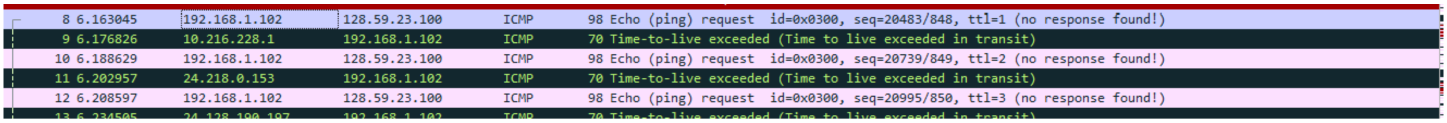
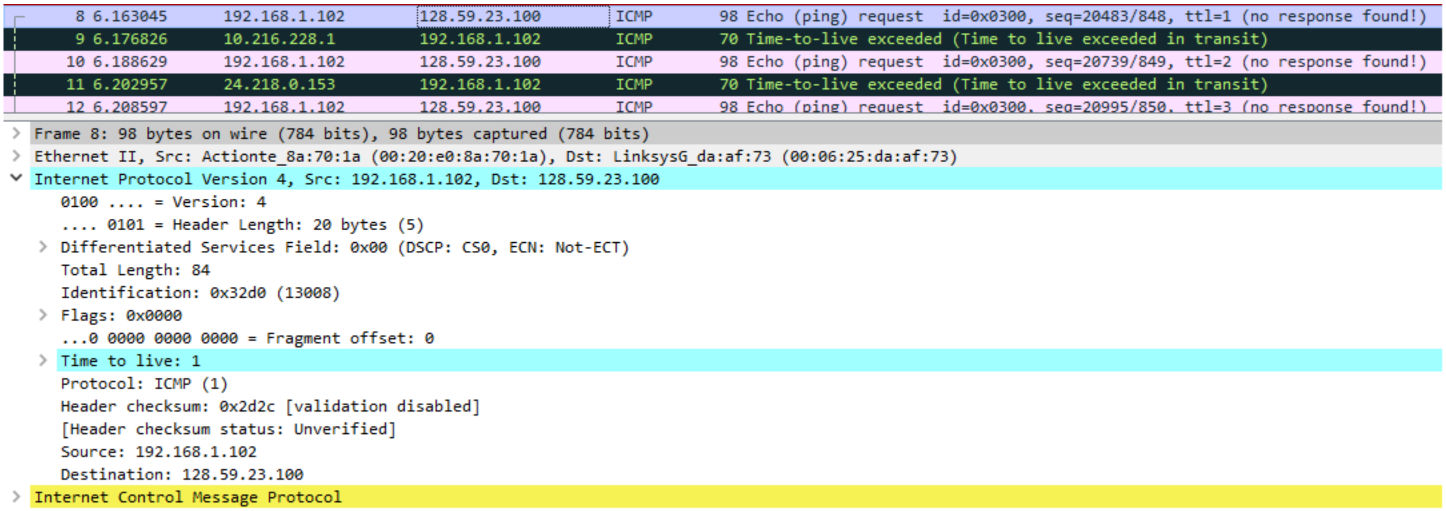
1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?



```
  8 6.163045   192.168.1.102   128.59.23.100   ICMP   98 Echo (ping) request  id=0x0300, seq=20483/848, ttl=1 (no response found!)
  9 6.176826   10.216.228.1    192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
 10 6.188629   192.168.1.102   128.59.23.100   ICMP   98 Echo (ping) request  id=0x0300, seq=20739/849, ttl=2 (no response found!)
 11 6.202957   24.218.0.153    192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
 12 6.208597   192.168.1.102   128.59.23.100   ICMP   98 Echo (ping) request  id=0x0300, seq=20995/850, ttl=3 (no response found!)
 13 6.234505   24.128.190.197  192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
```

