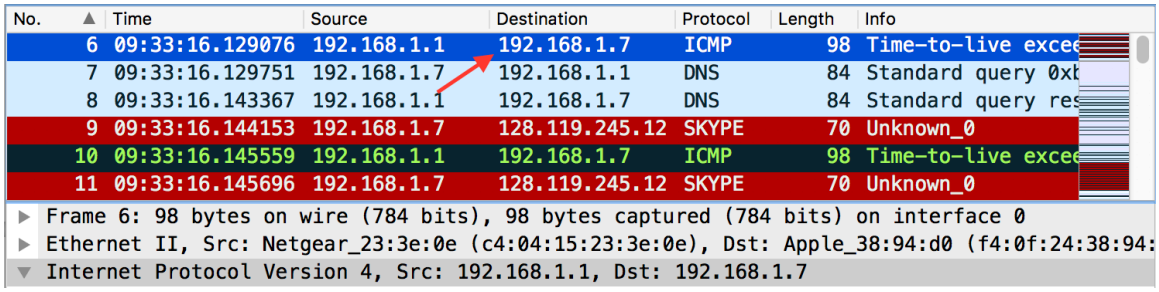
Class: CS-372
Term: Fall 2017
Author: Jon-Eric Cook
Date: November 19, 2017
Lab: #4

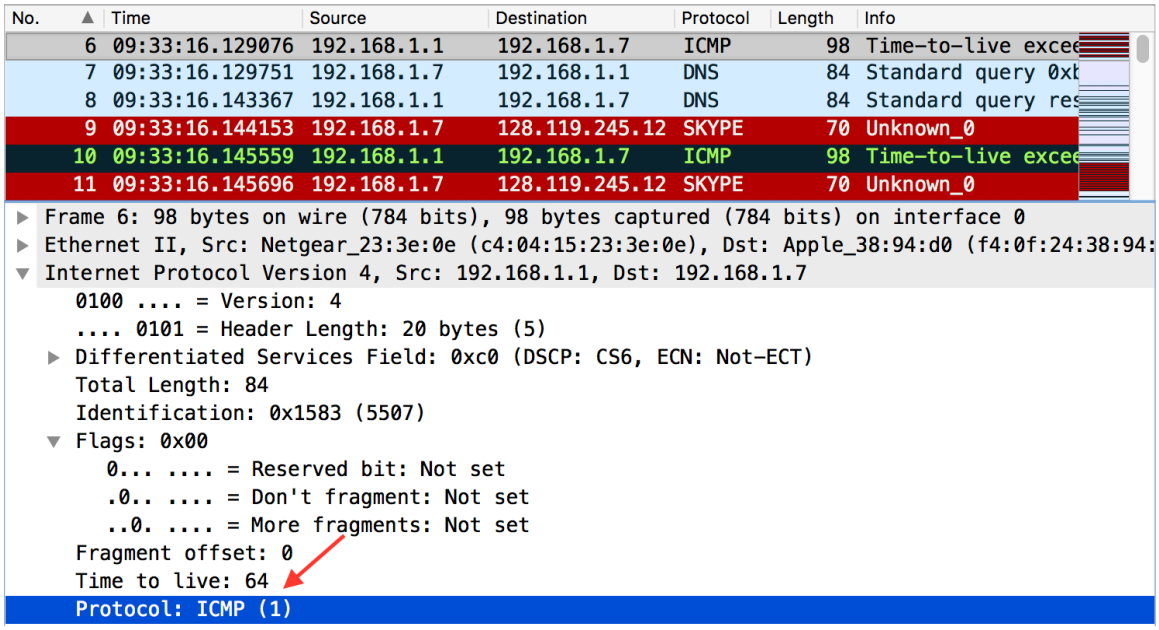
1) What is the IP address of your computer?

Answer:
192.168.1.7
See screenshot below.



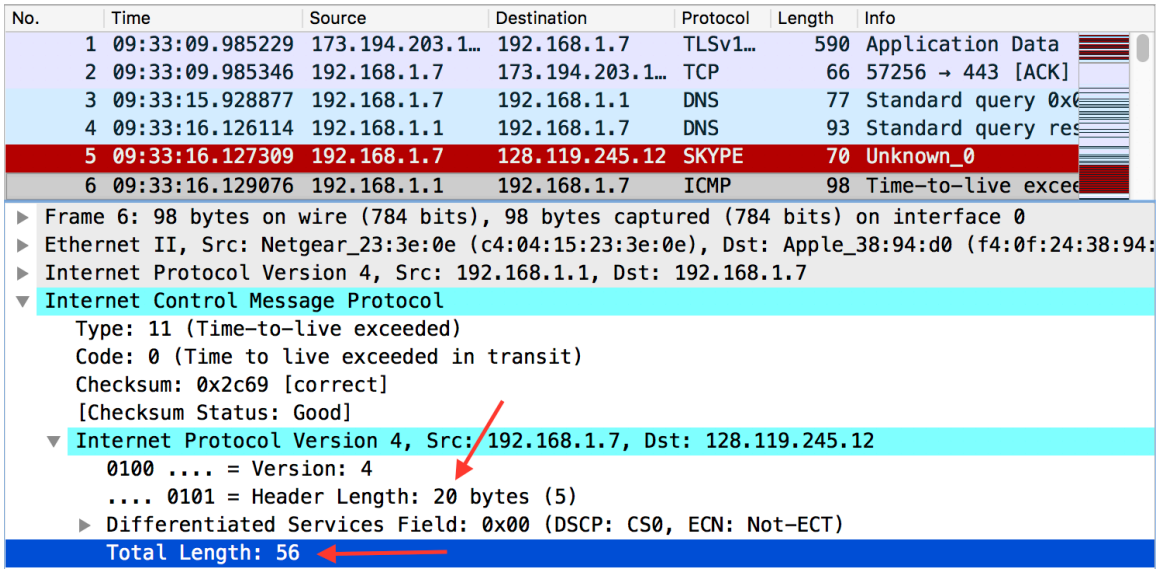
2) Within the IP packet header, what is the value in the upper layer protocol field?

Answer:
ICMP (1)
See screenshot below.



