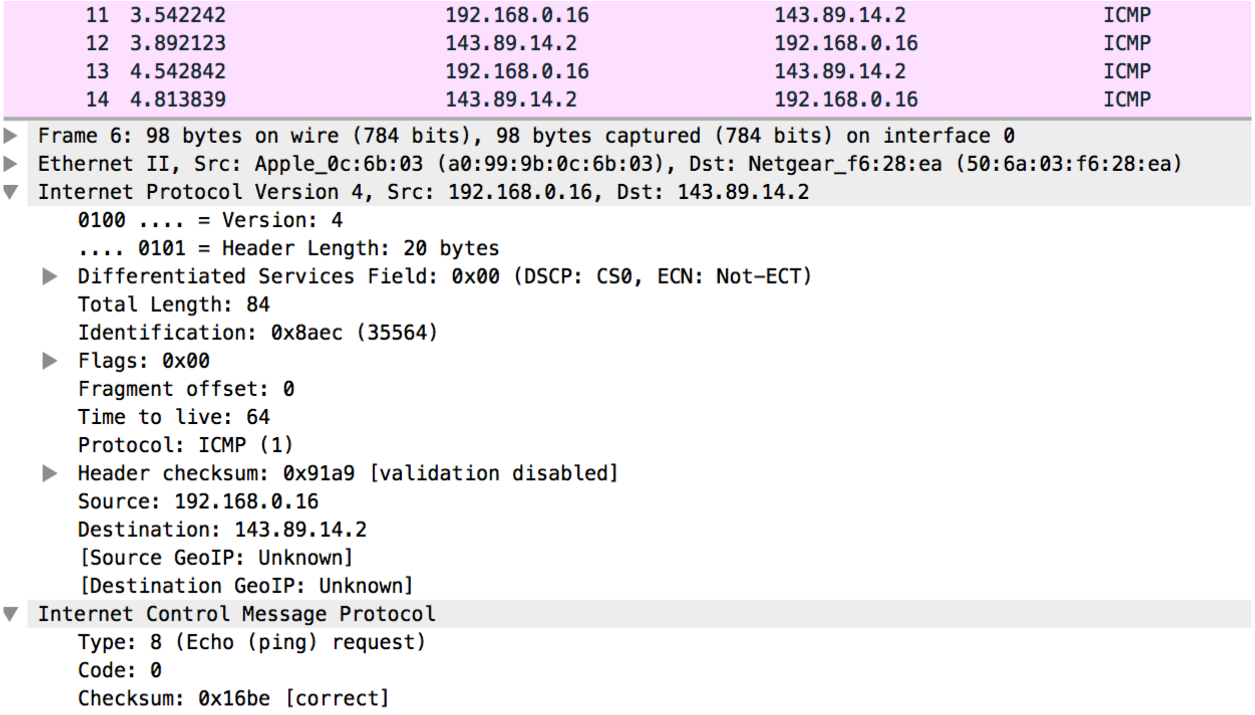
Course: Computer Networks(ECE/CSC 570)
Instructor: Mihail L. Sichitiu
Description: Spring 2016, Wireshark Assignment 3 Solutions.
Student Name: Himangshu Ranjan Borah
Student ID: 200105222
Unity ID: hborah

Answer No 1:



