

# Csc 4220/6220 Fall 2018 Assignment#1

1) Capture the packets with Wireshark when you access a website and see how many protocols are involved in the packet-transfer and list them by making screenshot like above with filters for each.

2) Find your own IP address in the screenshot that you take and provide a screenshot of it too.

My IP address is 192.168.0.12. There are 3 protocols (not including the link layer of the router and computer) being TCP, IPv4, and HTTP for a single TCP frame connected to oldweb.today

The screenshot displays the Wireshark interface with a packet capture filter set to 'http'. The packet list shows several HTTP requests and responses. The selected packet (No. 2357) is an HTTP 200 OK response. The packet details pane shows the following structure:

- Frame 2357: 244 bytes on wire (1952 bits), 244 bytes captured (1952 bits) on interface 0
- Linux cooked capture
- Internet Protocol Version 4, Src: 52.22.31.4, Dst: 192.168.0.12
- Transmission Control Protocol, Src Port: 80, Dst Port: 48602, Seq: 14481, Ack: 355, Len: 176
- [6 Reassembled TCP Segments (14656 bytes): #2347(2896), #2349(1448), #2351(2896), #2353(1448), #2355(5792), #2357(176)]
- Hypertext Transfer Protocol
- Line-based text data: text/html

The packet bytes pane shows the raw data of the selected packet, which is an HTTP 200 OK response. The status bar at the bottom indicates that the selected packet is a Hypertext Transfer Protocol (http), 165 bytes, and that there are 3218 packets displayed, with 54 (1.7%) shown in the current view.

3) Try to get the screenshots of your http messages with both GET and OK for one of the requested services and measure the time difference between those messages. (To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.

It took less than .06 milliseconds for the messages to transfer.

2345	2018-08-28 21:35:39.688789913	192.168.0.12	52.22.31.4	HTTP	422 GET / HTTP/1.1
2357	2018-08-28 21:35:39.748914842	52.22.31.4	192.168.0.12	HTTP	244 HTTP/1.1 200 OK (text/html)

### GET request packet details.

```
▶ Frame 2345: 422 bytes on wire (3376 bits), 422 bytes captured (3376 bits) on interface 0
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 192.168.0.12, Dst: 52.22.31.4
▶ Transmission Control Protocol, Src Port: 48602, Dst Port: 80, Seq: 1, Ack: 1, Len: 354
▼ Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
    [GET / HTTP/1.1\r\n]
    [Severity level: Chat]
    [Group: Sequence]
    Request Method: GET
    Request URI: /
    Request Version: HTTP/1.1
    Host: oldweb.today\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:59.0) Gecko/20100101 Firefox/59.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: https://www.google.com/\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://oldweb.today/]
    [HTTP request 1/4]
    [Response in frame: 2357]
    [Next request in frame: 2359]
```

### OK response packet details and HTML payload.

```
Wireshark · Packet 2357 · wireshark_any_20180828213307_IPvW97
▶ Internet Protocol Version 4, Src: 52.22.31.4, Dst: 192.168.0.12
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 48602, Seq: 14481, Ack: 355, Len: 176
▶ [6 Reassembled TCP Segments (14656 bytes): #2347(2896), #2349(1448), #2351(2896), #2353(1448), #2355(5792), #2357(176)]
▼ Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    [HTTP/1.1 200 OK\r\n]
    [Severity level: Chat]
    [Group: Sequence]
    Request Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
    Server: nginx/1.15.2\r\n
    Date: Wed, 29 Aug 2018 01:35:39 GMT\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    Content-Length: 14491\r\n
    Connection: keep-alive\r\n
    \r\n
    [HTTP response 1/4]
    [Time since request: 0.060124929 seconds]
    [Request in frame: 2345]
    [Next request in frame: 2359]
    [Next response in frame: 2449]
    File Data: 14491 bytes
  Line-based text data: text/html
    <!doctype html>\n
    <head>\n
      <meta charset="utf-8">\n
      \n
      <title>oldweb.today</title>\n
      \n
      <script>\n
        (function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){\n
          (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o),\n
          m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m)\n
        })(window,document,'script','//www.google-analytics.com/analytics.js','ga');\n
        \n
        \n
        \n
        ga('create', 'UA-768502-10', 'auto');\n
        ga('send', 'pageview');\n
        \n
        \n
```

