ECE361 – Computer Networks

Wireshark Lab 4: IP

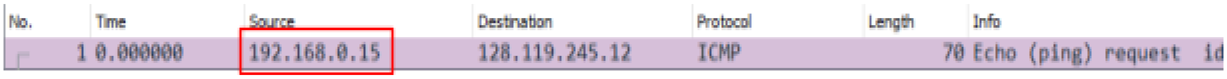
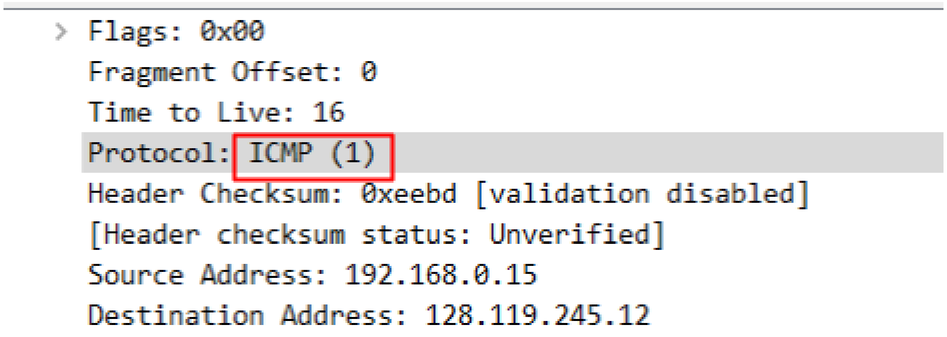
First Name: Tianyi (Nora)   Last Name: Xu

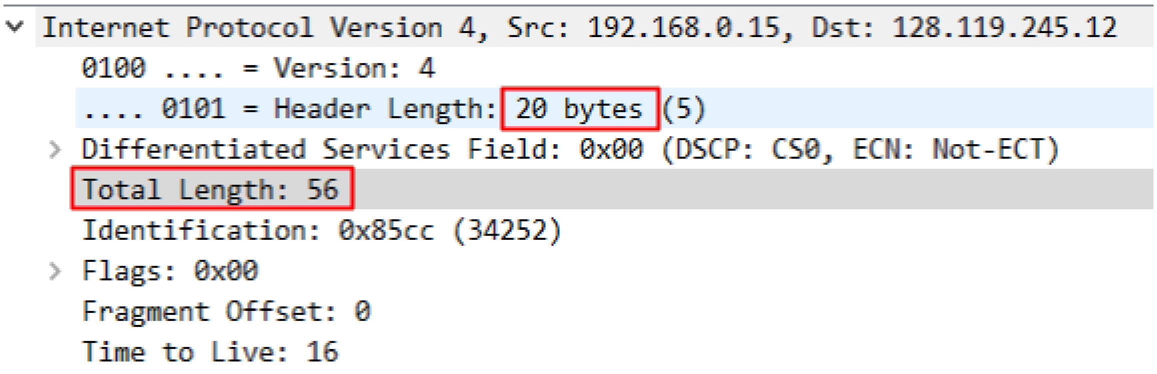
First Name: Yanyi (Will)   Last Name: Zhang

Group Details:

Student #: 1003130809 Student #: 1003327517

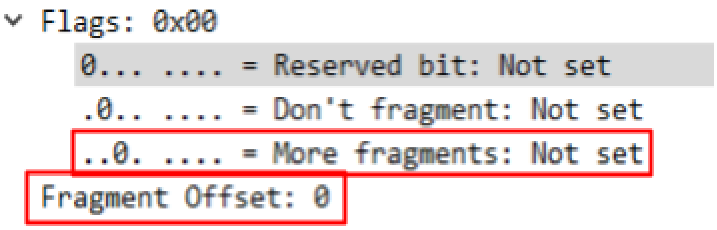
Mark:

<table>
<tr><th></th><th>Question</th><th>Answer</th></tr>
<tr><td>1</td><td>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?</td><td>IP address of my computer:
192.168.0.15</td></tr>
<tr><td colspan="3">
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.0.15 128.119.245.12 ICMP 70 Echo (ping) request id</td></tr>
<tr><td>2</td><td>Within the IP packet header, what is the value in the upper layer protocol field?</td><td>1(ICMP)</td></tr>
<tr><td colspan="3">
Flags: 0x00
Fragment Offset: 0
Time to Live: 16
Protocol: ICMP (1)
Header Checksum: 0xeebd [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.0.15
Destination Address: 128.119.245.12</td></tr>
<tr><td>3</td><td>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.</td><td>Bytes in the IP header = 20 bytes
Bytes in the payload = total length of IP datagram - header length = 56 - 20 = 36 bytes</td></tr>
</table>



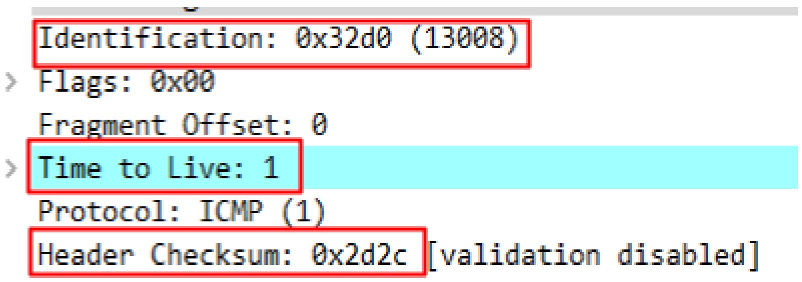
```
⌄ Internet Protocol Version 4, Src: 192.168.0.15, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x85cc (34252)
  › Flags: 0x00
    Fragment Offset: 0
    Time to Live: 16
```

4	Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.	No.Since the fragment offset bit is zero, it means this fragment is the first fragment. The more fragments bit is not set meaning there are no fragments following this fragment. It implies that this is the last fragment in the packet. Therefore, the IP datagram has not been fragmented.



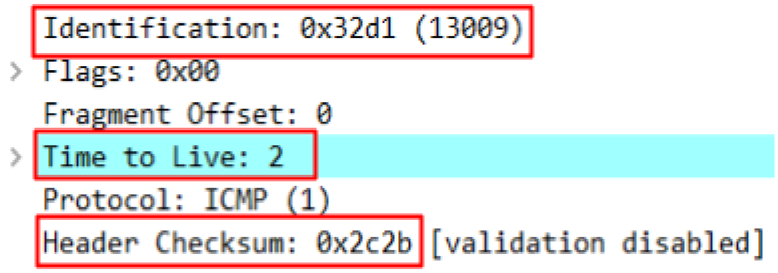
```
⌄ Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment Offset: 0
```

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?	Time to Live, Identification ID and checksum.



```
  Identification: 0x32d0 (13008)
› Flags: 0x00
  Fragment Offset: 0
› Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x2d2c [validation disabled]
```

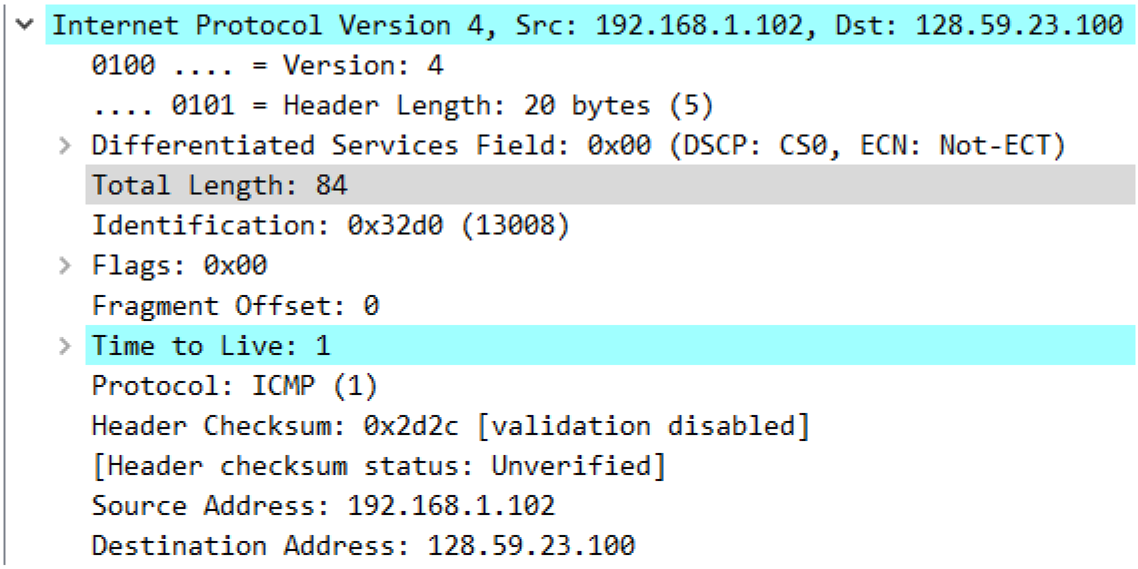
Packet 1



```
  Identification: 0x32d1 (13009)
> Flags: 0x00
  Fragment Offset: 0
> Time to Live: 2
  Protocol: ICMP (1)
  Header Checksum: 0x2c2b [validation disabled]
```

