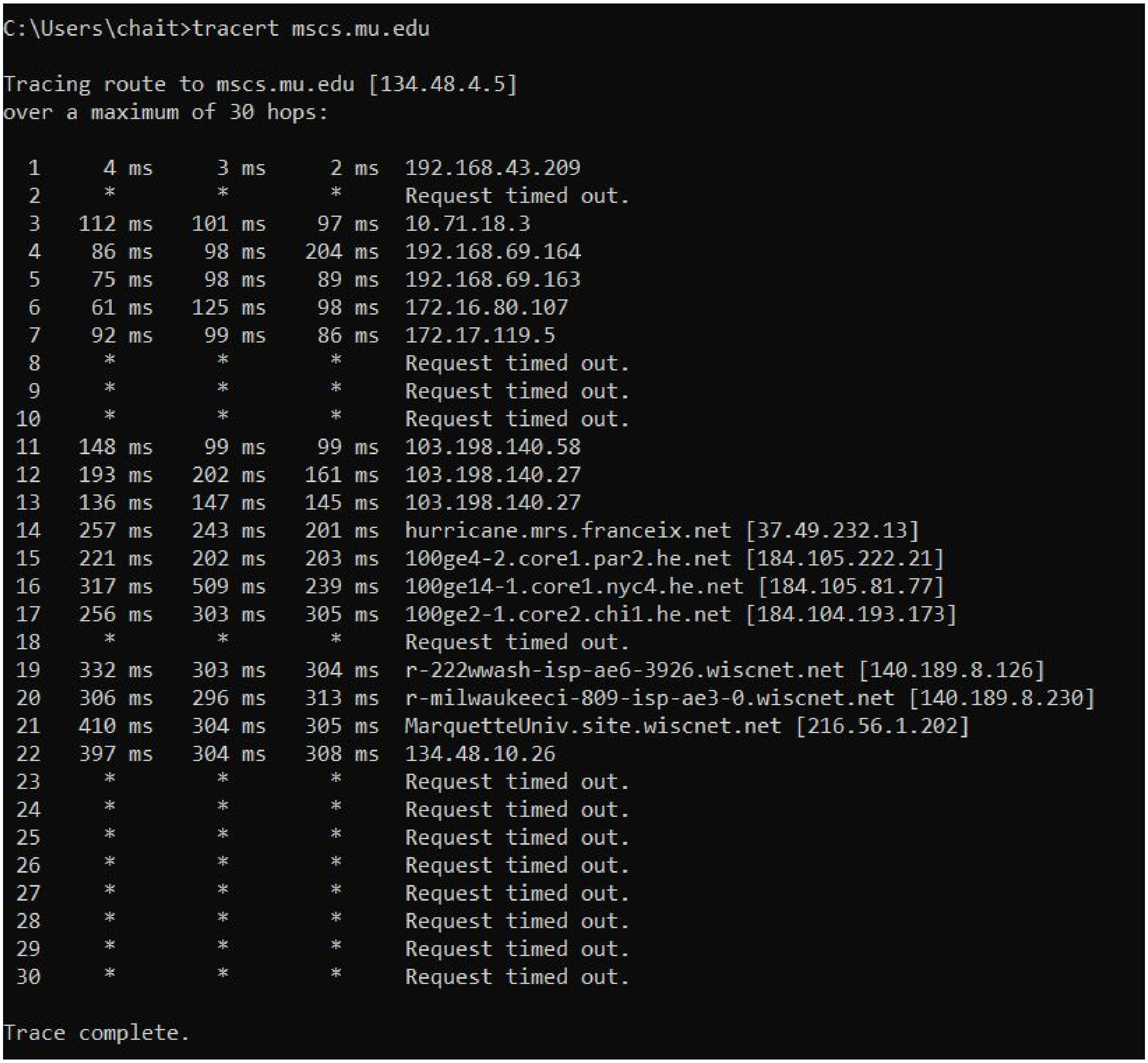
```
C:\Users\chait>netstat -t -n

Active Connections

  Proto  Local Address          Foreign Address        State           Offload State

  TCP    127.0.0.1:49670        127.0.0.1:49671        ESTABLISHED     InHost
  TCP    127.0.0.1:49671        127.0.0.1:49670        ESTABLISHED     InHost
  TCP    127.0.0.1:49878        127.0.0.1:51682        ESTABLISHED     InHost
  TCP    127.0.0.1:50109        127.0.0.1:50110        ESTABLISHED     InHost
  TCP    127.0.0.1:50110        127.0.0.1:50109        ESTABLISHED     InHost
  TCP    127.0.0.1:51682        127.0.0.1:49878        ESTABLISHED     InHost
  TCP    127.0.0.1:51683        127.0.0.1:51684        ESTABLISHED     InHost
  TCP    127.0.0.1:51684        127.0.0.1:51683        ESTABLISHED     InHost
  TCP    192.168.43.13:51689    40.90.189.152:443      ESTABLISHED     InHost
  TCP    192.168.43.13:51702    40.90.189.152:443      ESTABLISHED     InHost
  TCP    192.168.43.13:51813    13.227.165.57:443      ESTABLISHED     InHost
  TCP    192.168.43.13:51815    18.179.241.151:443     ESTABLISHED     InHost
  TCP    192.168.43.13:51821    52.114.159.32:443      CLOSE_WAIT      InHost
  TCP    192.168.43.13:51822    52.114.159.32:443      CLOSE_WAIT      InHost
  TCP    192.168.43.13:51825    13.227.165.57:443      ESTABLISHED     InHost
  TCP    192.168.43.13:51834    172.217.167.170:443    ESTABLISHED     InHost
  TCP    192.168.43.13:51836    172.217.160.170:443    CLOSE_WAIT      InHost
  TCP    192.168.43.13:51852    13.227.165.57:443      ESTABLISHED     InHost
  TCP    192.168.43.13:51981    157.240.16.52:443      ESTABLISHED     InHost
  TCP    192.168.43.13:51986    204.79.197.200:443     CLOSE_WAIT      InHost
  TCP    192.168.43.13:51987    13.107.18.11:443       CLOSE_WAIT      InHost
  TCP    192.168.43.13:51989    13.107.42.254:443      CLOSE_WAIT      InHost
  TCP    192.168.43.13:51990    13.107.53.254:443      CLOSE_WAIT      InHost
  TCP    192.168.43.13:51991    13.107.19.254:443      CLOSE_WAIT      InHost
  TCP    192.168.43.13:51993    117.18.237.29:80       CLOSE_WAIT      InHost
  TCP    192.168.43.13:51995    204.79.197.222:443     CLOSE_WAIT      InHost
  TCP    192.168.43.13:52023    52.5.194.233:443       ESTABLISHED     InHost
  TCP    192.168.43.13:52027    172.253.118.188:5228   ESTABLISHED     InHost
  TCP    192.168.43.13:52028    40.119.211.203:443     ESTABLISHED     InHost
  TCP    192.168.43.13:52029    162.125.19.131:443     ESTABLISHED     InHost
  TCP    192.168.43.13:52032    52.20.152.99:443       ESTABLISHED     InHost
  TCP    192.168.43.13:52042    74.125.200.188:5228    ESTABLISHED     InHost
  TCP    192.168.43.13:52051    162.125.36.2:443       ESTABLISHED     InHost
  TCP    192.168.43.13:52053    23.50.244.164:443      ESTABLISHED     InHost
  TCP    192.168.43.13:52054    216.58.196.78:443      ESTABLISHED     InHost
```

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 *.

