CSE Lab 4

WireShark TCP Lab

Aditya Balwani, SBUID : 109353920

Part 1

1. **What is the IP address of your host? What is the IP address of the destination host?**

My IP Address is 130.245.23.108. The IP address of the destination host is 143.89.14.2

2. **Why is it that an ICMP packet does not have source and destination port numbers?**

The ICMP Packet doesn't have a source and destination port number because it is designed to communicate between the network layer and not the application layer.

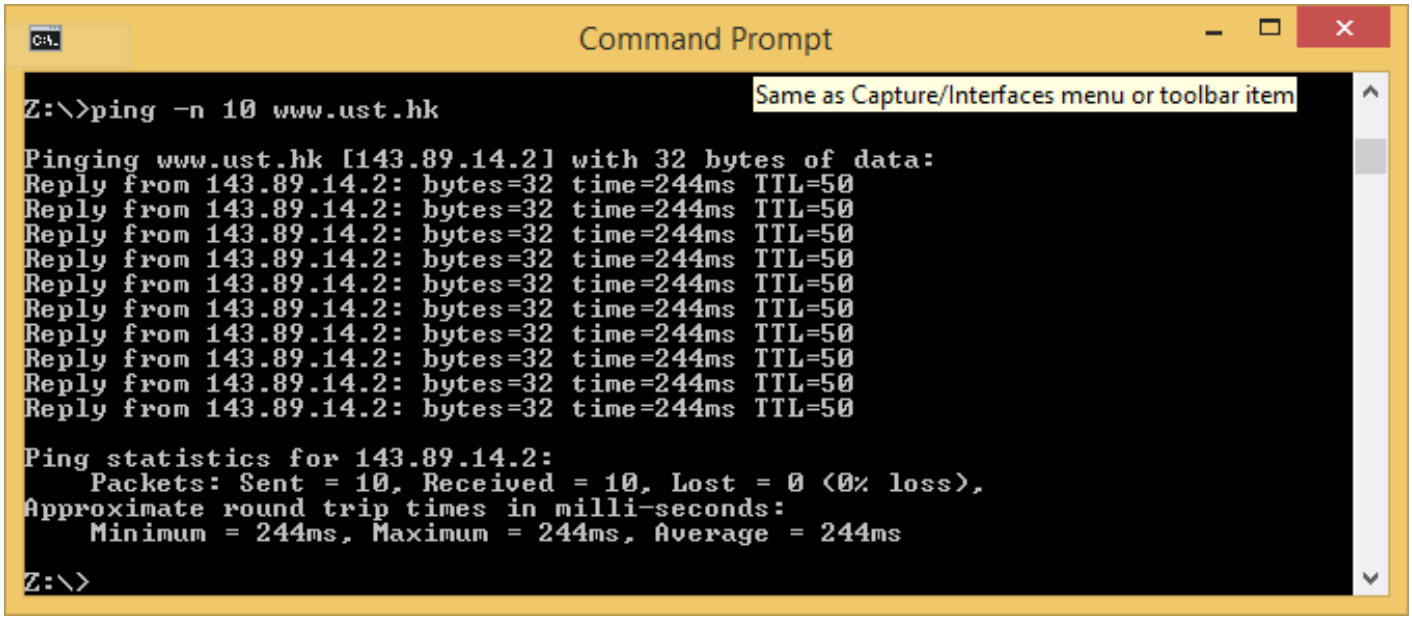
3. **Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?**

- The ICMP Type is 8
- THE ICMP Code number is 0
- The checksum is 16 bytes
- Sequence numbers:
    - BE is 16 bytes
    - LE is 16 bytes
- Identifiers

  - BE is 16 bytes
  - LE is 16 bytes

4. **Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?**

- The ICMP Type is 0
- THE ICMP Code number is 0
- The checksum is 16 bytes
- Sequence numbers:
  - BE is 16 bytes
  - LE is 16 bytes
- Identifiers
  - BE is 16 bytes
  - LE is 16 bytes



```
Z:\>ping -n 10 www.ust.hk

Pinging www.ust.hk [143.89.14.2] with 32 bytes of data:
Reply from 143.89.14.2: bytes=32 time=244ms TTL=50
Reply from 143.89.14.2: bytes=32 time=244ms TTL=50
Reply from 143.89.14.2: bytes=32 time=244ms TTL=50
Reply from 143.89.14.2: bytes=32 time=244ms TTL=50
Reply from 143.89.14.2: bytes=32 time=244ms TTL=50
Reply from 143.89.14.2: bytes=32 time=244ms TTL=50
Reply from 143.89.14.2: bytes=32 time=244ms TTL=50
Reply from 143.89.14.2: bytes=32 time=244ms TTL=50
Reply from 143.89.14.2: bytes=32 time=244ms TTL=50
Reply from 143.89.14.2: bytes=32 time=244ms TTL=50

Ping statistics for 143.89.14.2:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 244ms, Maximum = 244ms, Average = 244ms

Z:\>
```