192.168.1.102

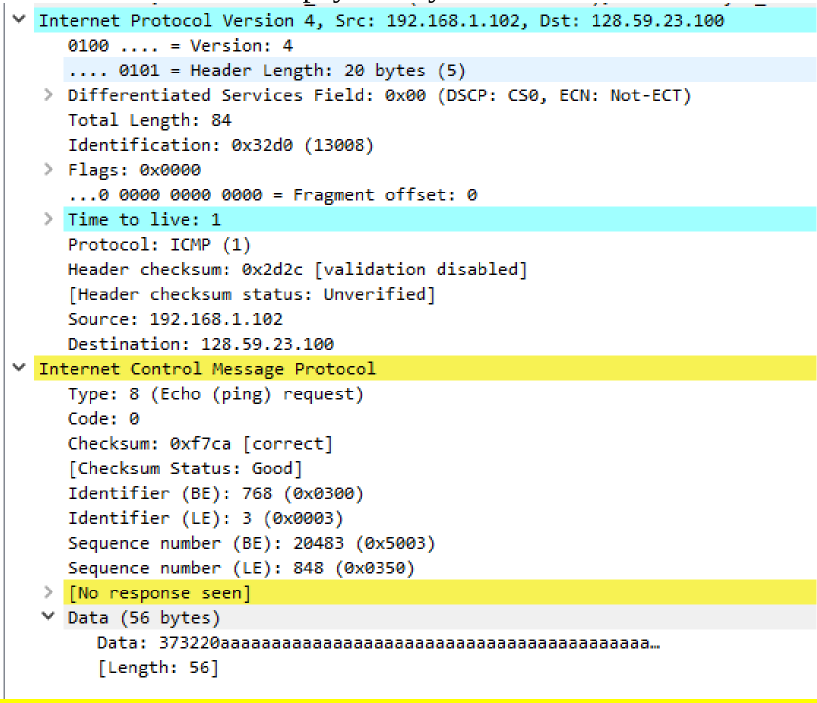
2. Within the IP packet header, what is the value in the upper layer protocol field?



```
  8 6.163045   192.168.1.102   128.59.23.100   ICMP   98 Echo (ping) request  id=0x0300, seq=20483/848, ttl=1 (no response found!)
  9 6.176826   10.216.228.1    192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
 10 6.188629   192.168.1.102   128.59.23.100   ICMP   98 Echo (ping) request  id=0x0300, seq=20739/849, ttl=2 (no response found!)
 11 6.202957   24.218.0.153    192.168.1.102   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
 12 6.208597   192.168.1.102   128.59.23.100   ICMP   98 Echo (ping) request  id=0x0300, seq=20995/850, ttl=3 (no response found!)
> 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: 0x0000
    ...0 0000 0000 0000 = 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
> Internet Control Message Protocol
```

ICMP : Internet control message protocol

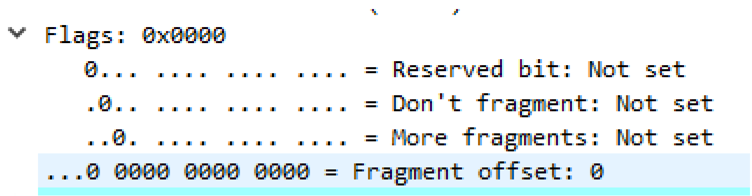
3. How many bytes are in the IP header? How many bytes are in the payload *of the IP datagram*? Explain how you determined the number of payload bytes.



```
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: 0x0000
    ...0 0000 0000 0000 = 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
v 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]
  v Data (56 bytes)
      Data: 373220aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa…
      [Length: 56]
```

The IP header is 20 bytes, total length 56 bytes, so payload is 56 – 20 = 36 bytes

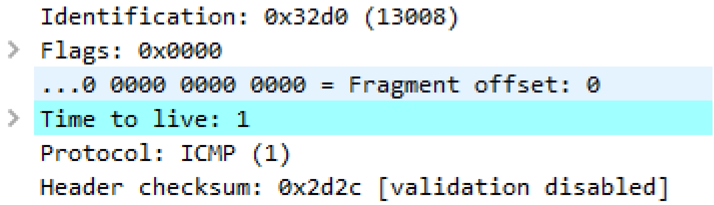
4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.



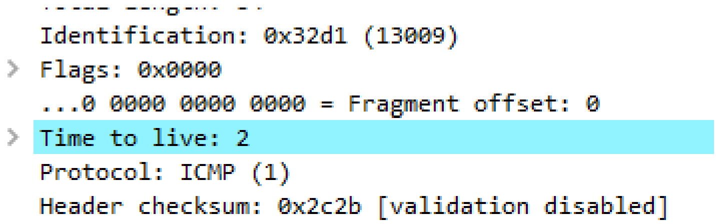
```
  Flags: 0x0000
    0... .... .... .... = Reserved bit: Not set
    .0.. .... .... .... = Don't fragment: Not set
    ..0. .... .... .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment offset: 0
```

Fragment offset is zero, therefore it has not been fragmented

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: 0x32d0 (13008)
> Flags: 0x0000
  ...0 0000 0000 0000 = Fragment offset: 0
> Time to live: 1
  Protocol: ICMP (1)
  Header checksum: 0x2d2c [validation disabled]
```