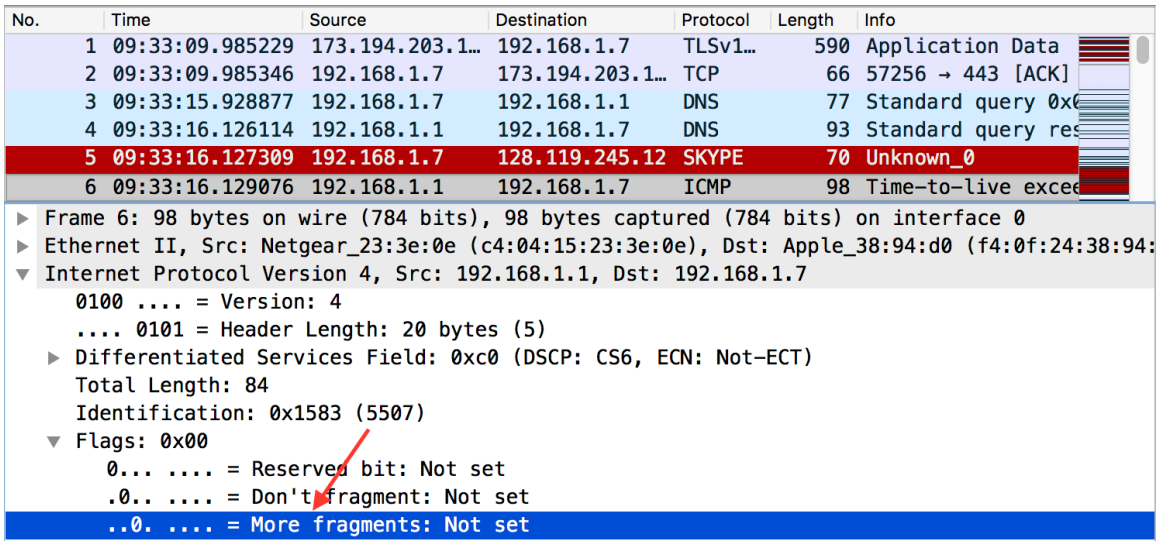
3) How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

Answer:
Bytes in IP header: 20
Bytes in payload of IP datagram: 36
Explanation: total length of 56 bytes minus header of 20 bytes equals 36 bytes
See screenshot below.



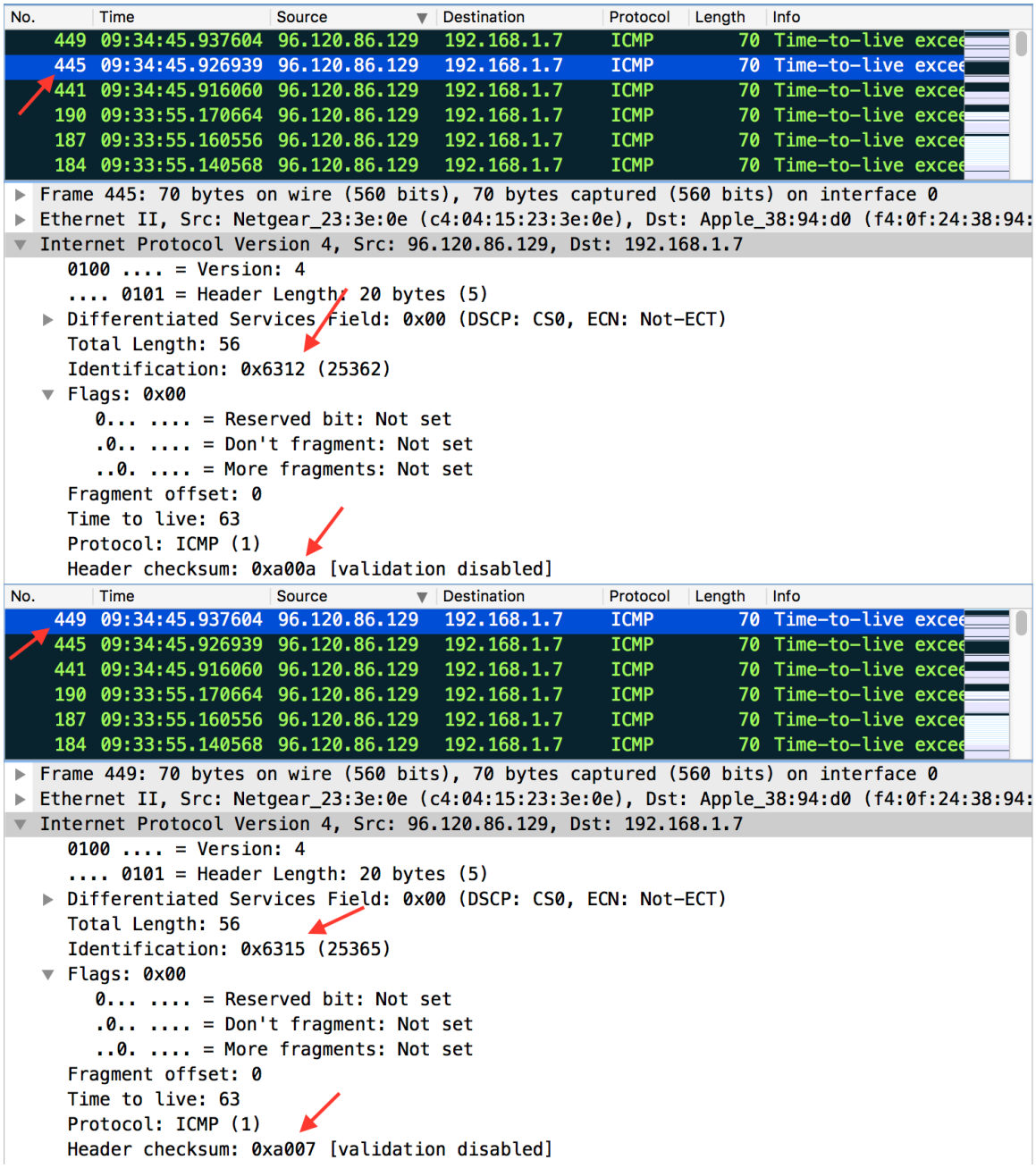
4) Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

Answer:
No
The more fragments bit is not set.
See screenshot below.



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?

Answer:
Identification and Header checksum
See screenshots below.