1.2.1 Experiments with Traceroute

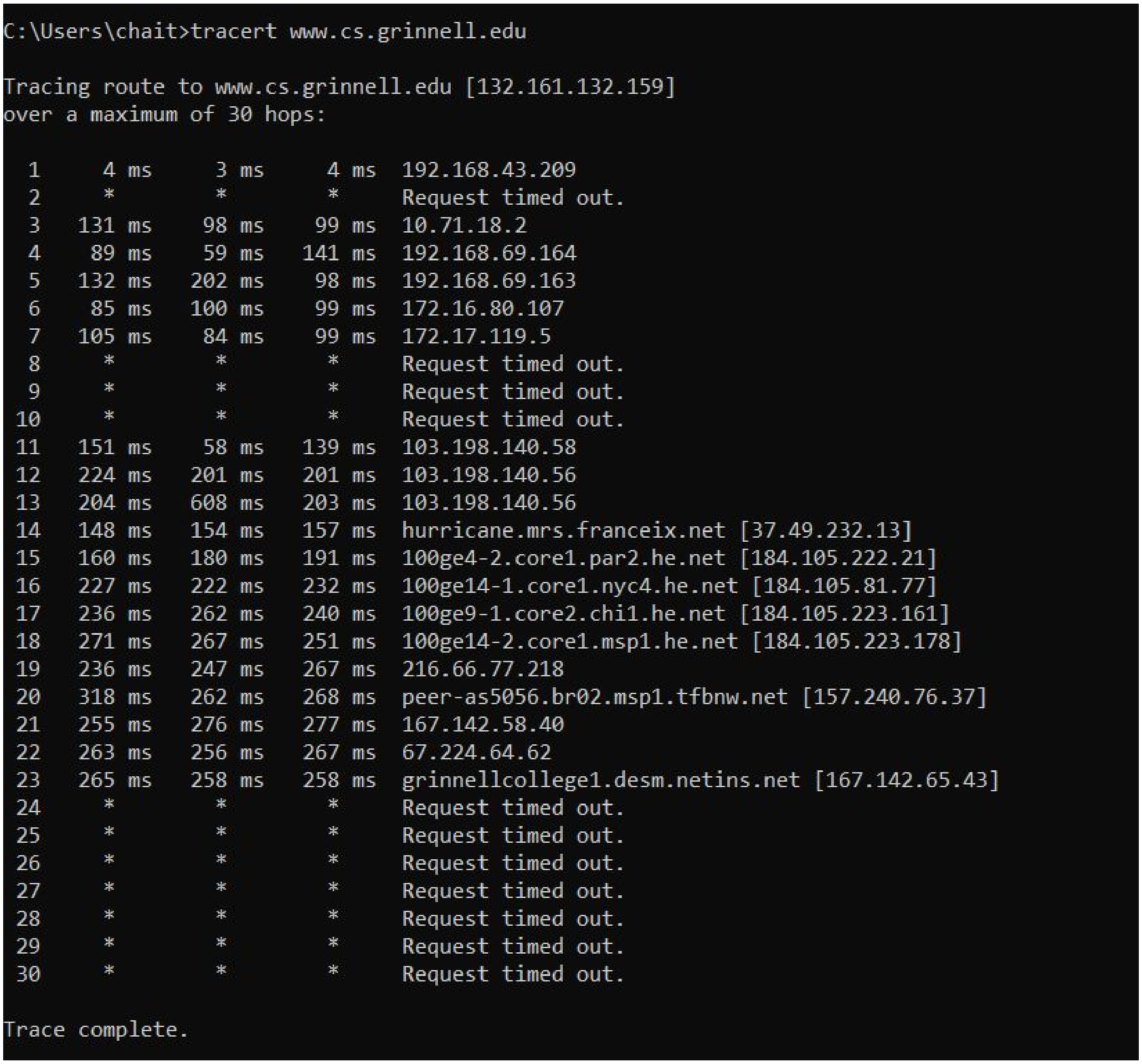
From **your machine** traceroute to the following hosts:

1. mscs.mu.edu



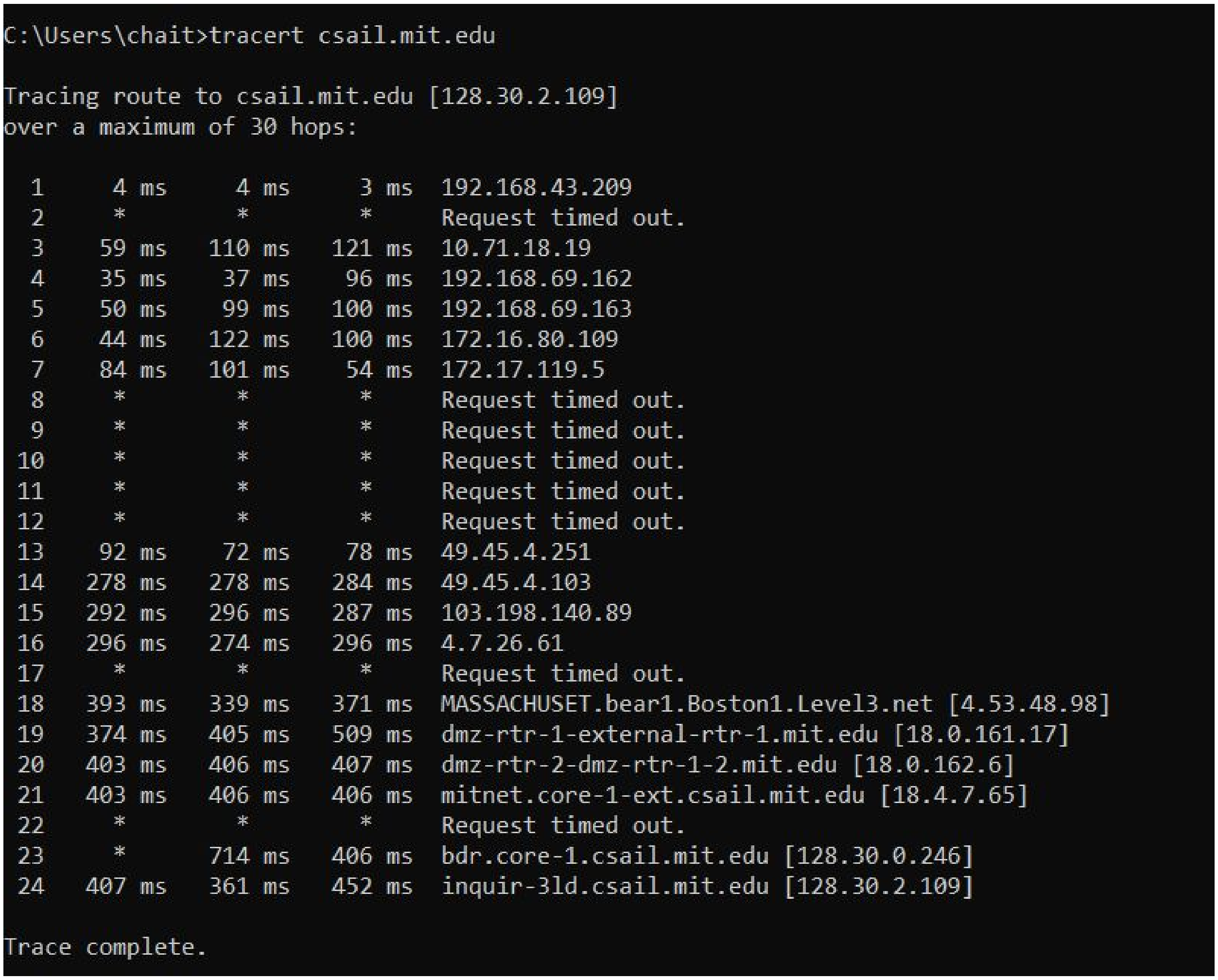
```
C:\Users\chait>tracert mscs.mu.edu

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

  1     4 ms     3 ms     2 ms  192.168.43.209
  2     *        *        *     Request timed out.
  3   112 ms   101 ms    97 ms  10.71.18.3
  4    86 ms    98 ms   204 ms  192.168.69.164
  5    75 ms    98 ms    89 ms  192.168.69.163
  6    61 ms   125 ms    98 ms  172.16.80.107
  7    92 ms    99 ms    86 ms  172.17.119.5
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11   148 ms    99 ms    99 ms  103.198.140.58
 12   193 ms   202 ms   161 ms  103.198.140.27
 13   136 ms   147 ms   145 ms  103.198.140.27
 14   257 ms   243 ms   201 ms  hurricane.mrs.franceix.net [37.49.232.13]
 15   221 ms   202 ms   203 ms  100ge4-2.core1.par2.he.net [184.105.222.21]
 16   317 ms   509 ms   239 ms  100ge14-1.core1.nyc4.he.net [184.105.81.77]
 17   256 ms   303 ms   305 ms  100ge2-1.core2.chi1.he.net [184.104.193.173]
 18     *        *        *     Request timed out.
 19   332 ms   303 ms   304 ms  r-222wwash-isp-ae6-3926.wiscnet.net [140.189.8.126]
 20   306 ms   296 ms   313 ms  r-milwaukeeci-809-isp-ae3-0.wiscnet.net [140.189.8.230]
 21   410 ms   304 ms   305 ms  MarquetteUniv.site.wiscnet.net [216.56.1.202]
 22   397 ms   304 ms   308 ms  134.48.10.26
 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.
```

2. www.cs.grinnell.edu



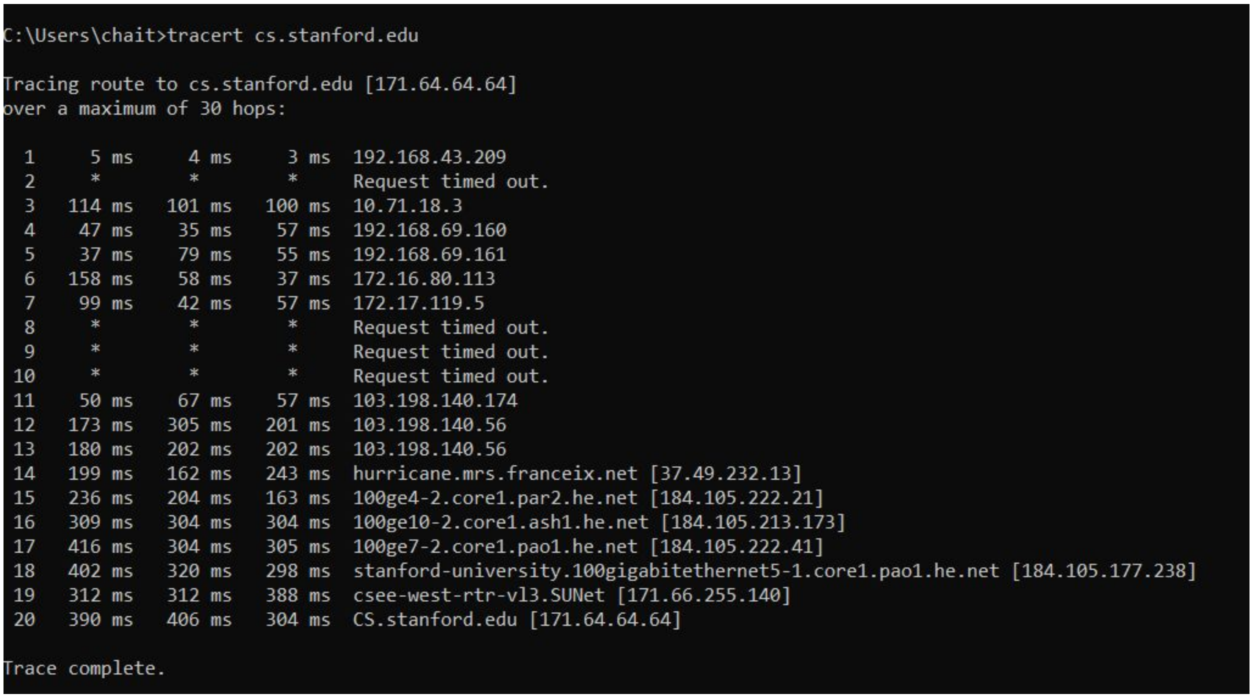
```
C:\Users\chait>tracert www.cs.grinnell.edu

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

  1     4 ms     3 ms     4 ms  192.168.43.209
  2     *        *        *     Request timed out.
  3   131 ms    98 ms    99 ms  10.71.18.2
  4    89 ms    59 ms   141 ms  192.168.69.164
  5   132 ms   202 ms    98 ms  192.168.69.163
  6    85 ms   100 ms    99 ms  172.16.80.107
  7   105 ms    84 ms    99 ms  172.17.119.5
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11   151 ms    58 ms   139 ms  103.198.140.58
 12   224 ms   201 ms   201 ms  103.198.140.56
 13   204 ms   608 ms   203 ms  103.198.140.56
 14   148 ms   154 ms   157 ms  hurricane.mrs.franceix.net [37.49.232.13]
 15   160 ms   180 ms   191 ms  100ge4-2.core1.par2.he.net [184.105.222.21]
 16   227 ms   222 ms   232 ms  100ge14-1.core1.nyc4.he.net [184.105.81.77]
 17   236 ms   262 ms   240 ms  100ge9-1.core2.chi1.he.net [184.105.223.161]
 18   271 ms   267 ms   251 ms  100ge14-2.core1.msp1.he.net [184.105.223.178]
 19   236 ms   247 ms   267 ms  216.66.77.218
 20   318 ms   262 ms   268 ms  peer-as5056.br02.msp1.tfbnw.net [157.240.76.37]
 21   255 ms   276 ms   277 ms  167.142.58.40
 22   263 ms   256 ms   267 ms  67.224.64.62
 23   265 ms   258 ms   258 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.
```

