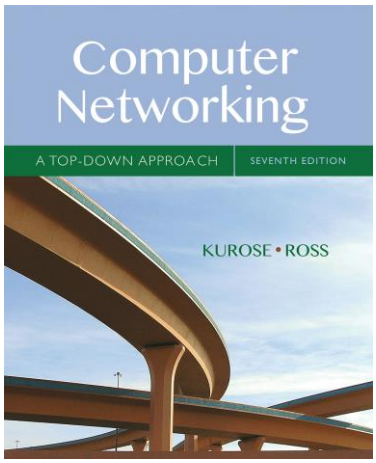
Name: Katie Schaumleffle

Wireshark Lab: IP v7.0

Supplement to *Computer Networking: A Top-Down Approach, 7th ed.*, J.F. Kurose and K.W. Ross

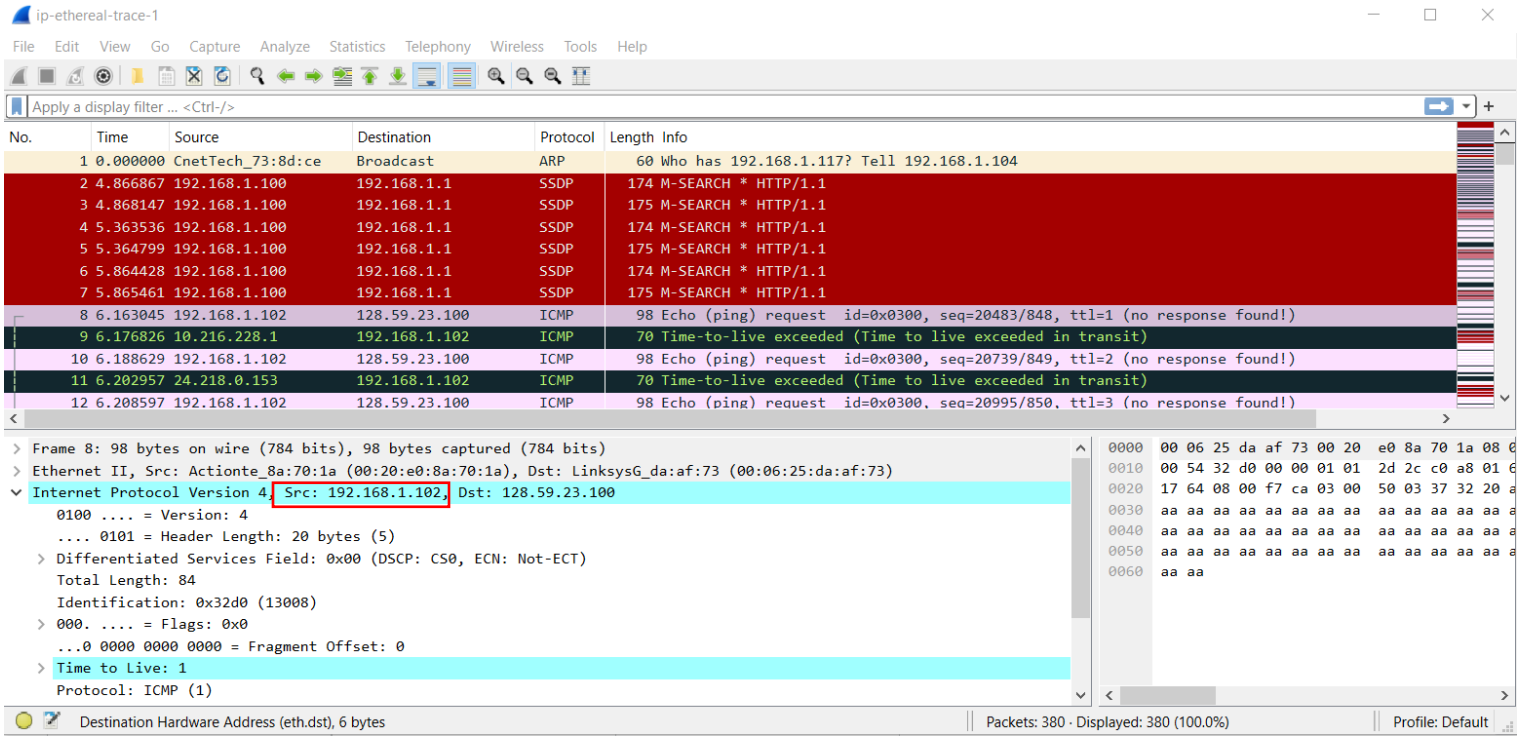


"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb

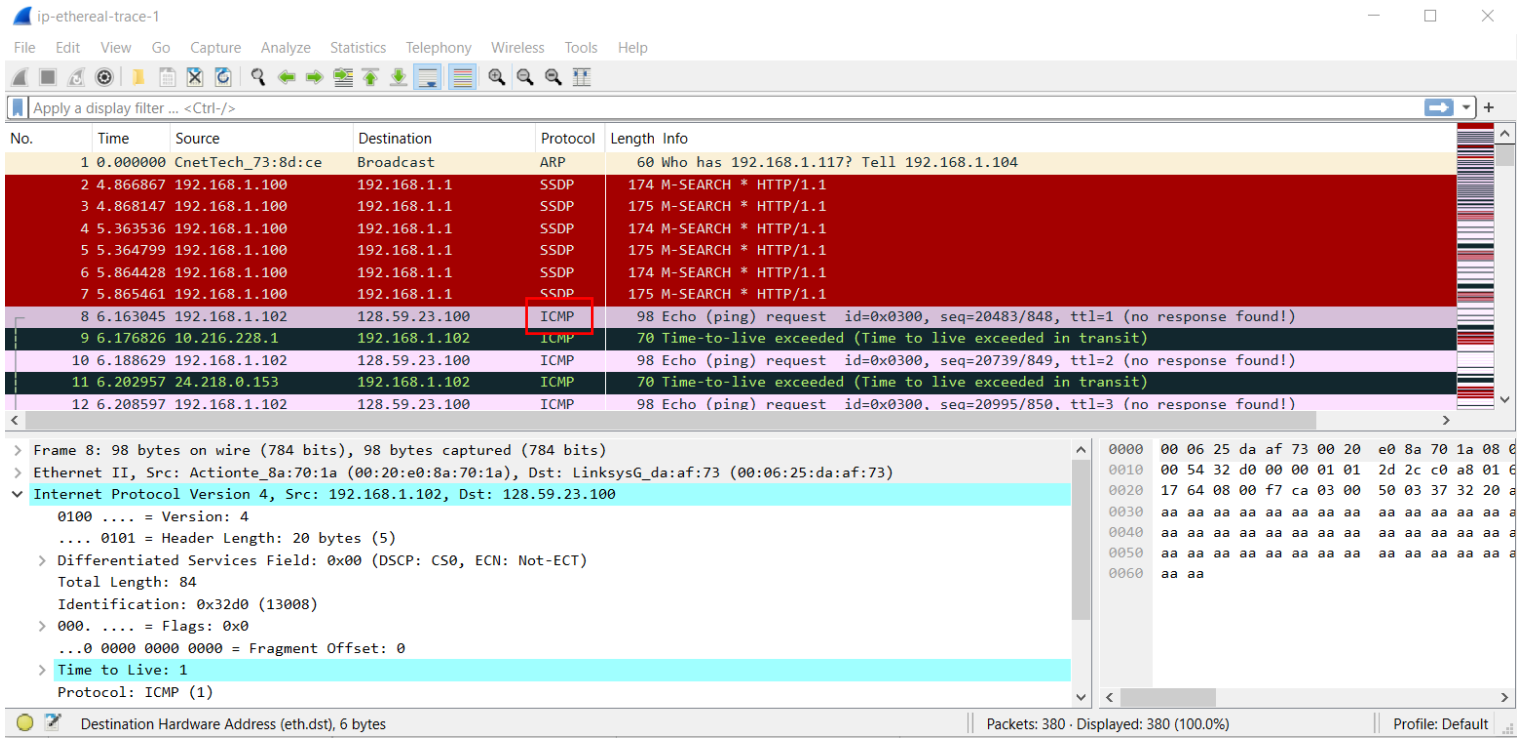
---

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.

