Họ tên : Lê Bảo Khánh
MSSV : 1911363
Lớp : L01

LAB 4a

(Using ip-ethereal-trace-1 trace file)

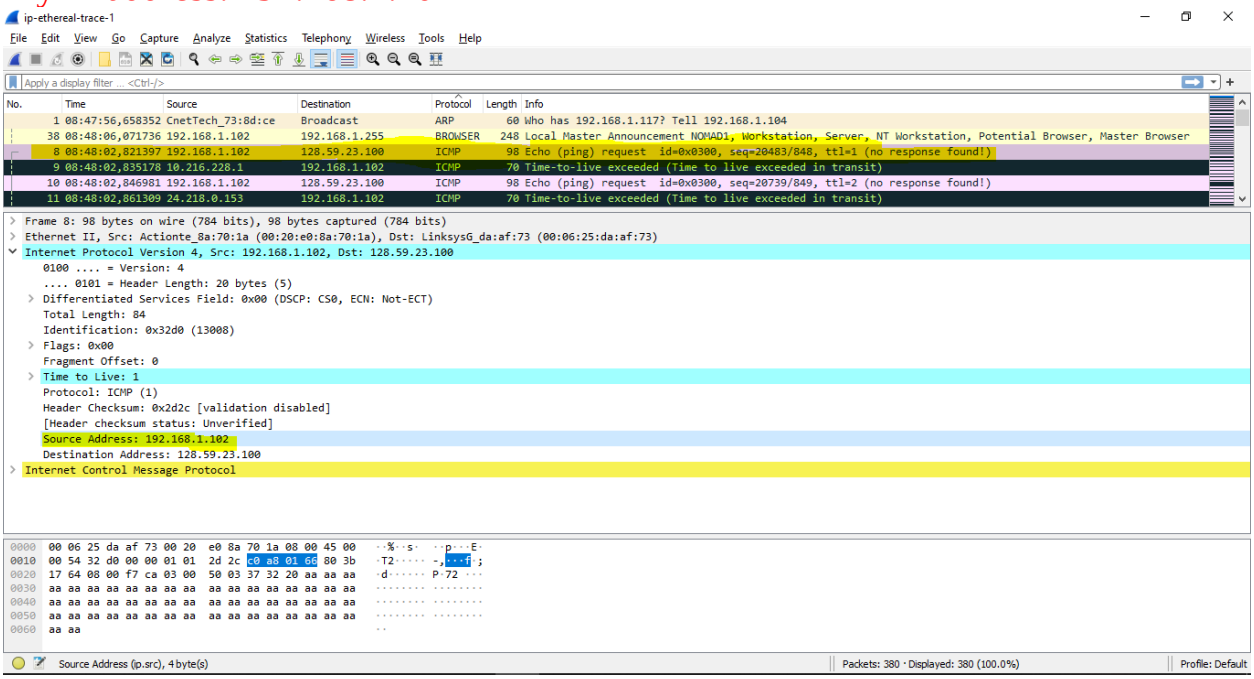
1. Capturing packets from an execution of traceroute

Part 1:

Question 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?

ANSWER:

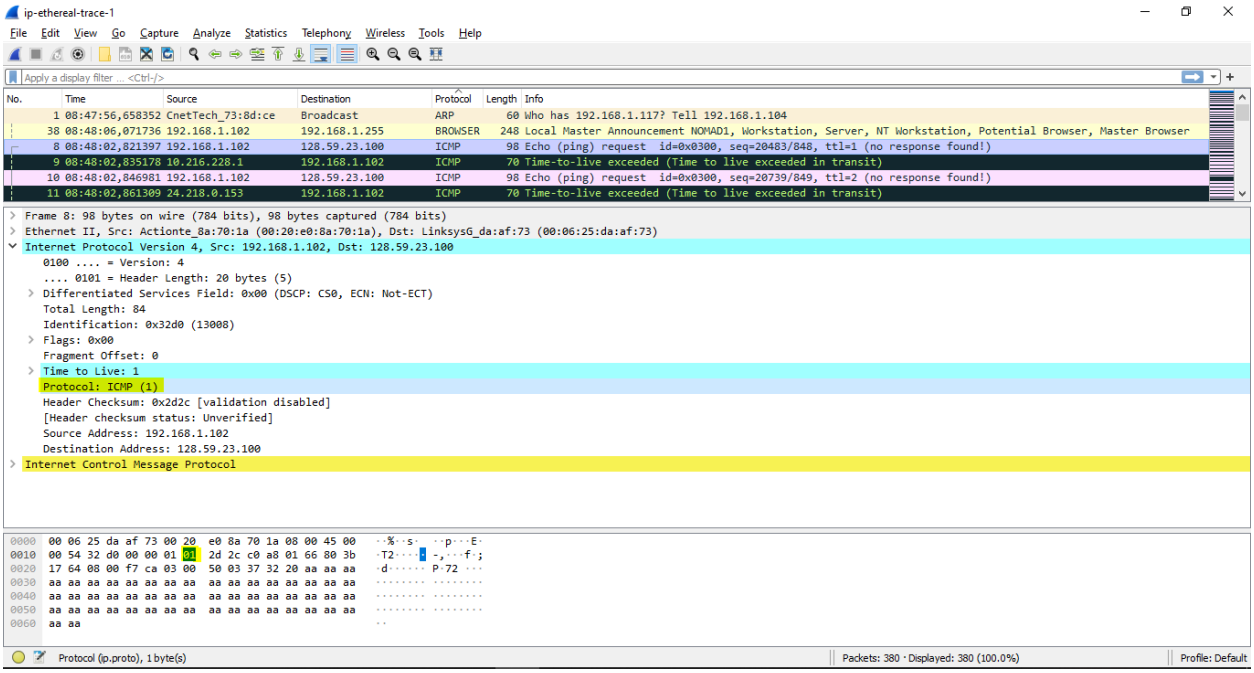
My IP address: 192.168.1.102



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

ANSWER:

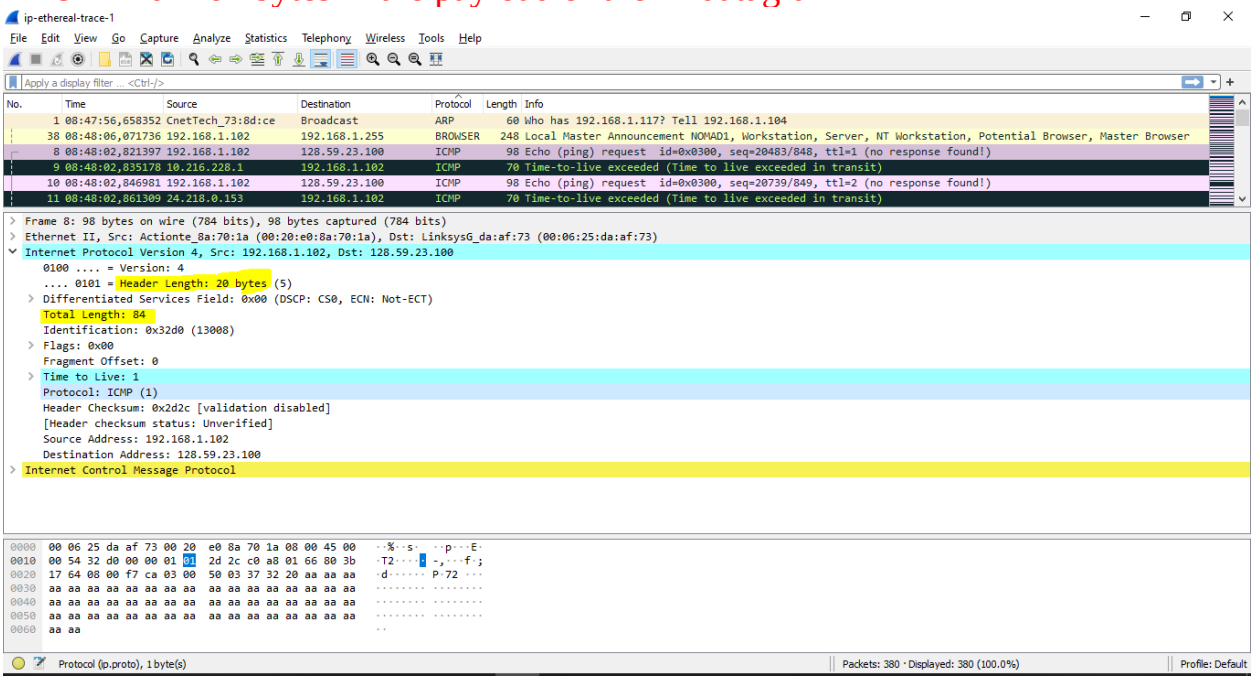
The value in the upper layer protocol field is ICMP (0x01)