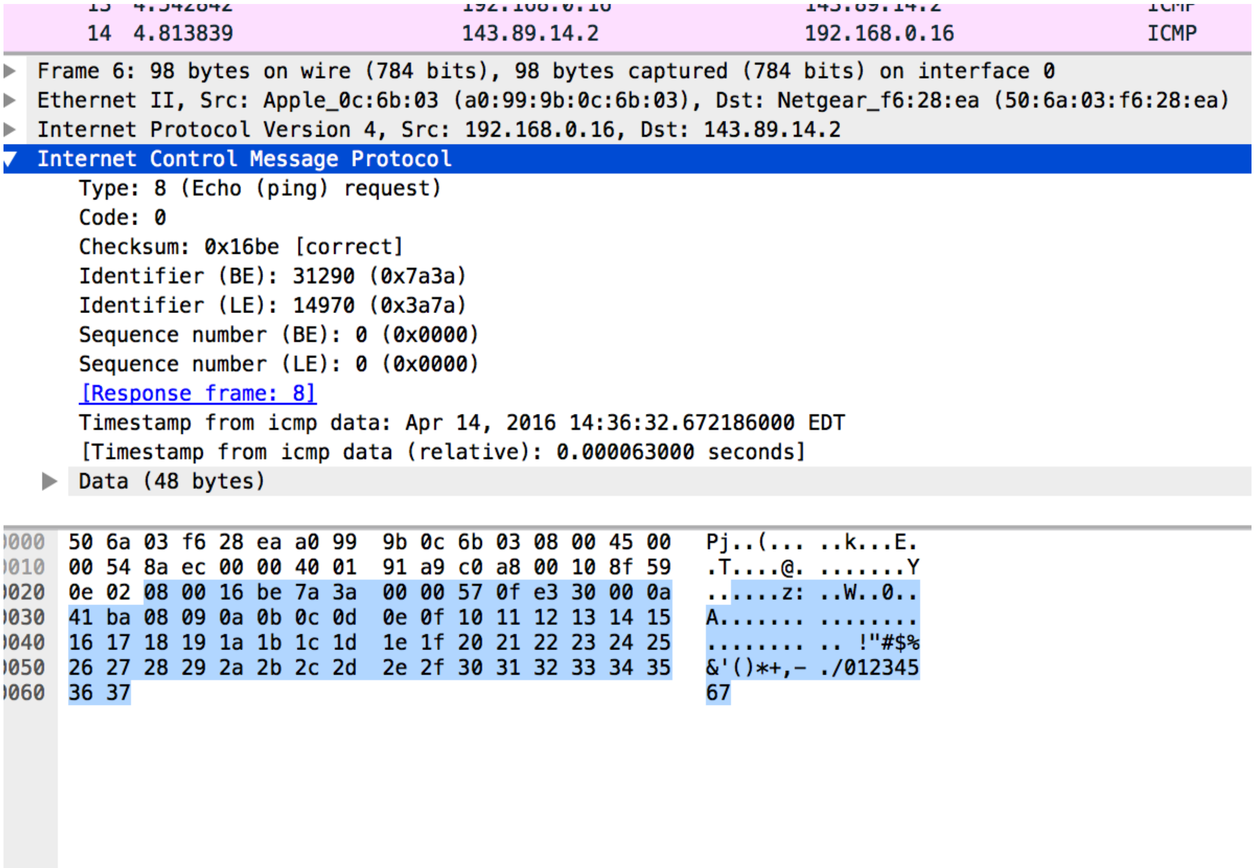
```
     11  3.542242                192.168.0.16            143.89.14.2             ICMP
     12  3.892123                143.89.14.2             192.168.0.16            ICMP
     13  4.542842                192.168.0.16            143.89.14.2             ICMP
     14  4.813839                143.89.14.2             192.168.0.16            ICMP
▶ Frame 6: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▶ Ethernet II, Src: Apple_0c:6b:03 (a0:99:9b:0c:6b:03), Dst: Netgear_f6:28:ea (50:6a:03:f6:28:ea)
▼ Internet Protocol Version 4, Src: 192.168.0.16, Dst: 143.89.14.2
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes
   ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 84
     Identification: 0x8aec (35564)
   ▶ Flags: 0x00
     Fragment offset: 0
     Time to live: 64
     Protocol: ICMP (1)
   ▶ Header checksum: 0x91a9 [validation disabled]
     Source: 192.168.0.16
     Destination: 143.89.14.2
     [Source GeoIP: Unknown]
     [Destination GeoIP: Unknown]
▼ Internet Control Message Protocol
     Type: 8 (Echo (ping) request)
     Code: 0
     Checksum: 0x16be [correct]
```

The IP address of my host : **192.168.0.16**
The IP address of the destination host : **143.89.14.2**

Answer No. 2:

The major usage of the ICMP packages was to deliver control messages between network layer and are purely interpreted by the network layer. It was not designed to handle data traffic to application layers. Port no. is something which is used to direct the payload to the application layer protocols. Since we don't need that in ICMP, so we don't have any port number in ICMP header. However, that have a "type" and a "code" combination using which the network layer determines what kind of an packet it is.