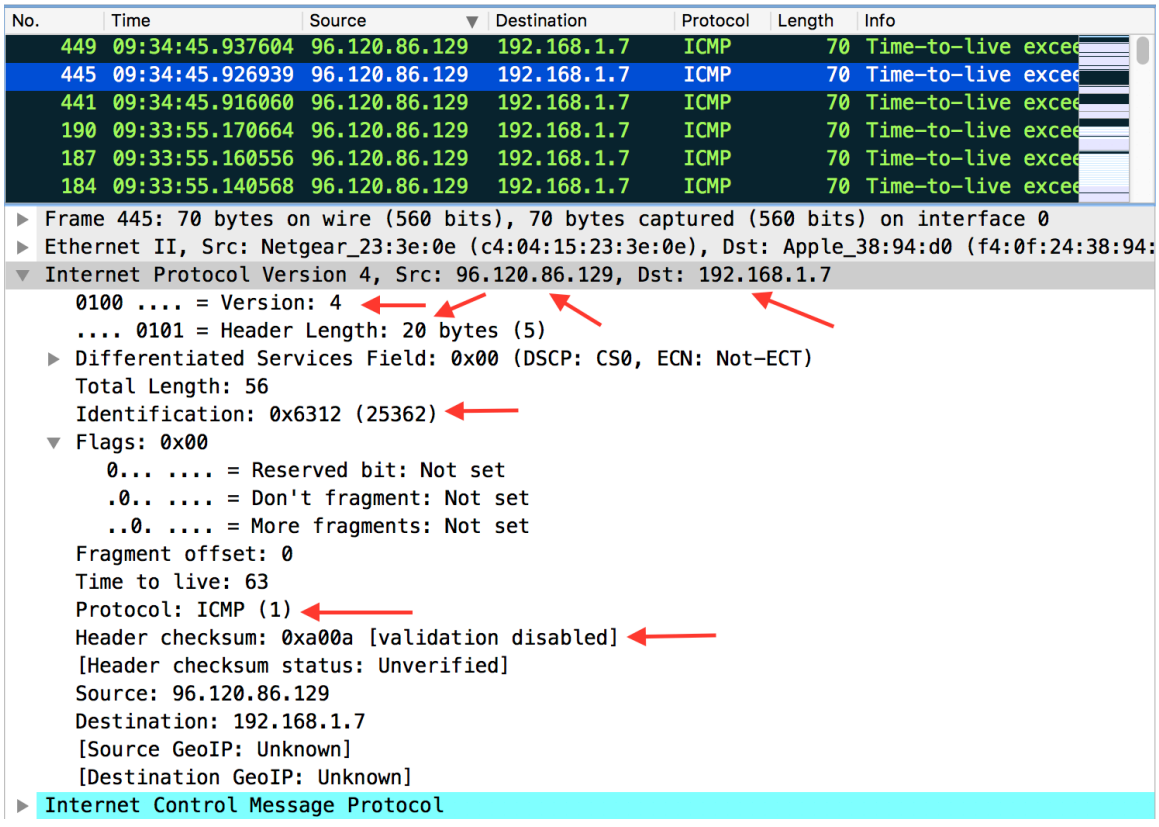
6) Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

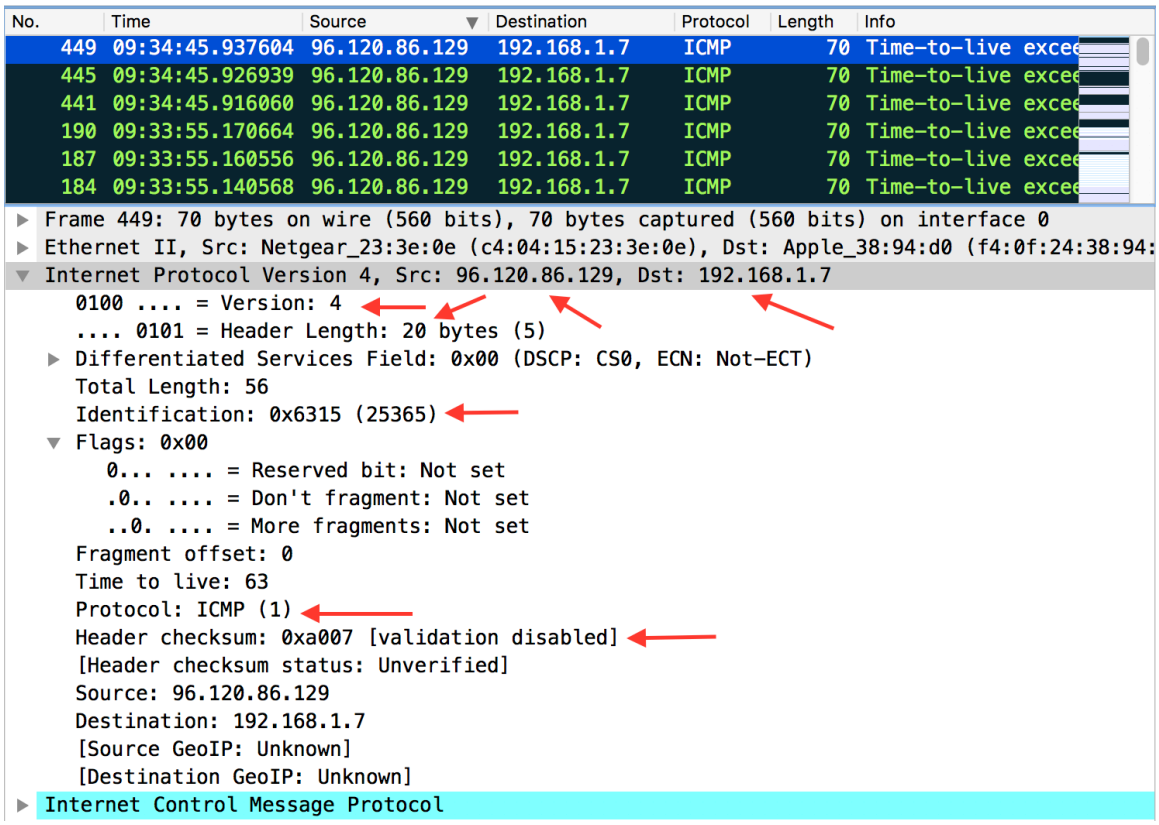
Answer:
Stays constant:
- Version (using IPv4 for all packets)
- Length of header (because of ICMP packets)
- Source IP (sending from the same source)
- Destination IP (sending to the same destination)
- Upper layer protocol (ICMP)
- Differentiated Services (all packets are ICMP, use same type of service)

Must stay constant:
- Version (IPv4) (use the same version for each datagram)
- Length of header (have the length of each datagram be the same)
- Source IP (send the datagram from the same location)
- Destination IP (send the datagram to the same destination)
- Upper layer protocol (ICMP) (use the same protocol)
- Differentiated Services (all packets are ICMP, use same type of service)

Must change:
- Header checksum (because the header being sent is different so there needs to be a different checksum to verify it)
- Identification (this needs to change as it identifies each packet being sent)

