

California State University, Monterey Bay

Week 7 – Lab 7

Group 10

Clarence Mitchell

CST311

Introduction to Computer Networks

SUMMER 2015

Instructor: Dr. Anand Seetharam

Questions and Answers

The following are the list of questions and related answers for this lab.

1. ICMP and Ping

```
C:\Windows\system32>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=166ms TTL=48
Reply from 143.89.14.2: bytes=32 time=162ms TTL=48
Reply from 143.89.14.2: bytes=32 time=164ms TTL=48
Reply from 143.89.14.2: bytes=32 time=163ms TTL=48
Reply from 143.89.14.2: bytes=32 time=164ms TTL=48
Reply from 143.89.14.2: bytes=32 time=161ms TTL=48
Reply from 143.89.14.2: bytes=32 time=161ms TTL=48
Reply from 143.89.14.2: bytes=32 time=167ms TTL=48
Reply from 143.89.14.2: bytes=32 time=163ms TTL=48
Reply from 143.89.14.2: bytes=32 time=173ms TTL=48

Ping statistics for 143.89.14.2:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 161ms, Maximum = 173ms, Average = 164ms

C:\Windows\system32>
```

Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)

Filter: icmp

No.	Time	Source	Destination	Protocol	Length	Info
27	2015-06-16 18:30:53.975396000	10.32.89.164	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=71/18176, ttl=128 (reply in 29)
29	2015-06-16 18:30:54.141525000	143.89.14.2	10.32.89.164	ICMP	74	Echo (ping) reply id=0x0001, seq=71/18176, ttl=48 (request in 27)
33	2015-06-16 18:30:54.984739000	10.32.89.164	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=72/18432, ttl=128 (reply in 35)
35	2015-06-16 18:30:55.147212000	143.89.14.2	10.32.89.164	ICMP	74	Echo (ping) reply id=0x0001, seq=72/18432, ttl=48 (request in 33)
37	2015-06-16 18:30:55.993359000	10.32.89.164	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=73/18688, ttl=128 (reply in 40)
40	2015-06-16 18:30:56.157152000	143.89.14.2	10.32.89.164	ICMP	74	Echo (ping) reply id=0x0001, seq=73/18688, ttl=48 (request in 37)
42	2015-06-16 18:30:57.002192000	10.32.89.164	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=74/18944, ttl=128 (reply in 44)
44	2015-06-16 18:30:57.165415000	143.89.14.2	10.32.89.164	ICMP	74	Echo (ping) reply id=0x0001, seq=74/18944, ttl=48 (request in 42)
46	2015-06-16 18:30:58.010946000	10.32.89.164	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=75/19200, ttl=128 (reply in 49)
49	2015-06-16 18:30:58.175079000	143.89.14.2	10.32.89.164	ICMP	74	Echo (ping) reply id=0x0001, seq=75/19200, ttl=48 (request in 46)
50	2015-06-16 18:30:59.019245000	10.32.89.164	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=76/19456, ttl=128 (reply in 51)
51	2015-06-16 18:30:59.180597000	143.89.14.2	10.32.89.164	ICMP	74	Echo (ping) reply id=0x0001, seq=76/19456, ttl=48 (request in 50)
58	2015-06-16 18:31:00.027724000	10.32.89.164	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=77/19712, ttl=128 (reply in 59)
59	2015-06-16 18:31:00.188775000	143.89.14.2	10.32.89.164	ICMP	74	Echo (ping) reply id=0x0001, seq=77/19712, ttl=48 (request in 58)
61	2015-06-16 18:31:01.033041000	10.32.89.164	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=78/19968, ttl=128 (reply in 63)
63	2015-06-16 18:31:01.200546000	143.89.14.2	10.32.89.164	ICMP	74	Echo (ping) reply id=0x0001, seq=78/19968, ttl=48 (request in 61)
71	2015-06-16 18:31:02.042503000	10.32.89.164	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=79/20224, ttl=128 (reply in 72)
72	2015-06-16 18:31:02.205854000	143.89.14.2	10.32.89.164	ICMP	74	Echo (ping) reply id=0x0001, seq=79/20224, ttl=48 (request in 71)
80	2015-06-16 18:31:03.047521000	10.32.89.164	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=80/20480, ttl=128 (reply in 81)
81	2015-06-16 18:31:03.221024000	143.89.14.2	10.32.89.164	ICMP	74	Echo (ping) reply id=0x0001, seq=80/20480, ttl=48 (request in 80)