Answer 3:



```
 13  4.542842      192.168.0.16      143.89.14.2      ICMP
 14  4.813839      143.89.14.2       192.168.0.16     ICMP
▶ Frame 6: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▶ Ethernet II, Src: Apple_0c:6b:03 (a0:99:9b:0c:6b:03), Dst: Netgear_f6:28:ea (50:6a:03:f6:28:ea)
▶ Internet Protocol Version 4, Src: 192.168.0.16, Dst: 143.89.14.2
▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x16be [correct]
    Identifier (BE): 31290 (0x7a3a)
    Identifier (LE): 14970 (0x3a7a)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    [Response frame: 8]
    Timestamp from icmp data: Apr 14, 2016 14:36:32.672186000 EDT
    [Timestamp from icmp data (relative): 0.000063000 seconds]
  ▶ Data (48 bytes)

0000  50 6a 03 f6 28 ea a0 99  9b 0c 6b 03 08 00 45 00   Pj..(... ..k...E.
0010  00 54 8a ec 00 00 40 01  91 a9 c0 a8 00 10 8f 59   .T....@. .......Y
0020  0e 02 08 00 16 be 7a 3a  00 00 57 0f e3 30 00 0a   ......z: ..W..0..
0030  41 ba 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   A....... ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

ICMP Type: 8(Echo ping request)
ICMP Code: 0

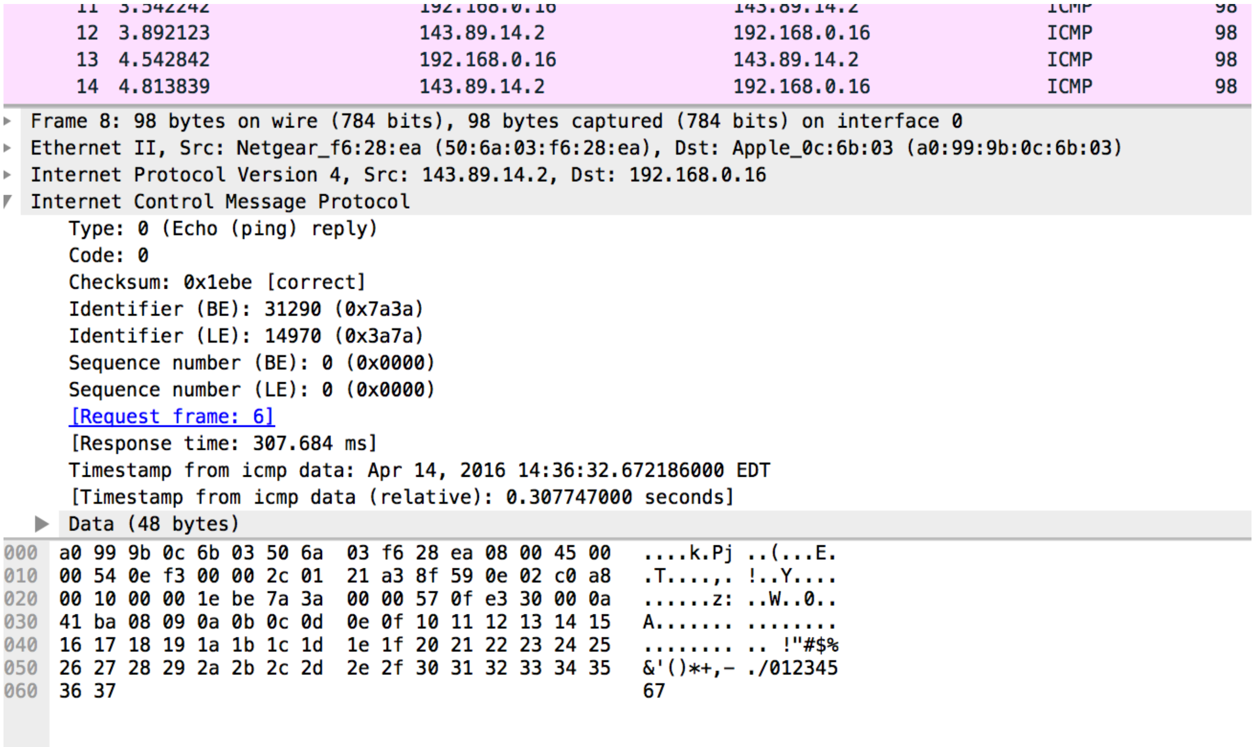
The field in ICMP packet:

1. Checksum
2. Identifier
3. Sequence No.
4. Data

Sizes:

Checksum, Sequence no and identifier has **2 bytes** each.

Answer 4:



```
   11  3.542242         192.168.0.16        143.89.14.2         ICMP        98
   12  3.892123         143.89.14.2         192.168.0.16        ICMP        98
   13  4.542842         192.168.0.16        143.89.14.2         ICMP        98
   14  4.813839         143.89.14.2         192.168.0.16        ICMP        98
▸ Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Netgear_f6:28:ea (50:6a:03:f6:28:ea), Dst: Apple_0c:6b:03 (a0:99:9b:0c:6b:03)
▸ Internet Protocol Version 4, Src: 143.89.14.2, Dst: 192.168.0.16
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x1ebe [correct]
    Identifier (BE): 31290 (0x7a3a)
    Identifier (LE): 14970 (0x3a7a)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    [Request frame: 6]
    [Response time: 307.684 ms]
    Timestamp from icmp data: Apr 14, 2016 14:36:32.672186000 EDT
    [Timestamp from icmp data (relative): 0.307747000 seconds]
  ▸ Data (48 bytes)
000  a0 99 9b 0c 6b 03 50 6a  03 f6 28 ea 08 00 45 00   ....k.Pj ..(...E.
010  00 54 0e f3 00 00 2c 01  21 a3 8f 59 0e 02 c0 a8   .T....,. !..Y....
020  00 10 00 00 1e be 7a 3a  00 00 57 0f e3 30 00 0a   ......z: ..W..0..
030  41 ba 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   A....... ........
040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
060  36 37                                              67
```

ICMP Type: 0(Echo ping reply)
ICMP Code: 0

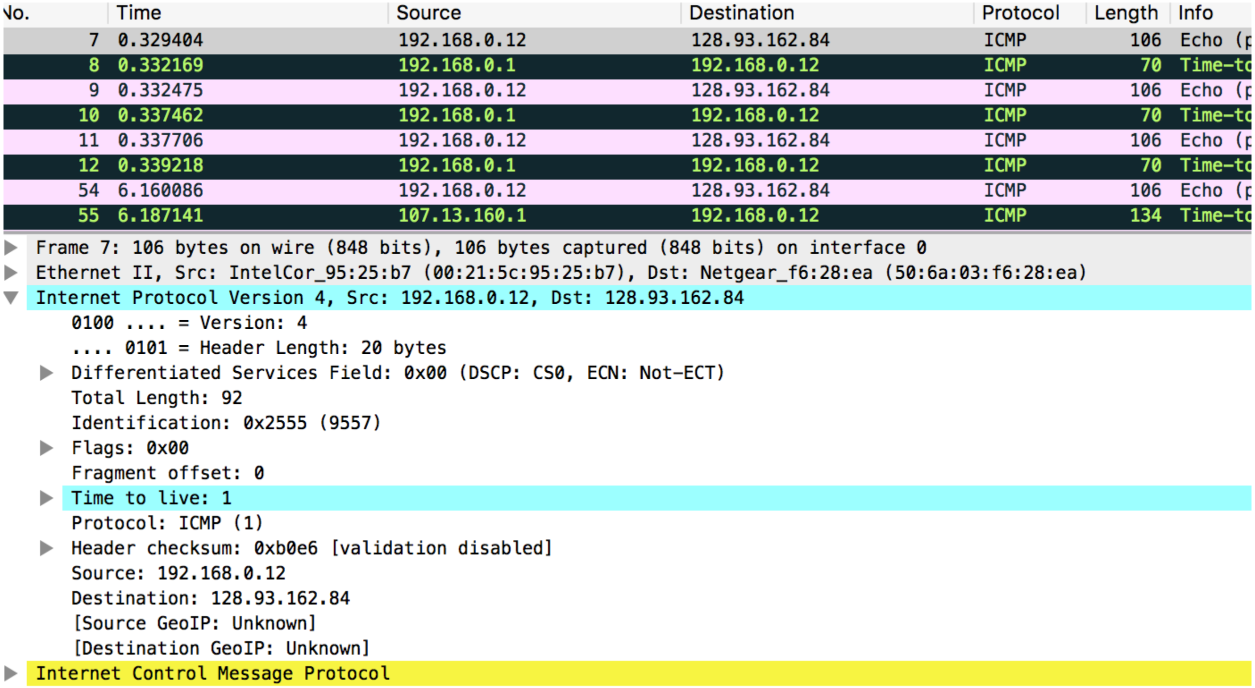
The field in ICMP packet:

1. Checksum
2. Identifier
3. Sequence No.
4. Data

Sizes:

Checksum, Sequence no and identifier has 2 bytes each.

Answer 5:



```
No.   Time       Source          Destination     Protocol  Length  Info
    7 0.329404   192.168.0.12    128.93.162.84   ICMP        106   Echo (p
    8 0.332169   192.168.0.1     192.168.0.12    ICMP         70   Time-to
    9 0.332475   192.168.0.12    128.93.162.84   ICMP        106   Echo (p
   10 0.337462   192.168.0.1     192.168.0.12    ICMP         70   Time-to
   11 0.337706   192.168.0.12    128.93.162.84   ICMP        106   Echo (p
   12 0.339218   192.168.0.1     192.168.0.12    ICMP         70   Time-to
   54 6.160086   192.168.0.12    128.93.162.84   ICMP        106   Echo (p
   55 6.187141   107.13.160.1    192.168.0.12    ICMP        134   Time-to
```

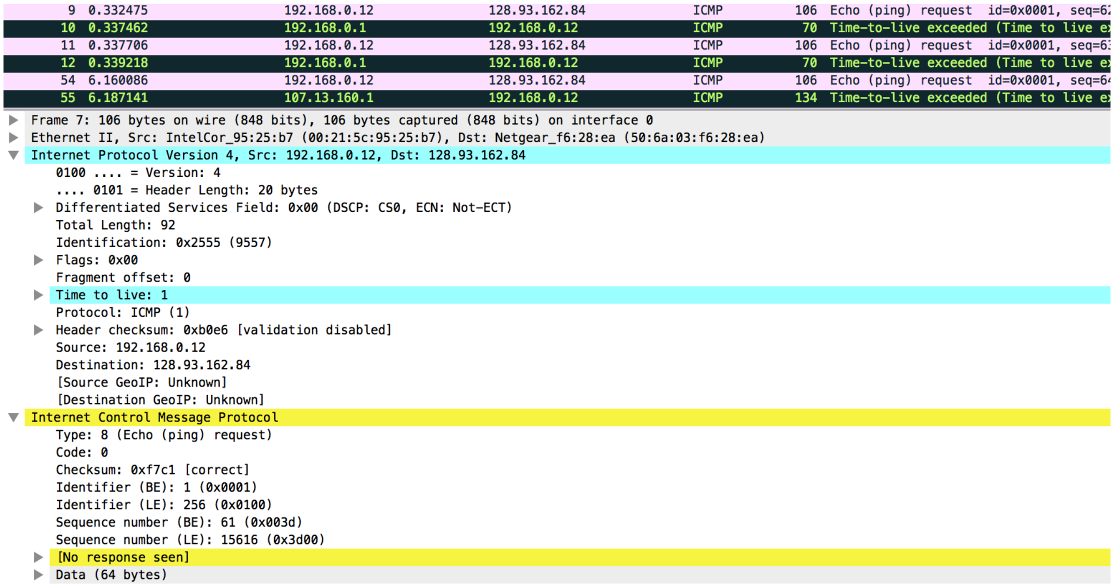
```
▶ Frame 7: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
▶ Ethernet II, Src: IntelCor_95:25:b7 (00:21:5c:95:25:b7), Dst: Netgear_f6:28:ea (50:6a:03:f6:28:ea)
▼ Internet Protocol Version 4, Src: 192.168.0.12, Dst: 128.93.162.84
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes
   ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 92
     Identification: 0x2555 (9557)
   ▶ Flags: 0x00
     Fragment offset: 0
   ▶ Time to live: 1
     Protocol: ICMP (1)
   ▶ Header checksum: 0xb0e6 [validation disabled]
     Source: 192.168.0.12
     Destination: 128.93.162.84
     [Source GeoIP: Unknown]
     [Destination GeoIP: Unknown]
▶ Internet Control Message Protocol
```

Host IP Address: 192.168.0.12
Destination IP Adress: 128.93.162.84

Answer 6:

If UDP packets were used instead of ICMP packets, then the upper layer protocol field value would not be 01 anymore. Rather it would be **17 which is the identifier fir UDP** protocol. Upper layer protocol field is used to let the receiving node know according to which protocol the unwrapping must happen in transport layer.

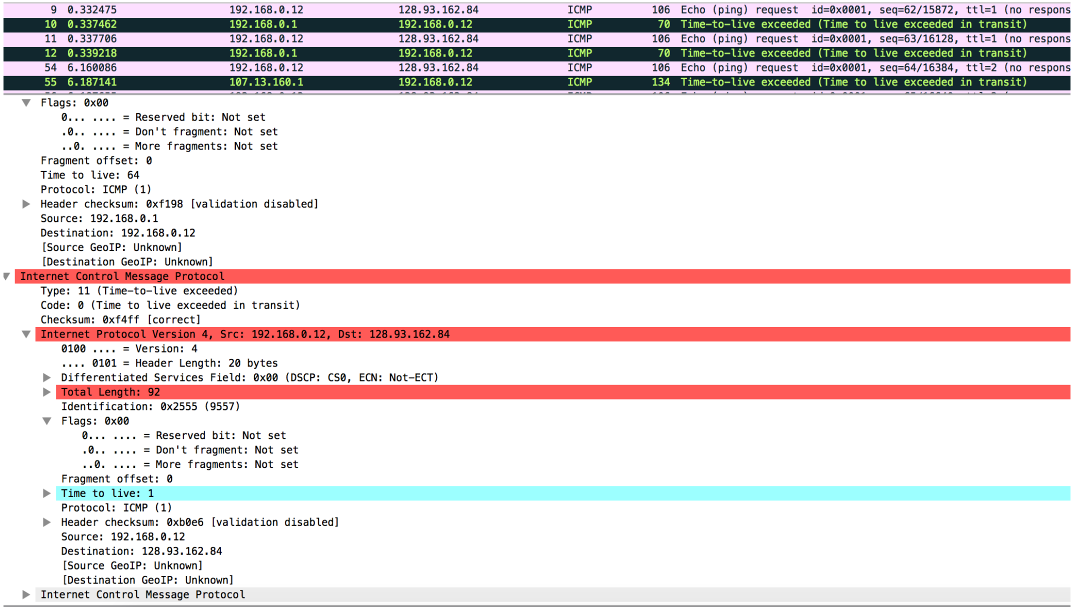
Answer 7:



```
   9  0.332475          192.168.0.12        128.93.162.84       ICMP       106  Echo (ping) request  id=0x0001, seq=62
  10  0.337462          192.168.0.1         192.168.0.12        ICMP        70  Time-to-live exceeded (Time to live ex
  11  0.337706          192.168.0.12        128.93.162.84       ICMP       106  Echo (ping) request  id=0x0001, seq=63
  12  0.339218          192.168.0.1         192.168.0.12        ICMP        70  Time-to-live exceeded (Time to live ex
  54  6.160086          192.168.0.12        128.93.162.84       ICMP       106  Echo (ping) request  id=0x0001, seq=64
  55  6.187141          107.13.160.1        192.168.0.12        ICMP       134  Time-to-live exceeded (Time to live ex
▶ Frame 7: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
▶ Ethernet II, Src: IntelCor_95:25:b7 (00:21:5c:95:25:b7), Dst: Netgear_f6:28:ea (50:6a:03:f6:28:ea)
▼ Internet Protocol Version 4, Src: 192.168.0.12, Dst: 128.93.162.84
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x2555 (9557)
  ▶ Flags: 0x00
    Fragment offset: 0
  ▶ Time to live: 1
    Protocol: ICMP (1)
  ▶ Header checksum: 0xb0e6 [validation disabled]
    Source: 192.168.0.12
    Destination: 128.93.162.84
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7c1 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 61 (0x003d)
    Sequence number (LE): 15616 (0x3d00)
  ▶ [No response seen]
  ▶ Data (64 bytes)
```

Analyzing both the packets, we see that the ICMP request packets are almost similar in both the cases, **except the TTL field** which is constant in case of ping and in case of trace route, it keep increasing by unity which is how trace route works.

Answer 8:

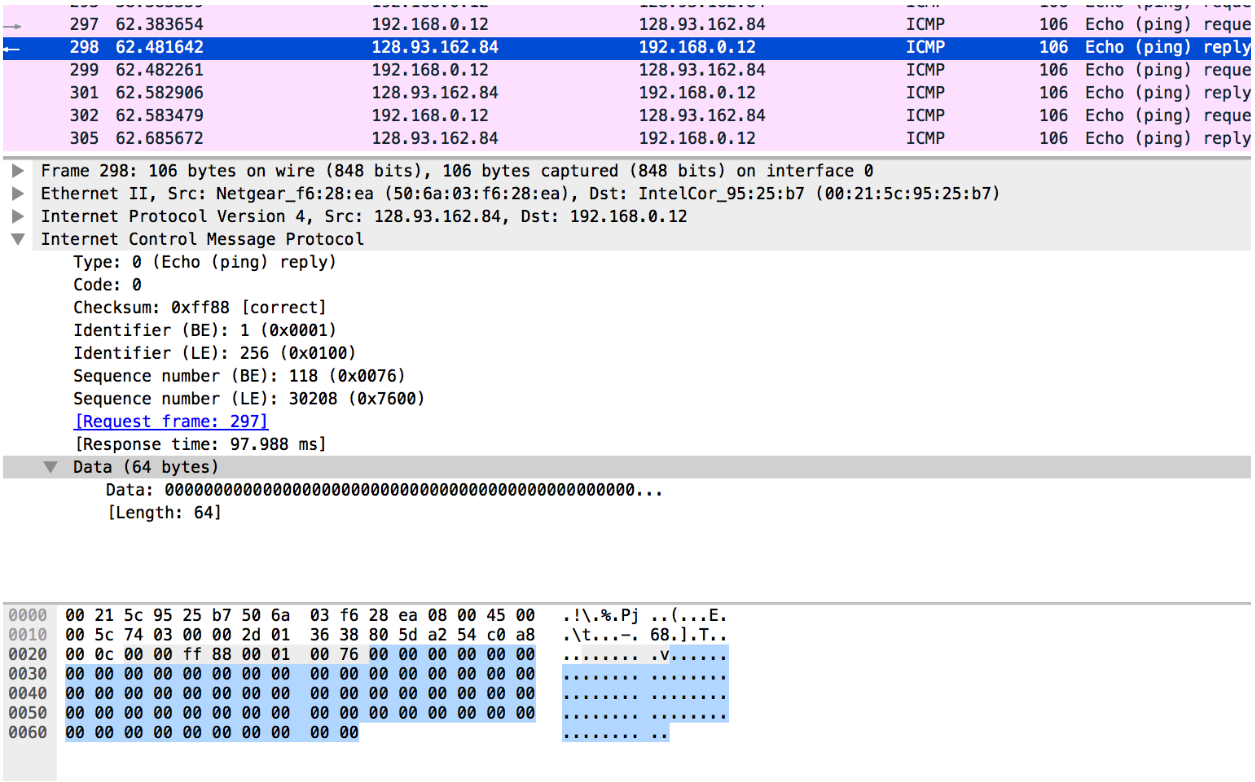