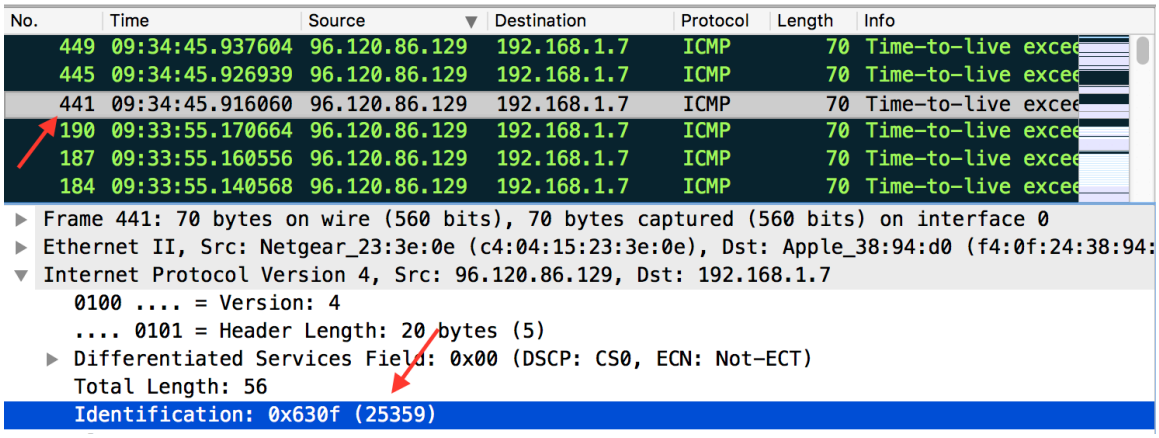
See screenshots below.

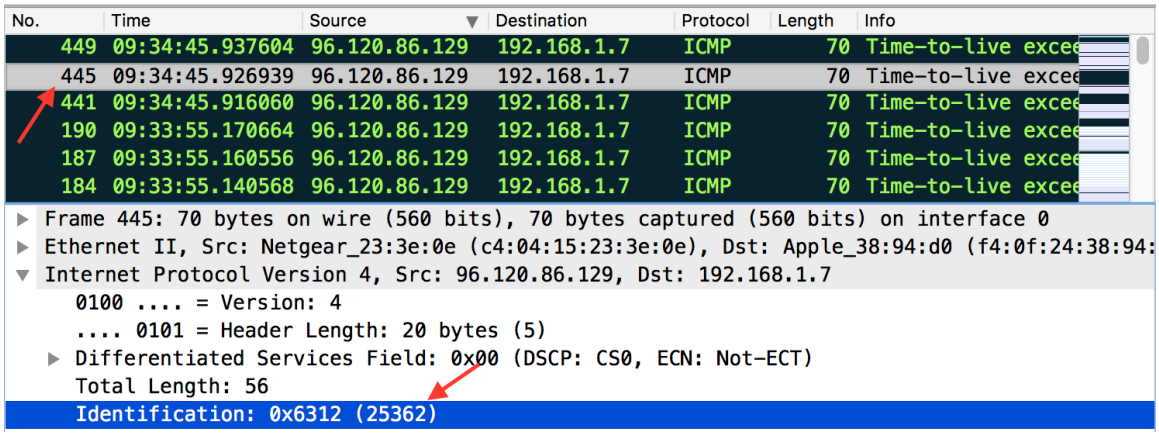




7) Describe the pattern you see in the values in the Identification field of the IP datagram.

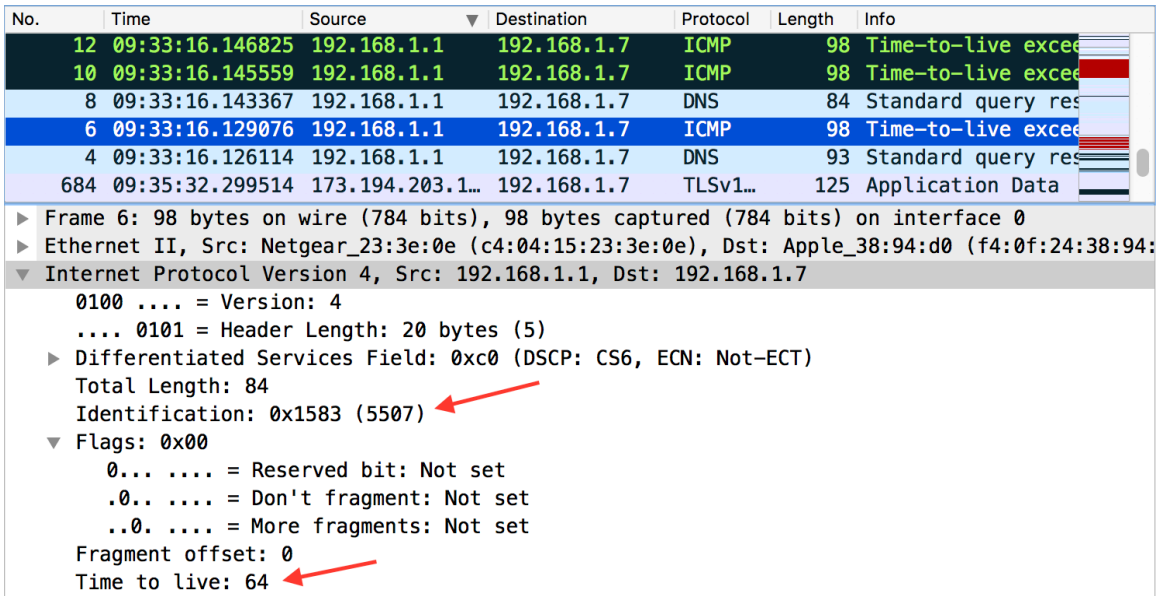
Answer:
It appears that the Identification field follows a pattern where the value is increased by one for each ICMP Echo request.
See the screenshot below.





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

Answer:
Identification: 5507
Time to live: 64
See screenshot below.



