

Part 1:

Pinging from terminal:

```
sweetbunny@sweetbunny-pc:~/Course_work/ec432$ ping -c 10 www.google.com
PING www.google.com (216.58.217.164) 56(84) bytes of data.
64 bytes from iad23s44-in-f164.1e100.net (216.58.217.164): icmp_seq=1 ttl=56 time=16.2 ms
64 bytes from iad23s44-in-f164.1e100.net (216.58.217.164): icmp_seq=2 ttl=56 time=16.8 ms
64 bytes from iad23s44-in-f164.1e100.net (216.58.217.164): icmp_seq=3 ttl=56 time=31.1 ms
64 bytes from iad23s44-in-f164.1e100.net (216.58.217.164): icmp_seq=4 ttl=56 time=16.9 ms
64 bytes from iad23s44-in-f164.1e100.net (216.58.217.164): icmp_seq=5 ttl=56 time=14.9 ms
64 bytes from iad23s44-in-f164.1e100.net (216.58.217.164): icmp_seq=6 ttl=56 time=16.8 ms
64 bytes from iad23s44-in-f164.1e100.net (216.58.217.164): icmp_seq=7 ttl=56 time=18.9 ms
64 bytes from iad23s44-in-f164.1e100.net (216.58.217.164): icmp_seq=8 ttl=56 time=10.9 ms
64 bytes from iad23s44-in-f164.1e100.net (216.58.217.164): icmp_seq=9 ttl=56 time=14.0 ms
64 bytes from iad23s44-in-f164.1e100.net (216.58.217.164): icmp_seq=10 ttl=56 time=13.4 ms

--- www.google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 39ms
rtt min/avg/max/mdev = 10.851/16.979/31.075/5.166 ms
```

Output of first packet captured in wireshark:

No.	Time	Source	Destination	Protocol	Length	Info
172	9.455847069	192.168.1.188	216.58.217.164	ICMP	98	Echo (ping) request id=0x347b, seq=4/1024, ttl=64 (reply in 174)

Frame 172: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: PcsCompu_5a:d2:b4 (08:00:27:5a:d2:b4), Dst: Verizon_cf:89:51 (20:c0:47:cf:89:51)
Internet Protocol Version 4, Src: 192.168.1.188, Dst: 216.58.217.164
Internet Control Message Protocol

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

My host = 192.168.1.188

Destination host = 216.58.217.164

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

Because ICMP (Internet Control Message Protocol) is used to facilitate informations between network-layer devices (from hosts to routers), not application-layer processes.

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?

ICMP type: 8

Code number: 0

Other fields: Checksum (2B), Identifier (2B), Sequence number (2B), Timestamp (8B) and Data (48B).

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?

ICMP type: 0

Code number: 0

Other fields: Checksum (2B), Identifier (2B), Sequence number (2B), Timestamp (8B) and Data (48B).

Part 2:

Tracerouting to www.google.com:

```
sweetbunny@sweetbunny-pc:~/Course_work/ece432s$ traceroute www.google.com
traceroute to www.google.com (216.58.217.68), 30 hops max, 60 byte packets
 1  FIOS_Quantum_Gateway.FIOS-router.home (192.168.1.1)  1.290 ms  1.394 ms  1.693 ms
 2  * * *
 3  B3359.PHLAPA-LCR-22.verizon-gni.net (100.41.6.20)  13.180 ms  B3359.PHLAPA-LCR-21.verizon-gni.net (100.41.6.18)  13.186 ms  B3359.PHLAPA-LCR-22.verizon-gni.net (100.41.6.20)  13.165 ms
 4  * * *
 5  * * *
 6  0.et-8-1-5.GW7.EMR6.ALTER.NET (140.222.233.31)  20.891 ms  18.792 ms  0.et-11-1-5.GW7.EMR6.ALTER.NET (140.222.234.65)  17.852 ms
 7  209.85.149.200 (209.85.149.200)  18.451 ms  9.456 ms  9.443 ms
 8  * * *
 9  108.170.229.254 (108.170.229.254)  17.589 ms  216.239.62.20 (216.239.62.20)  9.888 ms  108.170.226.198 (108.170.226.198)  11.191 ms
10  108.170.248.20 (108.170.248.20)  9.075 ms  108.170.248.84 (108.170.248.84)  11.588 ms  108.170.248.2 (108.170.248.2)  13.390 ms
11  209.85.254.239 (209.85.254.239)  7.598 ms  209.85.254.241 (209.85.254.241)  10.805 ms  8.125 ms
12  108.177.3.53 (108.177.3.53)  23.002 ms  22.351 ms  108.170.236.243 (108.170.236.243)  13.326 ms
13  216.239.48.100 (216.239.48.100)  13.068 ms  216.239.47.126 (216.239.47.126)  11.251 ms  216.239.49.196 (216.239.49.196)  19.469 ms
14  108.170.246.65 (108.170.246.65)  15.328 ms  14.596 ms  18.815 ms
15  216.239.51.37 (216.239.51.37)  9.604 ms  21.883 ms  21.717 ms
16  1ad2341-in-f4.1e100.net (216.58.217.68)  9.087 ms  19.334 ms  16.266 ms
```