4) Do packet capture in Wireshark and make a DNS query with nslookup in command-prompt like the one that has been mentioned above and provide the packet transfer screenshot for wireshark and DNS query in the command-prompt.

```
codefluent@codefluent-Lenovo-IdeaPad-Y510P: ~  
File Edit View Search Terminal Help  
codefluent@codefluent-Lenovo-IdeaPad-Y510P:~$ nslookup gsu.edu  
Server:                127.0.0.53  
Address:                127.0.0.53#53  
  
Non-authoritative answer:  
Name:   gsu.edu  
Address: 104.130.251.77
```

Wireshark packet capture analysis showing a DNS query and response for gsu.edu.

No.	Time	Source	Destination	Protocol	Length	Info
26	13.730595058	fe80::1205:b1ff:fe6...	fe80::bca3:75fa:8f8...	DHCPv6	168	Reply XID: 0xea1fcd CID: 000465cda4c4be938588e9c017affc7d4bdf IA
27	13.922300780	192.168.0.8	192.168.0.255	UDP	88	57621 → 57621 Len=44
28	15.568883701	192.168.0.8	224.0.0.251	MDNS	83	Standard query 0x0000 ANY DESKTOP-K46BDGS.local, "QM" question
29	15.570997243	fe80::65:2716:c5f0:...	ff02::fb	MDNS	103	Standard query 0x0000 ANY DESKTOP-K46BDGS.local, "QM" question
30	15.572949896	192.168.0.8	224.0.0.251	MDNS	177	Standard query response 0x0000 AAAA 2601:ca:8501:5db0::2 AAAA 2601:ca:8501:5db0::2
31	15.575046906	fe80::65:2716:c5f0:...	ff02::fb	MDNS	197	Standard query response 0x0000 AAAA 2601:ca:8501:5db0::2 AAAA 2601:ca:8501:5db0::2
32	16.790238239	fe80::1205:b1ff:fe6...	ff02::1	ICMPv6	176	Router Advertisement from 10:05:b1:66:dc:90
33	17.657252781	127.0.0.1	127.0.0.1	UDP	45	49546 → 49546 Len=1
34	17.657293660	::1	::1	UDP	65	47547 → 47547 Len=1
35	17.657337956	127.0.0.1	127.0.0.53	DNS	69	Standard query 0xe405 A gsu.edu
36	17.657497615	127.0.0.53	127.0.0.1	DNS	85	Standard query response 0xe405 A gsu.edu A 104.130.251.77
37	17.657733579	127.0.0.1	127.0.0.53	DNS	69	Standard query 0xa8f2 AAAA gsu.edu
38	17.657848367	127.0.0.53	127.0.0.1	DNS	69	Standard query response 0xa8f2 AAAA gsu.edu

Frame 38: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface 0  
Linux cooked capture  
Internet Protocol Version 4, Src: 127.0.0.53, Dst: 127.0.0.1  
User Datagram Protocol, Src Port: 53, Dst Port: 44913  
Domain Name System (response)

0000 00 00 03 04 00 06 00 00 00 00 00 00 00 00 00 .....  
0010 45 00 00 35 17 1c 40 00 40 11 25 66 7f 00 00 35 E..5..@.0.%f...5  
0020 7f 00 00 01 00 35 af 71 00 21 fe 68 a8 f2 81 80 .....5.q.!.h....  
0030 00 01 00 00 00 00 00 00 03 67 73 75 03 65 64 75 .....gsu.edu  
0040 00 00 1c 00 01 .....

wireshark\_any\_20180828182841\_IDATXX Packets: 48 · Displayed: 48 (100.0%) · Dropped: 0 (0.0%) Profile: Default

(Answers 5,6,7,8)

9 pm (5a)

US – google.com

21 routers (6a)

