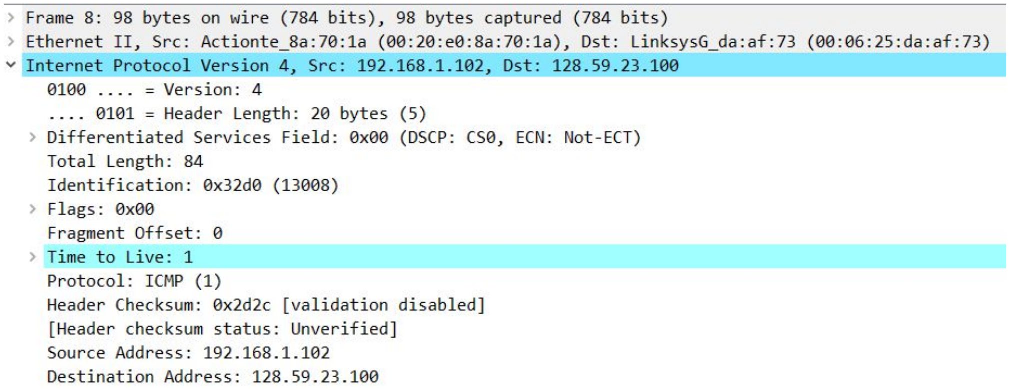
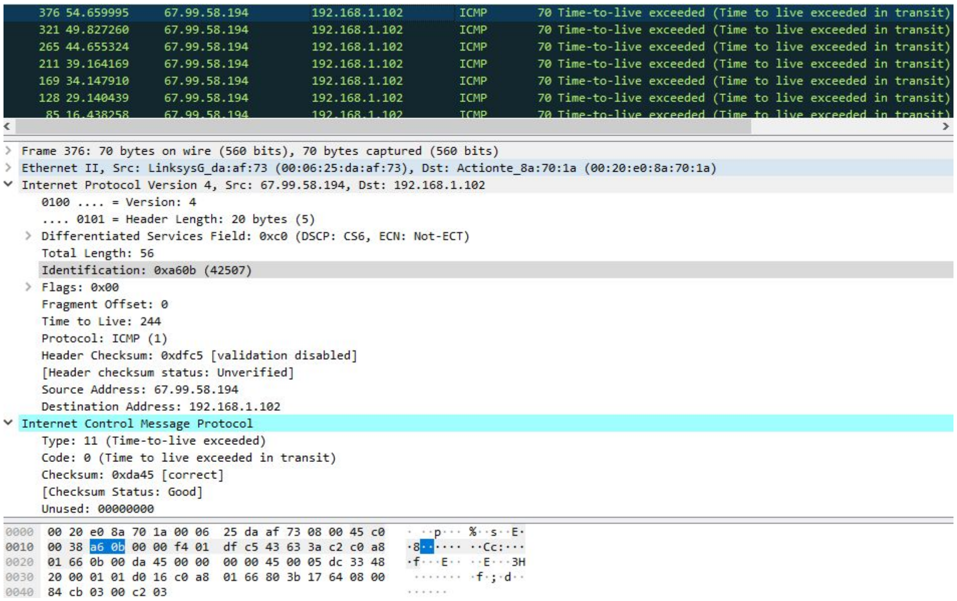
Melissa Jost
915842777
Section A03
Roberto Lozano
914294300
Section A01

WireShark Lab: IP

Note: This was done using ip-ethereal-trace-1 trace file

1. The IP address of this computer is 192.168.1.102.
    a. 

```
> 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)
v 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
    Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
```