```
  Identification: 0x32d1 (13009)
> Flags: 0x0000
  ...0 0000 0000 0000 = Fragment offset: 0
> Time to live: 2
  Protocol: ICMP (1)
  Header checksum: 0x2c2b [validation disabled]
```

Identification, Time to live, Header checksum

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

Fields that must change are Identification, Time to live, Header checksum

Identification because each IP packet must have unique ids

Time to live because each subsequent packet's time to live field is incremented by tracerouter

Header checksum since header change, so does header checksum

Fields that must stay constant are:

Source IP because packet's send from same host

Destination IP because each packet send to same destination

Header length because we are using ICMP

Version because each packet uses IPv4

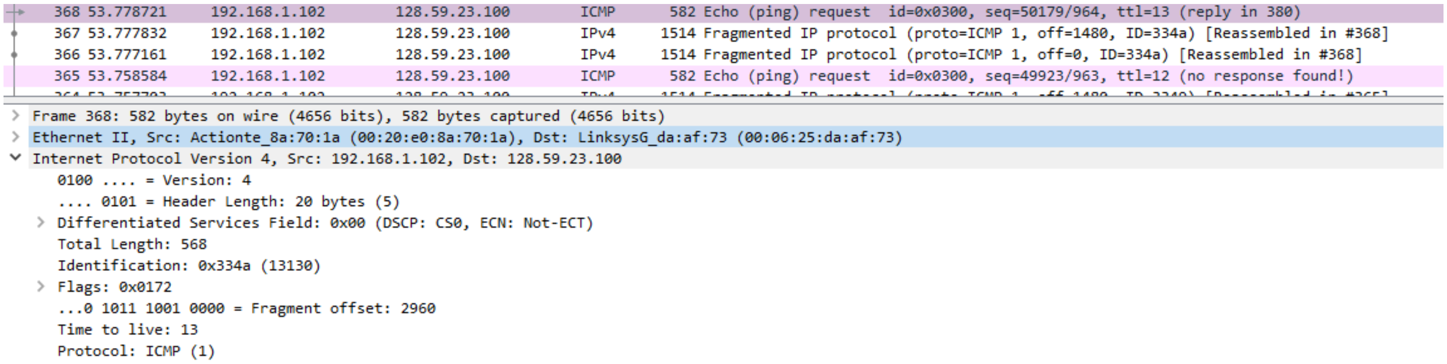
Upper Layer Protocol because each packet is ICMP

Differentiated Services because each packet uses same type of service class

7. Describe the pattern you see in the values in the Identification field of the IP Datagram

With each ICMP ping, identification field of IP header is incremented

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



```
368 53.778721   192.168.1.102   128.59.23.100   ICMP   582 Echo (ping) request  id=0x0300, seq=50179/964, ttl=13 (reply in 380)
367 53.777832   192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334a) [Reassembled in #368]
366 53.777161   192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=334a) [Reassembled in #368]
365 53.758584   192.168.1.102   128.59.23.100   ICMP   582 Echo (ping) request  id=0x0300, seq=49923/963, ttl=12 (no response found!)
364 53.757703   192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3349) [Reassembled in #365]
> Frame 368: 582 bytes on wire (4656 bits), 582 bytes captured (4656 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: 568
    Identification: 0x334a (13130)
  > Flags: 0x0172
    ...0 1011 1001 0000 = Fragment offset: 2960
    Time to live: 13
    Protocol: ICMP (1)
```

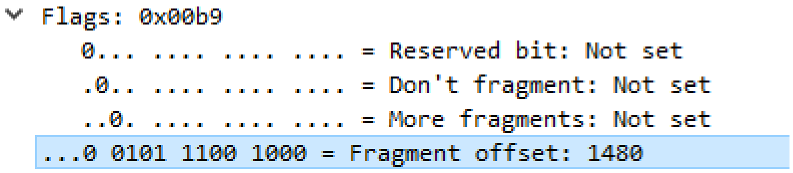
Identification field: 13130 (0x334a)

Time to live: 13

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?

Identification field changes because it is unique value. However time to live does not changes because time to live for first hop router is constant

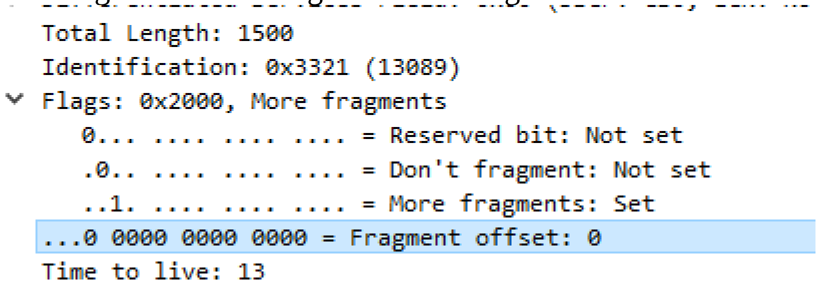
10. Find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 2000. Has that message been fragmented across more than one IP datagram?