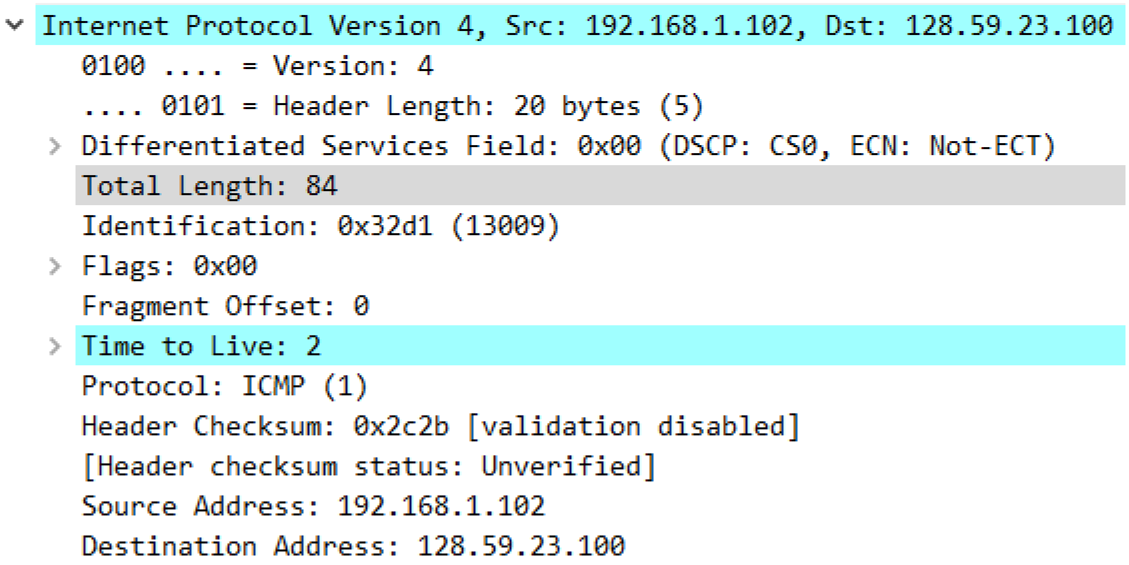
Packet 2

6	Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?	IP protocol version, header length, type of service, upper layer protocol source IP address, and destination IP address must stay constant. This is because the way ICMP works. It sends identical packets and only varies the TTL field to detect the distance from source to destination. Time to live and identification must change. Time to live chances due to the way ICMP works which is mentioned above. Identification ID changes since each packet is different.



```
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: 0x00
    Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
```

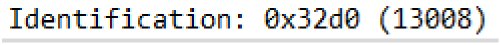
Packet 1



```
∨ 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: 0x32d1 (13009)
  > Flags: 0x00
    Fragment Offset: 0
  > Time to Live: 2
    Protocol: ICMP (1)
    Header Checksum: 0x2c2b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
```

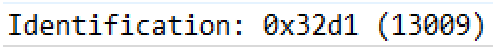
Packet 2

7	Describe the pattern you see in the values in the Identification field of the IP datagram.	The identification increment by 1 for each IP datagram.



```
Identification: 0x32d0 (13008)
```