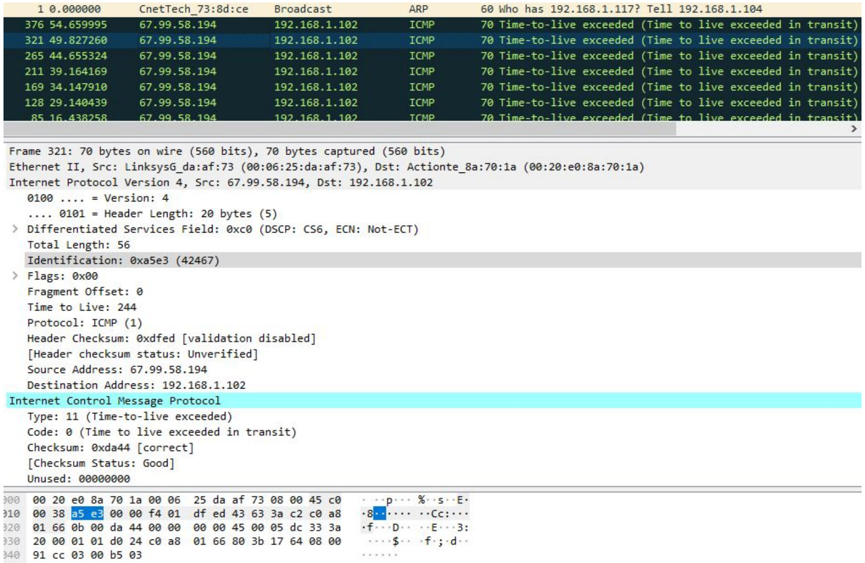
2. The value of the upper layer protocol field is ICMP.
3. There are 20 bytes in the IP header. There are 64 bytes in the payload of the IP datagram, which can be found by subtracting the total length from the amount of bytes in the header.
4. This IP datagram has not been fragmented because the fragment flag is set to 0.
5. The fields that always change are the Identification field, the Time to live value and the Header Checksum.
    a. 

```
376 54.659995   67.99.58.194    192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
321 49.827260   67.99.58.194    192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
265 44.655324   67.99.58.194    192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
211 39.164169   67.99.58.194    192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
169 34.147910   67.99.58.194    192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
128 29.140439   67.99.58.194    192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
 85 16.438258   67.99.58.194    192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)

> Frame 376: 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)
v Internet Protocol Version 4, Src: 67.99.58.194, 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: 0xa60b (42507)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 244
    Protocol: ICMP (1)
    Header Checksum: 0xdfc5 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 67.99.58.194
    Destination Address: 192.168.1.102
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xda45 [correct]
    [Checksum Status: Good]
    Unused: 00000000

0000  00 20 e0 8a 70 1a 00 06  25 da af 73 08 00 45 c0   · ··p··· %··s··E·
0010  00 38 a6 0b 00 00 f4 01  df c5 43 63 3a c2 c0 a8   ·8······ ··Cc:···
0020  01 66 0b 00 da 45 00 00  00 00 45 00 05 dc 33 48   ·f···E·· ··E···3H
0030  20 00 01 01 d0 16 c0 a8  01 66 80 3b 17 64 08 00    ······· ·f·;·d··
0040  84 cb 03 00 c2 03                                   ······
```

b.



