Rob Navarro
CS372

LAB 4

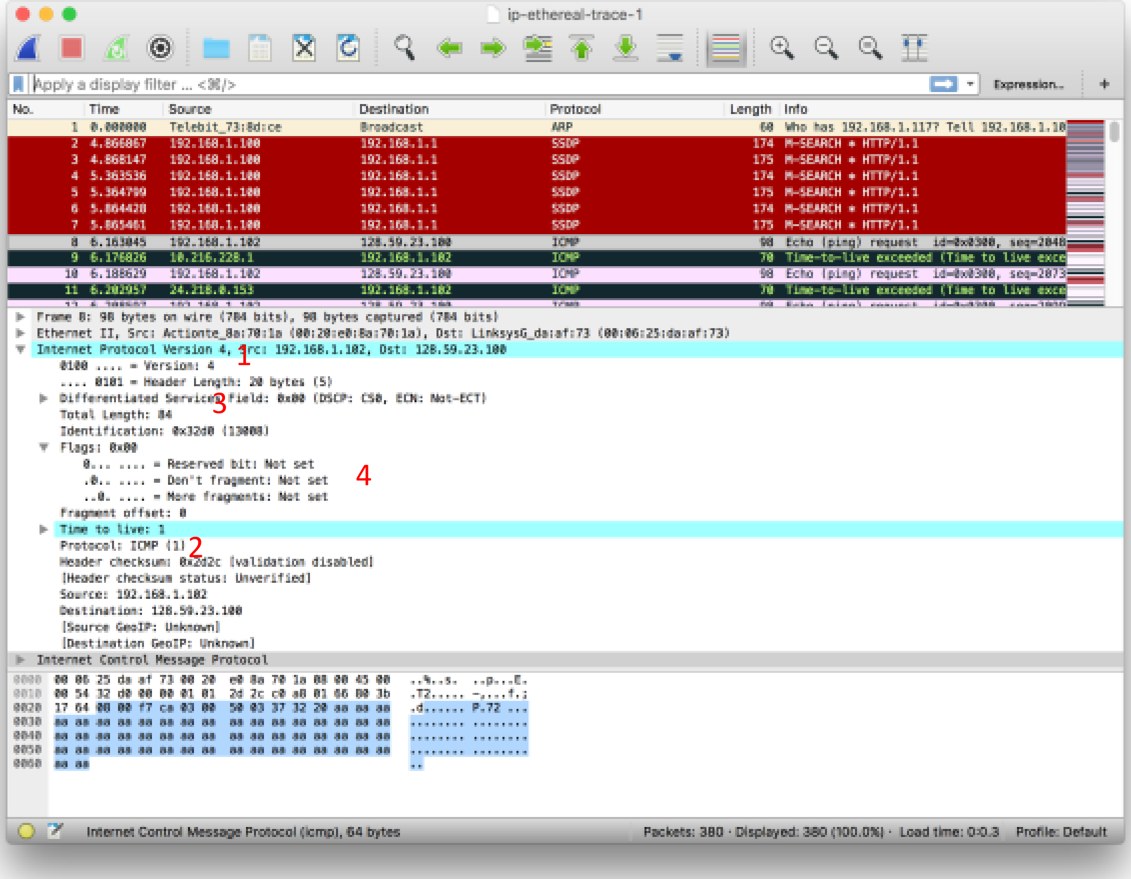
1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?
Answer: The IP address is 192.168.1.102

2. Within the IP packet header, what is the value in the upper layer protocol field?
Answer: ICMP (1)

3. How many bytes are in the IP header? How many bytes are in the payload *of the IP datagram*? Explain how you determined the number of payload bytes.
IP header: 20 bytes
Payload bytes: 64 bytes, we know this since the header was 20 bytes and the length of the message was 84. Thus, 84 – 20 gives us a payload of 64 bytes.

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.
Answer: The fragment bit is 0 so the IP datagram has not been fragmented.