```
v Flags: 0x00b9
    0... .... .... .... = Reserved bit: Not set
    .0.. .... .... .... = Don't fragment: Not set
    ..0. .... .... .... = More fragments: Not set
  ...0 0101 1100 1000 = Fragment offset: 1480
```

Since Fragment offset is not zero, It has been fragmented across more than one IP datagram

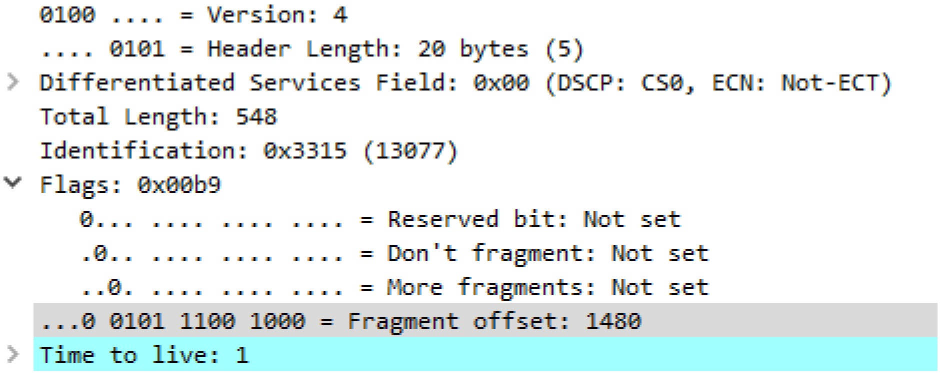
11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?