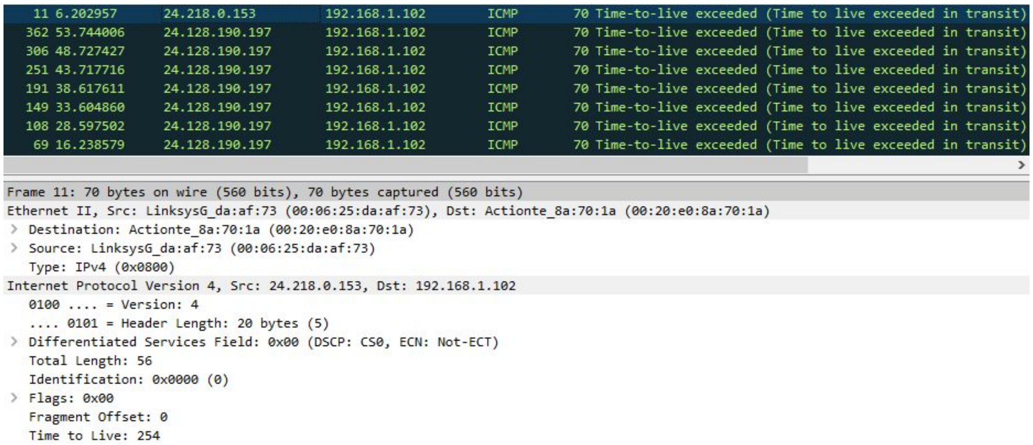
```
    1 0.000000    CnetTech_73:8d:ce   Broadcast       ARP    60 Who has 192.168.1.117? Tell 192.168.1.104
  376 54.659995   67.99.58.194        192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
  321 49.827260   67.99.58.194        192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
  265 44.655324   67.99.58.194        192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
  211 39.164169   67.99.58.194        192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
  169 34.147910   67.99.58.194        192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
  128 29.140439   67.99.58.194        192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
   85 16.438258   67.99.58.194        192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)

Frame 321: 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: 67.99.58.194, 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: 0xa5e3 (42467)
 > Flags: 0x00
   Fragment Offset: 0
   Time to Live: 244
   Protocol: ICMP (1)
   Header Checksum: 0xdfed [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 67.99.58.194
   Destination Address: 192.168.1.102
Internet Control Message Protocol
   Type: 11 (Time-to-live exceeded)
   Code: 0 (Time to live exceeded in transit)
   Checksum: 0xda44 [correct]
   [Checksum Status: Good]
   Unused: 00000000

000  00 20 e0 8a 70 1a 00 06  25 da af 73 08 00 45 c0   · ··p··· %··s··E·
010  00 38 a5 e3 00 00 f4 01  df ed 43 63 3a c2 c0 a8   ·8······ ··Cc:···
020  01 66 0b 00 da 44 00 00  00 00 45 00 05 dc 33 3a   ·f···D·· ··E···3:
030  20 00 01 01 d0 24 c0 a8  01 66 80 3b 17 64 08 00    ····$·· ·f·;·d··
040  91 cc 03 00 b5 03                                  ······
```

6. The fields that stay constant, and that must stay constant are the header length, the protocol and version, and the source and destination IP addresses. The fields that change are the identification field, the time to live, and the header checksum.
7. The pattern in the values in the Identification field of the IP datagram is that the value in the identification field always increased with each request that was sent.
8. The value in the Identification field is 0, and the value in the TTL field is 254.

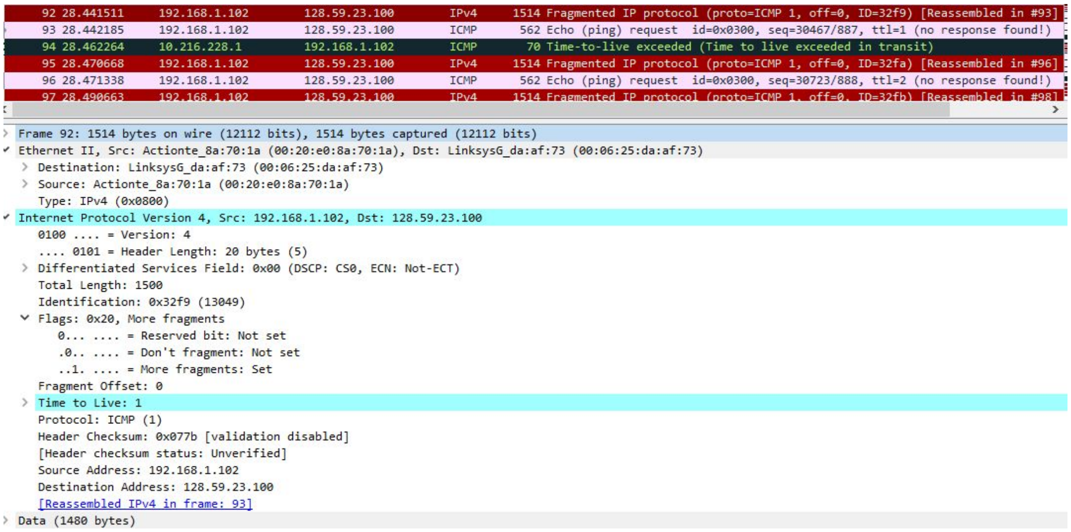
a.



```
   11 6.202957    24.218.0.153      192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
  362 53.744006   24.128.190.197    192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
  306 48.727427   24.128.190.197    192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
  251 43.717716   24.128.190.197    192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
  191 38.617611   24.128.190.197    192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
  149 33.604860   24.128.190.197    192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
  108 28.597502   24.128.190.197    192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
   69 16.238579   24.128.190.197    192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)

Frame 11: 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)
 > Destination: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
 > Source: LinksysG_da:af:73 (00:06:25:da:af:73)
   Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 24.218.0.153, Dst: 192.168.1.102
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 56
   Identification: 0x0000 (0)
 > Flags: 0x00
   Fragment Offset: 0
   Time to Live: 254
```

9. The identification field changes because it needs to be different for every datagram, but the TTL stays the same because we’re only looking at the first hop router.