```
   9  0.332475          192.168.0.12        128.93.162.84       ICMP       106  Echo (ping) request  id=0x0001, seq=62/15872, ttl=1 (no respons
  10  0.337462          192.168.0.1         192.168.0.12        ICMP        70  Time-to-live exceeded (Time to live exceeded in transit)
  11  0.337706          192.168.0.12        128.93.162.84       ICMP       106  Echo (ping) request  id=0x0001, seq=63/16128, ttl=1 (no respons
  12  0.339218          192.168.0.1         192.168.0.12        ICMP        70  Time-to-live exceeded (Time to live exceeded in transit)
  54  6.160086          192.168.0.12        128.93.162.84       ICMP       106  Echo (ping) request  id=0x0001, seq=64/16384, ttl=2 (no respons
  55  6.187141          107.13.160.1        192.168.0.12        ICMP       134  Time-to-live exceeded (Time to live exceeded in transit)
  ▼ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
  ▶ Header checksum: 0xf198 [validation disabled]
    Source: 192.168.0.1
    Destination: 192.168.0.12
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▼ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
  ▼ Internet Protocol Version 4, Src: 192.168.0.12, Dst: 128.93.162.84
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes
    ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    ▶ Total Length: 92
      Identification: 0x2555 (9557)
    ▼ Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
      Fragment offset: 0
    ▶ Time to live: 1
      Protocol: ICMP (1)
    ▶ Header checksum: 0xb0e6 [validation disabled]
      Source: 192.168.0.12
      Destination: 128.93.162.84
      [Source GeoIP: Unknown]
      [Destination GeoIP: Unknown]
  ▶ Internet Control Message Protocol
```

From

the above snapshot, we see that the ICMP error reply is **not same** as the echo request. It has more fields in header which includes the **IP header and the ICMP header** of the original packet for which the error has been generated.

Answer No. 9:



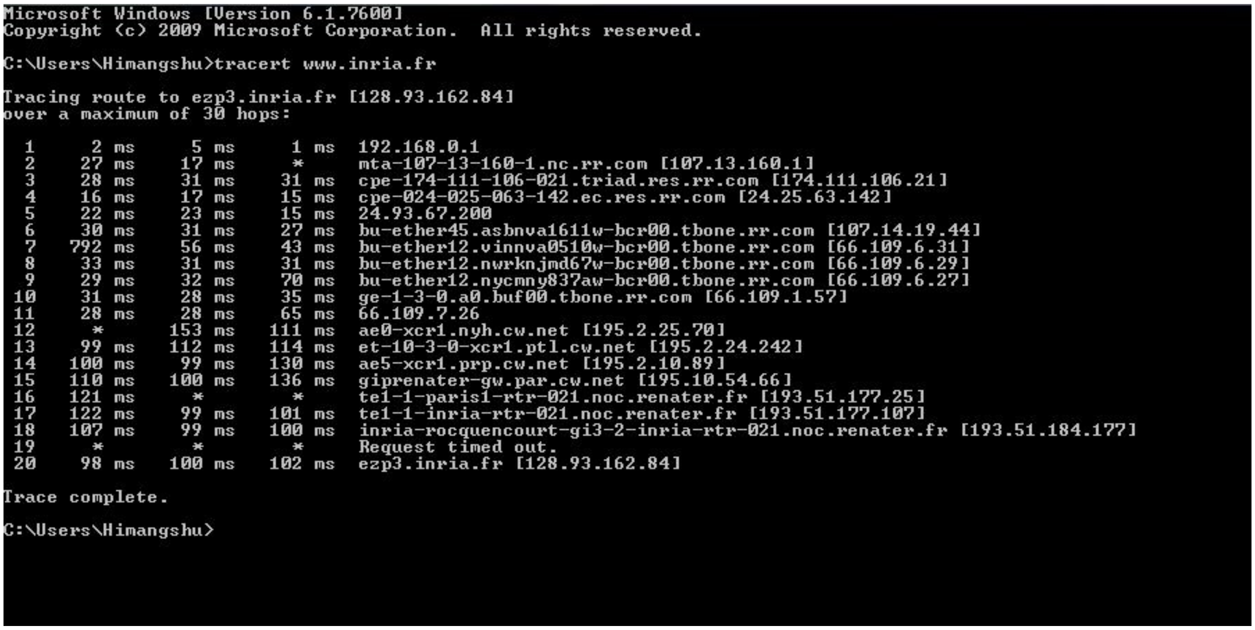
```
297  62.383654    192.168.0.12     128.93.162.84    ICMP    106  Echo (ping) reque
298  62.481642    128.93.162.84    192.168.0.12     ICMP    106  Echo (ping) reply
299  62.482261    192.168.0.12     128.93.162.84    ICMP    106  Echo (ping) reque
301  62.582906    128.93.162.84    192.168.0.12     ICMP    106  Echo (ping) reply
302  62.583479    192.168.0.12     128.93.162.84    ICMP    106  Echo (ping) reque
305  62.685672    128.93.162.84    192.168.0.12     ICMP    106  Echo (ping) reply
```