Wireshark's packet sniffing:

The image shows the Wireshark network protocol analyzer interface. The top pane displays a list of captured packets on the 'eth0' interface. The bottom pane shows the details of the selected packet (No. 26), which is an ICMP error message (Type 11, Code 0) from 192.168.1.1 to 192.168.1.188. The packet length is 102 bytes. The details pane shows the following fields:

- Internet Control Message Protocol
- Type: 11 (Time-to-live exceeded)
- Code: 0 (Time to live exceeded in transit)
- Checksum: 0x691d [correct]
- [Checksum Status: Good]
- Internet Protocol Version 4, Src: 192.168.1.188, Dst: 216.58.217.68
- User Datagram Protocol, Src Port: 34625, Dst Port: 33434
- Data (32 bytes)

ICMP error message

```
No.    Time    Source        Destination    Protocol Length Info
 26 0.630121280 192.168.1.1    192.168.1.188  ICMP      102    Time-to-live exceeded (Time to live exceeded
in transit)
Frame 26: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
Ethernet II, Src: Verizon_cf:89:51 (28:c0:47:cf:89:51), Dst: PcsCompu_5a:d2:b4 (08:00:27:5a:d2:b4)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.188
Internet Control Message Protocol
  Type: 11 (Time-to-live exceeded)
  Code: 0 (Time to live exceeded in transit)
  Checksum: 0x691d [correct]
  [Checksum Status: Good]
  Internet Protocol Version 4, Src: 192.168.1.188, Dst: 216.58.217.68
  User Datagram Protocol, Src Port: 34625, Dst Port: 33434
  Data (32 bytes)
```

UDP probing message

```
No.      Time            Source                Destination           Protocol Length Info
 10 0.628837801    192.168.1.188        216.58.217.68        UDP              74      34625 → 33434 Len=32
Frame 10: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: PcsCompu_5a:d2:b4 (08:00:27:5a:d2:b4), Dst: Verizon_cf:89:51 (20:c0:47:cf:89:51)
Internet Protocol Version 4, Src: 192.168.1.188, Dst: 216.58.217.68
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0xd3b8 (54200)
Flags: 0x0000
Time to live: 1
Protocol: UDP (17)
Header checksum: 0x7215 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.188
Destination: 216.58.217.68
User Datagram Protocol, Src Port: 34625, Dst Port: 33434
Data (32 bytes)
```

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

My host = 192.168.1.188

Destination host 1 = 216.58.217.68

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?

It's 17

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 ICMP echo packet has the same fields as the ping 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 is different. It has different type (11 instead of 8) and fields such as checksum, identifier, sequence number and timestamp don't exist anymore. Also, it has both the IP header and the first 8B of the original ICMP packet from which the error is for.

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 packets have type 0 instead of 11. 11 means that they are expired. However, 0 means that the datagrams have arrived at the destination host before TTL expires.

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 measurements, the link from New York to Denver and from Denver to California has more delays than others.

In figure 4 from the lab, the link is from New York, USA to Pastourelle, France