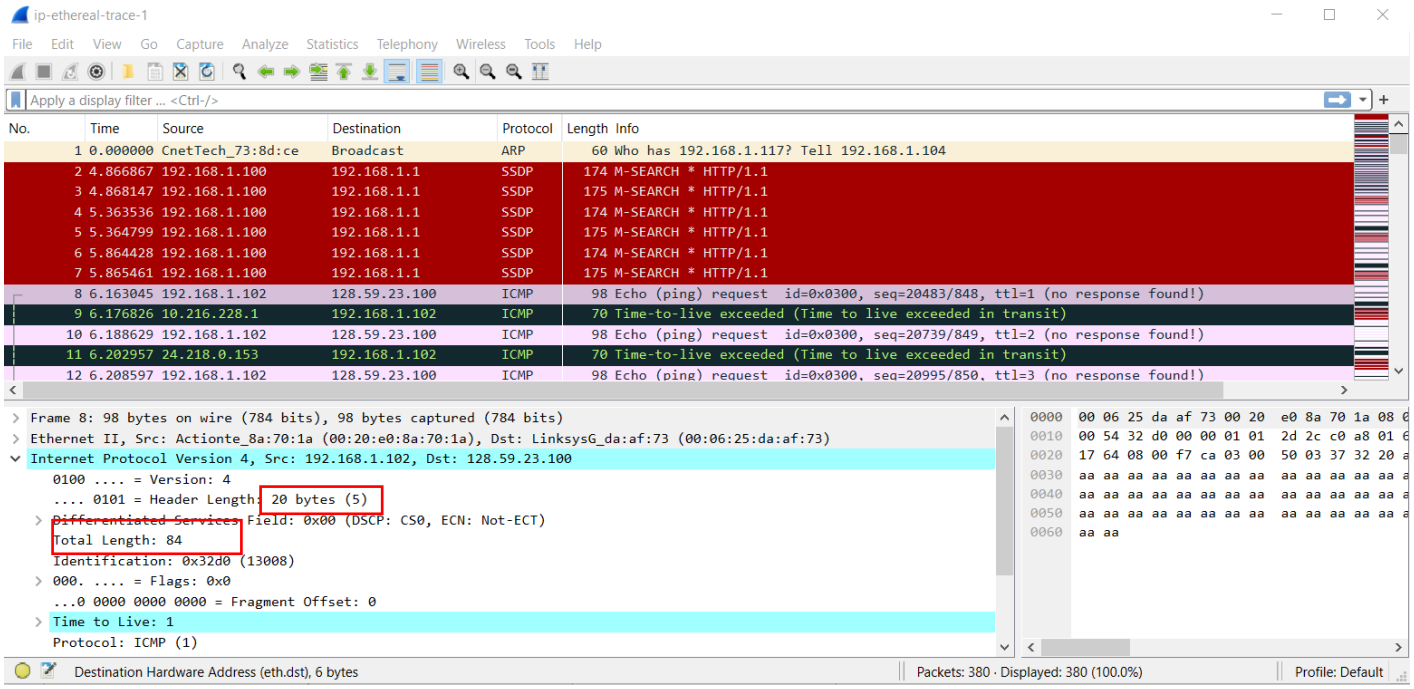
   What is the IP address of your computer? **192.168.1.102**



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

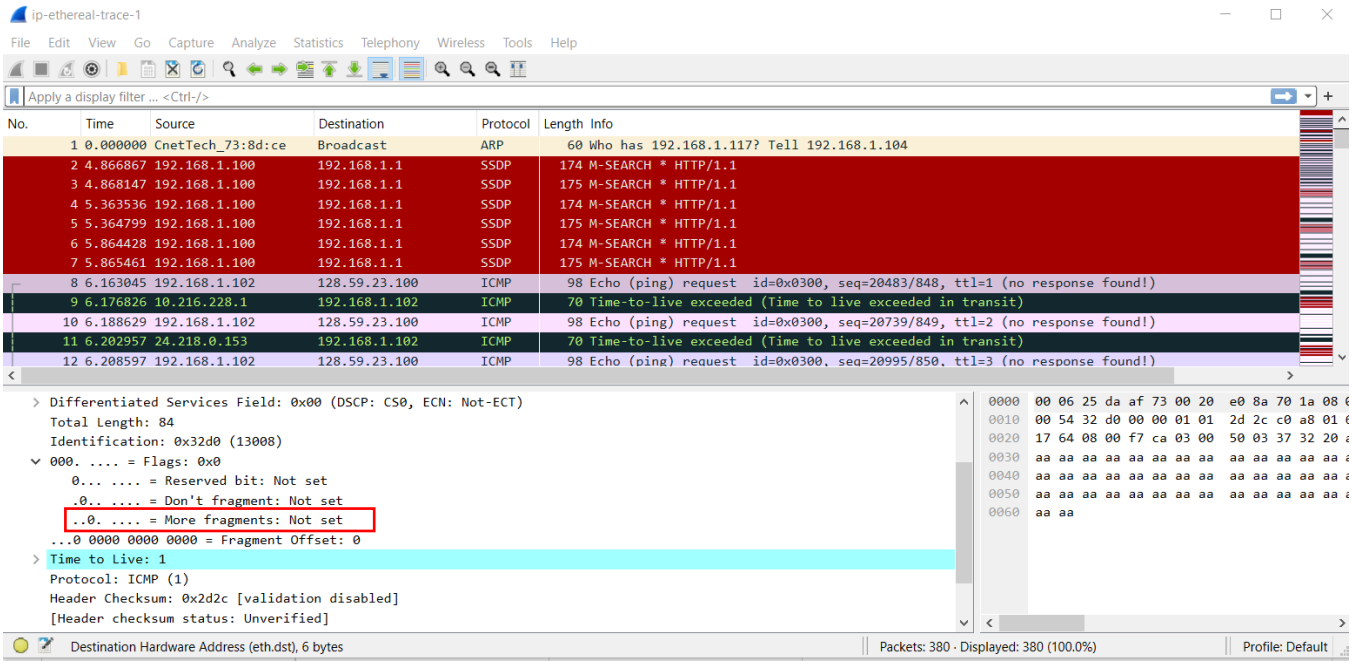


3. How many bytes are in the IP header? How many bytes are in the payload *of the IP datagram*? Explain how you determined the number of payload bytes.
   Header: 20 bytes
   Total bytes length: 84 bytes
   Payload of the IP datagram = 84-20 = 64 bytes



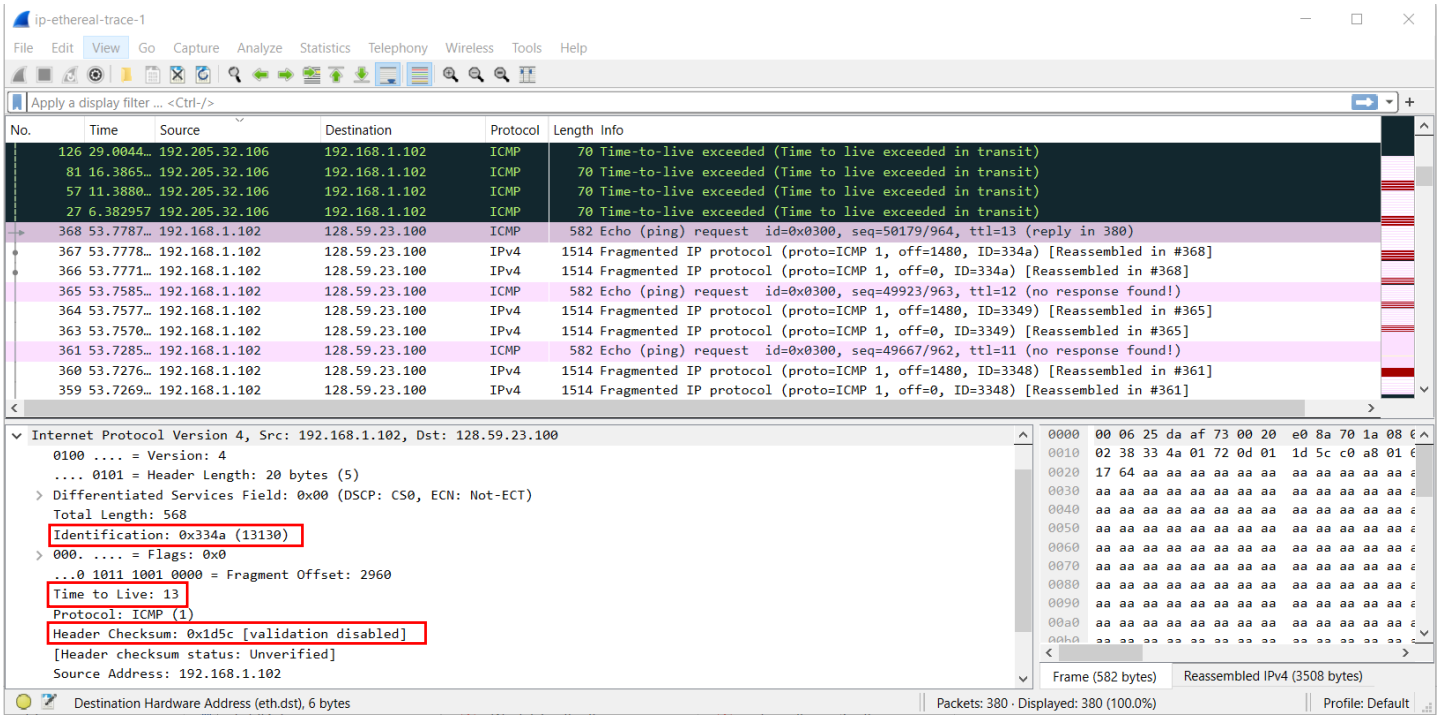
4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