3. csail.mit.edu



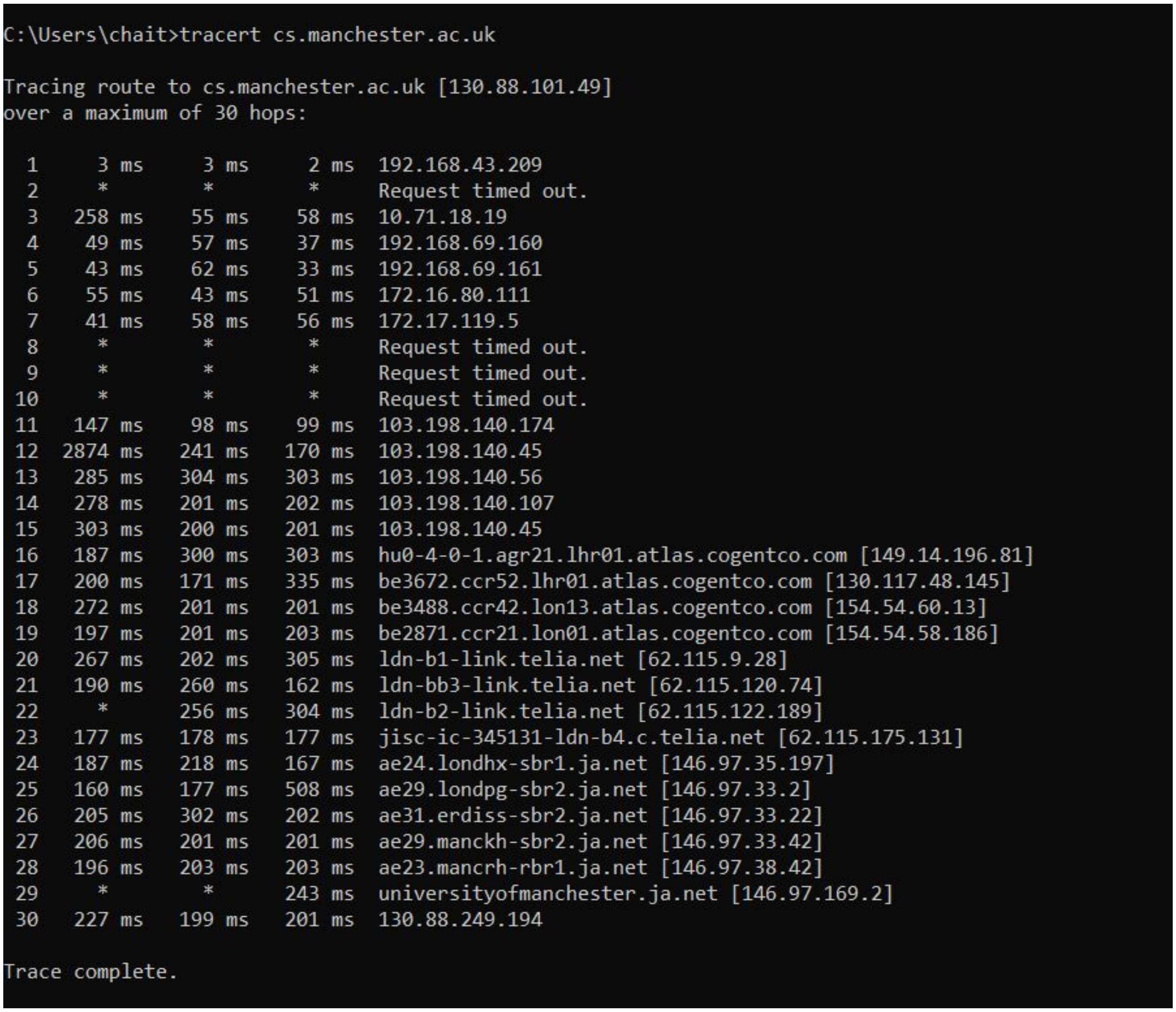
```
C:\Users\chait>tracert csail.mit.edu

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

  1     4 ms     4 ms     3 ms  192.168.43.209
  2     *        *        *     Request timed out.
  3    59 ms   110 ms   121 ms  10.71.18.19
  4    35 ms    37 ms    96 ms  192.168.69.162
  5    50 ms    99 ms   100 ms  192.168.69.163
  6    44 ms   122 ms   100 ms  172.16.80.109
  7    84 ms   101 ms    54 ms  172.17.119.5
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13    92 ms    72 ms    78 ms  49.45.4.251
 14   278 ms   278 ms   284 ms  49.45.4.103
 15   292 ms   296 ms   287 ms  103.198.140.89
 16   296 ms   274 ms   296 ms  4.7.26.61
 17     *        *        *     Request timed out.
 18   393 ms   339 ms   371 ms  MASSACHUSET.bear1.Boston1.Level3.net [4.53.48.98]
 19   374 ms   405 ms   509 ms  dmz-rtr-1-external-rtr-1.mit.edu [18.0.161.17]
 20   403 ms   406 ms   407 ms  dmz-rtr-2-dmz-rtr-1-2.mit.edu [18.0.162.6]
 21   403 ms   406 ms   406 ms  mitnet.core-1-ext.csail.mit.edu [18.4.7.65]
 22     *        *        *     Request timed out.
 23     *      714 ms   406 ms  bdr.core-1.csail.mit.edu [128.30.0.246]
 24   407 ms   361 ms   452 ms  inquir-3ld.csail.mit.edu [128.30.2.109]

Trace complete.
```