lab5cap1.pcap [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: icmp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
20	1.851877	130.245.23.108	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=64/16384, ttl=128 (reply in 23)
23	2.096517	143.89.14.2	130.245.23.108	ICMP	74	Echo (ping) reply id=0x0001, seq=64/16384, ttl=50 (request in 20)
24	2.856181	130.245.23.108	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=65/16640, ttl=128 (reply in 27)

```
⊞ Frame 20: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⊞ Ethernet II, Src: Universa_1c:c4:41 (00:21:86:1c:c4:41), Dst: Netscreen_ff:10:02 (00:10:db:ff:10:02)
⊞ Internet Protocol Version 4, Src: 130.245.23.108 (130.245.23.108), Dst: 143.89.14.2 (143.89.14.2)
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d1b [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 64 (0x0040)
    Sequence number (LE): 16384 (0x4000)
    [Response frame: 23]
  ⊞ Data (32 bytes)
```

```
0000  00 10 db ff 10 02 00 21  86 1c c4 41 08 00 45 00   ......! ...A..E.
0010  00 3c 04 69 00 00 80 01  00 00 82 f5 17 6c 8f 59   .<.i.... .....l.Y
0020  0e 02 08 00 4d 1b 00 01  00 40 61 62 63 64 65 66   ....M... .@abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Frame (frame), 74 bytes | Packets: 82 · Displayed: 20 (24.4%) · Load time: 0:00.000 | Profile: Default

lab5cap1.pcap [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: icmp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
20	1.851877	130.245.23.108	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=64/16384, ttl=128 (reply in 23)
23	2.096517	143.89.14.2	130.245.23.108	ICMP	74	Echo (ping) reply id=0x0001, seq=64/16384, ttl=50 (request in 20)
24	2.856181	130.245.23.108	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=65/16640, ttl=128 (reply in 27)

```
⊞ Frame 23: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⊞ Ethernet II, Src: Netscreen_ff:10:02 (00:10:db:ff:10:02), Dst: Universa_1c:c4:41 (00:21:86:1c:c4:41)
⊞ Internet Protocol Version 4, Src: 143.89.14.2 (143.89.14.2), Dst: 130.245.23.108 (130.245.23.108)
⊟ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x551b [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 64 (0x0040)
    Sequence number (LE): 16384 (0x4000)
    [Request frame: 20]
    [Response time: 244.640 ms]
  ⊞ Data (32 bytes)
```

```
0000  00 21 86 1c c4 41 00 10  db ff 10 02 08 00 45 00   .!...A.. ......E.
0010  00 3c bd 2f 00 00 32 01  93 d5 8f 59 0e 02 82 f5   .<./..2. ...Y....
0020  17 6c 00 00 55 1b 00 01  00 40 61 62 63 64 65 66   .l..U... .@abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

File: "C:\Users\Aditya\Dropbox\Notes\CSE3... | Packets: 82 · Displayed: 20 (24.4%) · Load time: 0:00.000 | Profile: Default

5. **What is the IP address of your host? What is the IP address of the target destination host?**

My IP Address is 130.245.23.108. The IP address of the destination host is 128.93.162.84