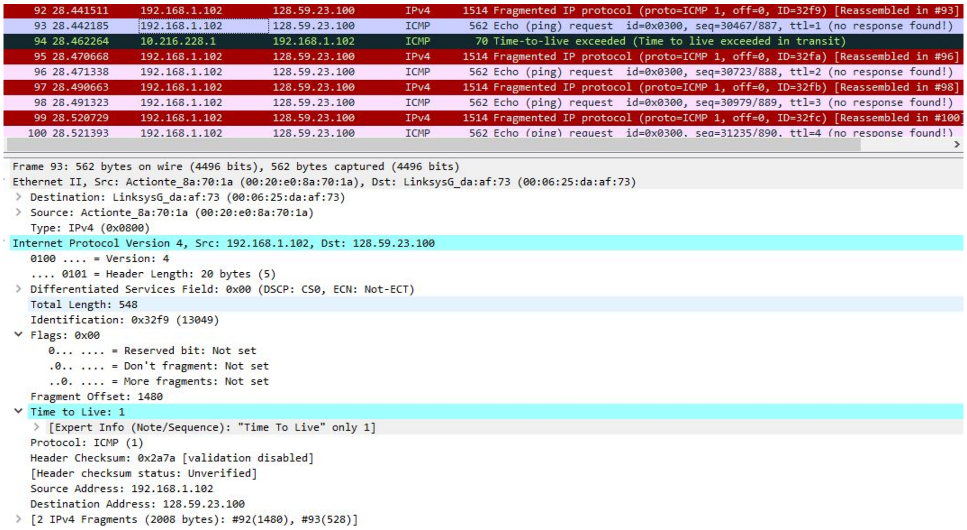


```
 92 28.441511   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
 93 28.442185   192.168.1.102   128.59.23.100   ICMP    562 Echo (ping) request  id=0x0300, seq=30467/887, ttl=1 (no response found!)
 94 28.462264   10.216.228.1    192.168.1.102   ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
 95 28.470668   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
 96 28.471338   192.168.1.102   128.59.23.100   ICMP    562 Echo (ping) request  id=0x0300, seq=30723/888, ttl=2 (no response found!)
 97 28.490663   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]

> 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)
  > Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
  > Source: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
    Type: IPv4 (0x0800)
✓ 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: 0x20, 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 Address: 192.168.1.102
    Destination Address: 128.59.23.100
    [Reassembled IPv4 in frame: 93]
> Data (1480 bytes)
```

10.

11. We know that this datagram has been fragmented because the more fragments flag has been set to 1, indicating that this is one in a series of fragments. We know that this is the first fragment because the fragment offset has been set to 0. This IP datagram has a length of 1500 bits.
12. We know that this isn't the first datagram fragment because it has a fragment offset, and we know there aren't any more fragments because the more fragments flag is set to 0.