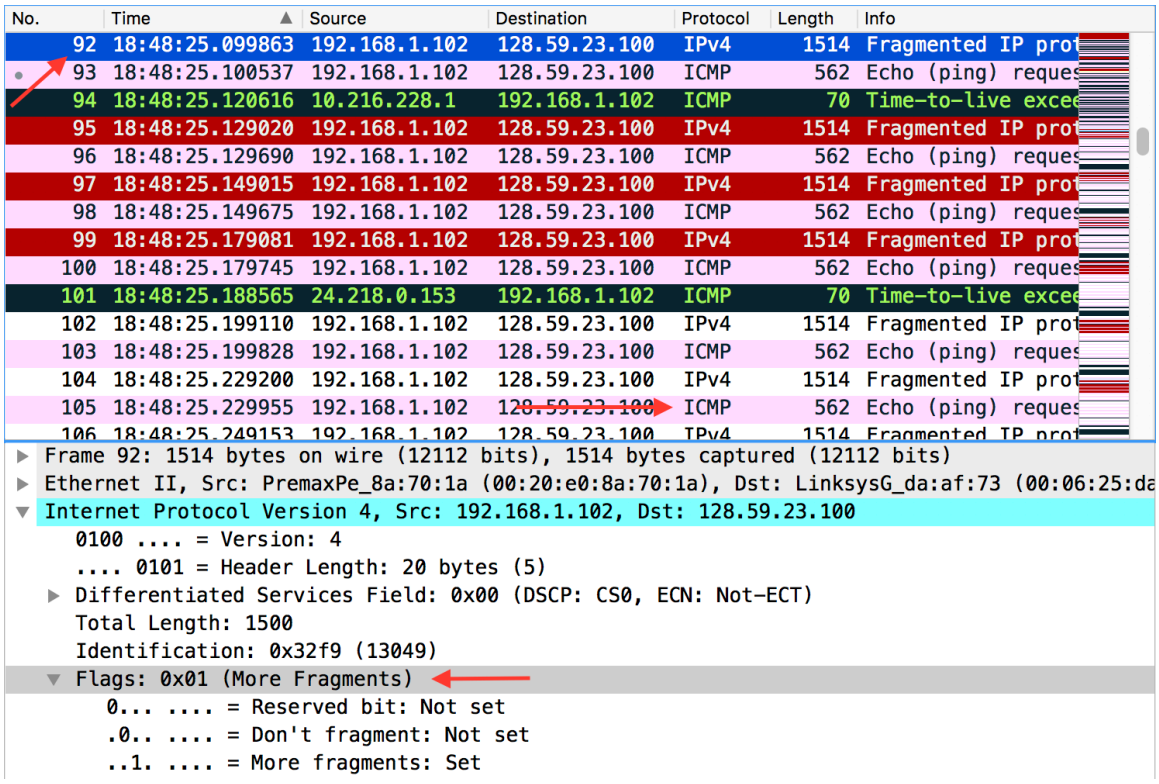
9) Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router Why?

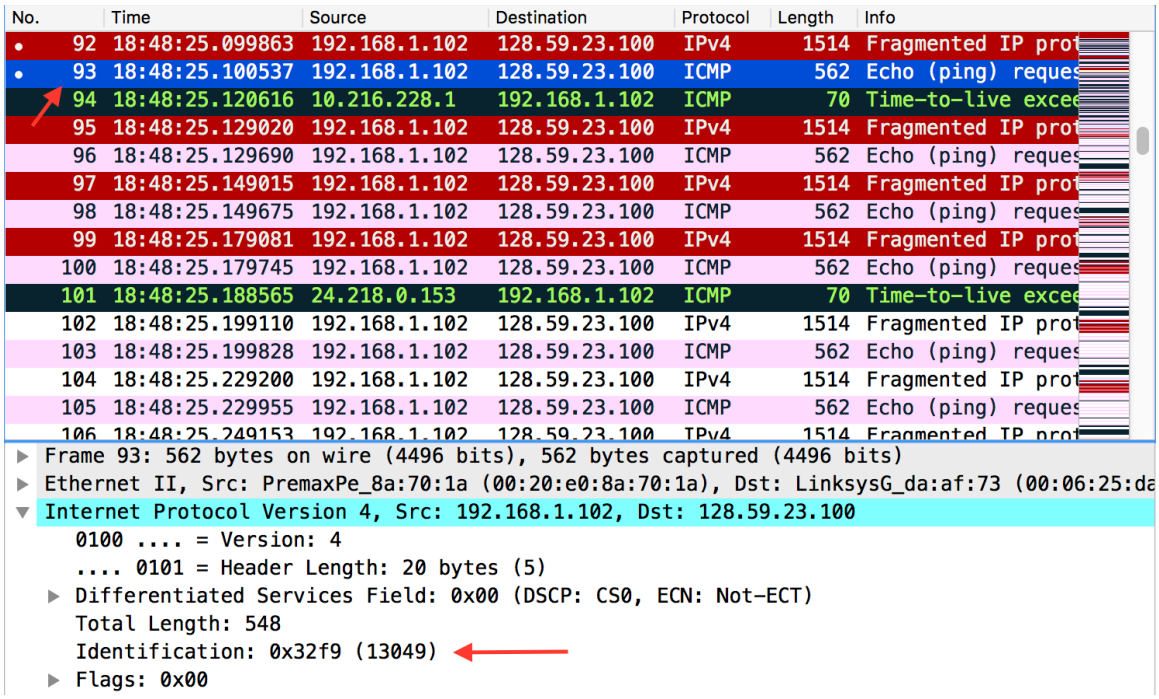
Answer:
No, the Identification field does change for all the ICMP TTL-exceeded replies. This is so because the Identification field is unique. If there were in fact two or more IP datagrams that had the same Identification value, this would mean that they are fragments of a single large IP datagram.
The TTL field remains unchanged because the TTL for the first hop router is always the same.

NOTE: For questions 10-15, I will be using the ip-ethereal-trace-1 packet from http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip

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?

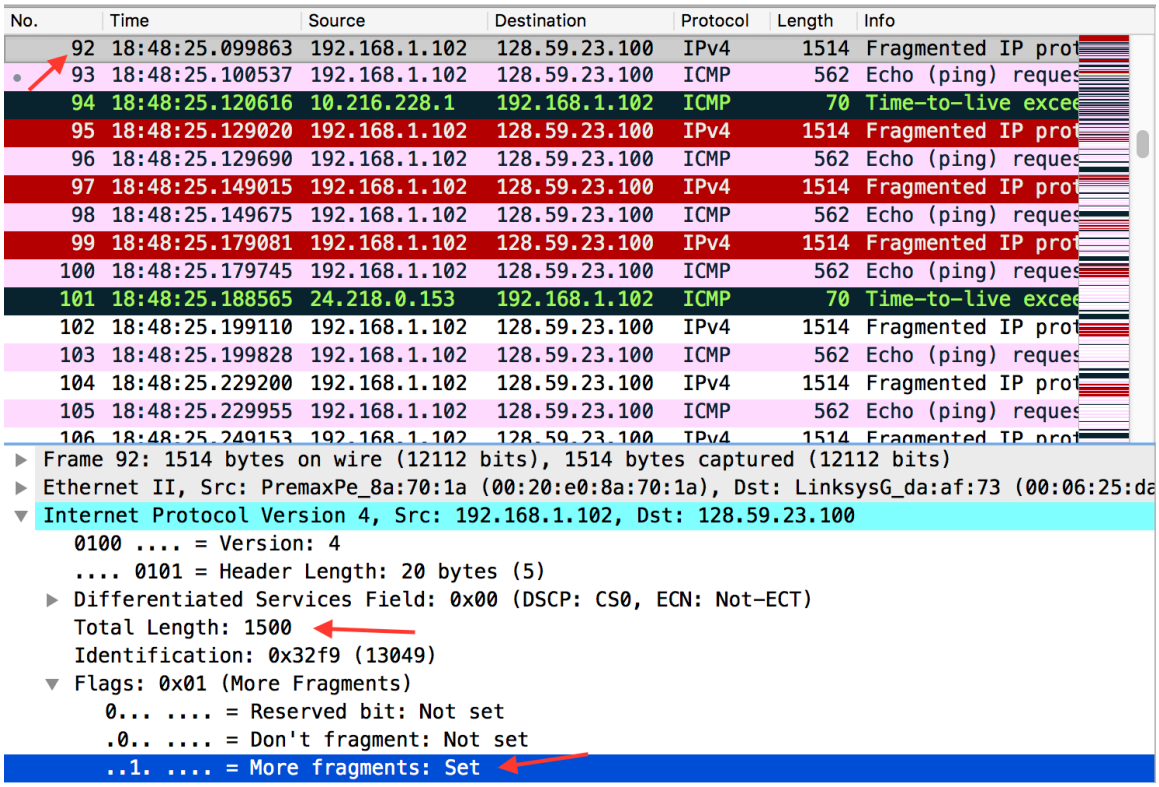
Answer:
Yes, the message has been fragmented across more than one IP datagram.
See screenshots below.