6. **If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?**

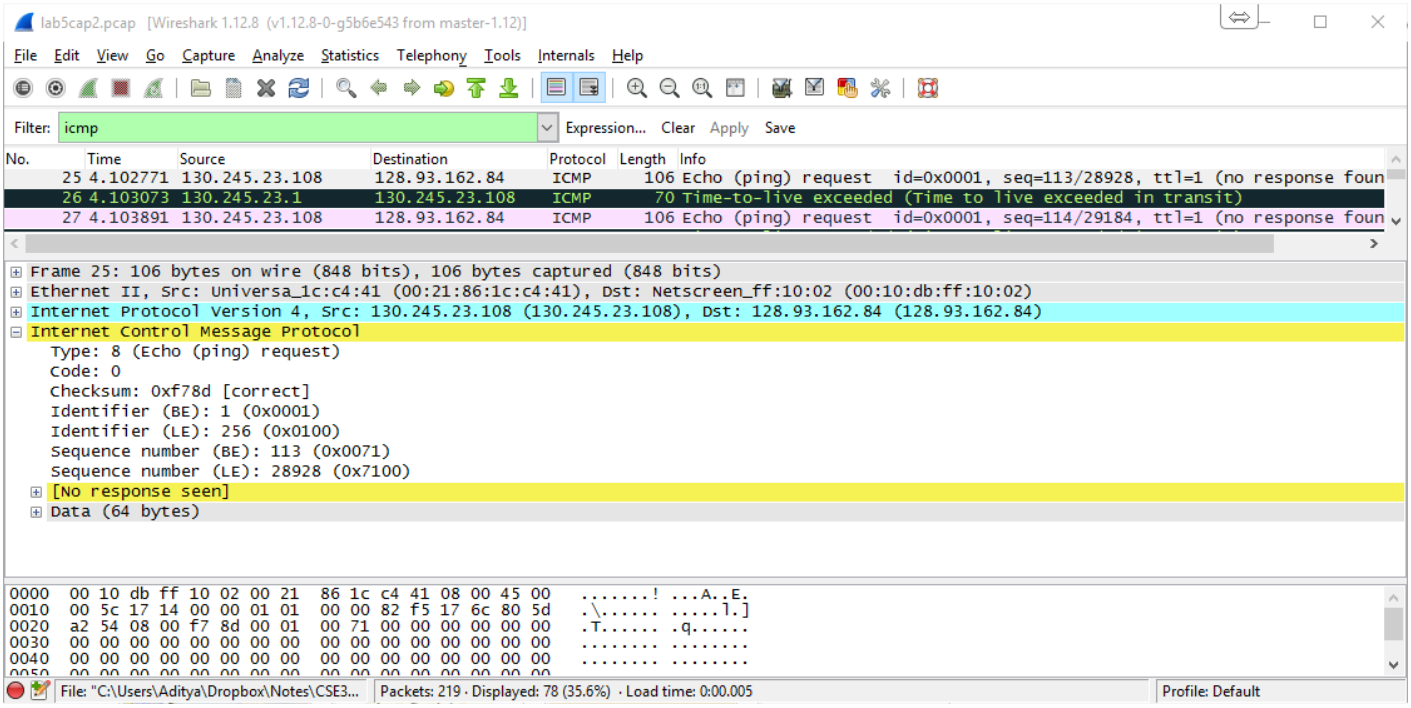
No if ICMP sent UDP packets, the IP protocol number would then be 11

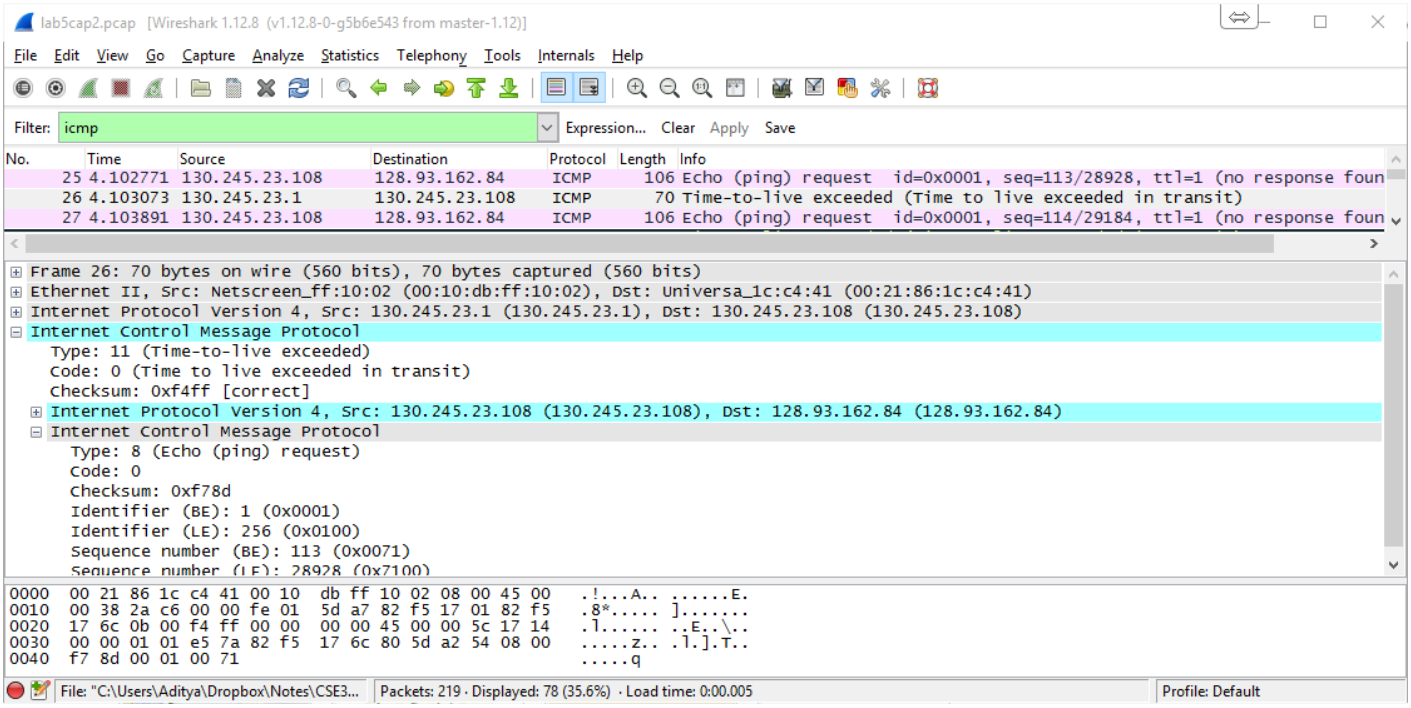
7. **Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?**

