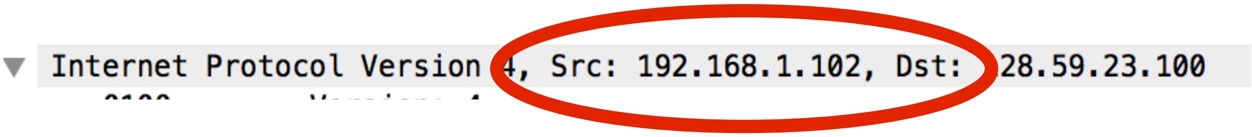
Vijay Kumar Lab 4 Lab Completed using ip-ethereal-trace-1 from lab

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?

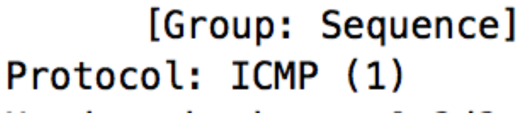
My IP address is: 192.168.1.102



```
▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
```

2. Within the IP packet header, what is the value in the upper layer protocol field?

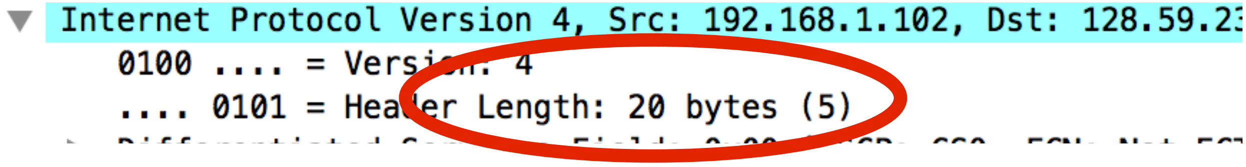
Protocol: ICMP (1)



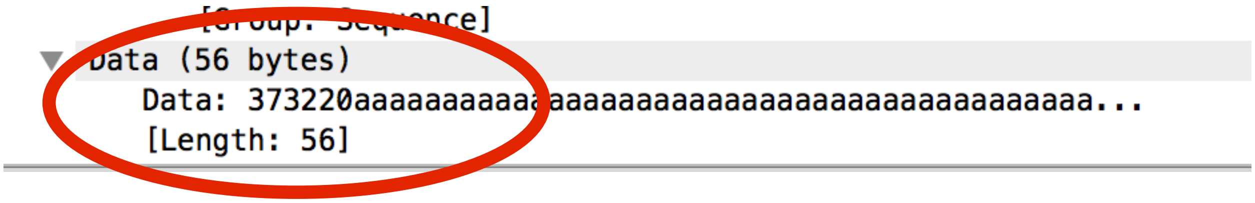
```
        [Group: Sequence]
  Protocol: ICMP (1)
```

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.

There are 20 bytes in the IP header and 56 bytes in the datagram. The datagram payload bytes is specified in the Data portion of the ICMP details in the IP header.



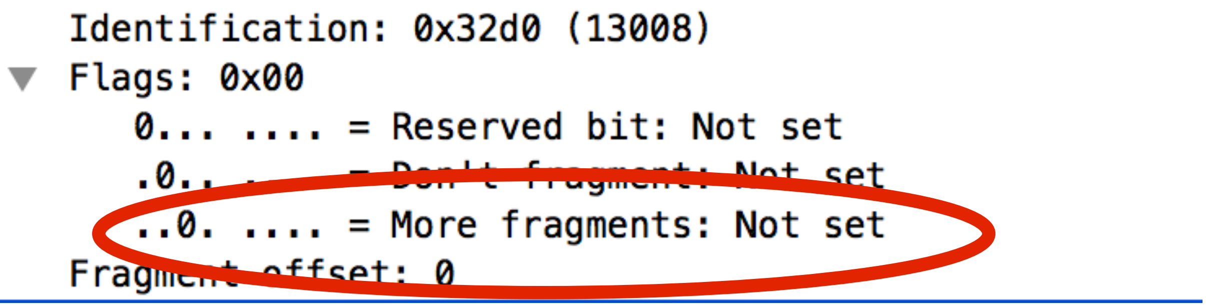
```
▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT
```



```
            [Group: Sequence]
 ▼ Data (56 bytes)
      Data: 373220aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa...
      [Length: 56]
```