   This has not been fragmented. We can see that the "more fragments" flag is set to 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?

   The fields in the IP datagram that always change from one datagram to the next within the ICMP messages sent by the computer are: Identification, Time to live, and Header checksum.



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

The fields that must stay constant are:

Version- All packets use IPv4

Header length- The headers are the same length for ICMP packets

Total length- The total length stays the same for ICMP packets

Differentiated Service Fields- All packets are ICMP, therefore they use the same type of service class.

Source IP- All packets are sent from the same source.

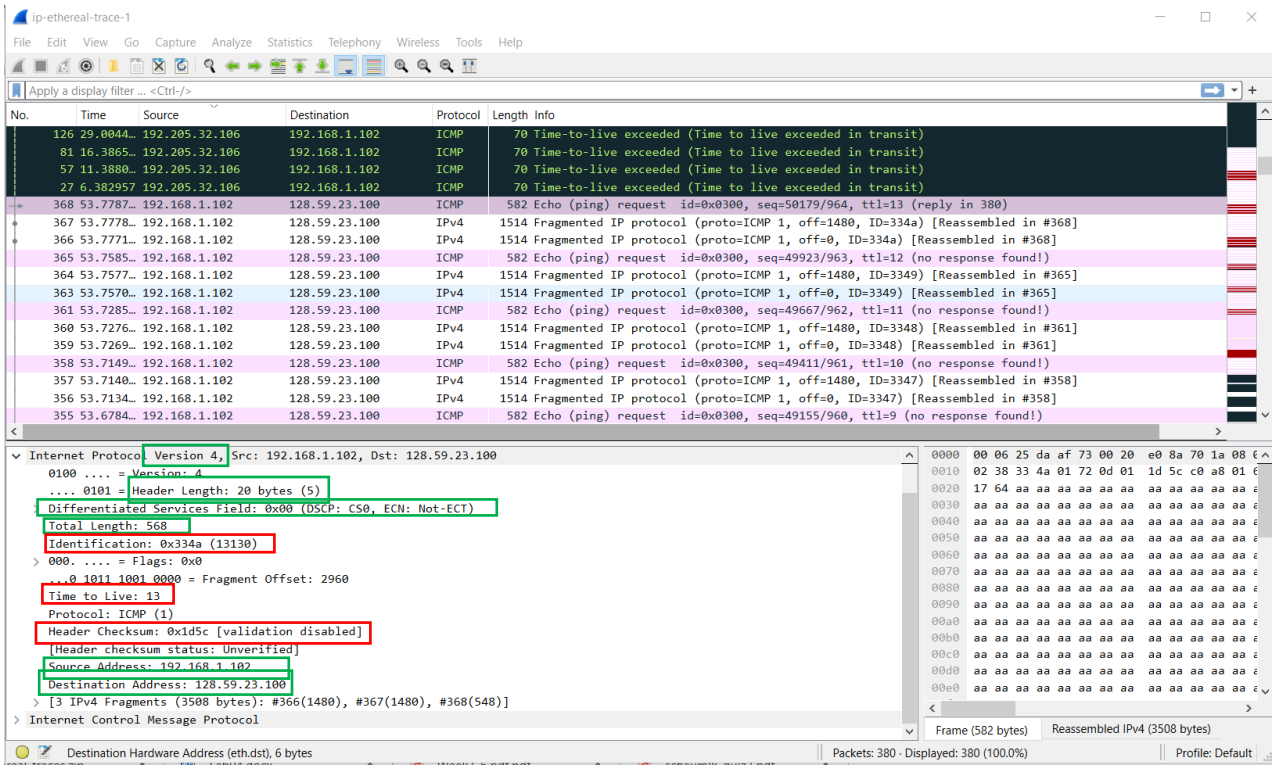
Destination IP- All packets were sent to the same destination.

The fields that must change are:

Identification- Each packet has a unique ID

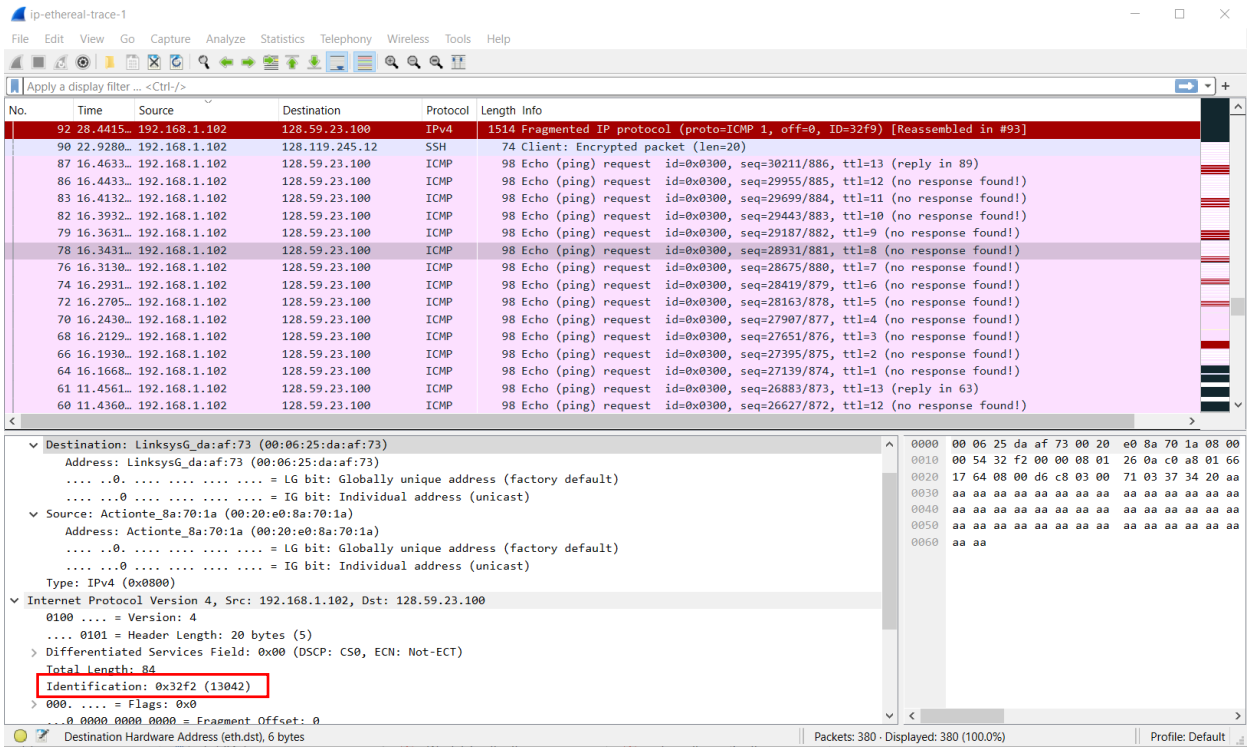
Time to live- The traceroute increments each subsequent packet