No. Time Source Destination Protocol Length Info
92 18:48:25.099863 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
93 18:48:25.100537 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) reques
94 18:48:25.120616 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live excee
95 18:48:25.129020 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
96 18:48:25.129690 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) reques
97 18:48:25.149015 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
98 18:48:25.149675 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) reques
99 18:48:25.179081 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
100 18:48:25.179745 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) reques
101 18:48:25.188565 24.218.0.153 192.168.1.102 ICMP 70 Time-to-live excee
102 18:48:25.199110 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
103 18:48:25.199828 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) reques
104 18:48:25.229200 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
105 18:48:25.229955 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) reques
106 18:48:25.249153 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
Frame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
Ethernet II, Src: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da
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

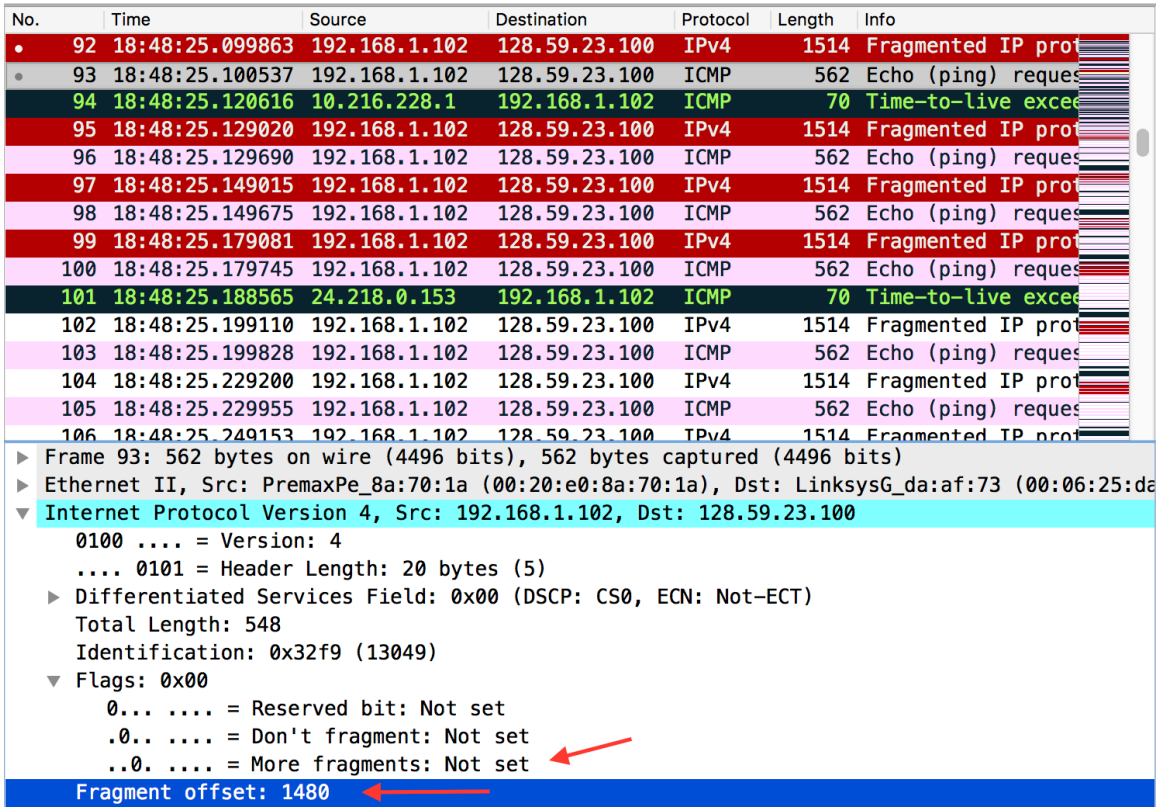
11) Screenshot the first fragmented IP datagram (with sufficient details to answer these questions). What information in the IP header indicates that the datagram has been fragmented? What information in the IP header indicates whether this is the first fragment of the fragment versus a letter fragment?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

Answer:
The Flags bit for more fragments is set. This indicates that the datagram has been fragmented. Also, because the fragment offset is set to 0, this tells us that this is the first fragment. The length of the first fragmented datagram is 1500, including the header.
See screenshot below.