Rob Navarro
CS372



```
No.  Time      Source            Destination     Protocol  Length Info
  1  0.000000  Telebit_73:8d:ce  Broadcast       ARP           60 Who has 192.168.1.117? Tell 192.168.1.10
  2  4.866867  192.168.1.100     192.168.1.1     SSDP         174 M-SEARCH * HTTP/1.1
  3  4.868147  192.168.1.100     192.168.1.1     SSDP         175 M-SEARCH * HTTP/1.1
  4  5.363536  192.168.1.100     192.168.1.1     SSDP         174 M-SEARCH * HTTP/1.1
  5  5.364799  192.168.1.100     192.168.1.1     SSDP         175 M-SEARCH * HTTP/1.1
  6  5.864420  192.168.1.100     192.168.1.1     SSDP         174 M-SEARCH * HTTP/1.1
  7  5.865461  192.168.1.100     192.168.1.1     SSDP         175 M-SEARCH * HTTP/1.1
  8  6.163045  192.168.1.102     128.59.23.100   ICMP          98 Echo (ping) request  id=0x0300, seq=2048
  9  6.176826  10.216.228.1      192.168.1.102   ICMP          70 Time-to-live exceeded (Time to live exce
 10  6.188629  192.168.1.102     128.59.23.100   ICMP          98 Echo (ping) request  id=0x0300, seq=2073
 11  6.202957  24.218.0.153      192.168.1.102   ICMP          70 Time-to-live exceeded (Time to live exce
```

```
▶ Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▶ Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d0 (13008)
  ▼ 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: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▶ Internet Control Message Protocol
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ..%..s.  ..p...E.
0010  00 54 32 d0 00 00 01 01  2d 2c c0 a8 01 66 80 3b   .T2.....  -,...f.;
0020  17 64 08 00 f7 ca 03 00  50 03 37 32 20 aa aa aa   .d......  P.72 ...
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
0050  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
0060  aa aa                                              ..
```

Internet Control Message Protocol (icmp), 64 bytes   Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.3   Profile: Default

5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?

- Identification
- Time to live
- Header Checksum

6. Which fields stay constant? Which of the fields *must* stay constant? Which fields must change? Why?

Answer: The fields that stay constant and must stay constant are:

- header length – since these are all ICMP packets
- source/dest ip –since we are sending the data to the same spot
- upper layer protocol – since these are all ICMP packets
- version – We are using IPv4

The fields that change:

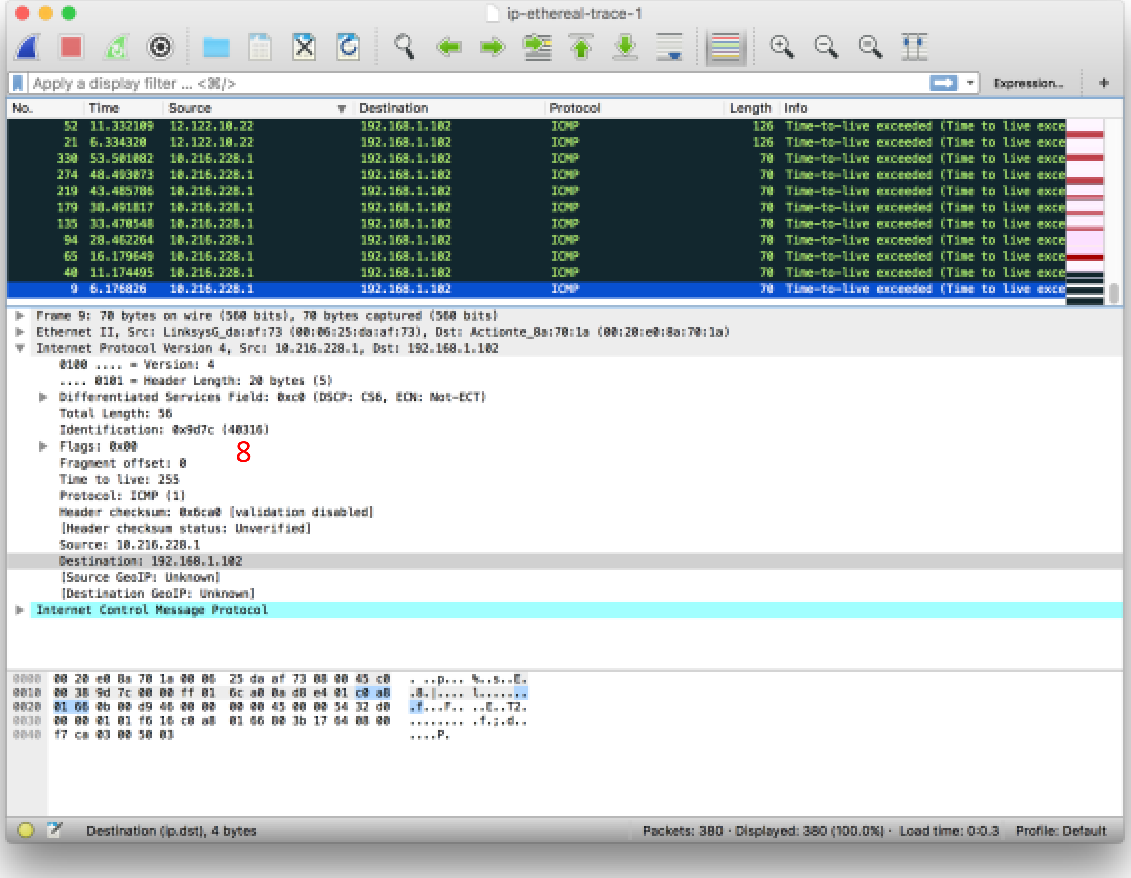
- Identification – packets need different ids
- TTL – traceroute increases the TTL