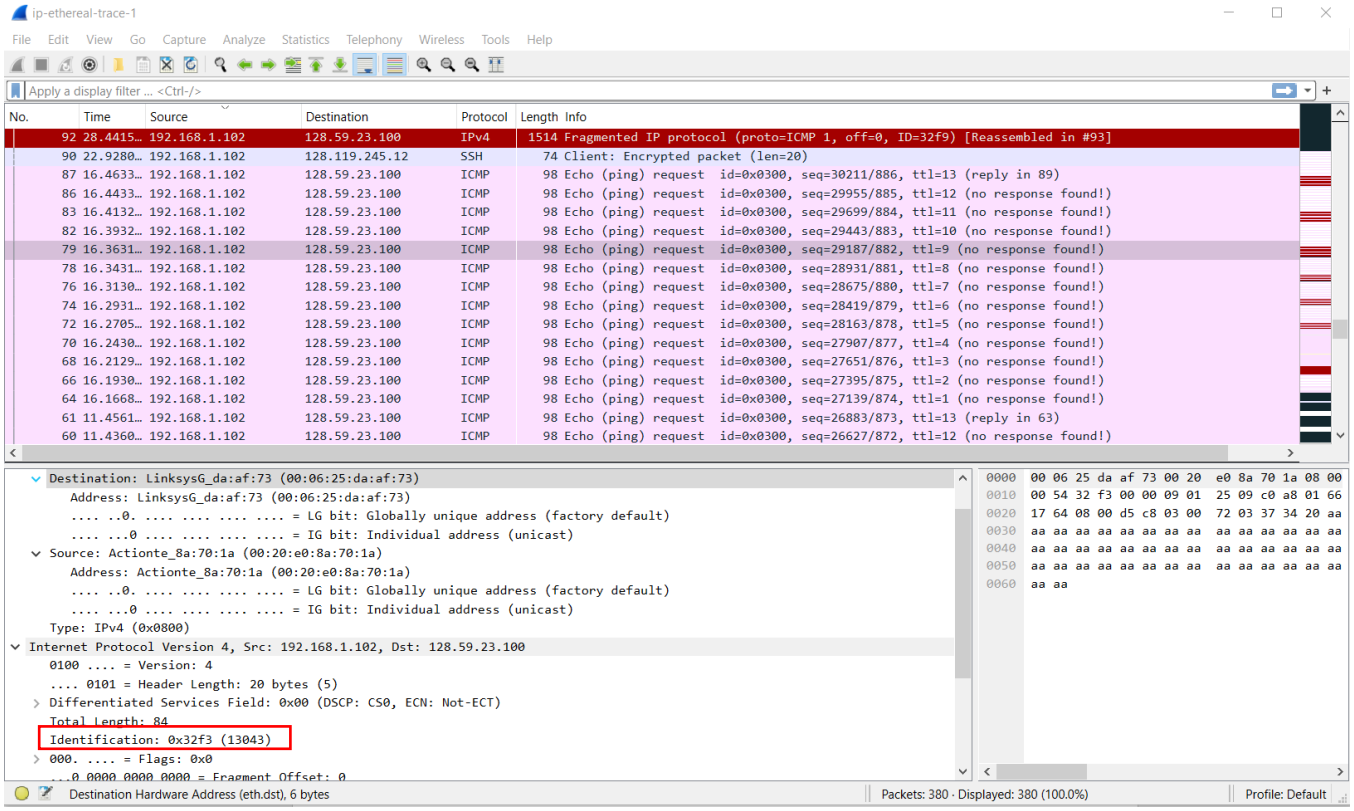
Header checksum- The header changes, therefore the checksum changes, too.



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

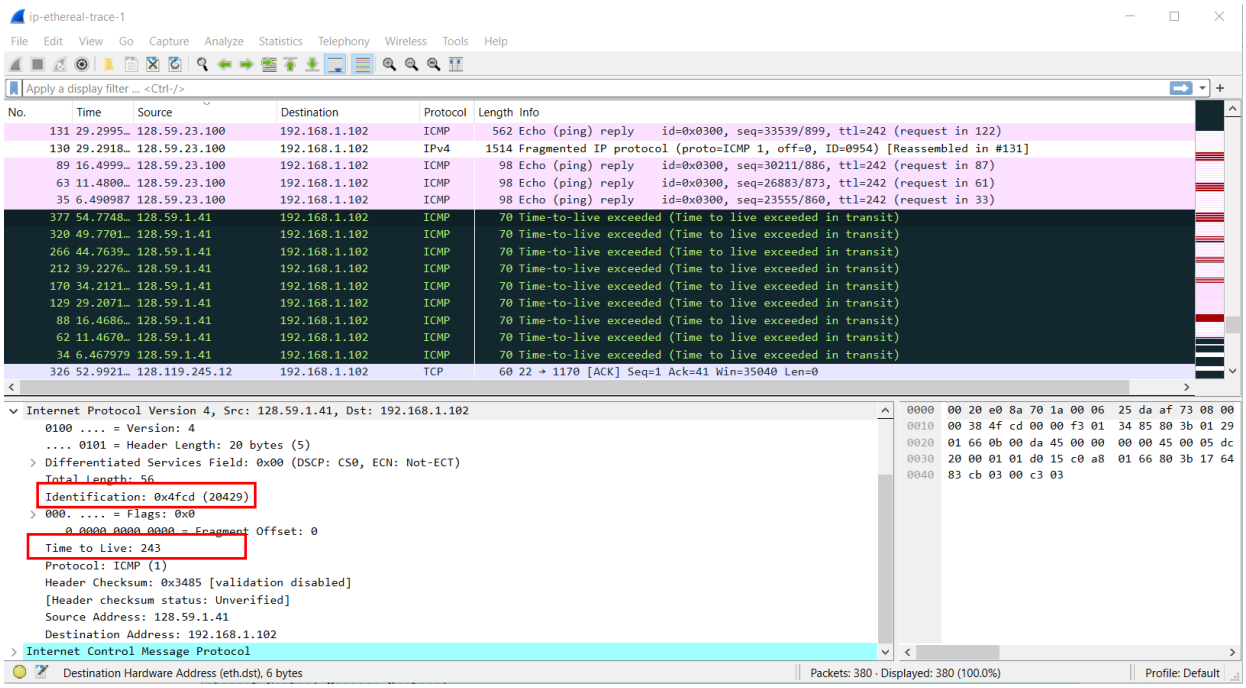
The pattern I see in the values in the ID field of the IP datagram, is that for each ICMP request, the identification increments.