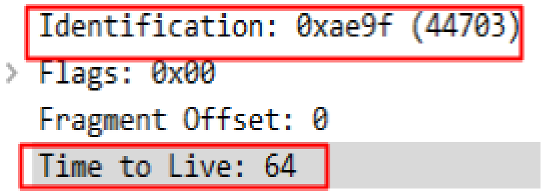
packet 1



```
Identification: 0x32d1 (13009)
```

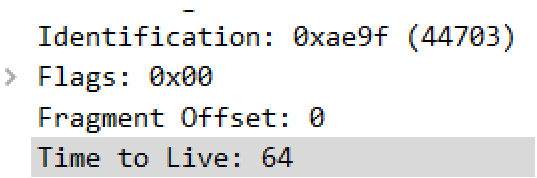
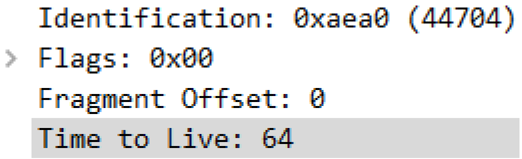
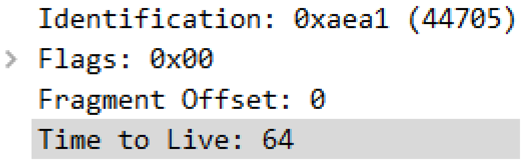
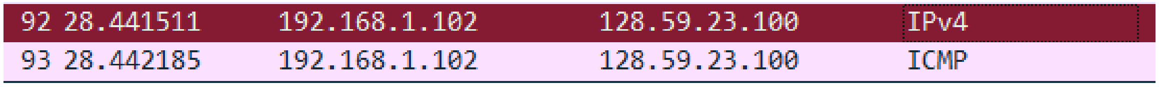
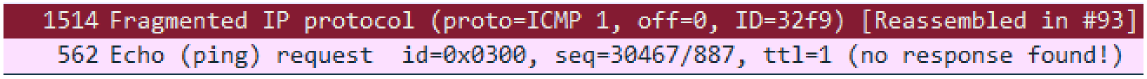
packet 2

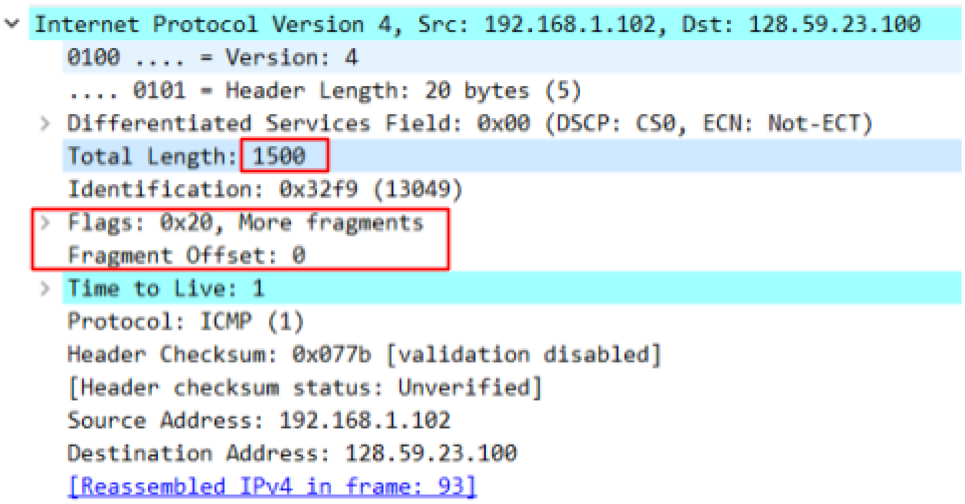
8	What is the value in the Identification field and the TTL field?	Identification: 0xae9f (44703) TTL: 64



```
  Identification: 0xae9f (44703)
> Flags: 0x00
  Fragment Offset: 0
  Time to Live: 64
```