Frame 27: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Ethernet II, Src: HonHaiPr_62:0a:cb (ac:d1:b8:62:0a:cb), Dst: AsustekC_92:e5:90 (e0:3f:49:92:e5:90)

Internet Protocol Version 4, Src: 10.32.89.164 (10.32.89.164), Dst: 143.89.14.2 (143.89.14.2)

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x4d14 [correct]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 71 (0x0047)

Sequence number (LE): 18176 (0x4700)

[Response frame: 29]

Data (32 bytes)

0000 e0 3f 49 92 e5 90 ac d1 b8 62 0a cb 08 00 45 00 .?I.....b....E.

0010 00 3c 07 7e 00 00 80 01 32 24 0a 20 59 a4 8f 59 .<~....2\$.Y.Y

0020 0e 02 08 00 4d 14 00 01 00 47 61 62 63 64 65 66M....gabcdef

0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmnopqrstuv

0040 77 61 62 63 64 65 66 67 68 69 wabcdefgh

Packets: 87 - Displayed: 20 (23.0%) - Dropped: 0 (0.0%)

Profile: Default

- What is the IP address of your host? What is the IP address of the destination host?
 - My host IP address is 10.32.89.164
 - The destination host IP address is 143.89.14.2
- Why is it that an ICMP packet does not have source and destination port numbers?
 - The ICMP packet does not have source and destination port numbers because it was designed to communicate network-layer information between hosts and routers, not between application layer processes.
- 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 is 8, ICMP code is 0.
 - Checksum, identifier, sequence number and data fields.
 - Checksum has 2 bytes, Sequence number has 2 bytes, and Identifier has 2 bytes
- 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?

Wireshark packet capture showing ICMP ping request and reply between 10.32.89.164 and 143.89.14.2. The packet list shows a sequence of ping requests and replies. The packet details pane for frame 29 shows an Echo (ping) reply with type 0, code 0, and fields for checksum, identifier, sequence number, and data. The packet bytes pane shows the raw data of the ICMP reply.

No.	Time	Source	Destination	Protocol	Length	Info
27	2015-06-16 18:30:53.975396000	10.32.89.164	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=71/18176, ttl=128 (reply in 29)
29	2015-06-16 18:30:54.141525000	143.89.14.2	10.32.89.164	ICMP	74	Echo (ping) reply id=0x0001, seq=71/18176, ttl=48 (request in 27)
33	2015-06-16 18:30:54.984739000	10.32.89.164	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=72/18432, ttl=128 (reply in 35)
35	2015-06-16 18:30:55.147212000	143.89.14.2	10.32.89.164	ICMP	74	Echo (ping) reply id=0x0001, seq=72/18432, ttl=48 (request in 33)
37	2015-06-16 18:30:55.993359000	10.32.89.164	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=73/18688, ttl=128 (reply in 40)
40	2015-06-16 18:30:56.157152000	143.89.14.2	10.32.89.164	ICMP	74	Echo (ping) reply id=0x0001, seq=73/18688, ttl=48 (request in 37)
42	2015-06-16 18:30:57.002192000	10.32.89.164	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=74/18944, ttl=128 (reply in 44)
44	2015-06-16 18:30:57.165415000	143.89.14.2	10.32.89.164	ICMP	74	Echo (ping) reply id=0x0001, seq=74/18944, ttl=48 (request in 42)
46	2015-06-16 18:30:58.010946000	10.32.89.164	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=75/19200, ttl=128 (reply in 49)
49	2015-06-16 18:30:58.175079000	143.89.14.2	10.32.89.164	ICMP	74	Echo (ping) reply id=0x0001, seq=75/19200, ttl=48 (request in 46)
50	2015-06-16 18:30:59.019245000	10.32.89.164	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=76/19456, ttl=128 (reply in 51)
51	2015-06-16 18:30:59.180597000	143.89.14.2	10.32.89.164	ICMP	74	Echo (ping) reply id=0x0001, seq=76/19456, ttl=48 (request in 50)
58	2015-06-16 18:31:00.027724000	10.32.89.164	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=77/19712, ttl=128 (reply in 59)
59	2015-06-16 18:31:00.188775000	143.89.14.2	10.32.89.164	ICMP	74	Echo (ping) reply id=0x0001, seq=77/19712, ttl=48 (request in 58)
61	2015-06-16 18:31:01.033041000	10.32.89.164	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=78/19968, ttl=128 (reply in 63)
63	2015-06-16 18:31:01.200546000	143.89.14.2	10.32.89.164	ICMP	74	Echo (ping) reply id=0x0001, seq=78/19968, ttl=48 (request in 61)
71	2015-06-16 18:31:02.042503000	10.32.89.164	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=79/20224, ttl=128 (reply in 72)
72	2015-06-16 18:31:02.205854000	143.89.14.2	10.32.89.164	ICMP	74	Echo (ping) reply id=0x0001, seq=79/20224, ttl=48 (request in 71)
80	2015-06-16 18:31:03.047521000	10.32.89.164	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=80/20480, ttl=128 (reply in 81)
81	2015-06-16 18:31:03.221024000	143.89.14.2	10.32.89.164	ICMP	74	Echo (ping) reply id=0x0001, seq=80/20480, ttl=48 (request in 80)

