## COMP 3203 Wireshark 9

Name: Nirmith Victor D'Almeida

Number: 101160124

- 1. The IP address of host is 192.168.1.101. IP address of the source is 143.89.14.34.
- 2. Since they are designed to communicate network layer information between hosts and routers and not between application layer processes.
- The ICMP type number is 8 and code is 0
   The other fields present are Checksum, Identifier, Sequence Number and Data fields.
   They are each 2 bytes.

```
Time
                                      Destination
                                                        Protocol Length Info
     3 0.001656
                    192.168.1.101
                                      143.89.14.34 ICMP 74 Echo (ping) re
     4 0.415098
                    143.89.14.34
                                      192.168.1.101
                                                       ICMP
                                                                74 Echo (ping) re
Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (0
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 143.89.14.34
V Internet Control Message Protocol
   Type: 8 (Echo (ping) request)
   Code: 0
   Checksum: 0xe45a [correct]
   [Checksum Status: Good]
   Identifier (BE): 512 (0x0200)
   Identifier (LE): 2 (0x0002)
   Sequence Number (BE): 26369 (0x6701)
   Sequence Number (LE): 359 (0x0167)
    [Response frame: 4]
  v Data (32 bytes)
```

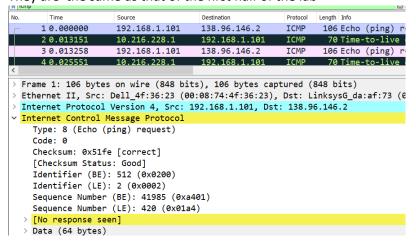
4. Type is 0 and code is 0.

It contains checksum, Identifier, Sequence number and Data.

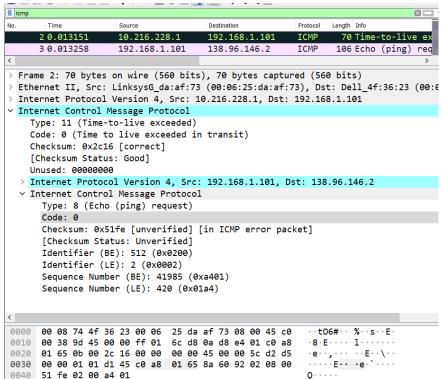
The checksum, sequence number and identifier fields are 2 bytes each respectively.

5. IP Address of the host is 192.168.1.101 Target destination is 138.96.146.2

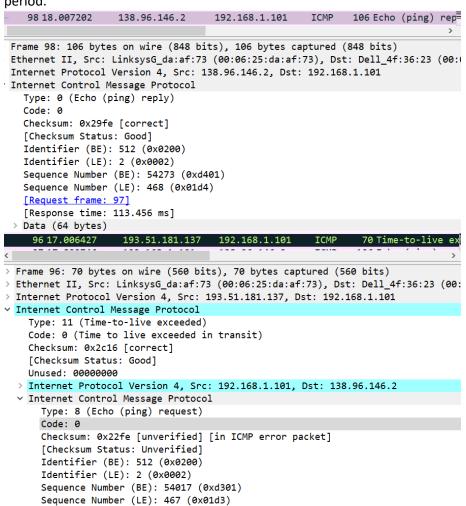
- 6. Instead of 01 it would be switched to 0 X 11.
- 7. They are the same as that of the first half of the lab



8. They include the IP header as well.



9. Their Message type is 0 rather than 11 from the TTL expired. the main reason is because they made it all the way to the destination within the Time to live period.



10. There is a significant delay between step 9 and 10 as seen in the ss of figure 4 Whereas in my ss (the black one) we can see it from step 11 and 12 For figure 4 the link is New York City or nyc open transit and Pastourelle opentransit

```
C:\Users\nirmi>tracert www.inria.fr
Tracing route to inria.fr [128.93.162.83]
over a maximum of 30 hops:
              3 ms
                              3 ms
                                               3 ms mynetwork [192.168.2.1]
   2
              9 ms
                             10 ms
                                             13 ms 10.11.3.89
                                                           Request timed out.
             10 ms
                                              10 ms dis33-ottawa23_ae3.net.bell.ca [64.230.52.63]
                             10 ms
                                                           Request timed out.
                                                           Request timed out.
            27 ms
                             28 ms
                                             26 ms cr01-toroon2147w-bundle-ether9.net.bell.ca [142.124.127.118]
                                                           Request timed out.
                                             30 ms tcore3-chicagocp-bundle-ether15.net.bell.ca [142.124.127.96]
            28 ms
                             38 ms
                                             27 ms bx10-chicagodt_ae0.net.bell.ca [64.230.78.173]
26 ms bx10-chicagodt_et-8/1/2_ae8.net.bell.ca [184.150.181.36]
            27 ms
                             30 ms
            65 ms
                             28 ms
                                           119 ms et-3-3-0.cr2-par7.ip4.gtt.net [213.200.119.214]
116 ms renater-gw-ix1.gtt.net [77.67.123.206]
           119 ms
                           121 ms
           118 ms
                           115 ms
                                          118 ms tel-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
119 ms inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr [193.51.184.177]
           116 ms
                           117 ms
          119 ms
                           119 ms
                                           118 ms unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
                           118 ms
  16
          121 ms
                                           120 ms prod-inriafr-cms.inria.fr [128.93.162.83]
           119 ms
                           120 ms
Trace complete.
Command Prompt
                                                                                                                                                                                     _ | D | X
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>tracert www.inria.fr
Tracing route to www.inria.fr [138.96.146.2]
over a maximum of 30 hops:
                                                                 10.216.228.1
24.218.0.153
bar01-p4-0.wsfdhei.ma.attbb.net [24.128.190.197]
bar02-p6-0.ndhmhei.ma.attbb.net [24.128.0.101]
12.125.47.49
12.123.40.218
tbr2-c11.n54ny.ip.att.net [12.122.10.22]
ggr2-p3120.n54ny.ip.att.net [12.123.3.189]
att-gv.nyc.opentransit.net [192.205.32.138]
P4-0.PASCRI.Pastourelle.opentransit.net [193.251.241.133]
P9-0.AUCRI.Aubervilliers.opentransit.net [193.251.243.29]
P6-0.BAGCRI.Bagnolet.opentransit.net [193.251.241.93]
ggrenoble-post-0.cssi.renater.fr [193.51.179.238]
nice-pos2-0.cssi.renater.fr [193.51.179.238]
inria-nice.cssi.renater.fr [193.51.181.37]
www.inria.fr [138.96.146.2]
            13 ms
21 ms
12 ms
16 ms
15 ms
17 ms
22 ms
23 ms
26 ms
98 ms
98 ms
104 ms
114 ms
114 ms
1129 ms
                                                 13 ms
13 ms
13 ms
15 ms
15 ms
17 ms
22 ms
23 ms
25 ms
98 ms
108 ms
1103 ms
1114 ms
1114 ms
```

Trace complete.
C:\WINDOWS\SYSTEM32>\_