- Header checksum – since the header data changes.

7. Describe the pattern you see in the values in the Identification field of the IP datagram.
Answer: The identification field increases by 1.

8. What is the value in the Identification field and the TTL field?
Answer:

- Identification: 40316
- TTL: 255


ip-ethereal-trace-1
Apply a display filter ... <⌘/>
Expression...
+
8
Destination (ip.dst), 4 bytes
Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.3
Profile: Default

```
No.   Time       Source         Destination    Protocol  Length  Info
   52 11.332109  12.122.10.22   192.168.1.102  ICMP         126  Time-to-live exceeded (Time to live exce
   21 6.334320   12.122.10.22   192.168.1.102  ICMP         126  Time-to-live exceeded (Time to live exce
  330 53.501082  10.216.228.1   192.168.1.102  ICMP          70  Time-to-live exceeded (Time to live exce
  274 48.493873  10.216.228.1   192.168.1.102  ICMP          70  Time-to-live exceeded (Time to live exce
  219 43.485706  10.216.228.1   192.168.1.102  ICMP          70  Time-to-live exceeded (Time to live exce
  179 38.491817  10.216.228.1   192.168.1.102  ICMP          70  Time-to-live exceeded (Time to live exce
  135 33.470548  10.216.228.1   192.168.1.102  ICMP          70  Time-to-live exceeded (Time to live exce
   94 28.462264  10.216.228.1   192.168.1.102  ICMP          70  Time-to-live exceeded (Time to live exce
   65 16.179649  10.216.228.1   192.168.1.102  ICMP          70  Time-to-live exceeded (Time to live exce
   40 11.174495  10.216.228.1   192.168.1.102  ICMP          70  Time-to-live exceeded (Time to live exce
    9 6.176826   10.216.228.1   192.168.1.102  ICMP          70  Time-to-live exceeded (Time to live exce
```

```
▶ Frame 9: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
▶ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
▼ Internet Protocol Version 4, Src: 10.216.228.1, Dst: 192.168.1.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x9d7c (40316)
  ▶ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x6ca0 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.216.228.1
    Destination: 192.168.1.102
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▶ Internet Control Message Protocol
```

```
0000  00 20 e0 8a 70 1a 00 06  25 da af 73 08 00 45 c0   . ..p... %..s..E.
0010  00 38 9d 7c 00 00 ff 01  6c a0 0a d8 e4 01 c0 a8   .8.|.... l.......
0020  01 66 0b 00 d9 46 00 00  00 00 45 00 00 54 32 d0   .f...F.. ..E..T2.
0030  00 00 01 01 f6 16 c0 a8  01 66 00 3b 17 64 08 00   ........ .f.;.d..
0040  f7 ca 03 00 50 03                                   ....P.
```