The echo packet has the same fields as the query packet

8. **Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?**

The error packet contains the IP header of the original packet and the original ICMP packet





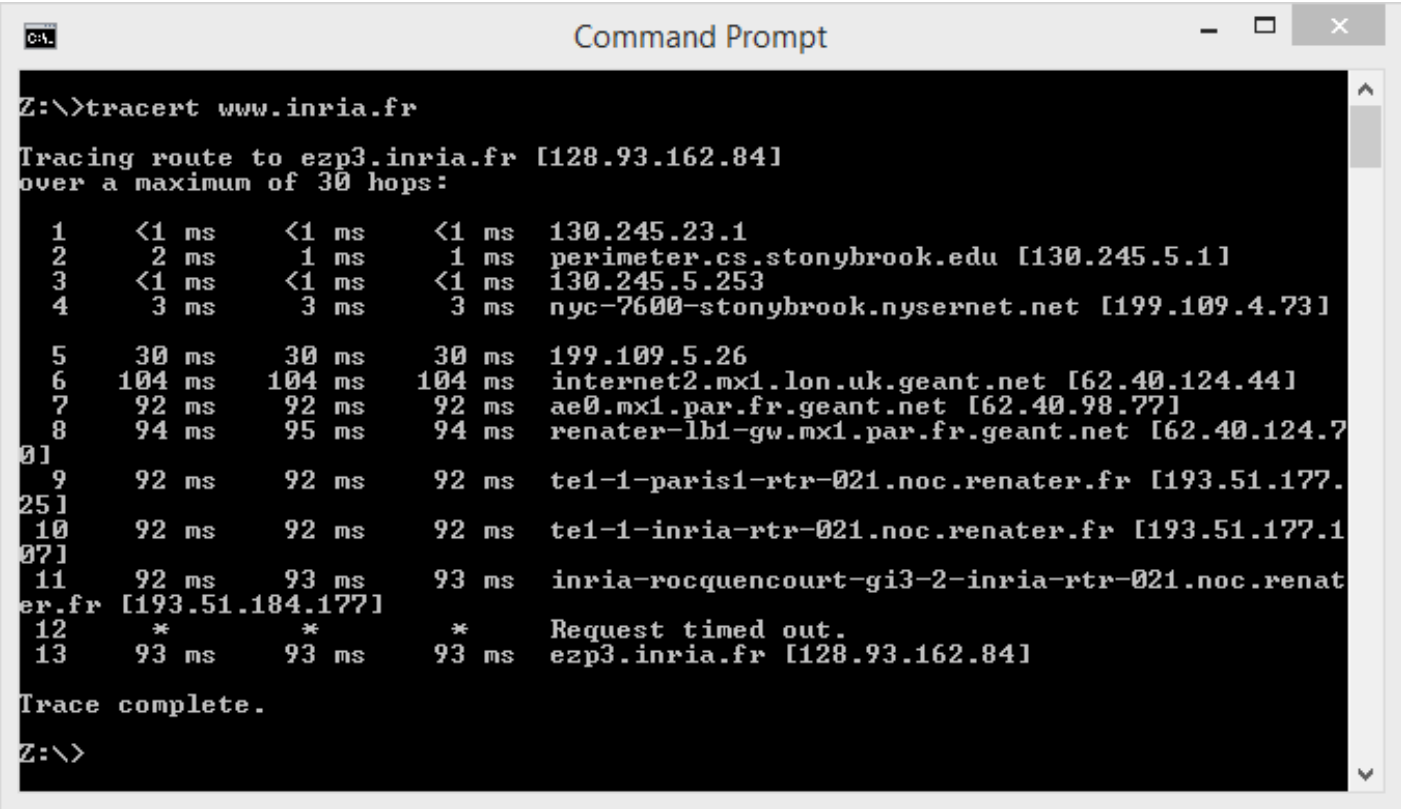
9. **Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?**