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

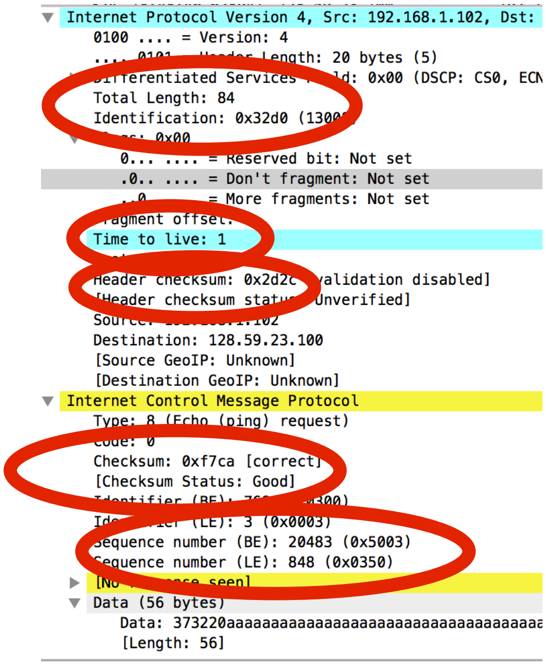
No, the datagram has not been fragmented. We can make this conclusion because the ‘More fragments’ flag has not been set.



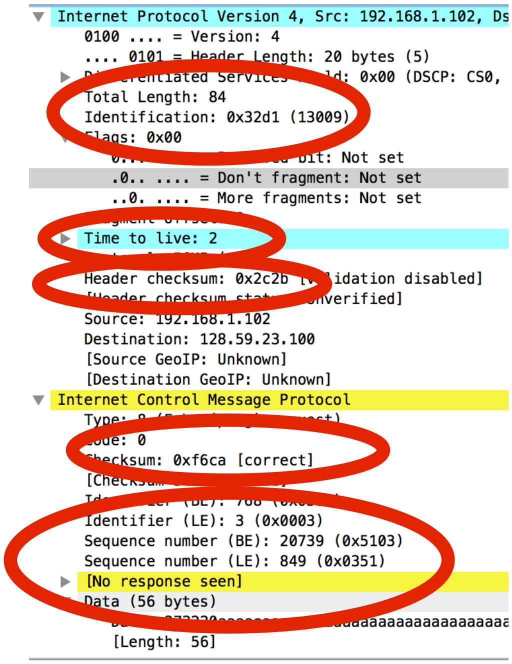
```
    Identification: 0x32d0 (13008)
▼   Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
```

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?

- Header checksum - IP Header
- Identification - IP Header
- Time to Live - IP Header
- Sequence number (LE) - ICMP
- Sequence number (BE) - ICMP
- Checksum - ICMP



```
▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst:
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN
    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
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7ca [correct]
    [Checksum Status: Good]
    Identifier (BE): 768 (0x0300)
    Identifier (LE): 3 (0x0003)
    Sequence number (BE): 20483 (0x5003)
    Sequence number (LE): 848 (0x0350)
  ▶ [No response seen]
  ▼ Data (56 bytes)
      Data: 373220aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
      [Length: 56]
```



```
▼ Internet Protocol Version 4, Src: 192.168.1.102, Ds
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0,
    Total Length: 84
    Identification: 0x32d1 (13009)
  ▼ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
  ▶ Time to live: 2
    Protocol: ICMP (1)
    Header checksum: 0x2c2b [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
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf6ca [correct]
    [Checksum Status: Good]
    Identifier (BE): 768 (0x0300)
    Identifier (LE): 3 (0x0003)
    Sequence number (BE): 20739 (0x5103)
    Sequence number (LE): 849 (0x0351)
  ▶ [No response seen]
  ▼ Data (56 bytes)
      Data: 373220aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
      [Length: 56]
```

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

The ICMP Type and Code do not change as 8 is the predefined message type for an echo request and 0 is the code that is associated with it.

Source and Destination do not change, since the route from source to destination is what we are attempting to trace.

Protocol : ICMP (1) remains unchanged as this is the protocol we use during a trace route.

In a traceroute the Time to Live must increment by 1 each time to effectively trace the route of the path from source to destination.