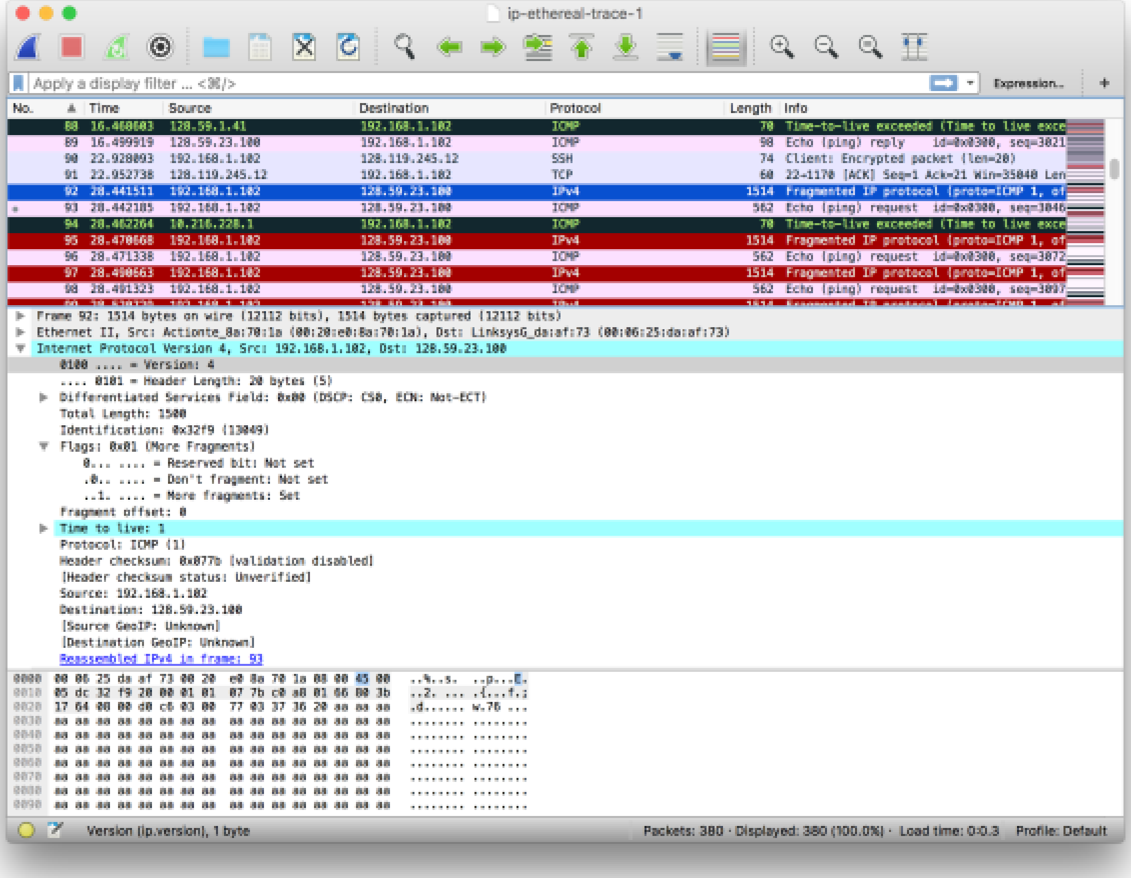
9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?
Answer: The identification field changes for each request because it must be unique. The TTL field stays the same since the TTL from the first hop router does not change.

10. Find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 2000. Has that message been fragmented across more than one IP datagram?
Answer: Yes, it has been fragmented.

Rob Navarro
CS372

11. Screenshot the first fragment of the fragmented IP datagram (with sufficient details to answer these questions). What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

Answer: The more fragments flag has been set to 1, which indicates the data has been fragmented. We can also tell which fragment is first by looking at the fragment offset. For the first fragment, it is 0. The length of this datagram is 1500 bytes, including the header.