4. cs.stanford.edu



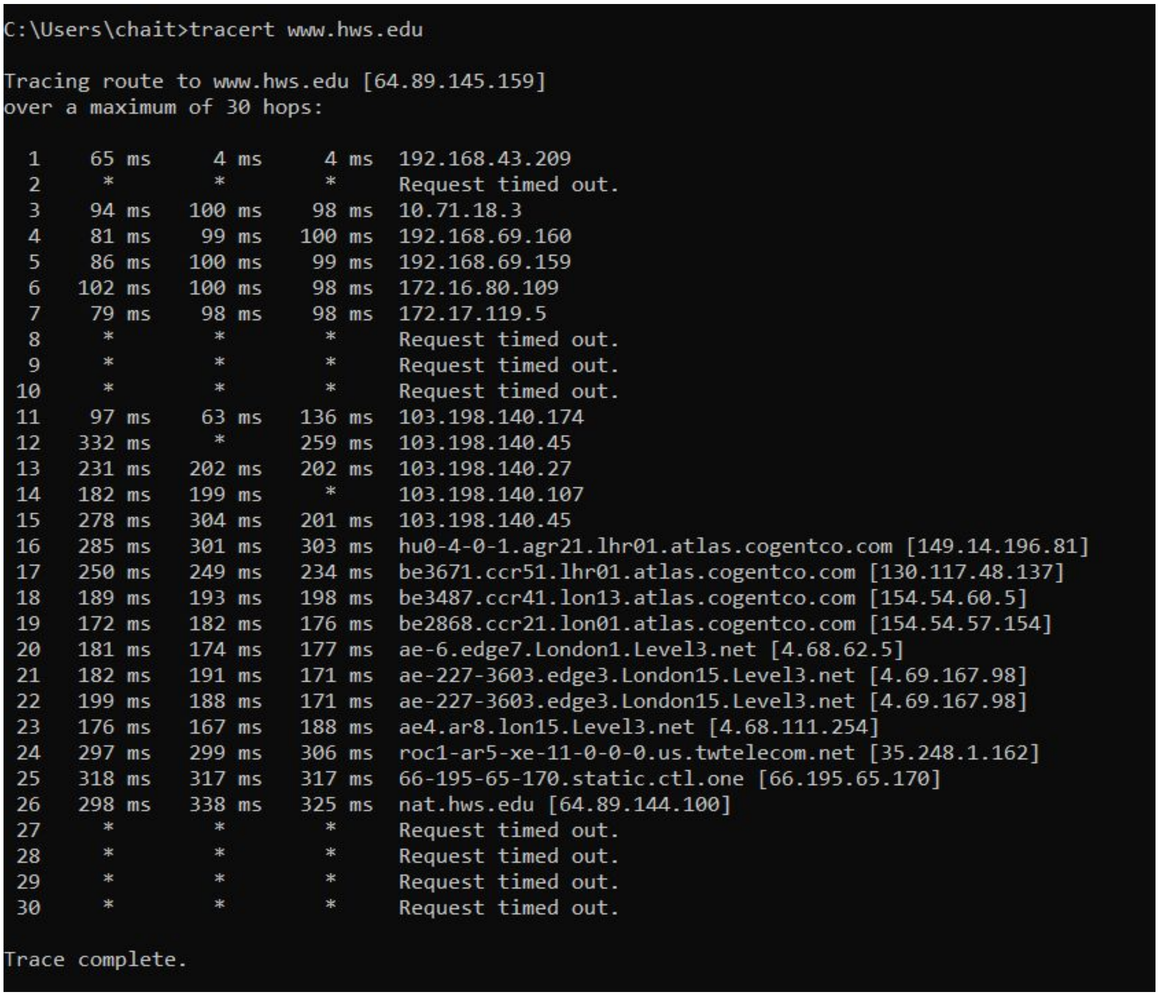
```
C:\Users\chait>tracert cs.stanford.edu

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

  1     5 ms     4 ms     3 ms  192.168.43.209
  2     *        *        *     Request timed out.
  3   114 ms   101 ms   100 ms  10.71.18.3
  4    47 ms    35 ms    57 ms  192.168.69.160
  5    37 ms    79 ms    55 ms  192.168.69.161
  6   158 ms    58 ms    37 ms  172.16.80.113
  7    99 ms    42 ms    57 ms  172.17.119.5
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11    50 ms    67 ms    57 ms  103.198.140.174
 12   173 ms   305 ms   201 ms  103.198.140.56
 13   180 ms   202 ms   202 ms  103.198.140.56
 14   199 ms   162 ms   243 ms  hurricane.mrs.franceix.net [37.49.232.13]
 15   236 ms   204 ms   163 ms  100ge4-2.core1.par2.he.net [184.105.222.21]
 16   309 ms   304 ms   304 ms  100ge10-2.core1.ash1.he.net [184.105.213.173]
 17   416 ms   304 ms   305 ms  100ge7-2.core1.pao1.he.net [184.105.222.41]
 18   402 ms   320 ms   298 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 19   312 ms   312 ms   388 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 20   390 ms   406 ms   304 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

5. cs.manchester.ac.uk

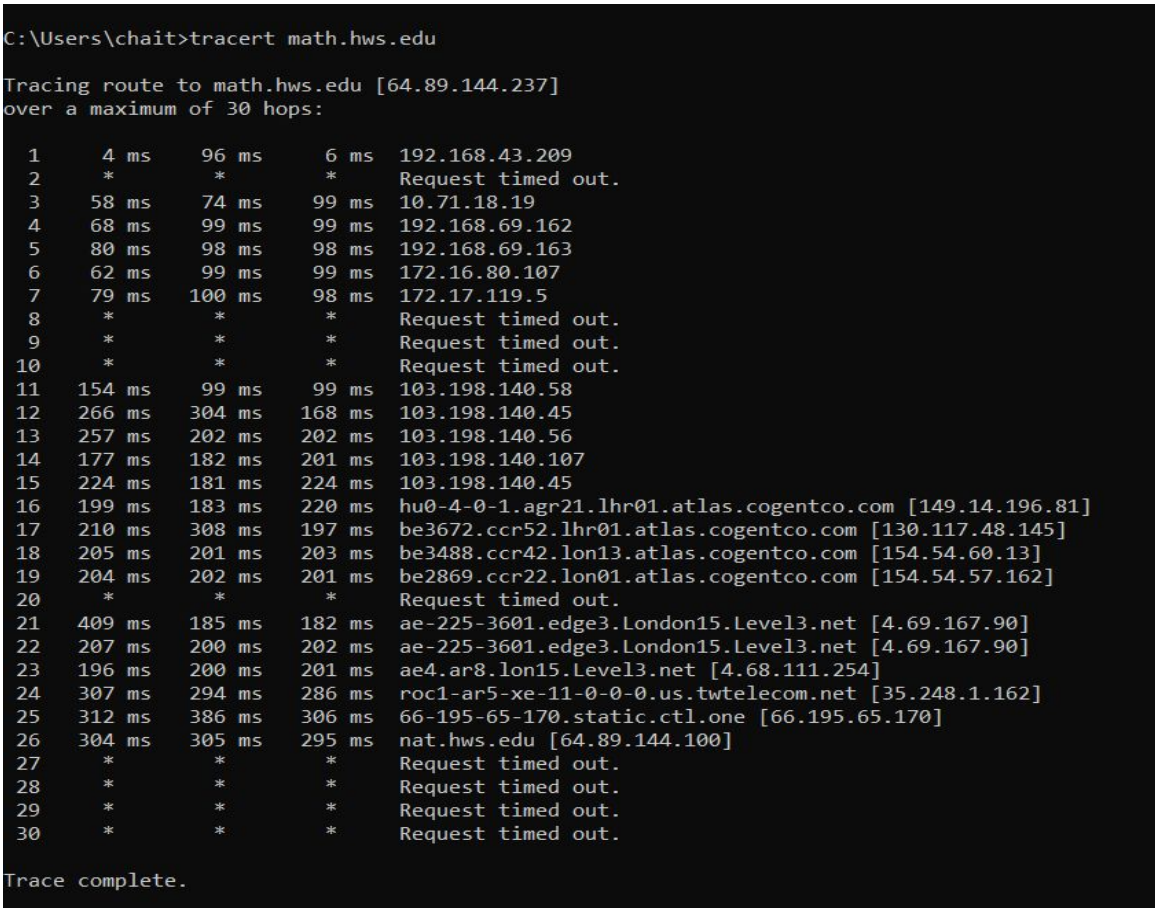