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

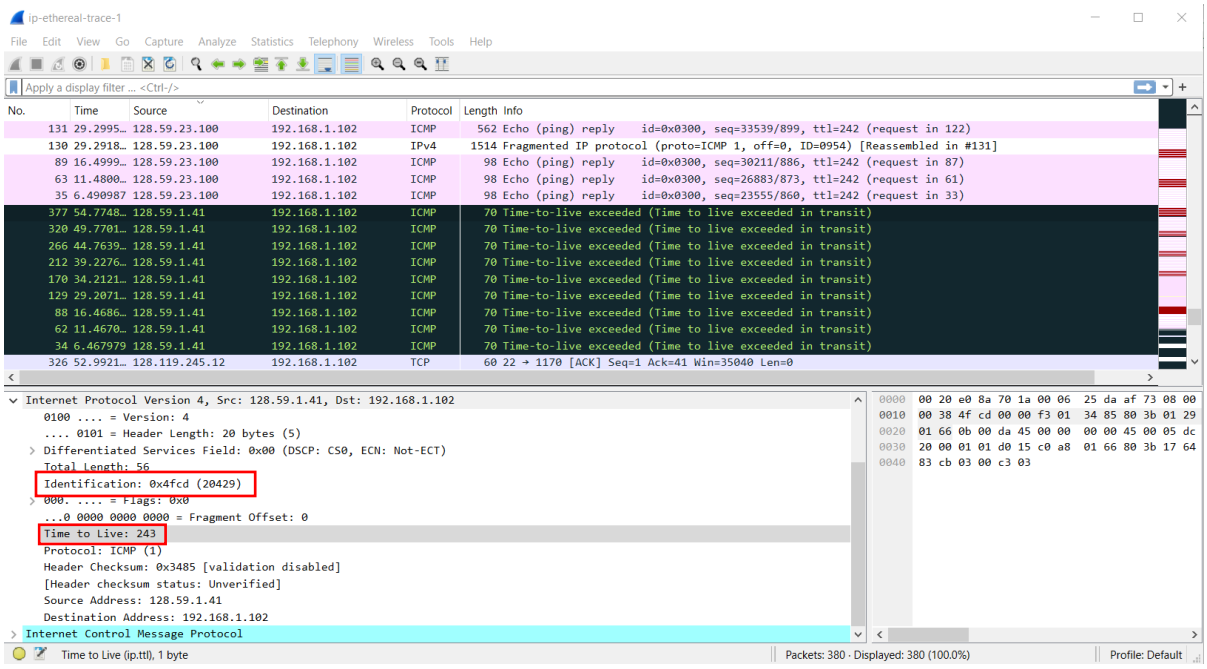
ID field: 20429
TTL field: 243

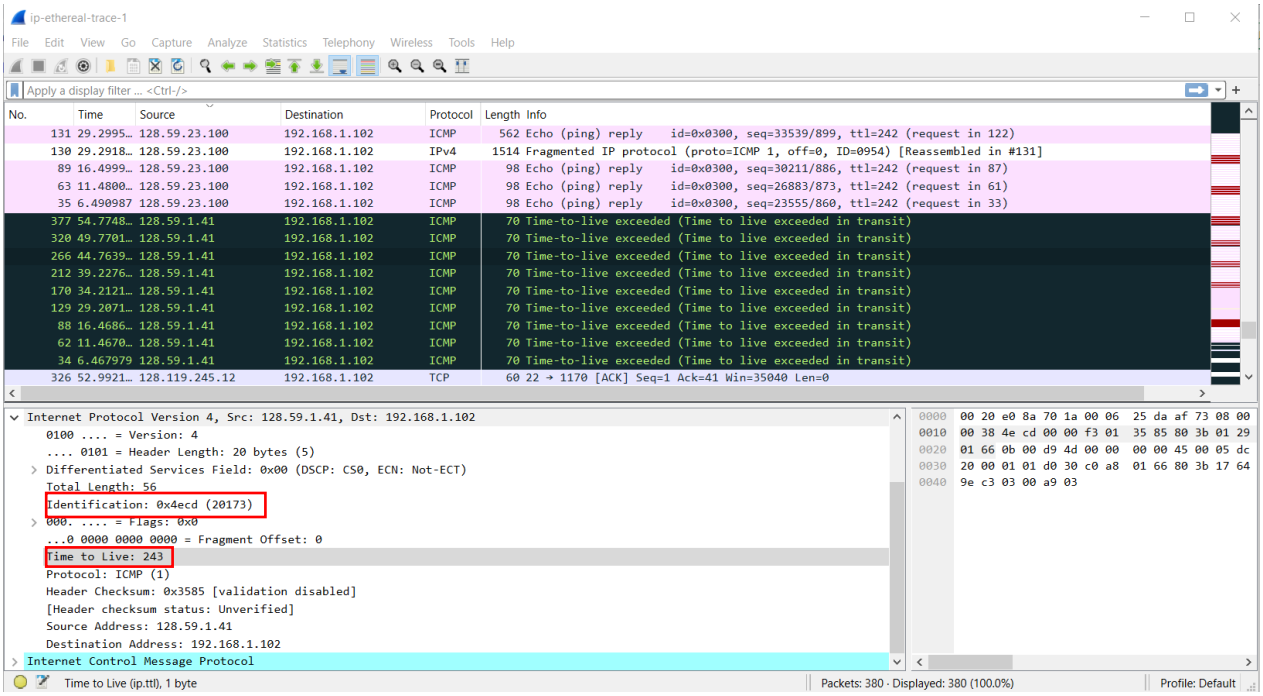


9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

The Time to live remains unchanged for all the ICMP TTL-exceeded replies sent to the computer by the nearest router because the TTL for the first hop router is always going to be the same.

The ID changes for all of the ICMP TTL-exceeded replies because the ID field has a unique value.



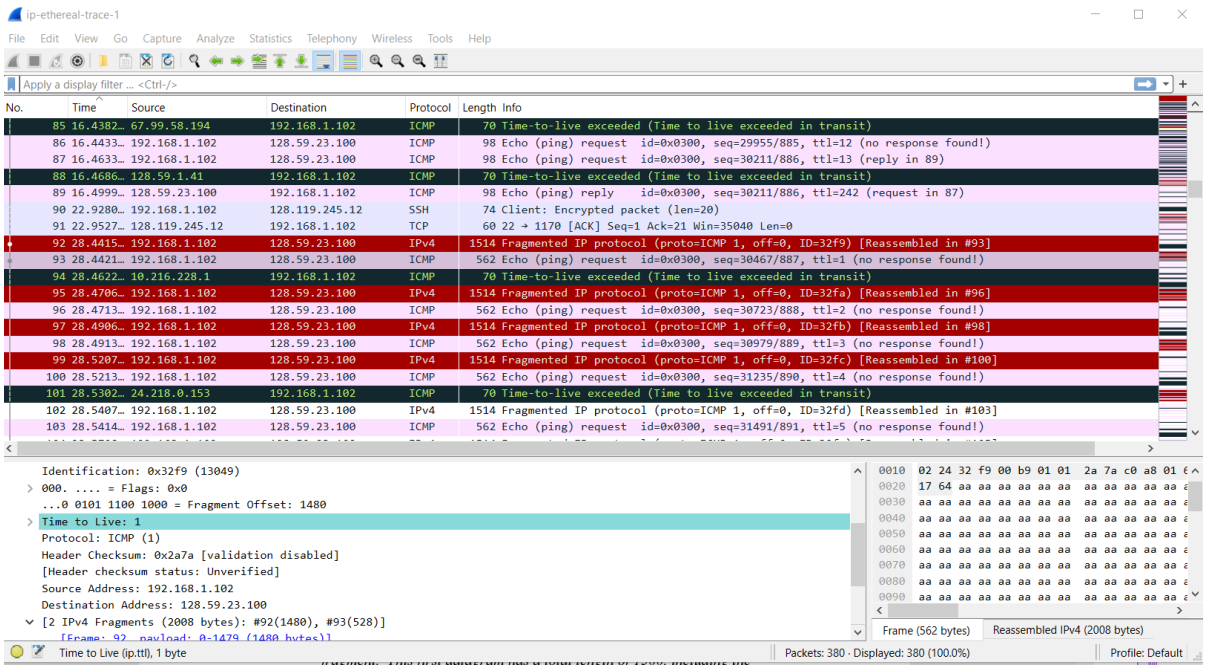


Fragmentation

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, the packet has been fragmented across more than one IP datagram.