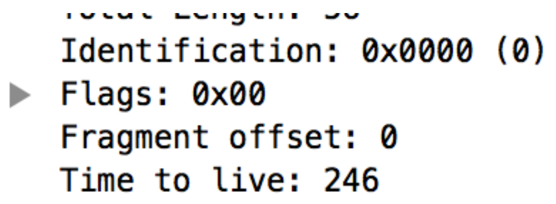
The Identification must change each new request, to ensure fresh data.

7. Describe the pattern you see in the values in the Identification field of the IP datagram. Next (with the packets still sorted by source address) find the series of ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router.

The Identification field in each IP datagram is incremented by 1.

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

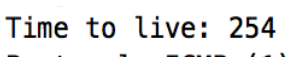
Identification Field: 0x0000
TTL field: 246



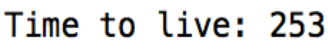
```
   Identification: 0x0000 (0)
▶  Flags: 0x00
   Fragment offset: 0
   Time to live: 246
```

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?

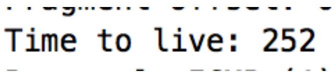
The Identification field is always 0x0000.
However, the TTL field uses a few different values. Either 246, 244, 252, 253 or 254
The TTL exceeding response does not need an identification code, because it is the end of the transaction between the router and the host. The identification field is valuable if data is being sent that may need reference.
The TTL field differs based on the router that is sending the TTL-exceeded message. I imagine the TTL is adjusted to ensure the message can reach it the original sender without being dropped.



```
Time to live: 254
```



```
Time to live: 253
```

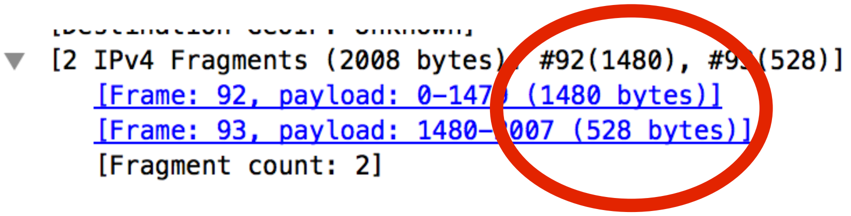


```
Time to live: 252
```

Sort the packet listing according to time again by clicking on the Time column.

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?

Yes, it has. The first payload is 1480 bytes and the second is 528 bytes.



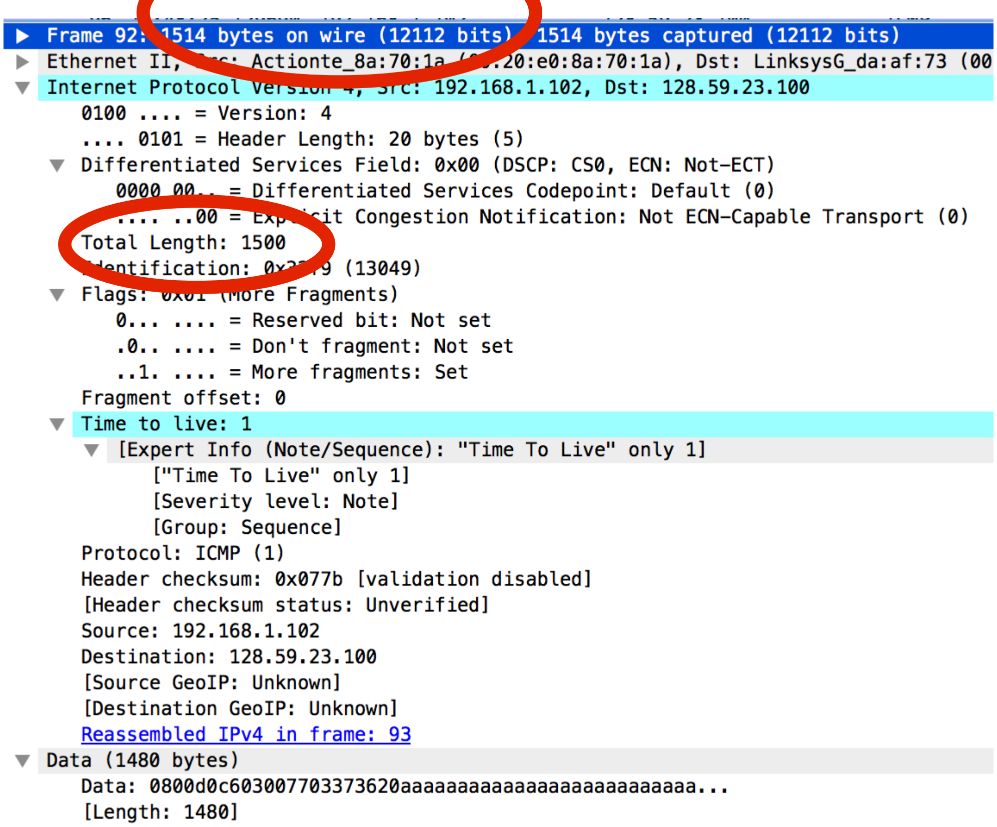
```
  [Destination GeoIP: Unknown]
▼ [2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
      [Frame: 92, payload: 0-1479 (1480 bytes)]
      [Frame: 93, payload: 1480-2007 (528 bytes)]
      [Fragment count: 2]
```