```
C:\Users\chait>tracert cs.manchester.ac.uk

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

  1     3 ms     3 ms     2 ms  192.168.43.209
  2     *        *        *     Request timed out.
  3   258 ms    55 ms    58 ms  10.71.18.19
  4    49 ms    57 ms    37 ms  192.168.69.160
  5    43 ms    62 ms    33 ms  192.168.69.161
  6    55 ms    43 ms    51 ms  172.16.80.111
  7    41 ms    58 ms    56 ms  172.17.119.5
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11   147 ms    98 ms    99 ms  103.198.140.174
 12  2874 ms   241 ms   170 ms  103.198.140.45
 13   285 ms   304 ms   303 ms  103.198.140.56
 14   278 ms   201 ms   202 ms  103.198.140.107
 15   303 ms   200 ms   201 ms  103.198.140.45
 16   187 ms   300 ms   303 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 17   200 ms   171 ms   335 ms  be3672.ccr52.lhr01.atlas.cogentco.com [130.117.48.145]
 18   272 ms   201 ms   201 ms  be3488.ccr42.lon13.atlas.cogentco.com [154.54.60.13]
 19   197 ms   201 ms   203 ms  be2871.ccr21.lon01.atlas.cogentco.com [154.54.58.186]
 20   267 ms   202 ms   305 ms  ldn-b1-link.telia.net [62.115.9.28]
 21   190 ms   260 ms   162 ms  ldn-bb3-link.telia.net [62.115.120.74]
 22     *      256 ms   304 ms  ldn-b2-link.telia.net [62.115.122.189]
 23   177 ms   178 ms   177 ms  jisc-ic-345131-ldn-b4.c.telia.net [62.115.175.131]
 24   187 ms   218 ms   167 ms  ae24.londhx-sbr1.ja.net [146.97.35.197]
 25   160 ms   177 ms   508 ms  ae29.londpg-sbr2.ja.net [146.97.33.2]
 26   205 ms   302 ms   202 ms  ae31.erdiss-sbr2.ja.net [146.97.33.22]
 27   206 ms   201 ms   201 ms  ae29.manckh-sbr2.ja.net [146.97.33.42]
 28   196 ms   203 ms   203 ms  ae23.mancrh-rbr1.ja.net [146.97.38.42]
 29     *        *      243 ms  universityofmanchester.ja.net [146.97.169.2]
 30   227 ms   199 ms   201 ms  130.88.249.194

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.



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

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

  1    65 ms     4 ms     4 ms  192.168.43.209
  2     *        *        *     Request timed out.
  3    94 ms   100 ms    98 ms  10.71.18.3
  4    81 ms    99 ms   100 ms  192.168.69.160
  5    86 ms   100 ms    99 ms  192.168.69.159
  6   102 ms   100 ms    98 ms  172.16.80.109
  7    79 ms    98 ms    98 ms  172.17.119.5
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11    97 ms    63 ms   136 ms  103.198.140.174
 12   332 ms     *      259 ms  103.198.140.45
 13   231 ms   202 ms   202 ms  103.198.140.27
 14   182 ms   199 ms     *     103.198.140.107
 15   278 ms   304 ms   201 ms  103.198.140.45
 16   285 ms   301 ms   303 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 17   250 ms   249 ms   234 ms  be3671.ccr51.lhr01.atlas.cogentco.com [130.117.48.137]
 18   189 ms   193 ms   198 ms  be3487.ccr41.lon13.atlas.cogentco.com [154.54.60.5]
 19   172 ms   182 ms   176 ms  be2868.ccr21.lon01.atlas.cogentco.com [154.54.57.154]
 20   181 ms   174 ms   177 ms  ae-6.edge7.London1.Level3.net [4.68.62.5]
 21   182 ms   191 ms   171 ms  ae-227-3603.edge3.London15.Level3.net [4.69.167.98]
 22   199 ms   188 ms   171 ms  ae-227-3603.edge3.London15.Level3.net [4.69.167.98]
 23   176 ms   167 ms   188 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 24   297 ms   299 ms   306 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 25   318 ms   317 ms   317 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 26   298 ms   338 ms   325 ms  nat.hws.edu [64.89.144.100]
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```



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

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

  1     4 ms    96 ms     6 ms  192.168.43.209
  2     *        *        *     Request timed out.
  3    58 ms    74 ms    99 ms  10.71.18.19
  4    68 ms    99 ms    99 ms  192.168.69.162
  5    80 ms    98 ms    98 ms  192.168.69.163
  6    62 ms    99 ms    99 ms  172.16.80.107
  7    79 ms   100 ms    98 ms  172.17.119.5
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11   154 ms    99 ms    99 ms  103.198.140.58
 12   266 ms   304 ms   168 ms  103.198.140.45
 13   257 ms   202 ms   202 ms  103.198.140.56
 14   177 ms   182 ms   201 ms  103.198.140.107
 15   224 ms   181 ms   224 ms  103.198.140.45
 16   199 ms   183 ms   220 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 17   210 ms   308 ms   197 ms  be3672.ccr52.lhr01.atlas.cogentco.com [130.117.48.145]
 18   205 ms   201 ms   203 ms  be3488.ccr42.lon13.atlas.cogentco.com [154.54.60.13]
 19   204 ms   202 ms   201 ms  be2869.ccr22.lon01.atlas.cogentco.com [154.54.57.162]
 20     *        *        *     Request timed out.
 21   409 ms   185 ms   182 ms  ae-225-3601.edge3.London15.Level3.net [4.69.167.90]
 22   207 ms   200 ms   202 ms  ae-225-3601.edge3.London15.Level3.net [4.69.167.90]
 23   196 ms   200 ms   201 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 24   307 ms   294 ms   286 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 25   312 ms   386 ms   306 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 26   304 ms   305 ms   295 ms  nat.hws.edu [64.89.144.100]
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

Questions About Paths

Now look at the results you gathered and answer the following questions about the paths taken by your packets.

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

   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.