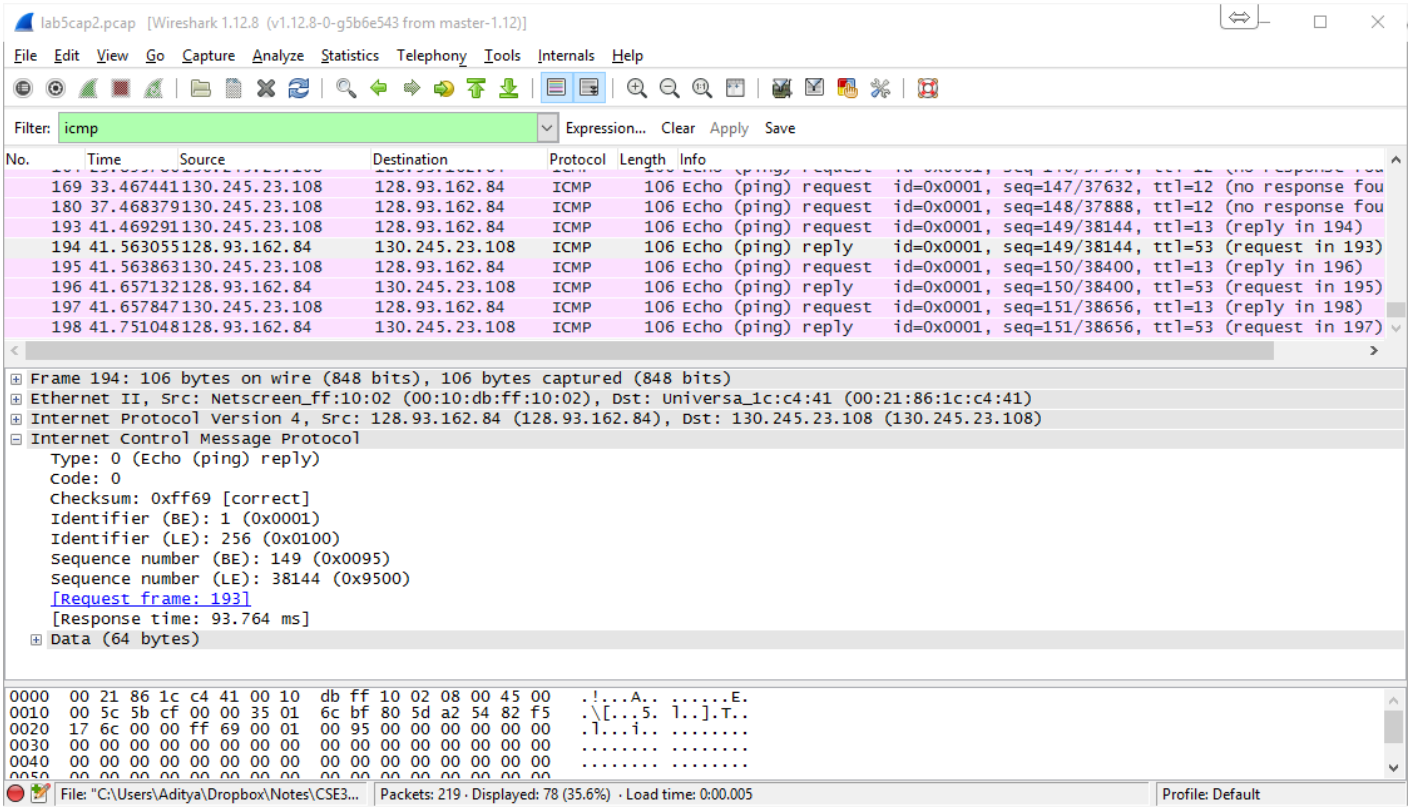
The last 3 ICMP packets received are Ping replies (type 0) instead of TTL Expired (type 11) because the packets have made their way to the destination

10. **Within the tracert measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this link?**

Within the tracert measurements, the link between step 5 to 6 has a significantly longer delay than others.

In figure 4, the link from step 9 to 10 has a delay significantly longer than others. This is the link from NYC to Pastourelle, France





Part 2

1. **Go to http://ping.stonybrook.edu, where is this site? What are IP addresses and the Host Name displayed for your computer?**

   The site is in Stony Brook, NY.