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?

The More Fragments Flag has been set, which means the node should expect more fragments to follow.

The Fragment Offset of the first fragment is set to 0, which tells the receiver that this is the first fragment.

This IP Datagram reads 1500 in the Total Length field. However, in the Frame portion of the details window, it reads “1514 bytes on the wire.”

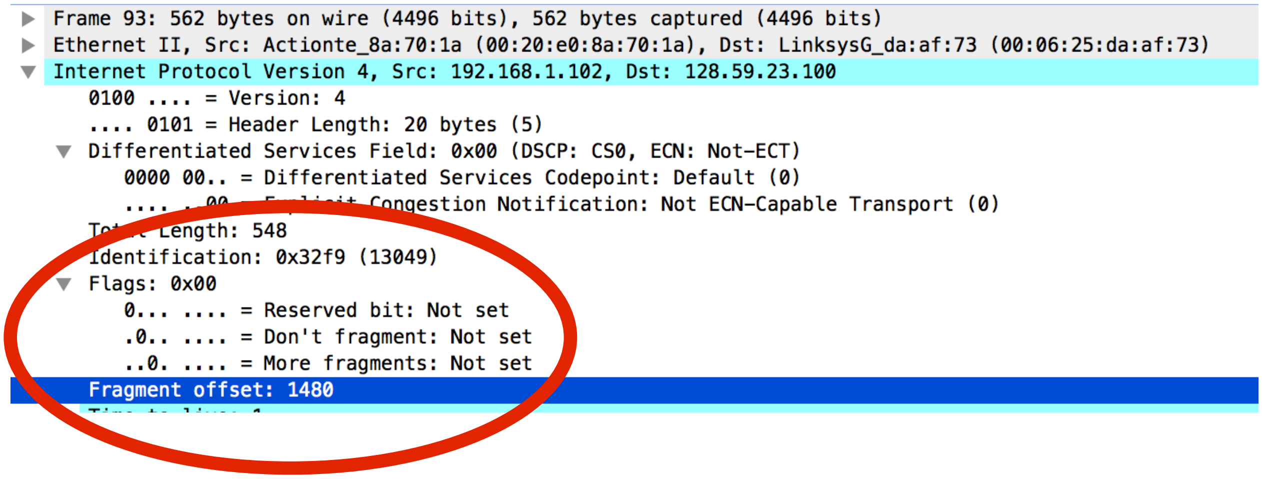


```
▶ Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
▶ Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00
▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
     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
      ▼ [Expert Info (Note/Sequence): "Time To Live" only 1]
           ["Time To Live" only 1]
           [Severity level: Note]
           [Group: Sequence]
     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
▼ Data (1480 bytes)
     Data: 0800d0c603007703373620aaaaaaaaaaaaaaaaaaaaaaaaa...
     [Length: 1480]
```

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?

The Fragment Offset of 1480 indicates this is not the first fragment in the datagram.