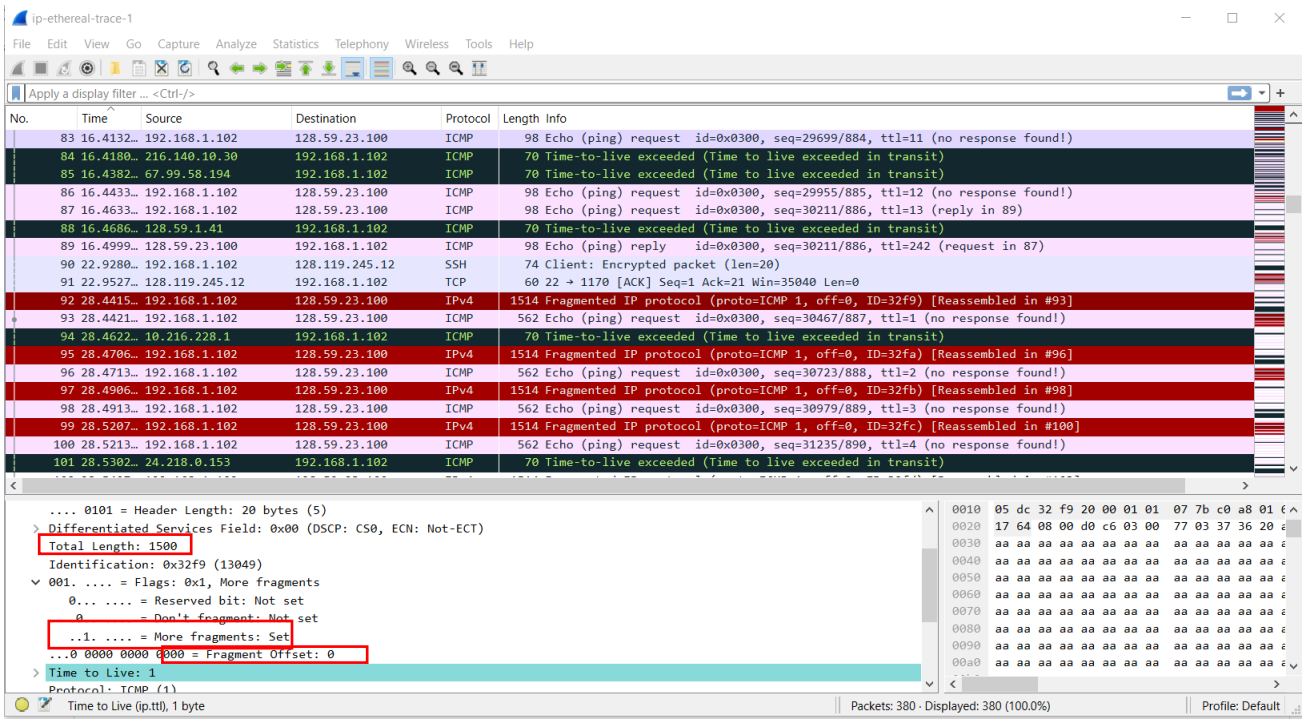


11. Screenshot the first fragment of the fragmented IP datagram (with sufficient details to answer these questions). What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment?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

The ”more fragment’s” is set to 1, which indicates that the datagram has been fragmented.

The fragment offset is set to 0, which indicates that this is the first fragment.

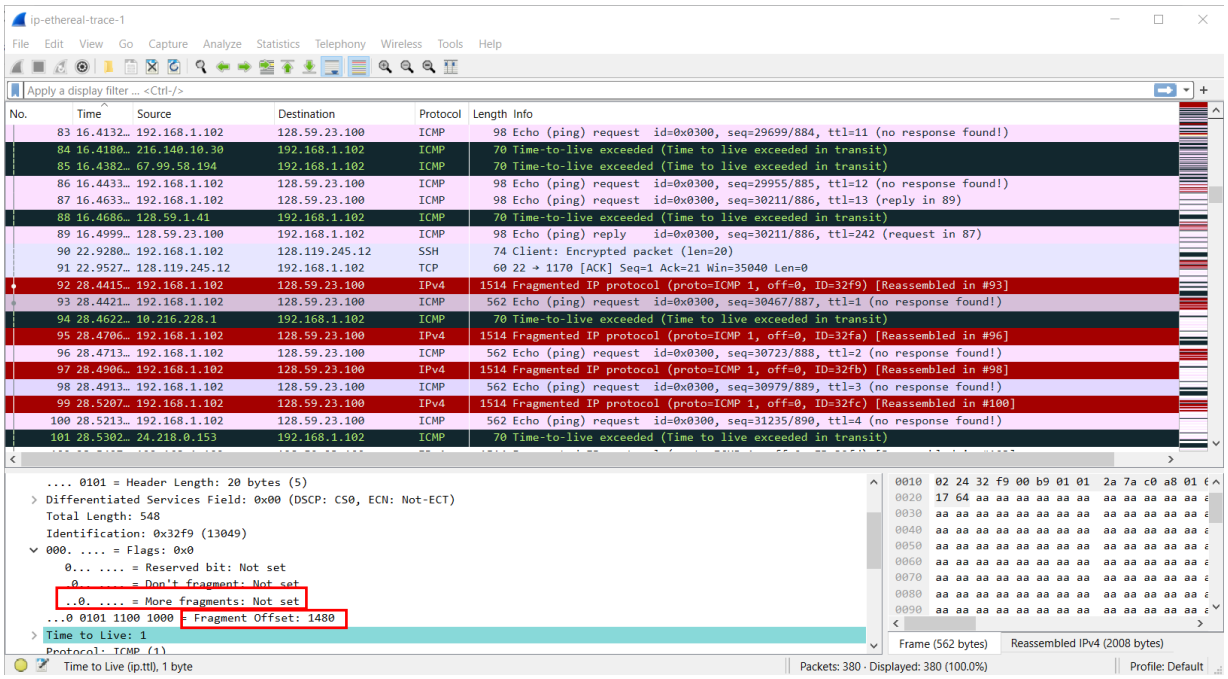
The IP datagram total length is 1500.



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?

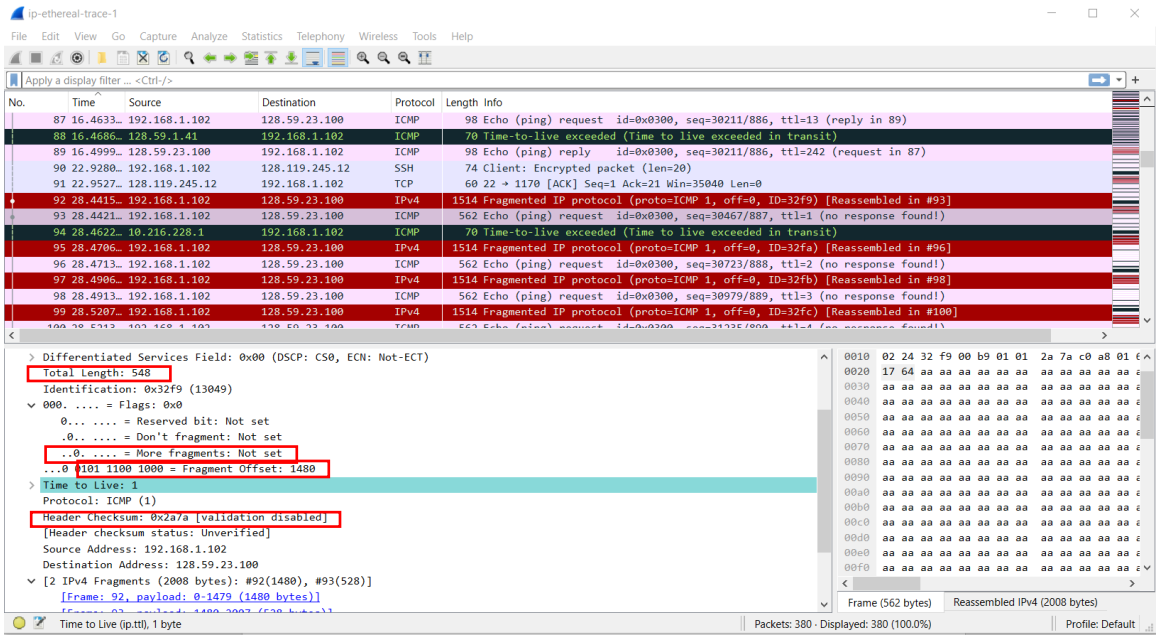
    The fragment offset is set to 1480, which indicates that this is not the first fragment.