Question 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:

20 bytes in the IP header
84 bytes total length
=> 84 – 20 = 64 bytes in the payload of the IP datagram

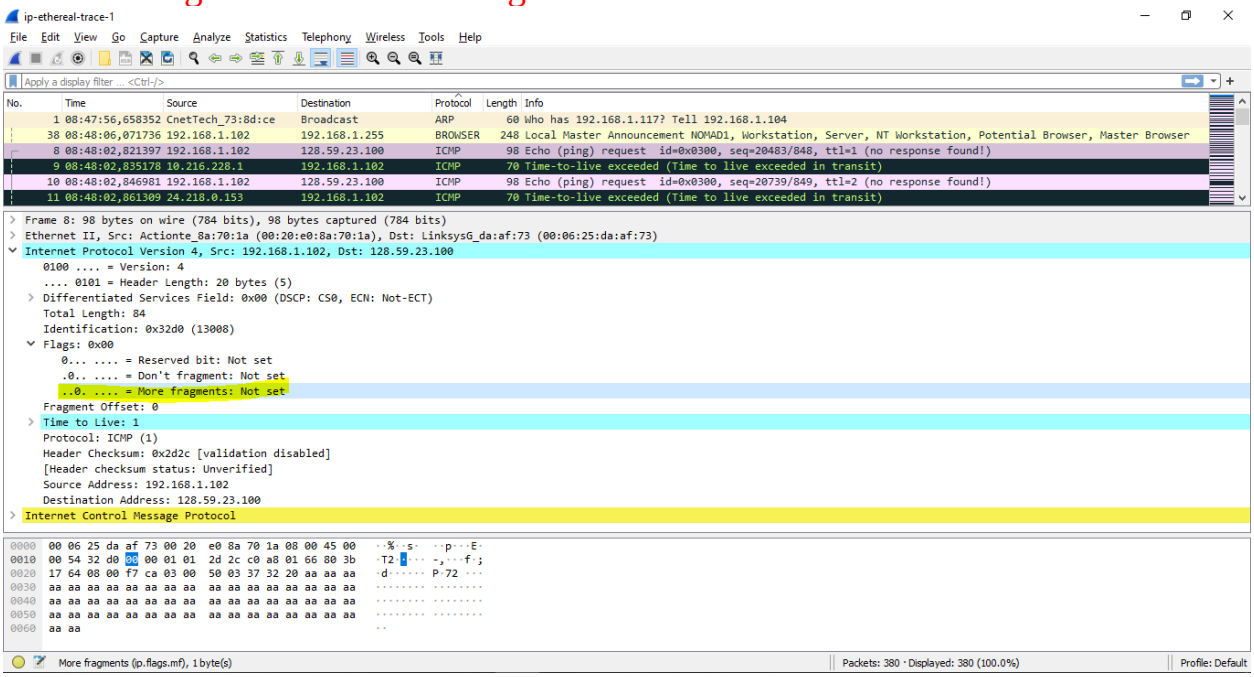


Question 4: Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

ANSWER:

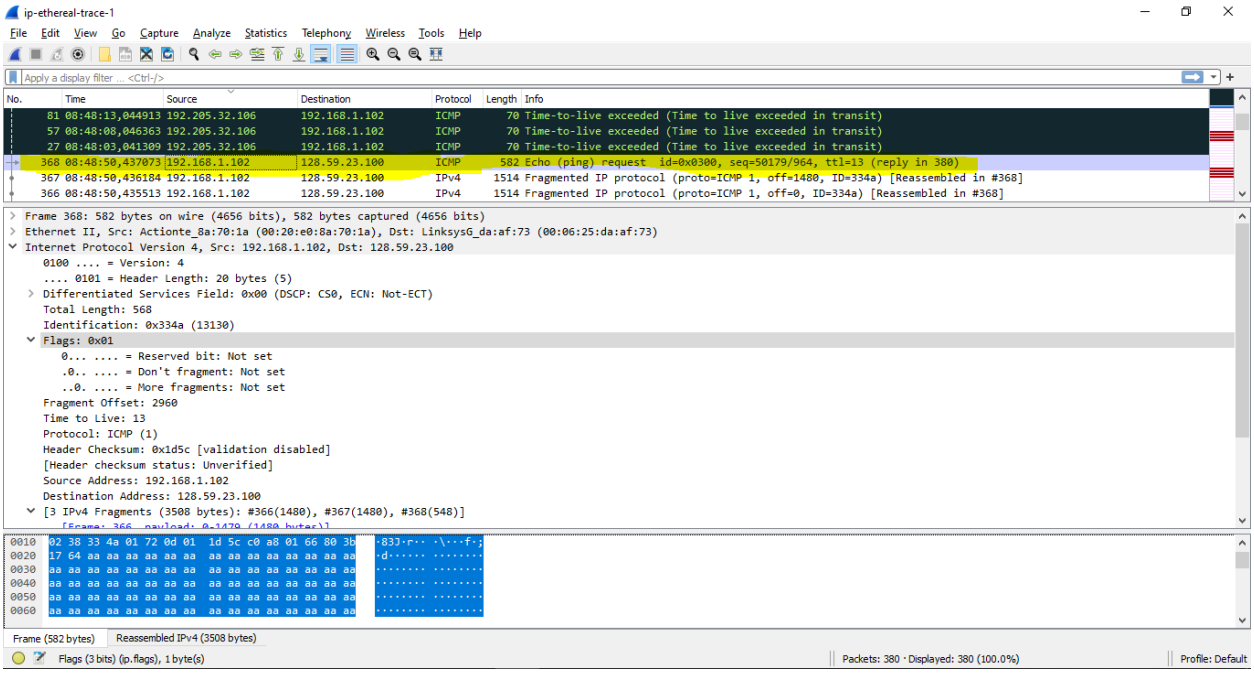
The more fragments bit is Not set

=> The datagram has not been fragmented.



Question 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 + TTL + Header checksum

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

ANSWER:

The fields that stay constant:

- Version (using IPv4 for all packets)
- Header length (these are ICMP packets)
- Differentiated Services (all packets are ICMP + same Type of Service class)
- Source IP (sending from the same source)
- Destination IP (sending to the same destination)
- Upper Layer Protocol (these are ICMP packets)

The fields that must stay constant:

- Version (using IPv4 for all packets)
- Header length (these are ICMP packets)
- Differentiated Services (all packets are ICMP + same Type of Service class)
- Source IP (sending from the same source)
- Destination IP (sending to the same destination)
- Upper Layer Protocol (these are ICMP packets)

The fields that must change:

- Identification(IP packets must have different ids)
- Time to live (traceroute increments for each subsequent packet)
- Header checksum (header changes -> need for checksum)

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

ANSWER:

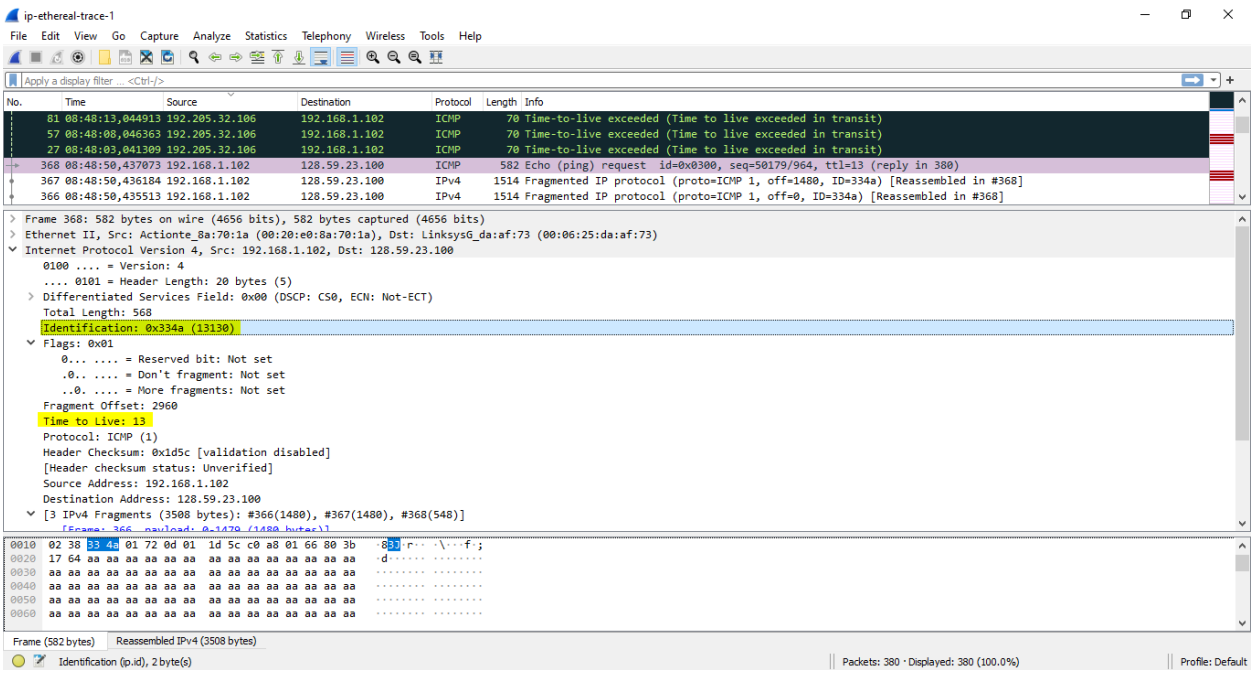
IP header Identification fields increase by 1 / ICMP Echo (ping) request.