The 5<sup>th</sup> router required 210.288ms round trip time as the largest delay. (7a)

```
codefluent@codefluent-Lenovo-IdeaPad-Y510P: ~  
File Edit View Search Terminal Help  
codefluent@codefluent-Lenovo-IdeaPad-Y510P:~$ traceroute google.com 2000  
traceroute to google.com (74.125.138.139), 30 hops max, 2000 byte packets  
 1 _gateway (192.168.0.1) 44.294 ms 57.536 ms 81.283 ms  
 2 96.120.4.29 (96.120.4.29) 115.519 ms 134.017 ms 153.684 ms  
 3 xe-4-1-0-sur01.k2gwinnett.ga.atlanta.comcast.net (68.86.110.9) 166.282 ms 178.863 ms 178.840 ms  
 4 ae-89-ar01.b0atlanta.ga.atlanta.comcast.net (96.108.174.81) 192.755 ms 198.030 ms 198.009 ms  
 5 be-7725-cr02.56marietta.ga.ibone.comcast.net (68.86.93.125) 203.479 ms 210.309 ms 210.288 ms  
 6 be-11486-pe03.56marietta.ga.ibone.comcast.net (68.86.85.254) 215.148 ms 16.376 ms 41.189 ms  
 7 23.30.207.254 (23.30.207.254) 41.149 ms 41.117 ms 41.096 ms  
 8 108.170.249.44 (108.170.249.44) 41.406 ms 41.393 ms 41.374 ms  
 9 108.170.236.236 (108.170.236.236) 41.679 ms 42.509 ms 42.505 ms  
10 108.170.230.67 (108.170.230.67) 42.791 ms 45.219 ms 48.181 ms  
11 108.170.231.171 (108.170.231.171) 115.954 ms 115.960 ms 56.266 ms  
12 * * *  
13 * * *  
14 * * *  
15 * * *  
16 * * *  
17 * * *  
18 * * *  
19 * * *  
20 * * *  
21 yt-in-f139.1e100.net (74.125.138.139) 33.491 ms 33.732 ms 35.048 ms
```

UK – google.co.uk

22 routers (6a)

5<sup>th</sup> router had a RTT of 186.612ms (7a)

```
codefluent@codefluent-Lenovo-IdeaPad-Y510P: ~  
File Edit View Search Terminal Help  
codefluent@codefluent-Lenovo-IdeaPad-Y510P:~$ traceroute google.co.uk 2000  
traceroute to google.co.uk (64.233.177.94), 30 hops max, 2000 byte packets  
 1 _gateway (192.168.0.1) 18.612 ms 52.575 ms 65.913 ms  
 2 96.120.4.29 (96.120.4.29) 115.794 ms 115.781 ms 118.936 ms  
 3 xe-4-1-0-sur01.k2gwinnett.ga.atlanta.comcast.net (68.86.110.9) 137.053 ms 144.594 ms 162.585 ms  
 4 ae-89-ar01.b0atlanta.ga.atlanta.comcast.net (96.108.174.81) 162.572 ms 167.130 ms 167.117 ms  
 5 be-7725-cr02.56marietta.ga.ibone.comcast.net (68.86.93.125) 177.836 ms 178.425 ms 186.612 ms  
 6 be-11440-pe01.56marietta.ga.ibone.comcast.net (68.86.85.246) 188.829 ms 19.412 ms 18.723 ms  
 7 173.167.59.82 (173.167.59.82) 47.670 ms 47.667 ms 47.647 ms  
 8 * * *  
 9 108.170.225.104 (108.170.225.104) 68.724 ms 68.722 ms 108.170.225.106 (108.170.225.106) 68.689 ms  
10 108.170.249.44 (108.170.249.44) 68.672 ms 108.170.249.67 (108.170.249.67) 68.646 ms 68.622 ms  
11 72.14.233.145 (72.14.233.145) 68.598 ms 108.170.236.236 (108.170.236.236) 68.575 ms 72.14.233.145 (72.14.233.145) 69.4  
60 ms  
12 216.239.47.83 (216.239.47.83) 51.126 ms 209.85.142.149 (209.85.142.149) 31.143 ms 216.239.50.99 (216.239.50.99) 31.122  
ms  
13 * * *  
14 * * *  
15 * * *  
16 * * *  
17 * * *  
18 * * *  
19 * * *  
20 * * *  
21 * * *  
22 yx-in-f94.1e100.net (64.233.177.94) 18.227 ms 19.503 ms 17.268 ms
```

10pm (5b)

US – google.com

15 routers (6b)