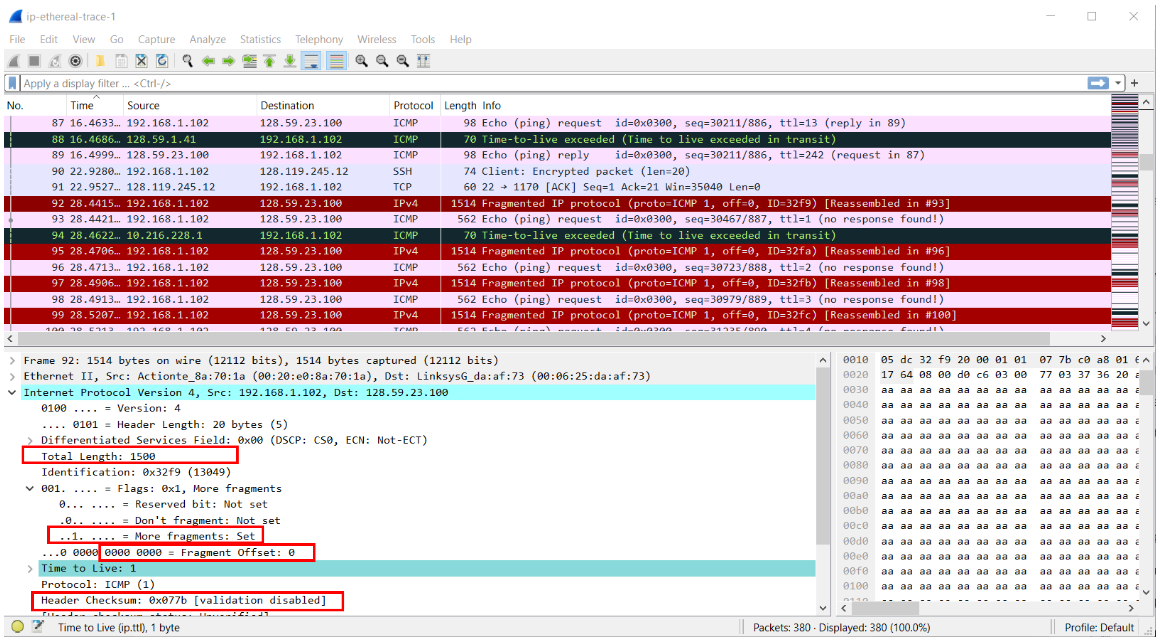
    There are no more fragments, the “more fragments” flag is set to 0.



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

The fields that change in the IP header between the fragments are: total length, flags, fragment offset, and checksum.

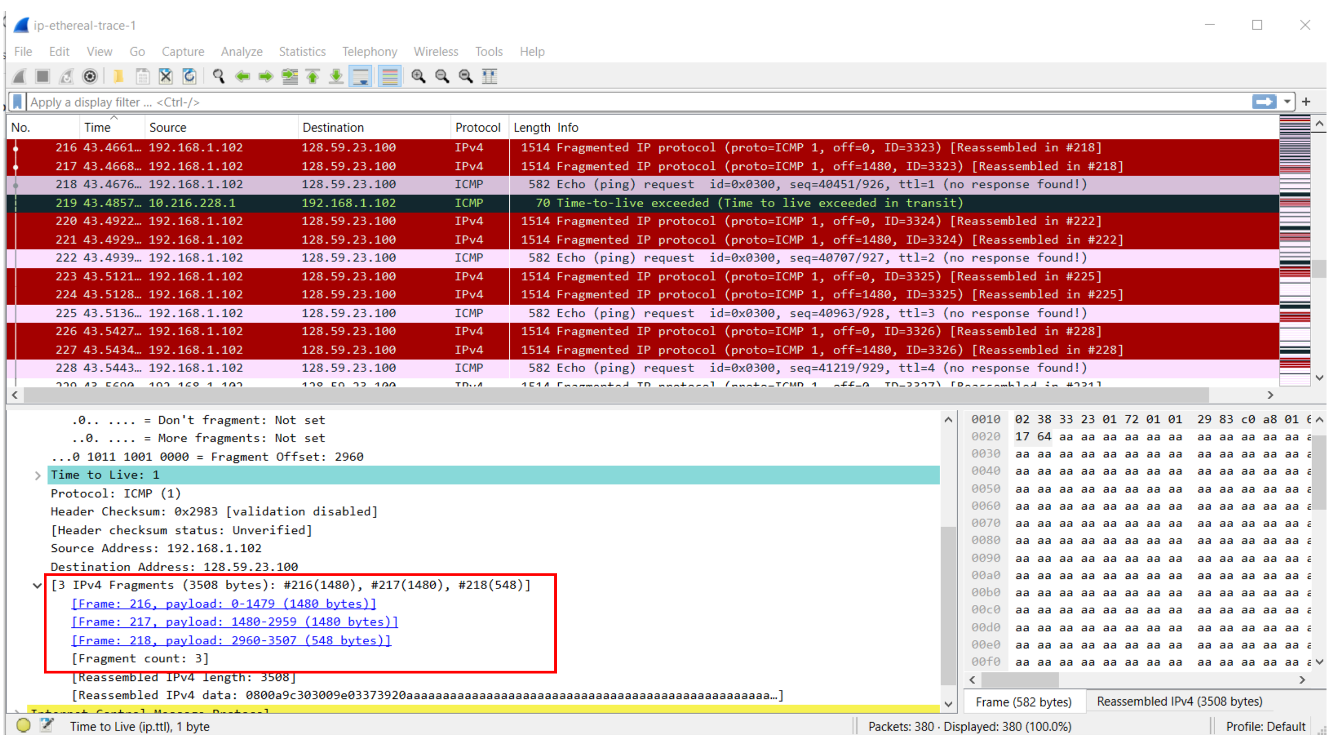




Now find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 3500.

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

3 fragments were created from the original datagram.