Question 8: What is the value in the Identification field and the TTL field?

ANSWER:

Identification: 0x0000334a (13130)

TTL: 13



Question 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:

- The identification field changes for all the ICMP TTL-exceeded replies because the identification field is a unique value. When two or more IP datagrams have the same identification value, then it means that these IP datagrams are fragments of a single large IP datagram.

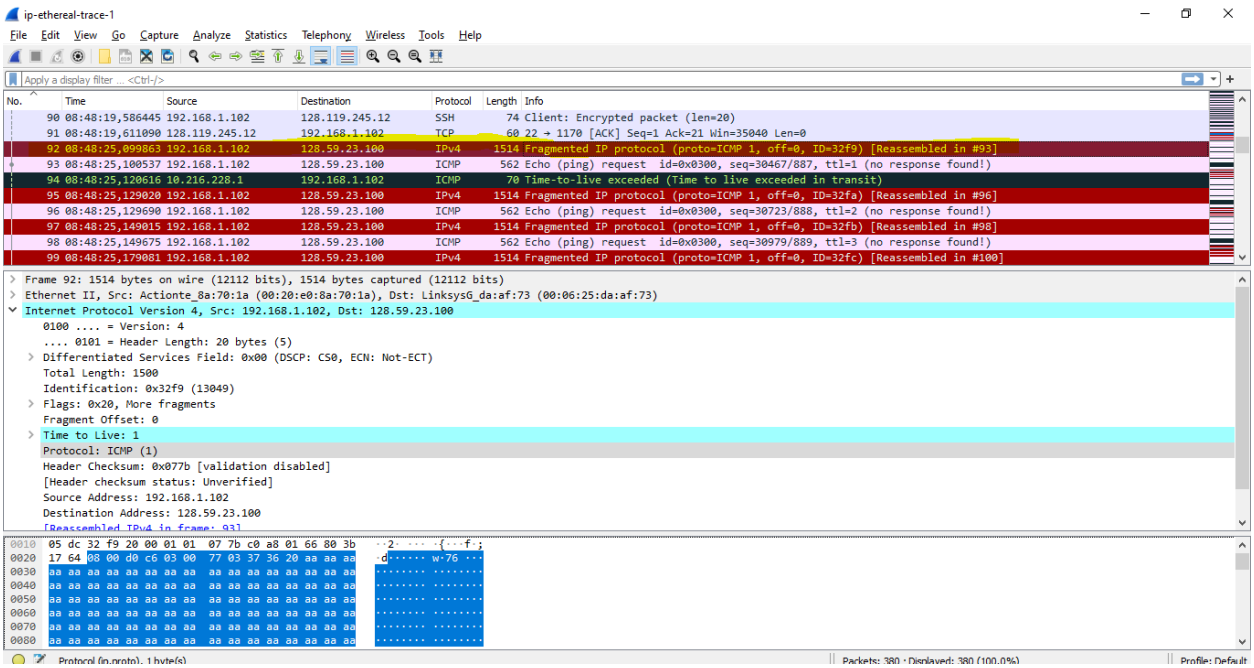
- The TLL field does not change because the time to live to the first hop router is always the same.