```
  Total Length: 1500
  Identification: 0x3321 (13089)
v Flags: 0x2000, More fragments
    0... .... .... .... = Reserved bit: Not set
    .0.. .... .... .... = Don't fragment: Not set
    ..1. .... .... .... = More fragments: Set
  ...0 0000 0000 0000 = Fragment offset: 0
  Time to live: 13
```

Since More fragments is set, it means that datagram has been fragmented. Because Fragment offset is equal to 0, it is first fragment. IP datagram is 1500 bytes long including header.

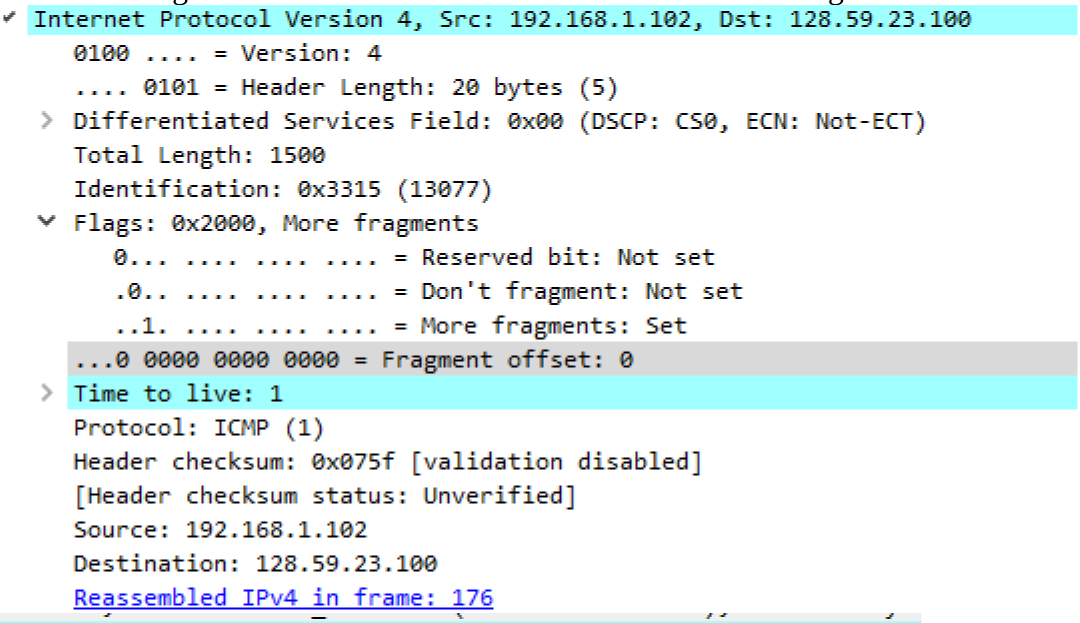
12. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?



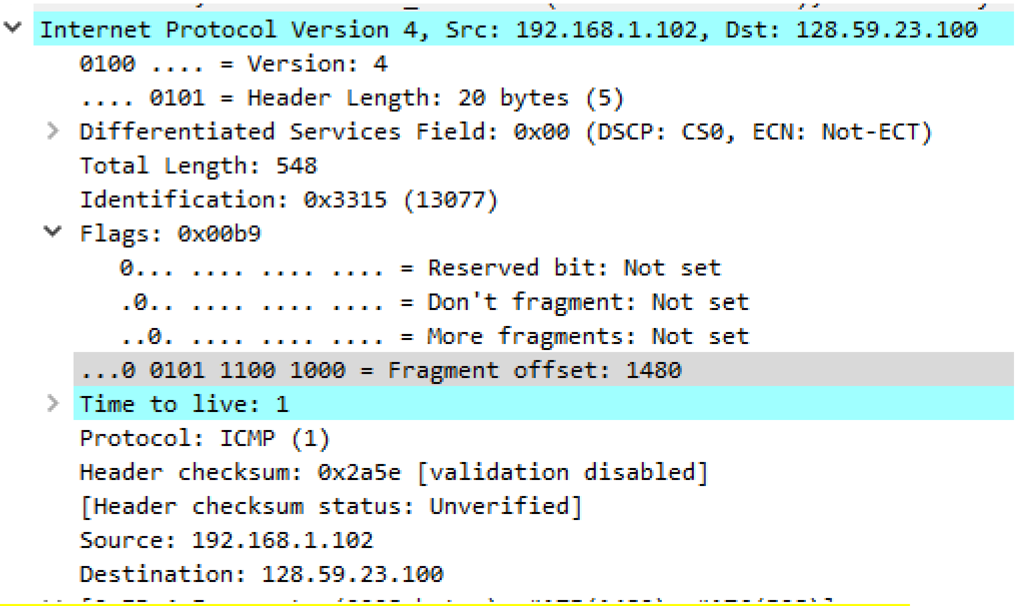
```
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 548
  Identification: 0x3315 (13077)
v Flags: 0x00b9
    0... .... .... .... = Reserved bit: Not set
    .0.. .... .... .... = Don't fragment: Not set
    ..0. .... .... .... = More fragments: Not set
  ...0 0101 1100 1000 = Fragment offset: 1480
> Time to live: 1
```

Since fragment offset is not 0, it is different fragment, not first. Because more fragments flag is not set, it means it is last fragment;

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



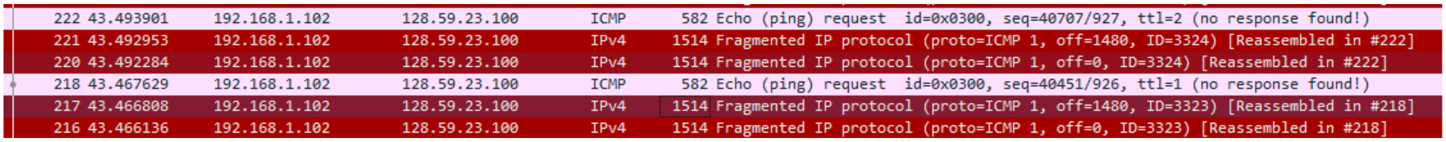
```
✔ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x3315 (13077)
  ⌄ Flags: 0x2000, More fragments
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..1. .... .... .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x075f [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    Reassembled IPv4 in frame: 176
```



```
⌄ 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: 0x3315 (13077)
  ⌄ Flags: 0x00b9
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..0. .... .... .... = More fragments: Not set
    ...0 0101 1100 1000 = Fragment offset: 1480
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x2a5e [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
```

Fields changes: Total length, Flags, Fragment offset, Header checksum

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



```
222 43.493901   192.168.1.102   128.59.23.100   ICMP    582 Echo (ping) request  id=0x0300, seq=40707/927, ttl=2 (no response found!)
221 43.492953   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled in #222]
220 43.492284   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
218 43.467629   192.168.1.102   128.59.23.100   ICMP    582 Echo (ping) request  id=0x0300, seq=40451/926, ttl=1 (no response found!)
217 43.466808   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
216 43.466136   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
```

Three

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

All three packets have different fragment offset and checksum. First and second fragments have same total length and more fragments set whereas last fragment have different total length and more fragments set off