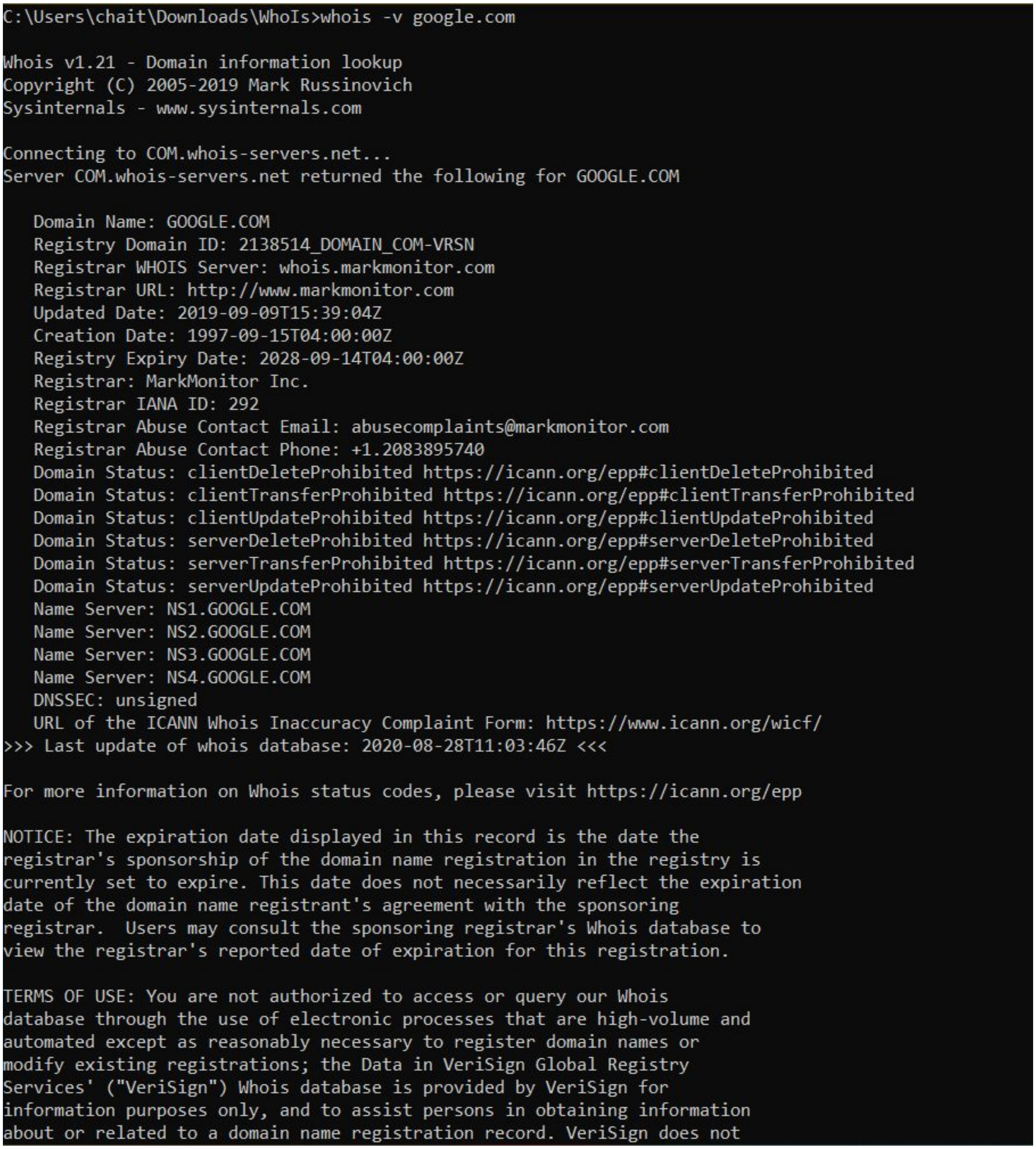
3. Is there a relationship between the number of nodes that show up in the traceroute and latency of the host (from your ping results above)? Does the same relationship hold for all hosts?

   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.

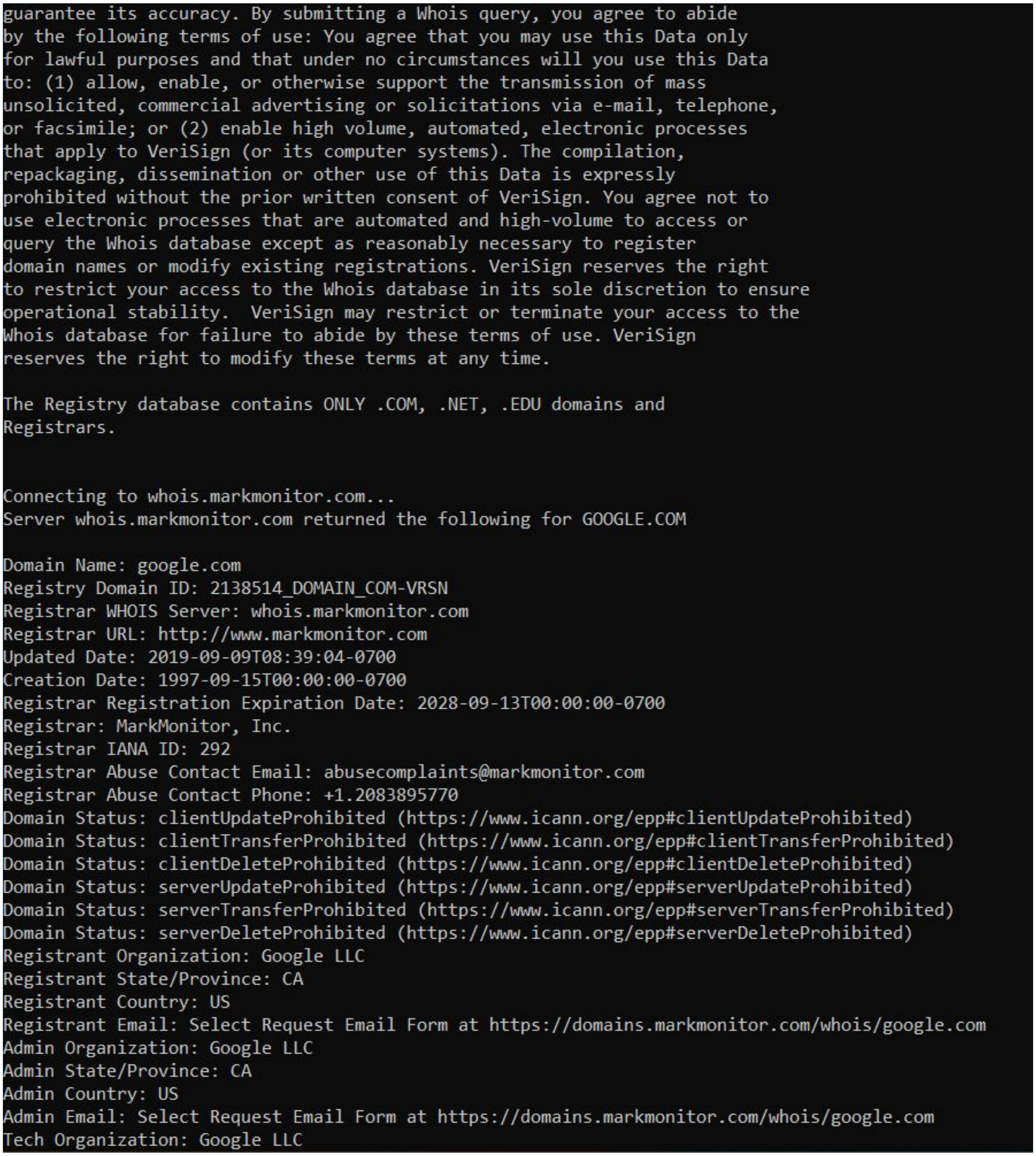
Whois — The *whois* command can give detailed information about domain names and IP addresses. If it is not installed on the computers then install it with command sudo apt-get install whois in. *Whois* can tell you what organization owns or is responsible for the name or address and where to contact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