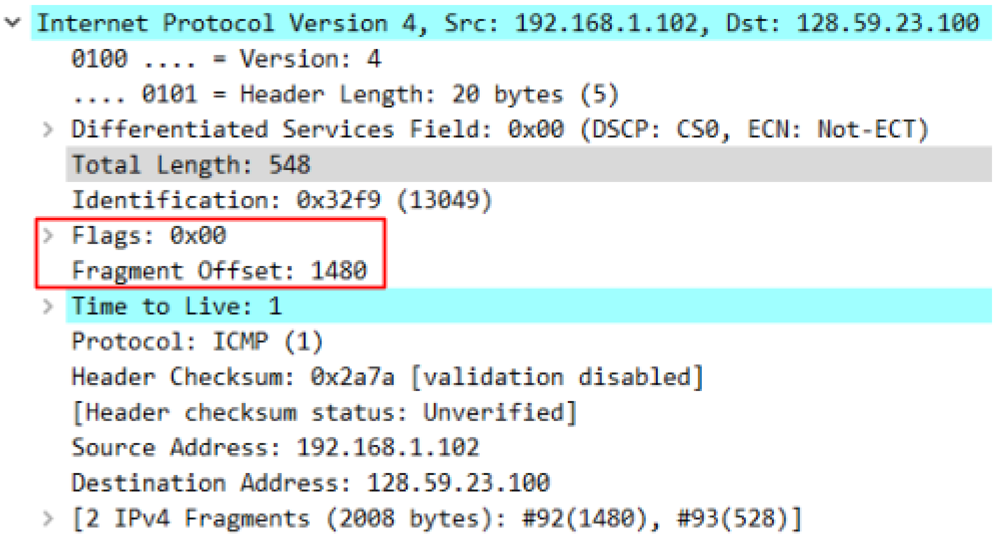
9	Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?	No. The identifications of the subsequent TTL-exceeded replies incremented by 1. The TTL stays constant at 64 since it is the recommended initial TTL value.

 Identification: 0xae9f (44703) Flags: 0x00 Fragment Offset: 0 Time to Live: 64 Packet 1  Identification: 0xaea0 (44704) Flags: 0x00 Fragment Offset: 0 Time to Live: 64 Packet 2  Identification: 0xaea1 (44705) Flags: 0x00 Fragment Offset: 0 Time to Live: 64 Packet 3		
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 message is fragmented into 2 IP datagrams. The "Info" column says fragmented IP protocol.
 92 28.441511 192.168.1.102 128.59.23.100 IPv4 93 28.442185 192.168.1.102 128.59.23.100 ICMP  1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93] 562 Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no response found!)		
11	Print out the first fragment of the fragmented IP datagram. 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 versus a latter fragment? How long is this IP datagram?	The "more fragments" flag indicates that the datagram has been fragmented. The fragment offset of 0 indicates this is the first fragment. The length of the IP datagram is 1500 bytes.