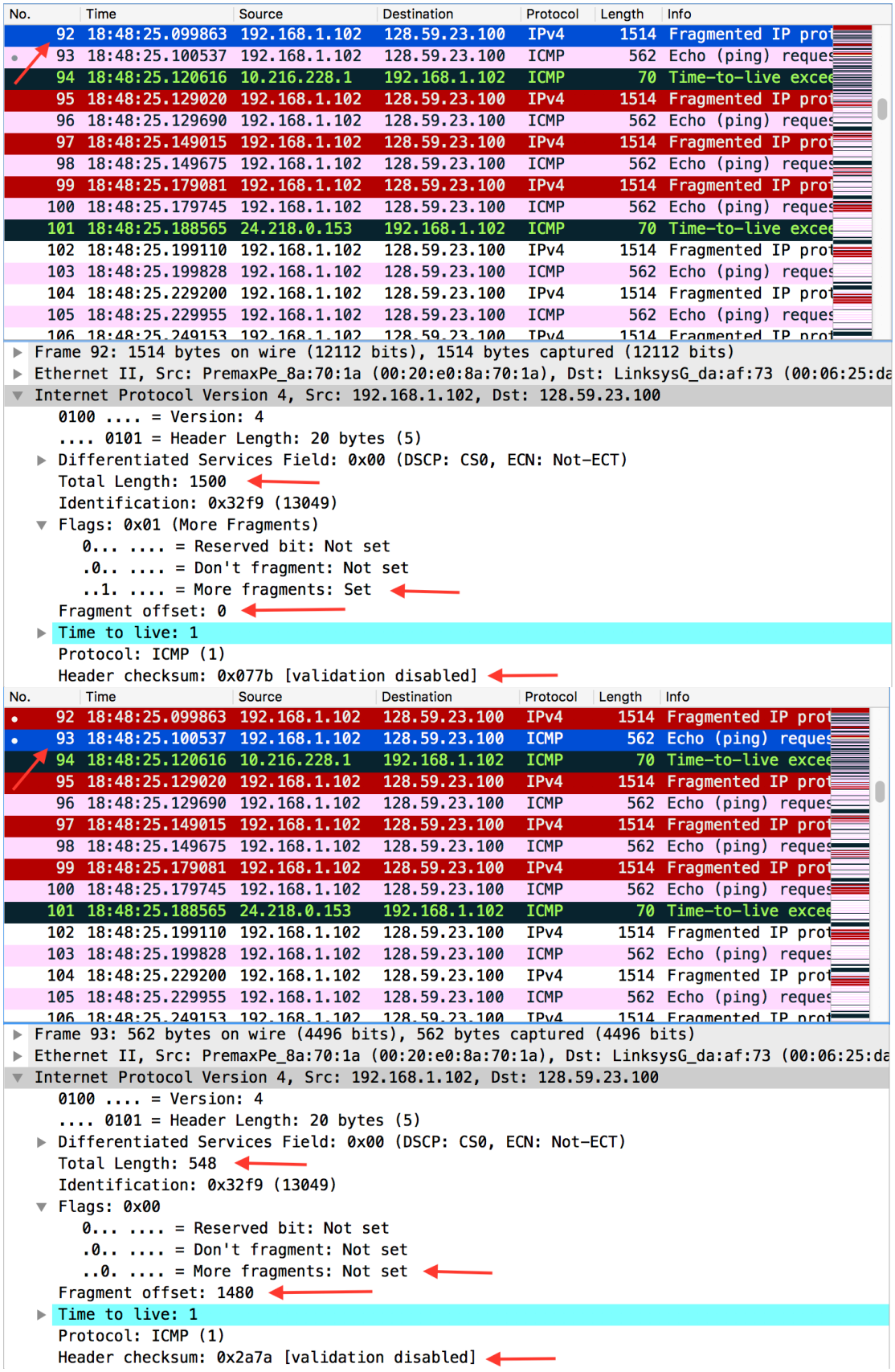
12) Screenshot the second fragmented IP datagram (with sufficient details to answer these questions). What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell?

Answer:
Seeing that the fragment offset is 1480, this indicates that this is not the first fragmented datagram. Also, it is the last fragment because the more fragments flag is not set.
See screenshot below.



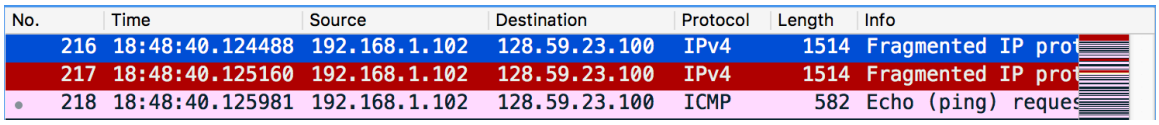
13) What fields change in the IP header between the first and second fragment?

Answer:
Total length, Flags, Fragment offset, Checksum
See screenshots below.



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

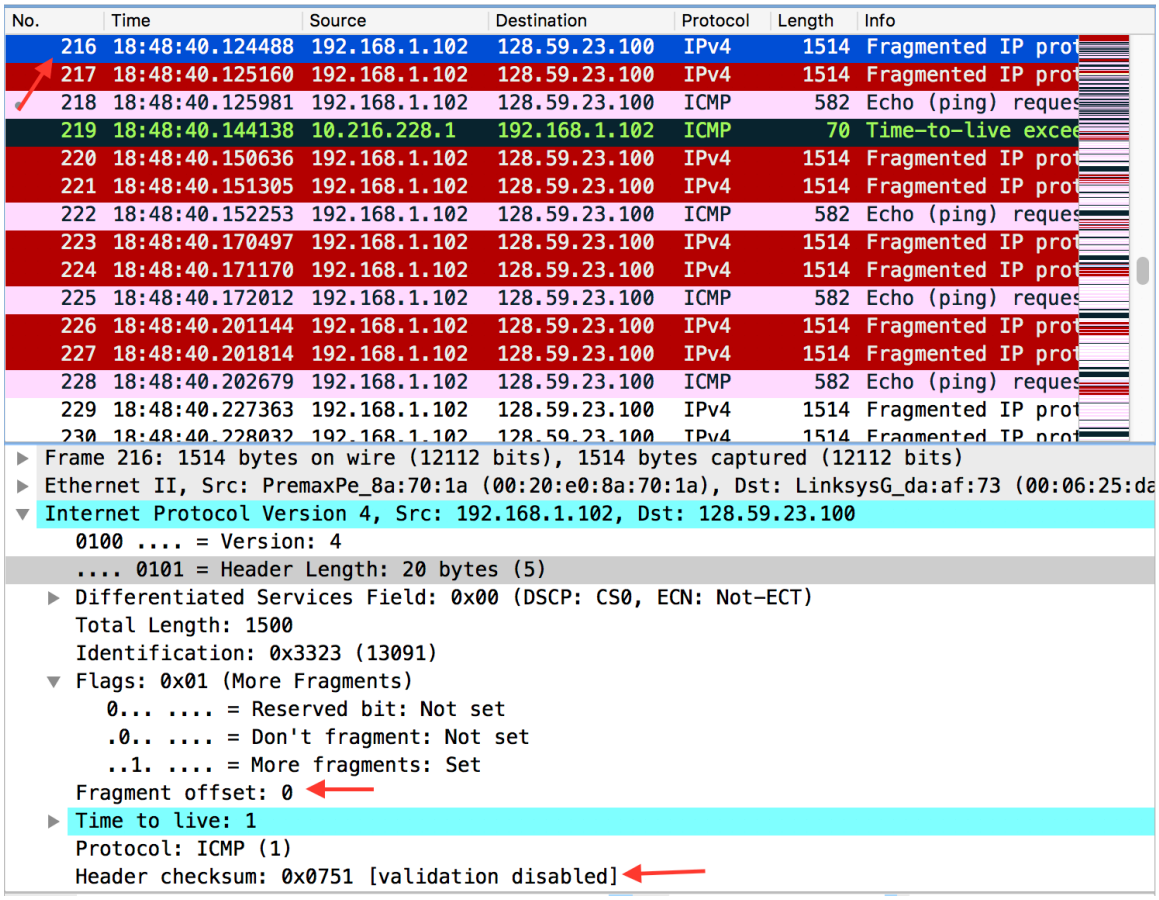
Answer:
3 fragments were created after changing to 3500 bytes
See screenshot below.