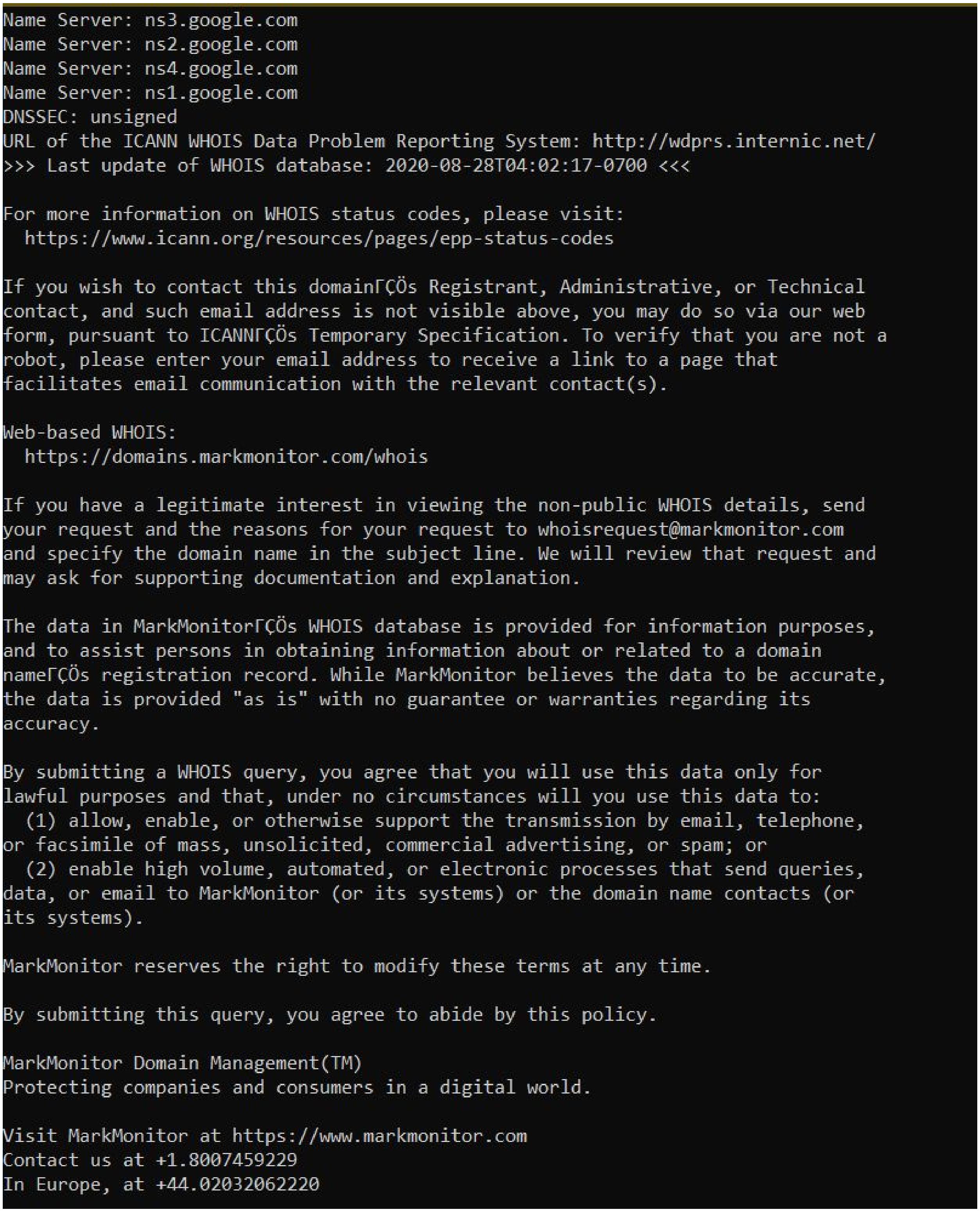
Exercise 4: (Short.) Use *whois* to investigate a well-known web site such as google.com or amazon.com, and write a couple of sentences about what you find out.



```
C:\Users\chait\Downloads\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: 2020-08-28T11:03:46Z <<<

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
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
```



```
Name Server: ns3.google.com
Name Server: ns2.google.com
Name Server: ns4.google.com
Name Server: ns1.google.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-08-28T04:02:17-0700 <<<

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,
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.

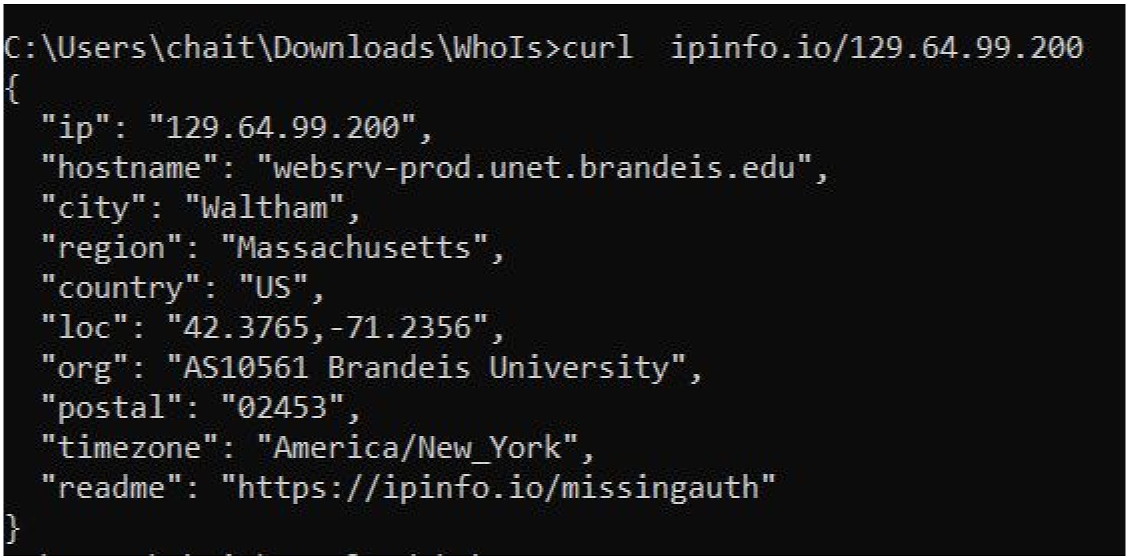
nslookup command is a program for querying Internet domain name servers (DNS).
nslookup has two modes, which are interactive and interactive.
Interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain.
Non-interactive mode is used to print just the name and requested information for a host or domain.
It is a network administration tool that helps diagnose and resolve DNS related issues.
Hence,with the help of it the outside IP address for spit.ac.in was found out.[2]
Alternatively, ping, fping and so on can be used to find out the IP address.

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.)



```
C:\Users\chait\Downloads\WhoIs>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"
}
```

Reference:

1. https://network-tools.com/trace/
2. https://www.2daygeek.com/linux-command-find-check-domain-ip-address/
3. https://www.cloudflare.com/learning/cdn/glossary/round-trip-time-rtt/

Conclusion:

1. I learned about some basic command line network utilities.
2. Also came to know about Network Latency, RTT and the factors impacting RTT.