   My IP, as displayed on the website is 130.245.68.25 and my hostname is not resolved

Speed-Test

2013.11.26	IPV4	Help

Server's time	Sat Nov 21 13:26:29 EST 2015
IPv4 Address	130.245.68.25
IPv6 Address	You can NOT reach IPv6 web sites, thus not V6 enabled
Host Name	unable to resolve 130.245.68.25
Name/Address	130.245.68.25
Ping count	1
Trace max hops	30
Type of Trace	UDP
Whois Srv for Trace	whois.ripe.net
Lookup type	A
Lookup server	recursion.stonybrook.edu
Whois server	whois.arin.net
Server For Dig	f.root-servers.net

Ping | Trace | Trace-W-AS | Lookup | Whois | Dig

2. **Use the "Ping" service on http://ping.stonybrook.edu, find the approximate round trip times (RTT) to a university on the east coast, a university on the west coast, a university in Europe, and a university in Asia respectively. What trend can you observe from these RTTs?**

   - East coast: Stony Brook university. Time : 0.257ms

pinging from *ping.stonybrook.edu* to **www.stonybrook.edu**

```
Sat Nov 21 13:31:47 EST 2015
```

```
Running
/bin/ping -c 1 www.stonybrook.edu
```

```
PING stonybrook.edu (129.49.2.176) 56(84) bytes of data.
64 bytes from www.stonybrook.edu (129.49.2.176): icmp_seq=1 ttl=63 time=0.257 ms

--- stonybrook.edu ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.257/0.257/0.257/0.000 ms
```

```
Sat Nov 21 13:31:47 EST 2015
```

   - East coast: UCLA. Time : 0.100ms

pinging from *ping.stonybrook.edu* to **www.ucla.edu**

```
Sat Nov 21 13:38:32 EST 2015
```

```
Running
/bin/ping -c 1 www.ucla.edu
```

```
PING gateway.lb.it.ucla.edu (164.67.228.152) 56(84) bytes of data.
64 bytes from gateway.lb.it.ucla.edu (164.67.228.152): icmp_seq=1 ttl=49 time=100 ms

--- gateway.lb.it.ucla.edu ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 100.878/100.878/100.878/0.000 ms
```

```
Sat Nov 21 13:38:32 EST 2015
```

- East coast: Cambridge University. Time : 0.108ms

pinging from *ping.stonybrook.edu* to **www.cam.ac.uk**

```
Sat Nov 21 14:50:42 EST 2015
```

```
Running
/bin/ping -c 1 www.cam.ac.uk
```

```
PING www.cam.ac.uk (131.111.150.25) 56(84) bytes of data.
64 bytes from primary.admin.cam.ac.uk (131.111.150.25): icmp_seq=1 ttl=50 time=108 ms

--- www.cam.ac.uk ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 108.745/108.745/108.745/0.000 ms
```

```
Sat Nov 21 14:50:42 EST 2015
```

- East coast: National University of Singapore. Time : 0.298ms

pinging from *ping.stonybrook.edu* to **www.nus.edu.sg**

```
Sat Nov 21 14:52:41 EST 2015
```

```
Running
/bin/ping -c 1 www.nus.edu.sg
```

```
PING www.nus.edu.sg (137.132.21.27) 56(84) bytes of data.
64 bytes from ddu.nus.edu.sg (137.132.21.27): icmp_seq=1 ttl=40 time=298 ms

--- www.nus.edu.sg ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 298.979/298.979/298.979/0.000 ms
```

```
Sat Nov 21 14:52:41 EST 2015
```

3. **Use the "Trace" service on http://ping.stonybrook.edu, trace a route to a university in the Netherlands, is there a link whose delay is significantly longer than others? Can you guess the location of the two routers on the end of this link? (2pts)**

   Yes, the link from step 4 to 5 has a delay much larger than the array. The IP at step 4 is located in NY, while the one on step 5 is in UK which is why the delay is long

Traceroute from *ping.stonybrook.edu* to **www.leiden.edu**

```
Sat Nov 21 14:58:52 EST 2015

Running
/usr/sbin/traceroute -m 30 www.leiden.edu

traceroute to www.leiden.edu (132.229.7.196), 30 hops max, 60 byte packets
 1  nocnoc.rtr.stonybrook.edu (129.49.7.1)  2.917 ms  3.072 ms  3.187 ms
 2  cronus-efs-ragg-100.noc.stonybrook.edu (129.49.7.74)  1.143 ms  1.073 ms  1.062 ms
 3  nyc-7600-stonybrook.nysernet.net (199.109.4.73)  3.394 ms  3.374 ms  3.344 ms
 4  199.109.5.26 (199.109.5.26)  29.848 ms  29.835 ms  29.826 ms
 5  internet2-gw.mx1.lon.uk.geant.net (62.40.124.44)  104.434 ms  104.395 ms  104.320 ms
 6  surfnet-bckp-gw.mx1.lon.uk.geant.net (62.40.124.210)  108.869 ms  109.125 ms  109.075 ms
 7  rul-router.customer.surf.net (145.145.20.2)  109.694 ms  109.813 ms  109.631 ms
```

4. **Now trace a university in Australia instead of Holland. What can you find out?**

   Yes, the link from step 10 to 11 has a delay much larger than the array. The IP at step 4 is located in Pacific, while the one is in Australia.