Frame 29: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 Ethernet II, Src: AsustekC_92:e5:90 (e0:3f:49:92:e5:90), Dst: HonHaiPr_62:0a:cb (ac:d1:b8:62:0a:cb)
 Internet Protocol Version 4, Src: 143.89.14.2 (143.89.14.2), Dst: 10.32.89.164 (10.32.89.164)
 Internet Control Message Protocol
 Type: 0 (Echo (ping) reply)
 Code: 0
 Checksum: 0x5514 [correct]
 Identifier (8E): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence number (8E): 71 (0x0047)
 Sequence number (LE): 18176 (0x4700)
 [Request frame: 27]
 [Response time: 166.129 ms]
 Data (32 bytes)

0000 ac d1 b8 62 0a cb e0 3f 49 92 e5 90 08 00 45 20 ...b...? I.....E
 0010 00 3c 5f c8 00 00 30 01 29 ba 8f 59 0e 02 0a 20 .<...0.)..Y...
 0020 59 a4 00 00 55 14 00 01 00 47 61 62 63 64 65 66 y...U... .Gabcdf
 0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstu
 0040 77 61 62 63 64 65 66 67 68 69 wabcdfgh i

- ICMP type is 0, ICMP code is 0.
- Checksum, identifier, sequence number and data fields.
- Checksum has 2 bytes, Sequence number has 2 bytes, and Identifier has 2 bytes

2. ICMP and Traceroute

```

Administrator: Command Prompt

C:\Windows\system32>tracert www.inria.fr

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

  0  4 ms  3 ms  3 ms  RT-AC68U-E590 [10.32.89.3]
  1  14 ms  13 ms  12 ms  96.120.14.181
  2  14 ms  12 ms  18 ms  xe-3-1-1-0-sur03.sacramento.ca.ccal.comcast.net
  3  14 ms  33 ms  13 ms  ae-2-0-ar01.sacramento.ca.ccal.comcast.net [162.
  4  14 ms  33 ms  13 ms  ae-2-0-ar01.sacramento.ca.ccal.comcast.net [162.
  5  21 ms  17 ms  18 ms  he-3-6-0-0-cr01.sanjose.ca.ibone.comcast.net [68
  6  90 ms  125 ms  *  Request timed out.
  7  43 ms  41 ms  50 ms  he-0-13-0-0-cr01.denverqwest.co.ibone.comcast.ne
  8  48 ms  42 ms  42 ms  he-0-2-0-4-cr02.denver.co.ibone.comcast.net [68.
  9  74 ms  74 ms  65 ms  he-10617-cr01.350ecermak.il.ibone.comcast.net [6
 10  67 ms  66 ms  75 ms  he-0-14-0-1-pe04.350ecermak.il.ibone.comcast.net
 11  81 ms  64 ms  69 ms  50-248-117-142-static.hfc.comcastbusiness.net [5
 12  157 ms  171 ms  166 ms  xe-2-0-0-xcr2.ash.cw.net [195.2.28.41]
 13  157 ms  160 ms  160 ms  ae4-xcr2.prp.cw.net [195.2.28.154]
 14  161 ms  162 ms  162 ms  ae8-xcr1.prp.cw.net [195.2.10.145]
 15  160 ms  158 ms  157 ms  giprenater-gw.par.cw.net [195.10.54.66]
 16  157 ms  156 ms  163 ms  te1-1-parisi-rtr-021.noc.renater.fr [193.51.177.
 17  156 ms  157 ms  156 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.177.1
 18  156 ms  157 ms  156 ms  inria-rocquencourt-gi3-2-inria-rtr-021.noc.renat
 19  *  *  *  Request timed out.
 20  157 ms  166 ms  158 ms  ezp3.inria.fr [128.93.162.84]

Trace complete.

C:\Windows\system32>