Part 2: Fragmentation

Question 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, that message has been fragmented across more than one IP datagram.



<u>Question 11:</u> 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?

ANSWER:

- The flag is set for more segments
  => Datagram has been fragmented
- The fragment offset = 0
  => 1st fragment (not a latter fragment)
- The datagram has a total length = 1500.

```
No.     Time              Source              Destination         Protocol Length Info
     92 08:48:25,099863   192.168.1.102       128.59.23.100       IPv4     1514   Fragmented IP protocol (proto=ICMP 1, off=0,
ID=32f9) [Reassembled in #93]
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)
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)
```

Question 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?

ANSWER:

- Fragment offset of 1480 => 2nd fragment
- There are no more fragments because the More Fragment flag is not set

```
No.     Time              Source              Destination         Protocol Length Info
     93 08:48:25,100537   192.168.1.102       128.59.23.100       ICMP     562    Echo (ping) request  id=0x0300, seq=30467/887,
ttl=1 (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)
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
    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)]
        [Frame: 92, payload: 0-1479 (1480 bytes)]
```

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

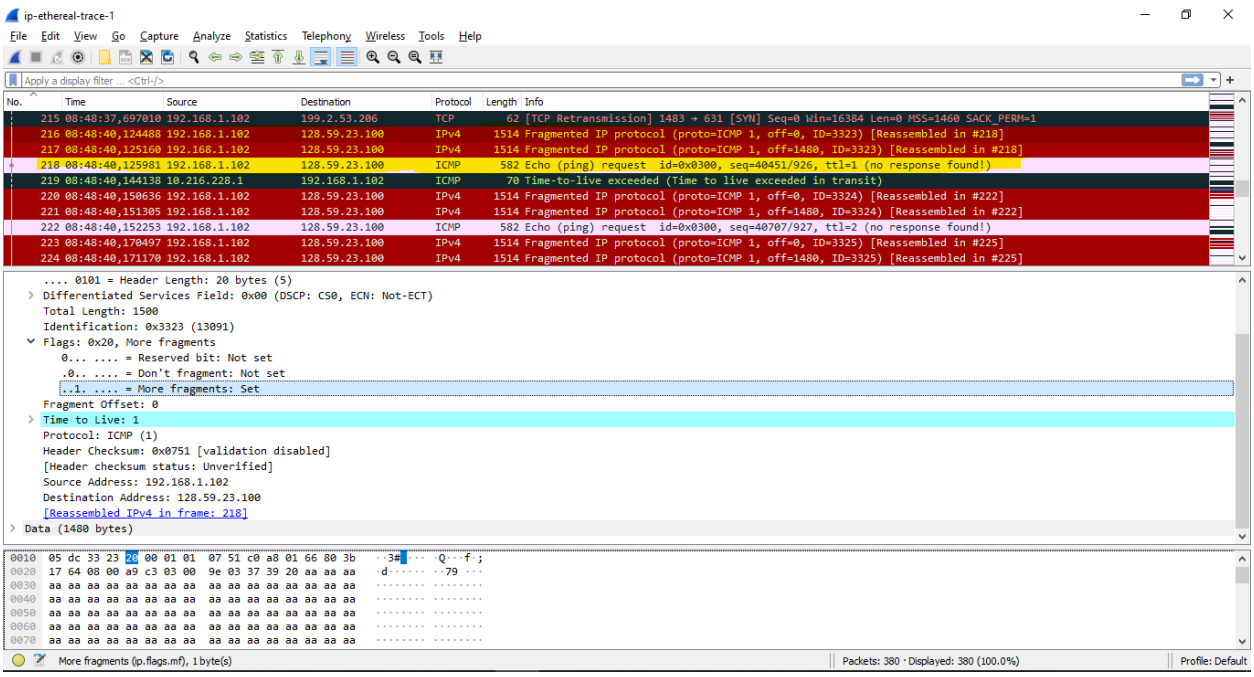
ANSWER:

Total Length
Flags
Fragment offset
Header checksum

Question 14: How many fragments were created from the original datagram?

ANSWER:

There are 3 fragments



Question 15: What fields change in the IP header among the fragments?

ANSWER:

- Between fragments 1, 2, 3: fragment offset and checksum changes
- Between fragments (1, 2) and 3: fragment offset, checksum, total length, the more fragments bit.