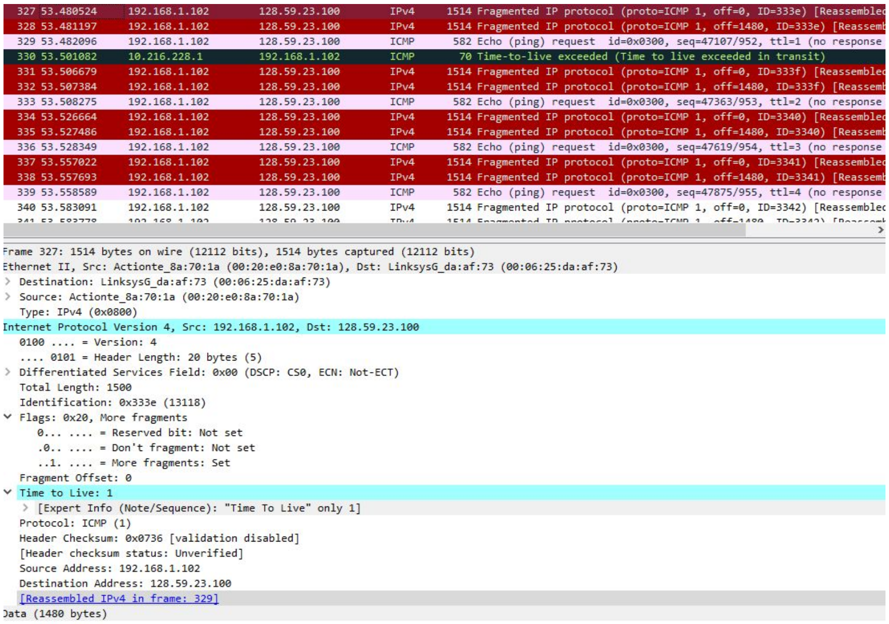


```
 92 28.441511   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
 93 28.442185   192.168.1.102   128.59.23.100   ICMP    562 Echo (ping) request  id=0x0300, seq=30467/887, ttl=1 (no response found!)
 94 28.462264   10.216.228.1    192.168.1.102   ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
 95 28.470668   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
 96 28.471338   192.168.1.102   128.59.23.100   ICMP    562 Echo (ping) request  id=0x0300, seq=30723/888, ttl=2 (no response found!)
 97 28.490663   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]
 98 28.491323   192.168.1.102   128.59.23.100   ICMP    562 Echo (ping) request  id=0x0300, seq=30979/889, ttl=3 (no response found!)
 99 28.520729   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc) [Reassembled in #100
100 28.521393   192.168.1.102   128.59.23.100   ICMP    562 Echo (ping) request  id=0x0300, seq=31235/890, ttl=4 (no response found!)

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)
  > Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
  > Source: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
    Type: IPv4 (0x0800)
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
    > [Expert Info (Note/Sequence): "Time To Live" only 1]
    Protocol: ICMP (1)
    Header Checksum: 0x2a7a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
  > [2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
```

   a.

13. The header checksum, length, and fragment flags change between the first and second fragments.
14. Three fragments were created from the original datagram.

a. 

```
327 53.480524   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=333e) [Reassemble
328 53.481197   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=333e) [Reassem
329 53.482096   192.168.1.102   128.59.23.100   ICMP    582 Echo (ping) request  id=0x0300, seq=47107/952, ttl=1 (no response
330 53.501082   10.216.228.1    192.168.1.102   ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
331 53.506679   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=333f) [Reassemble
332 53.507384   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=333f) [Reassem
333 53.508275   192.168.1.102   128.59.23.100   ICMP    582 Echo (ping) request  id=0x0300, seq=47363/953, ttl=2 (no response
334 53.526664   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3340) [Reassemble
335 53.527486   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3340) [Reassem
336 53.528349   192.168.1.102   128.59.23.100   ICMP    582 Echo (ping) request  id=0x0300, seq=47619/954, ttl=3 (no response
337 53.557022   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3341) [Reassemble
338 53.557693   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3341) [Reassem
339 53.558589   192.168.1.102   128.59.23.100   ICMP    582 Echo (ping) request  id=0x0300, seq=47875/955, ttl=4 (no response
340 53.583091   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3342) [Reassemble
341 53.583778   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3342) [Reassem

Frame 327: 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)
 > Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
 > Source: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
   Type: IPv4 (0x0800)
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: 0x333e (13118)
 v Flags: 0x20, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
   Fragment Offset: 0
 v Time to Live: 1
    > [Expert Info (Note/Sequence): "Time To Live" only 1]
   Protocol: ICMP (1)
   Header Checksum: 0x0736 [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 192.168.1.102
   Destination Address: 128.59.23.100
   [Reassembled IPv4 in frame: 329]
Data (1480 bytes)
```

15. The fragment offset, length, and header checksum change amongst fragments.