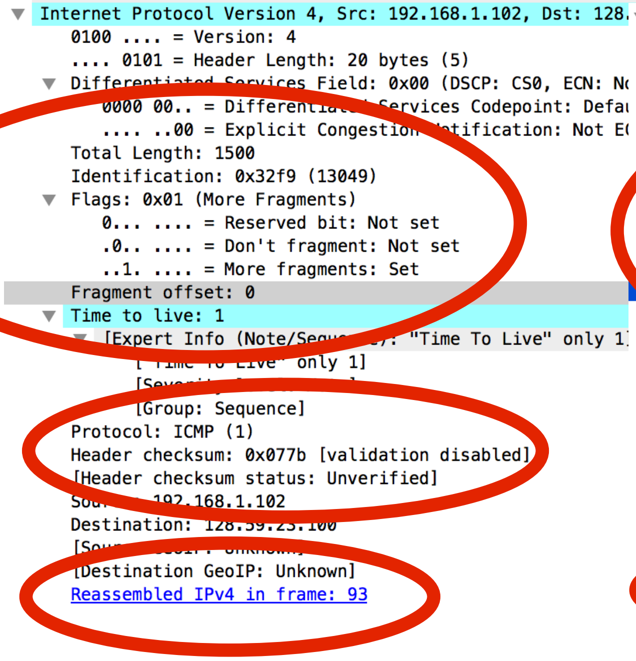
No, there are no more fragments to be expected. The receiver can expect no more fragments as shown by the More Fragments flag set to zero.



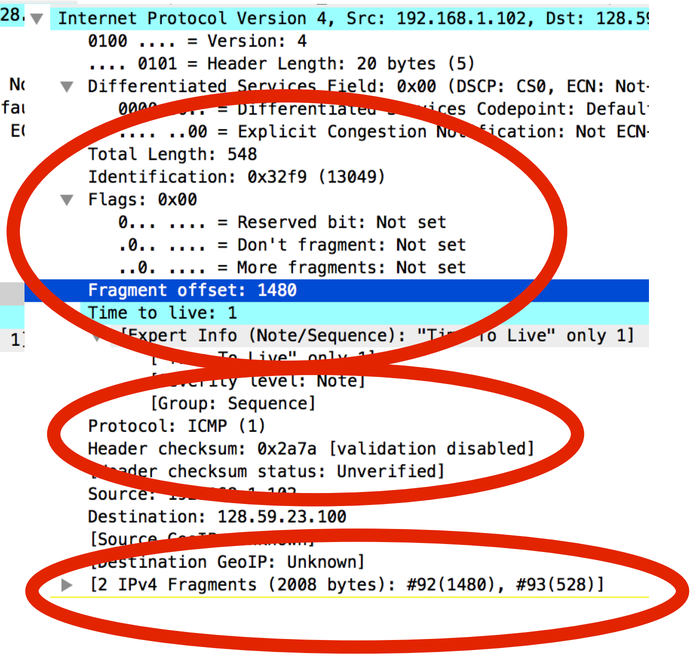
```
▶ Frame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
▶ Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
     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
```

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

- Header Checksum
- Flags field, specifically the “More fragments”
- Fragment Offset field
- Total Length
- Fragment listing field - drills down to list of fragments



```
▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: No
        0000 00.. = Differentiated Services Codepoint: Defau
        .... ..00 = Explicit Congestion Notification: Not E
     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
      ▼ [Expert Info (Note/Sequence): "Time To Live" only 1]
           ["Time To Live" only 1]
           [Severity level: Note]
           [Group: Sequence]
     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
```



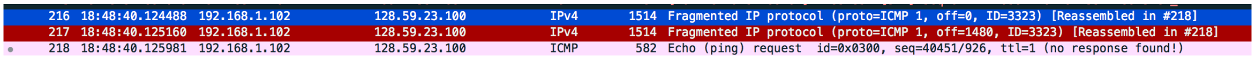
```
▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.5
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-
        0000 00.. = Differentiated Services Codepoint: Default
        .... ..00 = Explicit Congestion Notification: Not ECN-
     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]
           ["Time To Live" only 1]
           [Severity level: Note]
           [Group: Sequence]
     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)]
```

Vijay Kumar Lab 4 Lab Completed using ip-ethereal-trace-1 from lab

Now find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 3500.