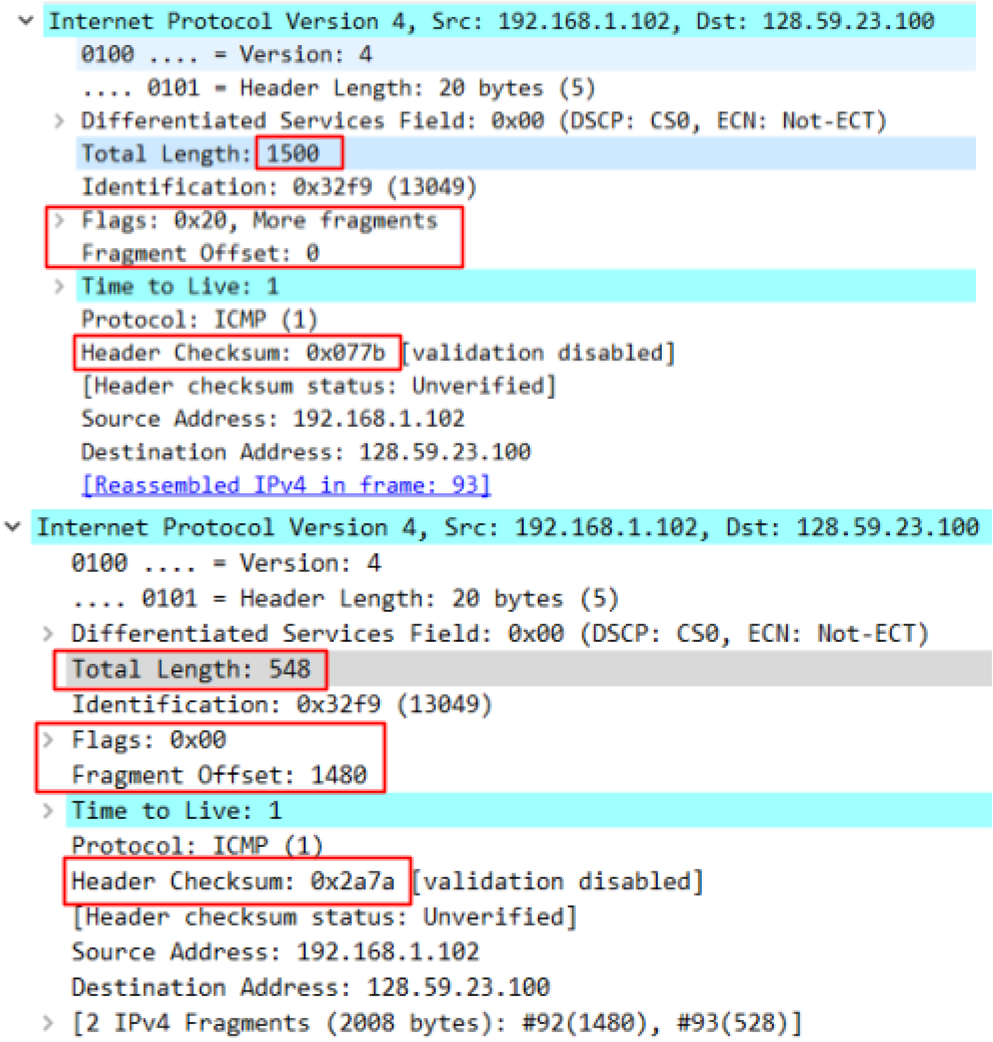
```
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x32f9 (13049)
  > Flags: 0x20, More fragments
    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]
```

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?	The fragment offset is non-zero meaning that this is not the first datagram fragment. The “more fragments” bit is unset indicating there are no more fragments.



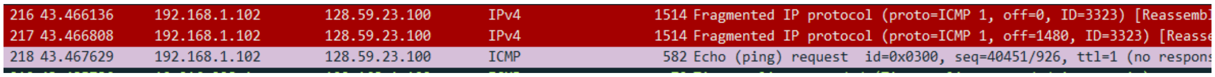
```
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 548
    Identification: 0x32f9 (13049)
  > Flags: 0x00
    Fragment Offset: 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)]
```

13	What fields change in the IP header between the first and second fragment?	Flags, fragment offset, packet total length and checksum.



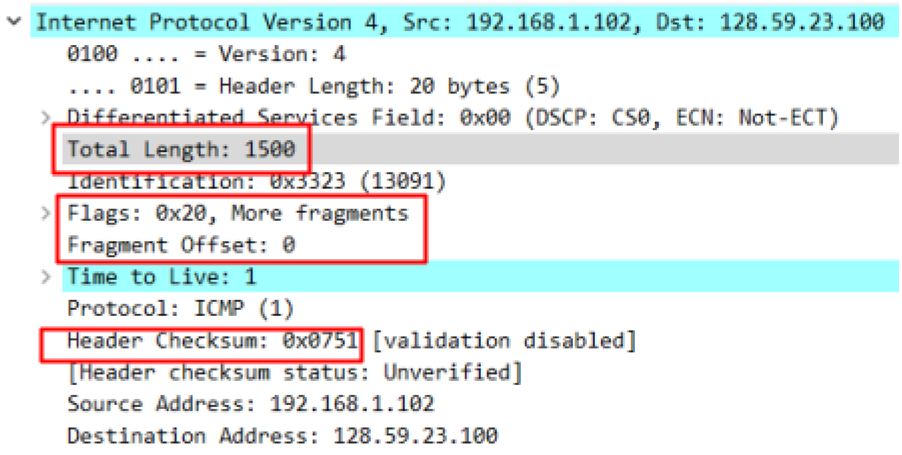
```
∨ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x32f9 (13049)
  > Flags: 0x20, More fragments
    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]
∨ 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
    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)]
```

14	How many fragments were created from the original datagram?	3 fragments. And the size of payload of each fragment is respectively 1480, 1480, 540, which gives a sum of 3500.