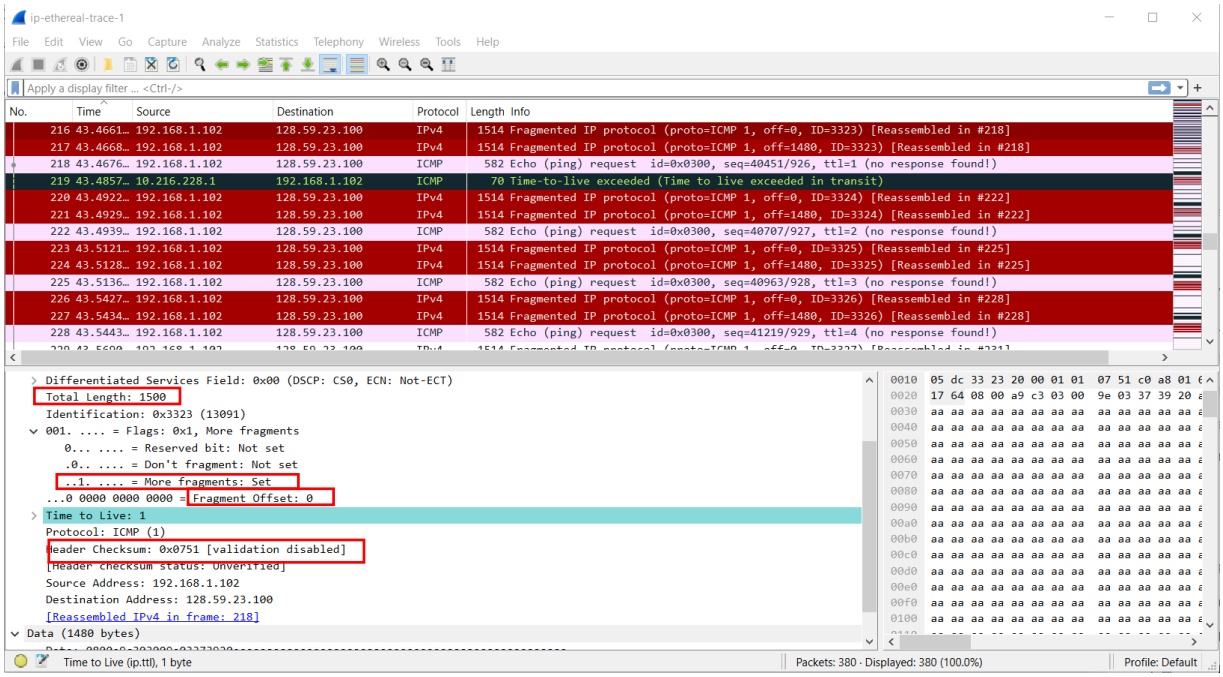


15. What fields change in the IP header among the fragments?

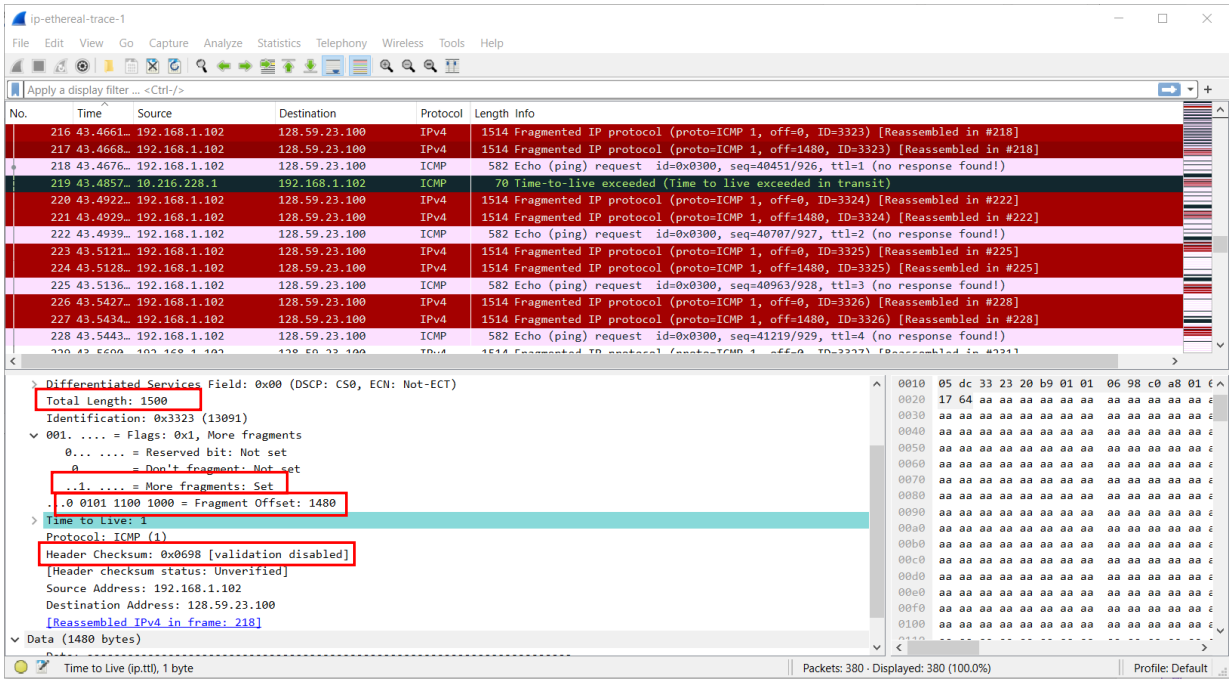
The IP header fields that change between all of the packets are: fragment offset and checksum.

The fields that change from 216 & 217 to 218: The first two packets differ from the last packet in total length, and flags. 216 & 217 have a total length of 1500, and the last packet has a length of 540. The first two packets have the "more fragments" flag set to 1, whereas 217 has that flag set to 0.

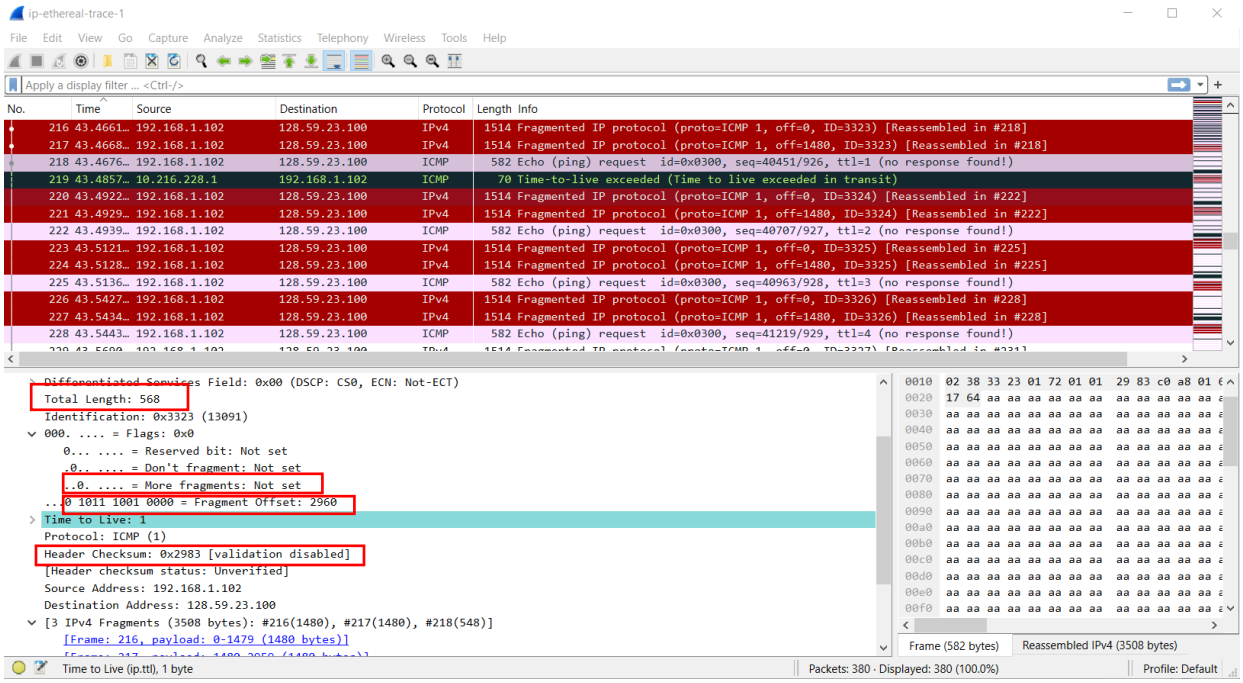
216:



217:


ip-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
216 43.4661… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217 43.4668… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218 43.4676… 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)
219 43.4857… 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
220 43.4922… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
221 43.4929… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled in #222]
222 43.4939… 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=40707/927, ttl=2 (no response found!)
223 43.5121… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3325) [Reassembled in #225]
224 43.5128… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3325) [Reassembled in #225]
225 43.5136… 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=40963/928, ttl=3 (no response found!)
226 43.5427… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3326) [Reassembled in #228]
227 43.5434… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3326) [Reassembled in #228]
228 43.5443… 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=41219/929, ttl=4 (no response found!)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x3323 (13091)
001. .... = Flags: 0x1, More fragments
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..1. .... = More fragments: Set
...0 1011 1001 0000 = Fragment Offset: 1480
Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x0698 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
[Reassembled IPv4 in frame: 218]
Data (1480 bytes)
0010 05 dc 33 23 20 b9 01 01 06 98 c0 a8 01 6
0020 17 64 aa aa aa aa aa aa aa aa aa aa aa aa
Time to Live (ip.ttl), 1 byte
Packets: 380 · Displayed: 380 (100.0%)
Profile: Default

218:


ip-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
216 43.4661… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217 43.4668… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218 43.4676… 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)
219 43.4857… 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
220 43.4922… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
221 43.4929… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled in #222]
222 43.4939… 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=40707/927, ttl=2 (no response found!)
223 43.5121… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3325) [Reassembled in #225]
224 43.5128… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3325) [Reassembled in #225]
225 43.5136… 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=40963/928, ttl=3 (no response found!)
226 43.5427… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3326) [Reassembled in #228]
227 43.5434… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3326) [Reassembled in #228]
228 43.5443… 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=41219/929, ttl=4 (no response found!)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 568
Identification: 0x3323 (13091)
000. .... = Flags: 0x0
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 1011 1001 0000 = Fragment Offset: 2960
Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x2983 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
[3 IPv4 Fragments (3508 bytes): #216(1480), #217(1480), #218(548)]
[Frame: 216, payload: 0-1479 (1480 bytes)]
0010 02 38 33 23 01 72 01 01 29 83 c0 a8 01 6
0020 17 64 aa aa aa aa aa aa aa aa aa aa aa aa
Frame (582 bytes)
Reassembled IPv4 (3508 bytes)
Time to Live (ip.ttl), 1 byte
Packets: 380 · Displayed: 380 (100.0%)
Profile: Default