Traceroute from *ping.stonybrook.edu* to **www.uq.edu.au**

```
Sat Nov 21 15:06:40 EST 2015

Running
/usr/sbin/traceroute -m 30 www.uq.edu.au

traceroute to www.uq.edu.au (130.102.131.70), 30 hops max, 60 byte packets
 1  nocnoc.rtr.stonybrook.edu (129.49.7.1)  0.965 ms  1.038 ms  1.208 ms
 2  cronus-efs-ragg-100.noc.stonybrook.edu (129.49.7.74)  1.080 ms  1.033 ms  1.017 ms
 3  nyc-7600-stonybrook.nysernet.net (199.109.4.73)  4.018 ms  4.006 ms  3.963 ms
 4  199.109.7.161 (199.109.7.161)  9.159 ms  9.140 ms  9.345 ms
 5  199.109.7.194 (199.109.7.194)  12.610 ms  12.437 ms  12.395 ms
 6  199.109.11.38 (199.109.11.38)  41.714 ms  41.771 ms  41.732 ms
 7  et-10-0-0.106.rtr.kans.net.internet2.edu (198.71.45.15)  53.536 ms  53.517 ms  53.488 ms
 8  et-4-0-0.110.rtr.salt.net.internet2.edu (198.71.45.19)  72.853 ms  72.467 ms  73.686 ms
 9  et-5-0-0.113.rtr.seat.net.internet2.edu (198.71.45.25)  88.834 ms  88.660 ms  88.643 ms
10  aarnet-2-lo-jmb-706.sttlwa.pacificwave.net (207.231.240.4)  88.737 ms  88.747 ms  88.705 ms
11  et-0-0-1.pe1.a.hnl.aarnet.net.au (202.158.194.109)  140.364 ms  140.231 ms  140.295 ms
12  et-2-0-0.pe2.brwy.nsw.aarnet.net.au (113.197.15.98)  235.348 ms  236.219 ms  236.173 ms
13  ge-5-1-0.bb1.b.bne.aarnet.net.au (202.158.194.68)  248.377 ms  248.168 ms  248.118 ms
14  ge-0-0-0.bb1.a.bne.aarnet.net.au (202.158.194.213)  248.501 ms  248.398 ms  247.889 ms
15  tengigabitethernet2-1.er2.uq.cpe.aarnet.net.au (202.158.209.3)  249.254 ms  249.065 ms  249.239 ms
16  gw2.er2.uq.cpe.aarnet.net.au (113.197.8.34)  249.778 ms  249.726 ms  249.708 ms
17  uq-se1-uq-gw1.router.uq.edu.au (130.102.159.1)  250.861 ms  249.720 ms  250.173 ms
18  talon-uq-se1.router.uq.edu.au (130.102.159.17)  250.046 ms  249.971 ms  250.168 ms
19  a82-2.nat.uq.edu.au (130.102.82.2)  250.069 ms  249.923 ms  249.960 ms
```

Part 3

1. **Go to http://www.slac.stanford.edu/cgi-bin/nph-traceroute.pl?target=ping.stonybrook.edu, where is this site? Why?**

   This site is located in Stamford univesity.

2. **Repeat Question 2, Parts (c) and (d). What observations can you make about the routes taken? E.g., can you guess where intermediate hops are? (3pts)**