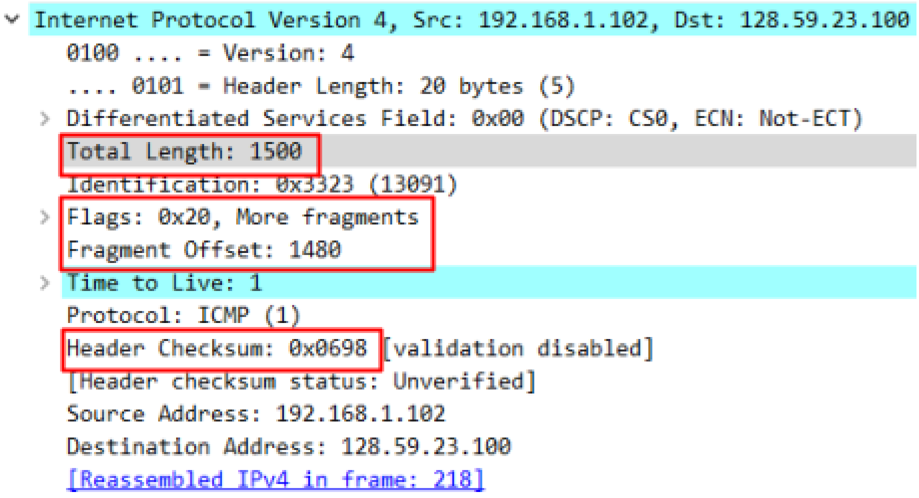
```
216 43.466136   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembl
217 43.466808   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reasse
218 43.467629   192.168.1.102   128.59.23.100   ICMP    582 Echo (ping) request  id=0x0300, seq=40451/926, ttl=1 (no respons
```

15	What fields change in the IP header among the fragments?	Flags, fragment offset, packet total length and checksum.



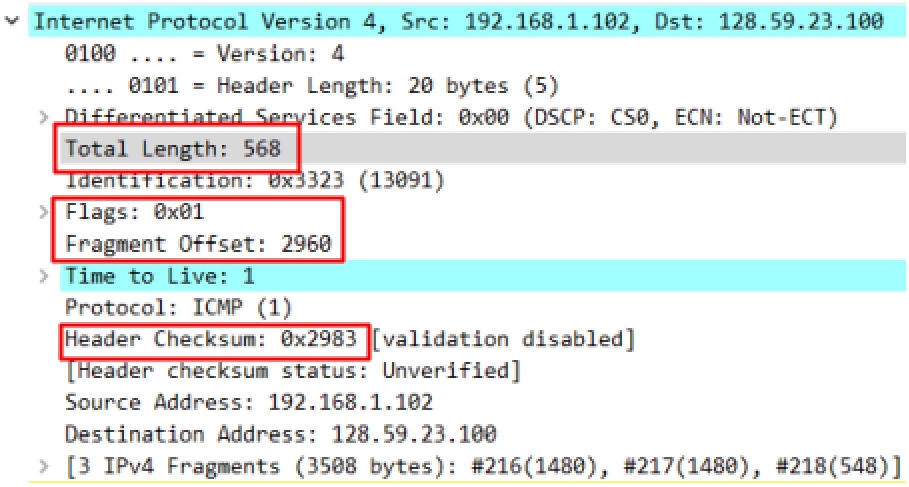
```
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x3323 (13091)
    Flags: 0x20, More fragments
    Fragment Offset: 0
    Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0751 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
```

Packet 1



```
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: 0x20, More fragments
    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]
```

Packet 2



```
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: 0x01
    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)]
```

Packet 3