Again the 5<sup>th</sup> router had a time of 46.976ms RTT for delay. (7b)

```
codefluent@codefluent-Lenovo-IdeaPad-Y510P: ~  
File Edit View Search Terminal Help  
codefluent@codefluent-Lenovo-IdeaPad-Y510P:~$ traceroute google.com 2000  
traceroute to google.com (172.217.4.14), 30 hops max, 2000 byte packets  
 1 _gateway (192.168.0.1) 3.155 ms 4.589 ms 4.569 ms  
 2 96.120.4.29 (96.120.4.29) 35.318 ms 35.311 ms 35.528 ms  
 3 xe-4-1-0-sur01.k2gwinnett.ga.atlanta.comcast.net (68.86.110.9) 35.777 ms 35.769 ms 36.131 ms  
 4 ae-89-ar01.b0atlanta.ga.atlanta.comcast.net (96.108.174.81) 36.124 ms 36.483 ms 38.403 ms  
 5 be-7725-cr02.56marietta.ga.ibone.comcast.net (68.86.93.125) 43.134 ms 43.124 ms 46.976 ms  
 6 be-11440-pe01.56marietta.ga.ibone.comcast.net (68.86.85.246) 47.695 ms 17.880 ms 35.802 ms  
 7 173.167.59.74 (173.167.59.74) 35.808 ms 35.807 ms 36.008 ms  
 8 * * *  
 9 108.170.225.112 (108.170.225.112) 35.957 ms 35.945 ms 35.932 ms  
10 108.170.249.35 (108.170.249.35) 40.135 ms 40.663 ms 41.096 ms  
11 72.14.233.145 (72.14.233.145) 46.240 ms 46.241 ms 108.170.236.236 (108.170.236.236) 46.910 ms  
12 216.239.59.152 (216.239.59.152) 35.502 ms 35.794 ms 35.792 ms  
13 108.170.249.161 (108.170.249.161) 29.508 ms 29.511 ms 35.279 ms  
14 * * *  
15 atl14s80-in-f14.1e100.net (172.217.4.14) 36.728 ms 47.801 ms 47.806 ms  
codefluent@codefluent-Lenovo-IdeaPad-Y510P:~$
```

UK – google.co.uk

22 routers (6b)

The 5<sup>th</sup> router had a time of 66.389ms RTT for delay. (7b)

```
codefluent@codefluent-Lenovo-IdeaPad-Y510P: ~  
File Edit View Search Terminal Help  
codefluent@codefluent-Lenovo-IdeaPad-Y510P:~$ traceroute google.co.uk 2000  
traceroute to google.co.uk (64.233.177.94), 30 hops max, 2000 byte packets  
 1 _gateway (192.168.0.1) 9.162 ms 20.440 ms 26.094 ms  
 2 96.120.4.29 (96.120.4.29) 54.405 ms 54.713 ms 54.698 ms  
 3 xe-4-1-0-sur01.k2gwinnett.ga.atlanta.comcast.net (68.86.110.9) 55.095 ms 55.078 ms 55.443 ms  
 4 ae-89-ar01.b0atlanta.ga.atlanta.comcast.net (96.108.174.81) 55.426 ms 55.739 ms 59.549 ms  
 5 be-7725-cr02.56marietta.ga.ibone.comcast.net (68.86.93.125) 61.718 ms 61.700 ms 66.389 ms  
 6 be-11440-pe01.56marietta.ga.ibone.comcast.net (68.86.85.246) 65.481 ms 16.315 ms 41.290 ms  
 7 173.167.59.82 (173.167.59.82) 41.255 ms 41.234 ms 41.212 ms  
 8 * * *  
 9 108.170.225.106 (108.170.225.106) 41.405 ms 108.170.225.104 (108.170.225.104) 42.878 ms 108.170.225.106 (108.170.225.106) 41.369 ms  
10 108.170.249.67 (108.170.249.67) 42.837 ms 45.303 ms 46.489 ms  
11 72.14.233.119 (72.14.233.119) 52.411 ms 52.403 ms 52.997 ms  
12 216.239.56.166 (216.239.56.166) 41.790 ms 209.85.248.53 (209.85.248.53) 41.745 ms 41.971 ms  
13 * * *  
14 * * *  
15 * * *  
16 * * *  
17 * * *  
18 * * *  
19 * * *  
20 * * *  
21 * * *  
22 yx-in-f94.1e100.net (64.233.177.94) 17.238 ms 21.200 ms 15.778 ms  
codefluent@codefluent-Lenovo-IdeaPad-Y510P:~$
```