No.	Time	Source	Destination	Protocol	Length	Info
216	18:48:40.124488	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
217	18:48:40.125160	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
218	18:48:40.125981	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) reques

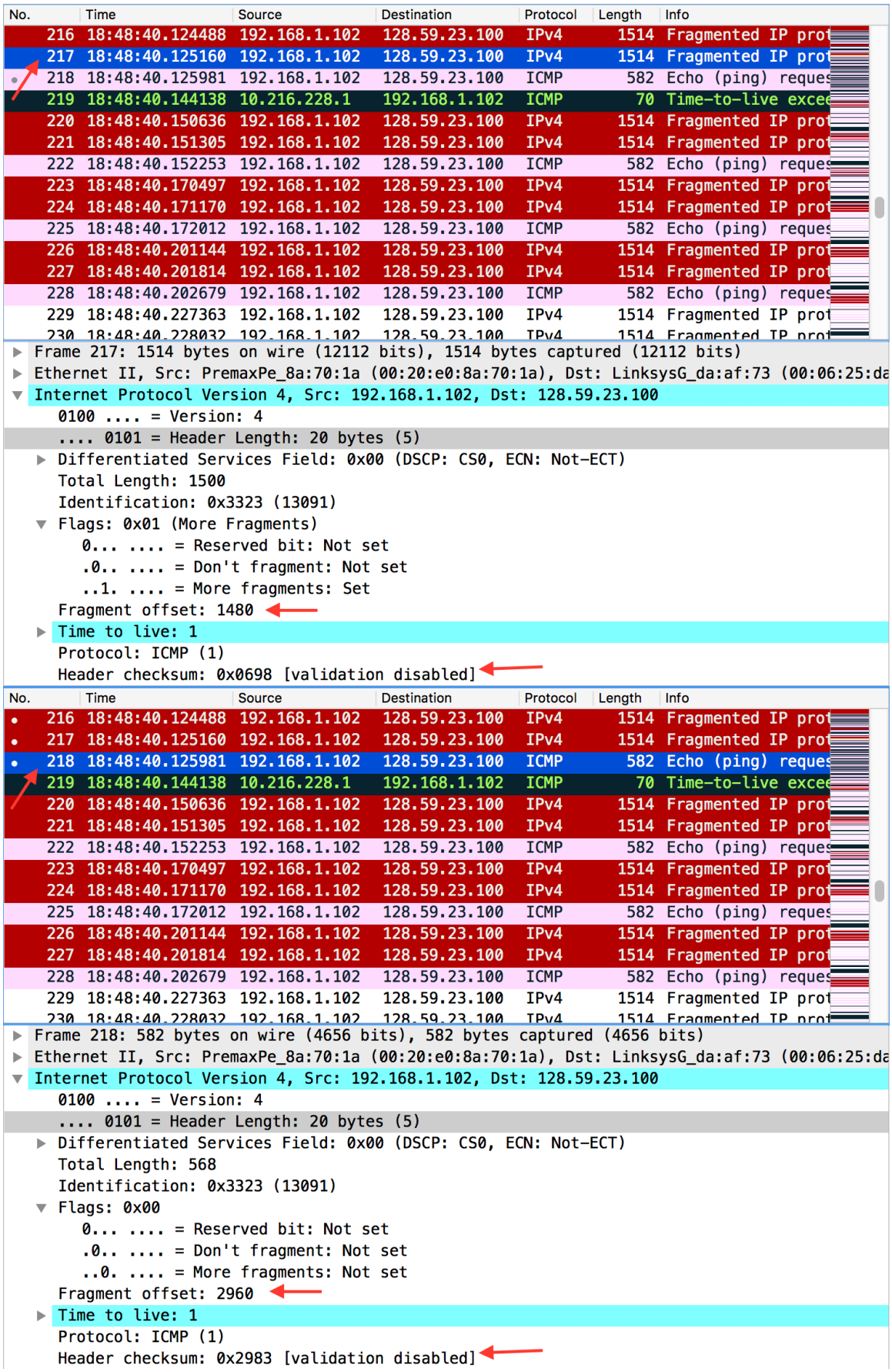
15) What fields changes in the IP header among the fragments?

Answer:
Fragment offset (0, 1480, 2960), Checksum
See screenshots below.



No.	Time	Source	Destination	Protocol	Length	Info
216	18:48:40.124488	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
217	18:48:40.125160	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
218	18:48:40.125981	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) reques
219	18:48:40.144138	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exce
220	18:48:40.150636	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
221	18:48:40.151305	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
222	18:48:40.152253	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) reques
223	18:48:40.170497	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
224	18:48:40.171170	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
225	18:48:40.172012	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) reques
226	18:48:40.201144	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
227	18:48:40.201814	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
228	18:48:40.202679	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) reques
229	18:48:40.227363	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
230	18:48:40.228032	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot

```
▶ Frame 216: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
▶ Ethernet II, Src: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da
▼ 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]
```


No. Time Source Destination Protocol Length Info
216 18:48:40.124488 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
217 18:48:40.125160 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
218 18:48:40.125981 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) reques
219 18:48:40.144138 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceed
220 18:48:40.150636 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
221 18:48:40.151305 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
222 18:48:40.152253 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) reques
223 18:48:40.170497 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
224 18:48:40.171170 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
225 18:48:40.172012 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) reques
226 18:48:40.201144 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
227 18:48:40.201814 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
228 18:48:40.202679 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) reques
229 18:48:40.227363 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
Frame 217: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da
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: 1480
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x0698 [validation disabled]
No. Time Source Destination Protocol Length Info
216 18:48:40.124488 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
217 18:48:40.125160 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
218 18:48:40.125981 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) reques
219 18:48:40.144138 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceed
220 18:48:40.150636 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
221 18:48:40.151305 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
222 18:48:40.152253 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) reques
223 18:48:40.170497 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
224 18:48:40.171170 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
225 18:48:40.172012 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) reques
226 18:48:40.201144 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
227 18:48:40.201814 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
228 18:48:40.202679 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) reques
229 18:48:40.227363 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP prot
Frame 218: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits)
Ethernet II, Src: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da
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: 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
Protocol: ICMP (1)
Header checksum: 0x2983 [validation disabled]