CSCI 4760 Programming Assignment
Spring 2018
Due 04/17/2018
Traceroute Analysis

In this programming assignment, you will write a program that takes in input a textual tcpdump trace of traffic generated by Traceroute. You specify each router address on the path to the destination and also the time taken to send and receive data to each router on the path by analyzing ICMP messages.

Please submit the source code, your tcpdump file and your output as a zip file on elc to the Drop Box.

Project Description:
you can generate your tcpdump and run traceroute by running two commands on two terminals. You write the tcpdump messages in a text file. In Windows, you need to install Windump and use tracert.
Trace route command will start to send packets with TTL=1 three times to first router. You need to find id of message and find the ICMP respond for that packet. Subtract the time between these messages and also IP address of the router.

As an example, consider the two packet logs reported below:

1296181912.313218 IP (tos 0x0, ttl 1, id 42733, offset 0, flags [none], proto TCP (6), length 60)
    128.192.76.178.53560 > 137.138.144.168.80: Flags [SEW], cksum 0x6cb7 (correct), seq 4193307588, win 5840, options [mss 1460,sackOK,TS val 3644222371 ecr 0,nop,wscale 2], length 0
1296181912.313237 IP (tos 0x0, ttl 1, id 42734, offset 0, flags [none], proto TCP (6), length 60)
    128.192.76.178.39026 > 137.138.144.168.80: Flags [SEW], cksum 0x1d7e (correct), seq 4169749803, win 5840, options [mss 1460,sackOK,TS val 3644222371 ecr 0,nop,wscale 2], length 0
1296181912.313248 IP (tos 0x0, ttl 1, id 42735, offset 0, flags [none], proto TCP (6), length 60)
    128.192.76.178.43882 > 137.138.144.168.80: Flags [SEW], cksum 0xd512 (correct), seq 3884555166, win 5840, options [mss 1460,sackOK,TS val 3644222371 ecr 0,nop,wscale 2], length 0

1296181912.313738 IP (tos 0xc0, ttl 255, id 55042, offset 0, flags [none], proto ICMP (1), length 56)

    128.192.76.129 > 128.192.76.178: **ICMP time exceeded** in-transit, length 36
        IP (tos 0x0, ttl 1, id 42733, offset 0, flags [none], proto TCP (6), length 60)

1296181912.313875 IP (tos 0xc0, ttl 255, id 55043, offset 0, flags [none], proto ICMP (1), length 56)

    128.192.76.129 > 128.192.76.178: **ICMP time exceeded** in-transit, length 36
        IP (tos 0x0, ttl 1, **id 42734**, offset 0, flags [none], proto TCP (6), length 60)

1296181912.314030 IP (tos 0xc0, ttl 255, id 55044, offset 0, flags [none], proto ICMP (1), length 56)

    128.192.76.129 > 128.192.76.178: **ICMP time exceeded** in-transit, length 36
        IP (tos 0x0, ttl 1, **id 42735**, offset 0, flags [none], proto TCP (6), length 60)

as we can see from the highlighted fields, source transmits three packets with TTL=1 to find the first router IP address. Each packet has an id number. From the packets above, the output should be:

TTL 1
128.192.76.129
0.52 ms
0.638 ms
0.782 ms

where *128.192.76.129* is the IP addresses of the router that generated the ICMP response, and *0.52 ms* is computed as (**1296181912.313738** - **1296181912.313218**) * 1000.

You need to continue to computer these information for all the routers in the path.