ip-ethereal-trace-1

Apply a display filter ... <⌘/>

Expression...

```
No.    Time        Source           Destination      Protocol  Length  Info
  88   16.460603   128.59.1.41      192.168.1.102    ICMP          70  Time-to-live exceeded (Time to live exce
  89   16.499919   128.59.23.100    192.168.1.102    ICMP          98  Echo (ping) reply    id=0x0300, seq=3821
  90   22.920093   192.168.1.102    128.119.245.12   SSH           74  Client: Encrypted packet (len=20)
  91   22.952738   128.119.245.12   192.168.1.102    TCP           60  22→1170 [ACK] Seq=1 Ack=21 Win=35040 Len
  92   28.441511   192.168.1.102    128.59.23.100    IPv4        1514  Fragmented IP protocol (proto=ICMP 1, of
  93   28.442105   192.168.1.102    128.59.23.100    ICMP         562  Echo (ping) request  id=0x0300, seq=3846
  94   28.462264   10.216.228.1     192.168.1.102    ICMP          70  Time-to-live exceeded (Time to live exce
  95   28.470668   192.168.1.102    128.59.23.100    IPv4        1514  Fragmented IP protocol (proto=ICMP 1, of
  96   28.471338   192.168.1.102    128.59.23.100    ICMP         562  Echo (ping) request  id=0x0300, seq=3072
  97   28.490663   192.168.1.102    128.59.23.100    IPv4        1514  Fragmented IP protocol (proto=ICMP 1, of
  98   28.491323   192.168.1.102    128.59.23.100    ICMP         562  Echo (ping) request  id=0x0300, seq=3097
```

```
▶ Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
▶ Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x32f9 (13049)
  ▼ Flags: 0x01 (More Fragments)
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    Fragment offset: 0
  ▶ Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x077b [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Reassembled IPv4 in frame: 93
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ..%..s.  ..p...E.
0010  05 dc 32 f9 20 00 01 01  07 7b c0 a8 01 66 80 3b   ..2. ...  .{...f.;
0020  17 64 08 00 d0 c6 03 00  77 03 37 36 20 aa aa aa   .d......  w.76 ...
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
0050  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
0060  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
0070  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
0080  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
0090  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
```

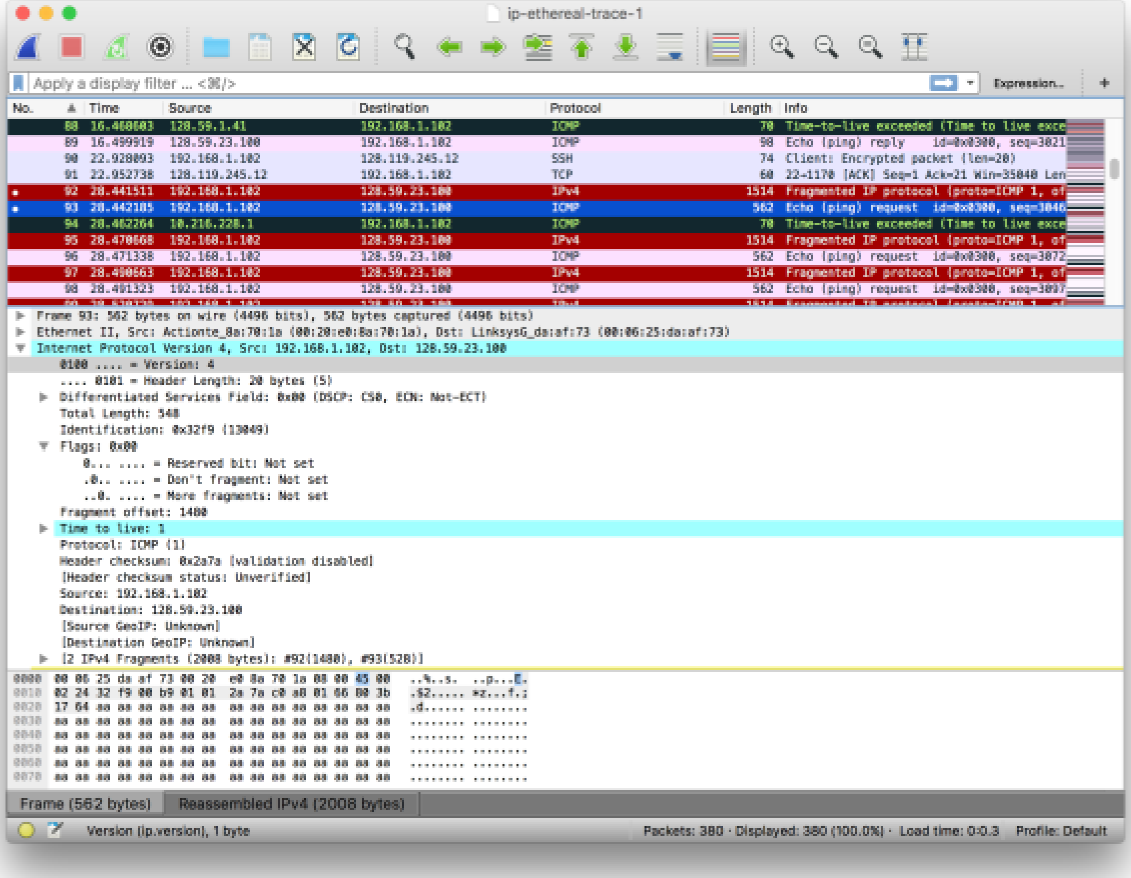
Version (ip.version), 1 byte

Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.3   Profile: Default

12. Screenshot the second fragment of the fragmented IP datagram (with sufficient details to answer these questions). What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?