```
▶ Frame 298: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
▶ Ethernet II, Src: Netgear_f6:28:ea (50:6a:03:f6:28:ea), Dst: IntelCor_95:25:b7 (00:21:5c:95:25:b7)
▶ Internet Protocol Version 4, Src: 128.93.162.84, Dst: 192.168.0.12
▼ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xff88 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 118 (0x0076)
    Sequence number (LE): 30208 (0x7600)
    [Request frame: 297]
    [Response time: 97.988 ms]
  ▼ Data (64 bytes)
      Data: 000000000000000000000000000000000000000000000000...
      [Length: 64]
```

```
0000  00 21 5c 95 25 b7 50 6a  03 f6 28 ea 08 00 45 00   .!\.%.Pj ..(...E.
0010  00 5c 74 03 00 00 2d 01  36 38 80 5d a2 54 c0 a8   .\t...-. 68.].T..
0020  00 0c 00 00 ff 88 00 01  00 76 00 00 00 00 00 00   ........ .v......
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00                     ........ ..
```

The last three packet are normal **Echo Ping Reply** packets and not **TTL Exceeded error** messages. This happens because the last hop is the destination system itself and hence the packets arrive there before the TTL gets expired. No it becomes the normal flow and the sender can know that the trace route is complete.

Answer 10:



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Himangshu>tracert www.inria.fr

Tracing route to ezp3.inria.fr [128.93.162.84]
over a maximum of 30 hops:

  1     2 ms     5 ms     1 ms  192.168.0.1
  2    27 ms    17 ms     *     mta-107-13-160-1.nc.rr.com [107.13.160.1]
  3    28 ms    31 ms    31 ms  cpe-174-111-106-021.triad.res.rr.com [174.111.106.21]
  4    16 ms    17 ms    15 ms  cpe-024-025-063-142.ec.res.rr.com [24.25.63.142]
  5    22 ms    23 ms    15 ms  24.93.67.200
  6    30 ms    31 ms    27 ms  bu-ether45.asbnva1611w-bcr00.tbone.rr.com [107.14.19.44]
  7   792 ms    56 ms    43 ms  bu-ether12.vinnva0510w-bcr00.tbone.rr.com [66.109.6.31]
  8    33 ms    31 ms    31 ms  bu-ether12.nwrknjmd67w-bcr00.tbone.rr.com [66.109.6.29]
  9    29 ms    32 ms    70 ms  bu-ether12.nycmny837aw-bcr00.tbone.rr.com [66.109.6.27]
 10    31 ms    28 ms    35 ms  ge-1-3-0.a0.buf00.tbone.rr.com [66.109.1.57]
 11    28 ms    28 ms    65 ms  66.109.7.26
 12     *      153 ms   111 ms  ae0-xcr1.nyh.cw.net [195.2.25.70]
 13    99 ms   112 ms   114 ms  et-10-3-0-xcr1.ptl.cw.net [195.2.24.242]
 14   100 ms    99 ms   130 ms  ae5-xcr1.prp.cw.net [195.2.10.89]
 15   110 ms   100 ms   136 ms  giprenater-gw.par.cw.net [195.10.54.66]
 16   121 ms     *        *     te1-1-paris1-rtr-021.noc.renater.fr [193.51.177.25]
 17   122 ms    99 ms   101 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
 18   107 ms    99 ms   100 ms  inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr [193.51.184.177]
 19     *        *        *     Request timed out.
 20    98 ms   100 ms   102 ms  ezp3.inria.fr [128.93.162.84]

Trace complete.

C:\Users\Himangshu>
```

In the trace above, we see that there is a significant delay between the router with IP 66.109.7.26 and the router with IP 195.2.25.70(between step 11 and 12). Who we check these two address in the implication finder application we get,

66.109.7.26 : Time Warner Cable, United States.
195.2.25.70 : Cable and Wireless Worldwide plc, United Kingdom.

So we see that the delay is due to the propagation time through the trans atlantic channel, which is an expected behavior.

Also, in the given figure 4 of the question document, we see that the delay is between IP : **192.205.32.138 : AT&T Services, United States.**

and

IP : 193.251.241.133 : France Telecom Long Distance, France.