11pm (5c)

US – google.com

10 routers (6c)

The 4<sup>th</sup> router with Comcast ISP took the longest round trip time with 221.461 ms. (7c)

```
codefluent@codefluent-Lenovo-IdeaPad-Y510P: ~  
File Edit View Search Terminal Help  
codefluent@codefluent-Lenovo-IdeaPad-Y510P:~$ traceroute google.com 2000  
traceroute to google.com (216.58.217.238), 30 hops max, 2000 byte packets  
 1 _gateway (192.168.0.1) 18.589 ms 36.893 ms 148.361 ms  
 2 96.120.4.29 (96.120.4.29) 155.678 ms 155.670 ms 155.653 ms  
 3 xe-4-1-0-sur01.k2gwinnett.ga.atlanta.comcast.net (68.86.110.9) 155.369 ms 161.358 ms 221.161 ms  
 4 ae-89-ar01.b0atlanta.ga.atlanta.comcast.net (96.108.174.81) 221.483 ms 221.477 ms 221.461 ms  
 5 be-7725-cr02.56marietta.ga.ibone.comcast.net (68.86.93.125) 199.898 ms 199.895 ms 200.646 ms  
 6 be-11491-pe04.56marietta.ga.ibone.comcast.net (68.86.83.178) 202.736 ms 17.993 ms 18.151 ms  
 7 as15169.56marietta.ga.ibone.comcast.net (66.208.229.138) 18.132 ms 32.472 ms 36.828 ms  
 8 108.170.249.161 (108.170.249.161) 69.784 ms 80.515 ms 80.512 ms  
 9 * * *  
10 atl14s38-in-f238.1e100.net (216.58.217.238) 80.444 ms 80.428 ms 84.968 ms  
codefluent@codefluent-Lenovo-IdeaPad-Y510P:~$
```

UK – google.co.uk

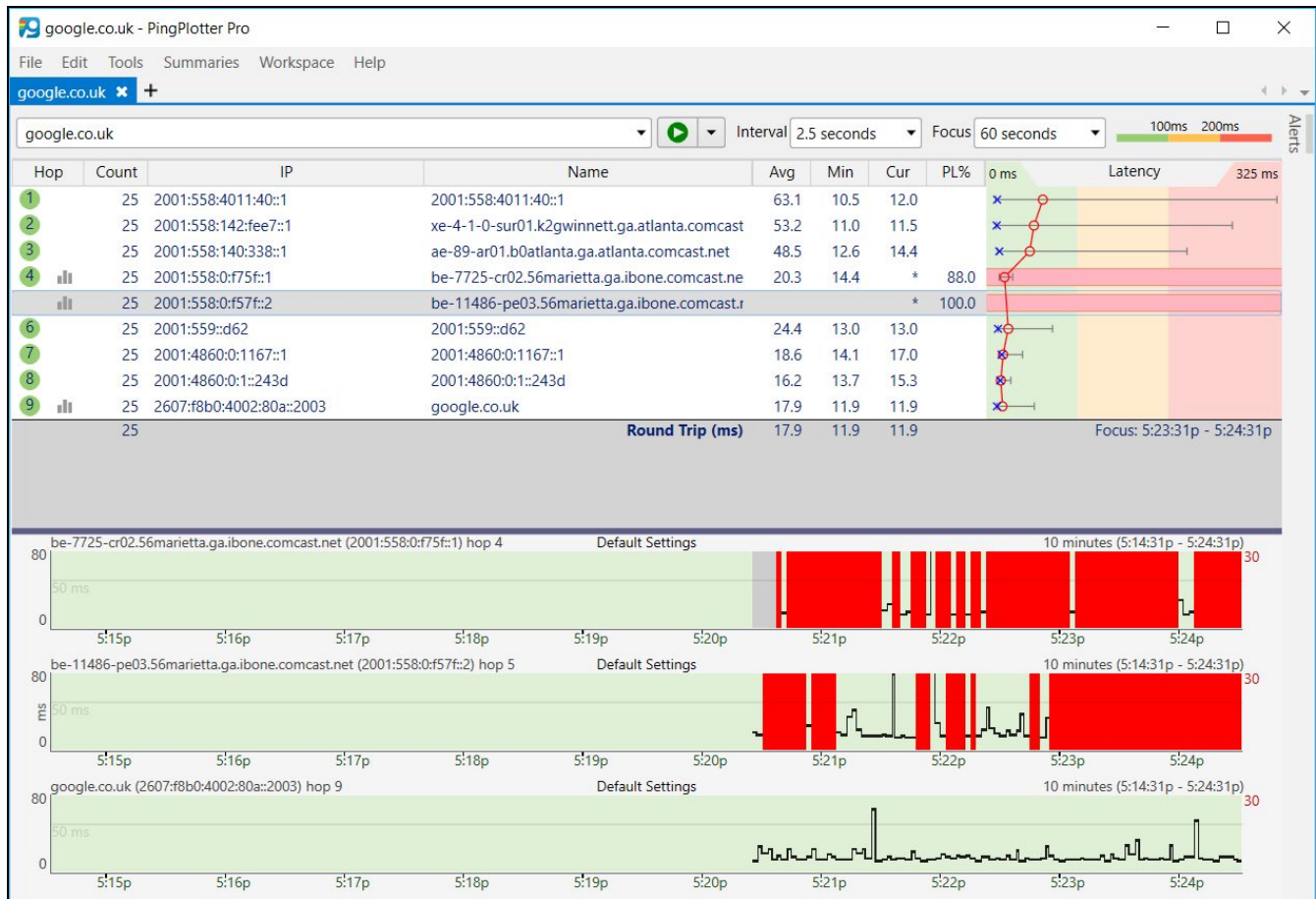
10 routers (6c) \*\*I did the command a few times, probably why its taking so little hops.