Answer: The fragment offset is 1480, which tells us this is not the first fragment. We can tell that this is the last fragment since the more fragments flag is 0.

Rob Navarro
CS372



ip-ethereal-trace-1

Apply a display filter ... <⌘/>

```
No.   Time        Source            Destination       Protocol  Length  Info
 88   16.468603   128.59.1.41       192.168.1.102     ICMP          70  Time-to-live exceeded (Time to live exce
 89   16.499919   128.59.23.100     192.168.1.102     ICMP          98  Echo (ping) reply    id=0x0300, seq=3021
 90   22.928093   192.168.1.102     128.119.245.12    SSH           74  Client: Encrypted packet (len=20)
 91   22.952738   128.119.245.12    192.168.1.102     TCP           60  22→1170 [ACK] Seq=1 Ack=21 Win=35040 Len
 92   28.441511   192.168.1.102     128.59.23.100     IPv4        1514  Fragmented IP protocol (proto=ICMP 1, of
 93   28.442105   192.168.1.102     128.59.23.100     ICMP         562  Echo (ping) request  id=0x0300, seq=3046
 94   28.462264   10.216.228.1      192.168.1.102     ICMP          70  Time-to-live exceeded (Time to live exce
 95   28.470668   192.168.1.102     128.59.23.100     IPv4        1514  Fragmented IP protocol (proto=ICMP 1, of
 96   28.471338   192.168.1.102     128.59.23.100     ICMP         562  Echo (ping) request  id=0x0300, seq=3072
 97   28.490663   192.168.1.102     128.59.23.100     IPv4        1514  Fragmented IP protocol (proto=ICMP 1, of
 98   28.491323   192.168.1.102     128.59.23.100     ICMP         562  Echo (ping) request  id=0x0300, seq=3097
```

```
▶ Frame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
▶ Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 548
    Identification: 0x32f9 (13049)
  ▼ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 1480
  ▶ Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x2a7a [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ▶ [2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ..%..s.  ..p...E.
0010  02 24 32 f9 00 b9 01 01  2a 7a c0 a8 01 66 80 3b   .$2.....  *z...f.;
0020  17 64 aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   .d......  ........
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
0050  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
0060  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
0070  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
```

Frame (562 bytes) | Reassembled IPv4 (2008 bytes)