```

*Wi-Fi [Wireshark 1.12.5 (v1.12.5-0-g5819e5b 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
13	2015-06-16 18:58:27.523572000	10.32.89.164	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=81/20736, ttl=1 (no response found!)
14	2015-06-16 18:58:27.528261000	10.32.89.3	10.32.89.164	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
15	2015-06-16 18:58:27.528868000	10.32.89.164	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=82/20992, ttl=1 (no response found!)
16	2015-06-16 18:58:27.531992000	10.32.89.3	10.32.89.164	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
17	2015-06-16 18:58:27.532604000	10.32.89.164	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=83/21248, ttl=1 (no response found!)
19	2015-06-16 18:58:27.535691000	10.32.89.3	10.32.89.164	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
27	2015-06-16 18:58:27.591257000	10.32.89.164	10.32.89.3	ICMP	161	Destination unreachable (Port unreachable)
29	2015-06-16 18:58:27.620840000	10.32.89.164	75.75.75.75	ICMP	135	Destination unreachable (Port unreachable)
32	2015-06-16 18:58:28.574559000	10.32.89.164	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=84/21504, ttl=2 (no response found!)
33	2015-06-16 18:58:28.588697000	96.120.14.181	10.32.89.164	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
34	2015-06-16 18:58:28.589489000	96.120.14.181	10.32.89.164	ICMP	70	Destination unreachable (Host unreachable)
35	2015-06-16 18:58:28.590950000	10.32.89.164	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=85/21760, ttl=2 (no response found!)
36	2015-06-16 18:58:28.603721000	96.120.14.181	10.32.89.164	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
37	2015-06-16 18:58:28.604532000	96.120.14.181	10.32.89.164	ICMP	70	Destination unreachable (Host unreachable)
38	2015-06-16 18:58:28.605981000	10.32.89.164	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=86/22016, ttl=2 (no response found!)
39	2015-06-16 18:58:28.617797000	96.120.14.181	10.32.89.164	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
40	2015-06-16 18:58:28.618733000	96.120.14.181	10.32.89.164	ICMP	70	Destination unreachable (Host unreachable)
107	2015-06-16 18:58:34.140415000	10.32.89.164	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=87/22272, ttl=3 (no response found!)
108	2015-06-16 18:58:34.154583000	69.139.197.241	10.32.89.164	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
109	2015-06-16 18:58:34.155715000	10.32.89.164	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=88/22528, ttl=3 (no response found!)
110	2015-06-16 18:58:34.167895000	69.139.197.241	10.32.89.164	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Frame 13: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0

Ethernet II, Src: HonHaiPR_62:0a:cb (ac:dl:b8:62:0a:cb), Dst: AsustekC_92:e5:90 (e0:3f:49:92:e5:90)

Internet Protocol Version 4, Src: 10.32.89.164 (10.32.89.164), Dst: 128.93.162.84 (128.93.162.84)

Version: 4

Header Length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))

Total Length: 92

Identification: 0x48f2 (18674)

Flags: 0x00

Fragment offset: 0

Time to live: 1

Protocol: ICMP (1)

Header checksum: 0xea39 [validation disabled]

Source: 10.32.89.164 (10.32.89.164)

Destination: 128.93.162.84 (128.93.162.84)

[Source GeoIP: unknown]

[Destination GeoIP: unknown]

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0xf7ad [correct]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 81 (0x0051)

Sequence number (LE): 20736 (0x5100)

[No response seen]

Data (64 bytes)

0000 e0 3f 49 92 e5 90 ac d1 b8 62 0a cb 08 00 45 00 .?I.....b....E.

0010 00 5c 48 f2 00 00 01 01 ea 39 0a 20 59 a4 80 5d .\H.....9.Y..]

0020 a2 54 08 00 f7 ad 00 01 00 51 00 00 00 00 00 00 .T.....Q.....