1E100.net is a google domain that took the longest round trip time with 262.706 ms. (7c)

```
codefluent@codefluent-Lenovo-IdeaPad-Y510P: ~  
File Edit View Search Terminal Help  
codefluent@codefluent-Lenovo-IdeaPad-Y510P:~$ traceroute google.co.uk 2000  
traceroute to google.co.uk (216.58.217.227), 30 hops max, 2000 byte packets  
 1 _gateway (192.168.0.1) 21.049 ms 20.988 ms *  
 2 96.120.4.29 (96.120.4.29) 175.919 ms 175.902 ms 225.905 ms  
 3 xe-4-1-0-sur01.k2gwinnett.ga.atlanta.comcast.net (68.86.110.9) 174.033 ms 174.023 ms 174.001 ms  
 4 ae-89-ar01.b0atlanta.ga.atlanta.comcast.net (96.108.174.81) 173.977 ms 173.955 ms 173.930 ms  
 5 * be-7725-cr02.56marietta.ga.ibone.comcast.net (68.86.93.125) 217.833 ms 224.597 ms  
 6 be-11486-pe03.56marietta.ga.ibone.comcast.net (68.86.85.254) 224.587 ms 40.117 ms 82.411 ms  
 7 23.30.207.254 (23.30.207.254) 122.368 ms 124.401 ms 130.603 ms  
 8 108.170.249.161 (108.170.249.161) 133.377 ms 190.013 ms 190.032 ms  
 9 * * *  
10 atl14s38-in-f3.1e100.net (216.58.217.227) 230.947 ms 238.933 ms 262.706 ms  
codefluent@codefluent-Lenovo-IdeaPad-Y510P:~$
```



9) Observe any packet-loss with any router in between source and destination and screenshot them like the one in the above in information section.



10) Briefly give an example for each of the delay in the network that have been mentioned in the class.

queuing delay: a packet for a video is being streamed onto the network, but the router has yet to process the first few frames of the video. the next packets containing the next frames of the video must wait till the previous ones are processed.

transmission delay: a packet is being sent out by a router, but the packet has a very large HTML payload so it takes some time for the router to send it out.

nodal processing delay: the router is processing some packets sees that the destination address is not within its routing table, so it must delay sending the packets until it can locate the destination via a broadcast.

propagation delay: a packet is being sent out by a router, but an IT person used a bad wire for the link so it'll take longer than usual to send the packet due to electronic interference.