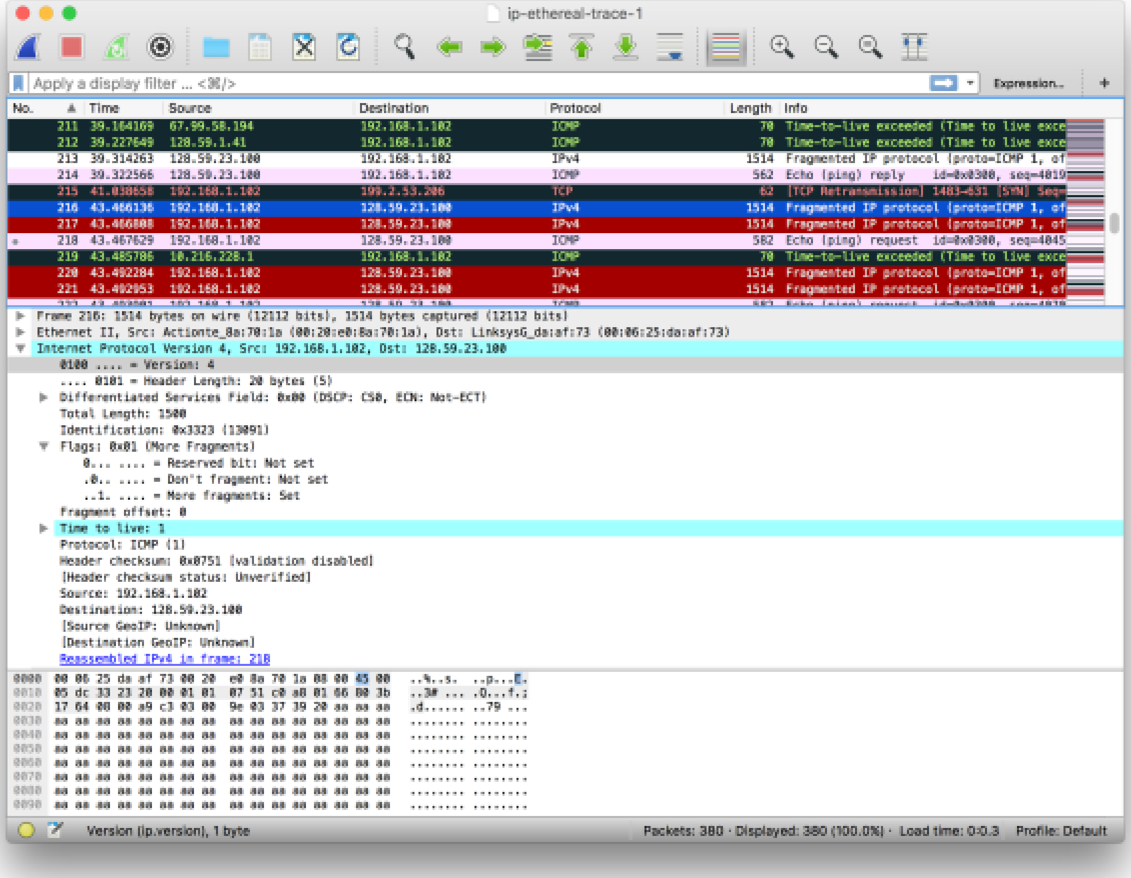
Version (ip.version), 1 byte | Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.3 | Profile: Default

13. What fields change in the IP header between the first and second fragment?

- total length
- flags
- fragment offset
- checksum

14. How many fragments were created from the original datagram?
Answer: 3 fragments were created.
15. What fields change in the IP header among the fragments?
Answer: The first two fragments contain the same flags and total length (1500), while the third fragment does not have any flags set and a length of 568. The fragment offset and checksum are different for all 3 fragments.

Rob Navarro
CS372



```
No.   Time       Source          Destination     Protocol  Length Info
 211  39.164169  67.99.58.194    192.168.1.102   ICMP          70 Time-to-live exceeded (Time to live exce
 212  39.227649  128.59.1.41     192.168.1.102   ICMP          70 Time-to-live exceeded (Time to live exce
 213  39.314263  128.59.23.100   192.168.1.102   IPv4        1514 Fragmented IP protocol (proto=ICMP 1, of
 214  39.322566  128.59.23.100   192.168.1.102   ICMP         562 Echo (ping) reply    id=0x0300, seq=4019
 215  41.038658  192.168.1.102   199.2.53.206    TCP           62 [TCP Retransmission] 1483→631 [SYN] Seq=
 216  43.466136  192.168.1.102   128.59.23.100   IPv4        1514 Fragmented IP protocol (proto=ICMP 1, of
 217  43.466808  192.168.1.102   128.59.23.100   IPv4        1514 Fragmented IP protocol (proto=ICMP 1, of
 218  43.467629  192.168.1.102   128.59.23.100   ICMP         582 Echo (ping) request  id=0x0300, seq=4045
 219  43.485786  10.216.228.1    192.168.1.102   ICMP          70 Time-to-live exceeded (Time to live exce
 220  43.492284  192.168.1.102   128.59.23.100   IPv4        1514 Fragmented IP protocol (proto=ICMP 1, of
 221  43.492053  192.168.1.102   128.59.23.100   IPv4        1514 Fragmented IP protocol (proto=ICMP 1, of
```

```
▶ Frame 216: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
▶ Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x3323 (13091)
  ▼ Flags: 0x01 (More Fragments)
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    Fragment offset: 0
  ▶ Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x0751 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Reassembled IPv4 in frame: 218
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ..%..s.  ..p...E.
0010  05 dc 33 23 20 00 01 01  07 51 c0 a8 01 66 80 3b   ..3# ...  .Q...f.;
0020  17 64 08 00 a9 c3 03 00  9e 03 37 39 20 aa aa aa   .d......  ..79 ...
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
0050  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
0060  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
0070  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
0080  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
0090  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
```

Version (ip.version), 1 byte

Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.3   Profile: Default