14. How many fragments were created from the original datagram?

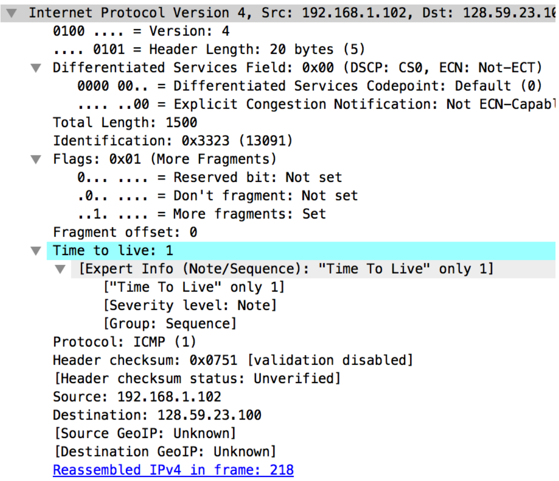
- 3 Fragments



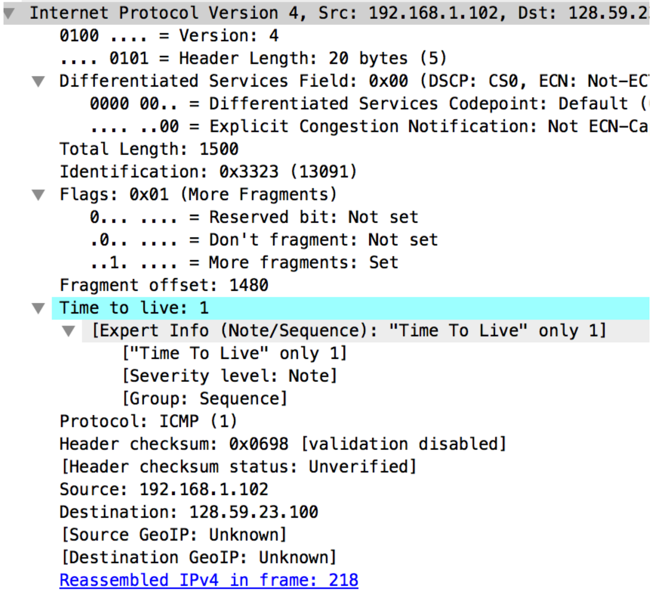
```
   216  18:48:40.124488  192.168.1.102     128.59.23.100     IPv4      1514  Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
   217  18:48:40.125160  192.168.1.102     128.59.23.100     IPv4      1514  Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
•  218  18:48:40.125981  192.168.1.102     128.59.23.100     ICMP       582  Echo (ping) request  id=0x0300, seq=40451/926, ttl=1 (no response found!)
```

15. What fields change in the IP header among the fragments?

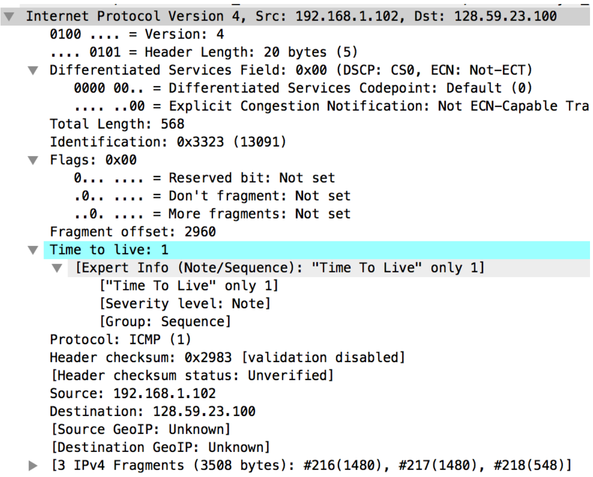
- Header Checksum
- Flags field, specifically the “More fragments”
- Fragment Offset field
- Total Length
- Fragment listing field - drills down to list of fragments



```
▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.1(
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capabl
    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
    ▼ [Expert Info (Note/Sequence): "Time To Live" only 1]
        ["Time To Live" only 1]
        [Severity level: Note]
        [Group: Sequence]
    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
```



```
▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-EC
      0000 00.. = Differentiated Services Codepoint: Default (
      .... ..00 = Explicit Congestion Notification: Not ECN-Ca
    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: 1480
  ▼ Time to live: 1
    ▼ [Expert Info (Note/Sequence): "Time To Live" only 1]
        ["Time To Live" only 1]
        [Severity level: Note]
        [Group: Sequence]
    Protocol: ICMP (1)
    Header checksum: 0x0698 [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
```



```
▼ 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)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Tra
    Total Length: 568
    Identification: 0x3323 (13091)
  ▼ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 2960
  ▼ Time to live: 1
    ▼ [Expert Info (Note/Sequence): "Time To Live" only 1]
        ["Time To Live" only 1]
        [Severity level: Note]
        [Group: Sequence]
    Protocol: ICMP (1)
    Header checksum: 0x2983 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ▶ [3 IPv4 Fragments (3508 bytes): #216(1480), #217(1480), #218(548)]
```