0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

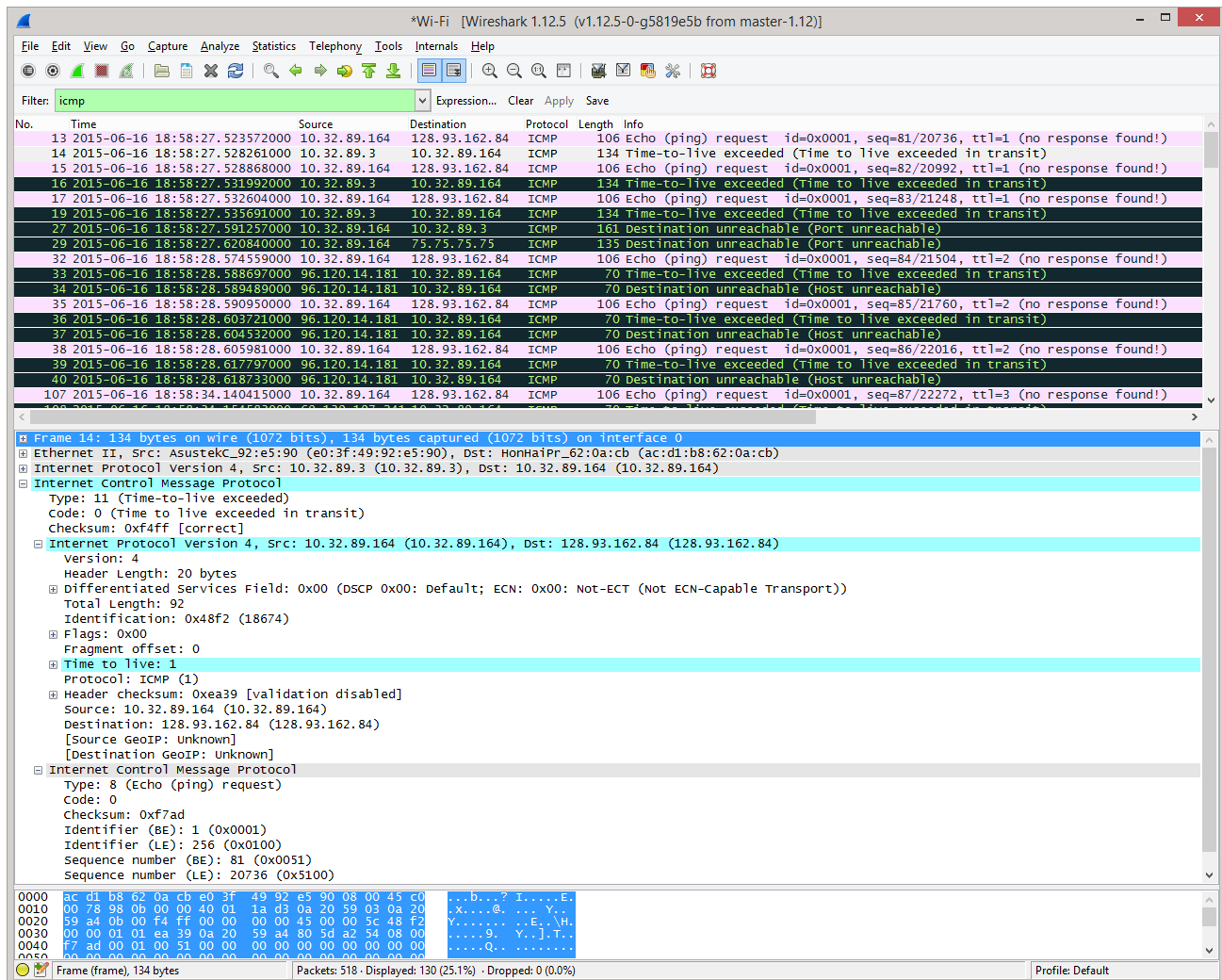
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0050 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 00 00 00 00 00

File: "C:\Users\Larsen\AppData\Local\Temp..." Packets: 518 - Displayed: 130 (25.1%) - Dropped: 0 (0.0%) Profile: Default

5. What is the IP address of your host? What is the IP address of the target destination host?
 - My host IP address is 10.32.89.164
 - The destination host IP address 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, the IP protocol number should be 0x11. (see <http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>)
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 and the ping query packet have the same fields.



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 IP header and the first 8 bytes of 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 packets are type 0, and they are different because all the datagrams made it to the host before the TTL expired.

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?
- Yes, in mine from 6 to 7 there was a long delay.
 - Yes, from 9 to 10 in figure 4.
 - In figure 4 the first location is Massachusetts and the second is France.