   - Leiden univesity

     The link from step 13 to 14 has a much longer delay

     The intermediate stops are in Denver, Washington, Chicago and kansas

```
Executing exec(traceroute -m 30 -q 3 132.229.7.196)
traceroute to 132.229.7.196 (132.229.7.196), 30 hops max, 40 byte packets
 1  134.79.197.131 (134.79.197.131)  0.947 ms  0.631 ms  0.679 ms
 2  rtr-core2-p2p-serv01-02.slac.stanford.edu (134.79.254.61)  0.435 ms  0.445 ms  0.393 ms
 3  rtr-fwcore1-trust-p2p-core1.slac.stanford.edu (134.79.254.134)  0.666 ms  0.800 ms  0.675 ms
 4  rtr-core1-p2p-fwcore1-untrust.slac.stanford.edu (134.79.254.137)  0.805 ms  0.524 ms  0.821 ms
 5  rtr-border1-p2p-core1.slac.stanford.edu (134.79.252.133)  1.088 ms  0.860 ms  0.819 ms
 6  rtr-border2-p2p-border1.slac.stanford.edu (192.68.191.253)  1.444 ms  1.335 ms  1.243 ms
 7  sunncr5-ip-c-slac.slac.stanford.edu (192.68.191.233)  1.857 ms  1.537 ms  1.520 ms
 8  sacrcr5-ip-a-sunncr5.es.net (134.55.40.5)  4.045 ms  4.251 ms  4.205 ms
 9  denvcr5-ip-a-sacrcr5.es.net (134.55.50.202)  25.167 ms  25.097 ms  25.250 ms
10  kanscr5-ip-a-denvcr5.es.net (134.55.49.58)  35.966 ms  35.733 ms  36.156 ms
11  chiccr5-ip-a-kanscr5.es.net (134.55.43.81)  46.705 ms  46.718 ms  46.723 ms
12  washcr5-ip-a-chiccr5.es.net (134.55.36.46)  70.703 ms  63.803 ms  63.754 ms
13  * * londcr5-ip-a-aofacr5.es.net (134.55.39.169)  138.919 ms
14  amstcr5-ip-a-londcr5.es.net (134.55.222.13)  146.158 ms  147.729 ms  146.262 ms
15  et-0-0-0.213.JNR01.Asd001A.surf.net (145.145.166.1)  145.930 ms  145.893 ms  145.844 ms
16  ae0.500.jnr01.asd002a.surf.net (145.145.80.81)  161.240 ms et-0-0-0.213.JNR01.Asd001A.surf.net (145.145.166.1)  145.856 ms  145.811 ms
17  ae0.500.jnr01.asd002a.surf.net (145.145.80.81)  145.625 ms  152.866 ms  222.297 ms
18  rul-router.customer.surf.net (145.145.20.2)  147.013 ms  146.687 ms  146.684 ms
```

   - Universtiy of Queensland

     The link from step 7 to 8 has a much longer delay.

     The intermediate stops are in the Pacific

```
Executing exec(traceroute -m 30 -q 3 130.102.131.70)
traceroute to 130.102.131.70 (130.102.131.70), 30 hops max, 40 byte packets
 1  134.79.197.131 (134.79.197.131)  1.623 ms  1.208 ms  0.674 ms
 2  rtr-core2-p2p-serv01-02.slac.stanford.edu (134.79.254.61)  0.400 ms  0.337 ms  0.392 ms
 3  rtr-fwcore1-trust-p2p-core1.slac.stanford.edu (134.79.254.134)  0.808 ms  0.737 ms  0.679 ms
 4  rtr-core1-p2p-fwcore1-untrust.slac.stanford.edu (134.79.254.137)  0.803 ms  0.559 ms  0.819 ms
 5  * * *
 6  sunncr5-ip-c-slac.slac.stanford.edu (192.68.191.233)  1.882 ms  1.548 ms  1.520 ms
 7  aarnet-2-is-jmb-778.sttlwa.pacificwave.net (207.231.245.4)  20.102 ms  18.063 ms  17.997 ms
 8  et-0-0-1.pe1.a.hnl.aarnet.net.au (202.158.194.109)  69.800 ms  69.890 ms  70.071 ms
 9  et-2-0-0.pe2.brwy.nsw.aarnet.net.au (113.197.15.98)  163.731 ms  163.644 ms  163.842 ms
10  ge-5-1-0.bb1.b.bne.aarnet.net.au (202.158.194.68)  177.609 ms  177.575 ms  177.385 ms
11  ge-0-0-0.bb1.a.bne.aarnet.net.au (202.158.194.213)  177.738 ms  177.504 ms  177.230 ms
12  tengigabitethernet2-1.er2.uq.cpe.aarnet.net.au (202.158.209.3)  178.873 ms  180.669 ms  178.897 ms
13  gw2.er2.uq.cpe.aarnet.net.au (113.197.8.34)  179.056 ms  179.029 ms  179.185 ms
14  uq-se1-uq-gw1.router.uq.edu.au (130.102.159.1)  180.547 ms  179.648 ms  179.721 ms
15  talon-uq-se1.router.uq.edu.au (130.102.159.17)  179.481 ms  179.400 ms  179.529 ms
16  a82-2.nat.uq.edu.au (130.102.82.2)  179.687 ms  179.617 ms  179.963 ms
```