Vlad Predovic

CS 372
Summer 2016

Lab 3: IP

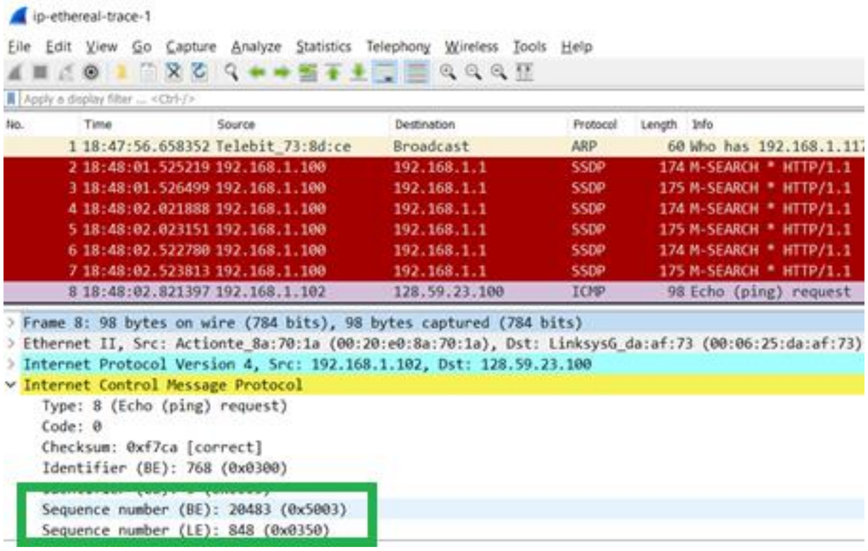
NOTE: USED IP-ETHEREAL-TRACE-1 for homework

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?

My computer: 192.168.1.102

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

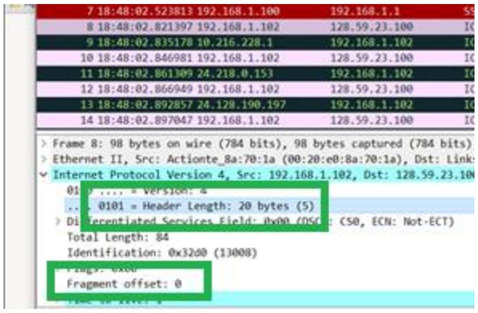
The value in the upper layer protocol field is ICMP 0x5003


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
    1 18:47:56.658352 Telebit_73:8d:ce     Broadcast       ARP          60 Who has 192.168.1.11
    2 18:48:01.525219 192.168.1.100        192.168.1.1     SSDP        174 M-SEARCH * HTTP/1.1
    3 18:48:01.526499 192.168.1.100        192.168.1.1     SSDP        175 M-SEARCH * HTTP/1.1
    4 18:48:02.021888 192.168.1.100        192.168.1.1     SSDP        174 M-SEARCH * HTTP/1.1
    5 18:48:02.023151 192.168.1.100        192.168.1.1     SSDP        175 M-SEARCH * HTTP/1.1
    6 18:48:02.522780 192.168.1.100        192.168.1.1     SSDP        174 M-SEARCH * HTTP/1.1
    7 18:48:02.523813 192.168.1.100        192.168.1.1     SSDP        175 M-SEARCH * HTTP/1.1
    8 18:48:02.821397 192.168.1.102        128.59.23.100   ICMP         98 Echo (ping) request

> 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)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7ca [correct]
    Identifier (BE): 768 (0x0300)
    Sequence number (BE): 20483 (0x5003)
    Sequence number (LE): 848 (0x0350)
```

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.



```
 7 18:48:02.523813 192.168.1.100      192.168.1.1
 8 18:48:02.821397 192.168.1.102      128.59.23.100
 9 18:48:02.835178 10.216.228.1       192.168.1.102
10 18:48:02.846981 192.168.1.102      128.59.23.100
11 18:48:02.861309 24.218.0.153       192.168.1.102
12 18:48:02.866949 192.168.1.102      128.59.23.100
13 18:48:02.892857 24.128.190.197     192.168.1.102
14 18:48:02.897047 192.168.1.102      128.59.23.100

> 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: Link
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.10
    01 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d0 (13008)
    Fragment offset: 0
```

There are 20 bytes in the IP header. In the instructions it said to initially send packets of length 56 bytes. Therefore, the payload must be 36 bytes.

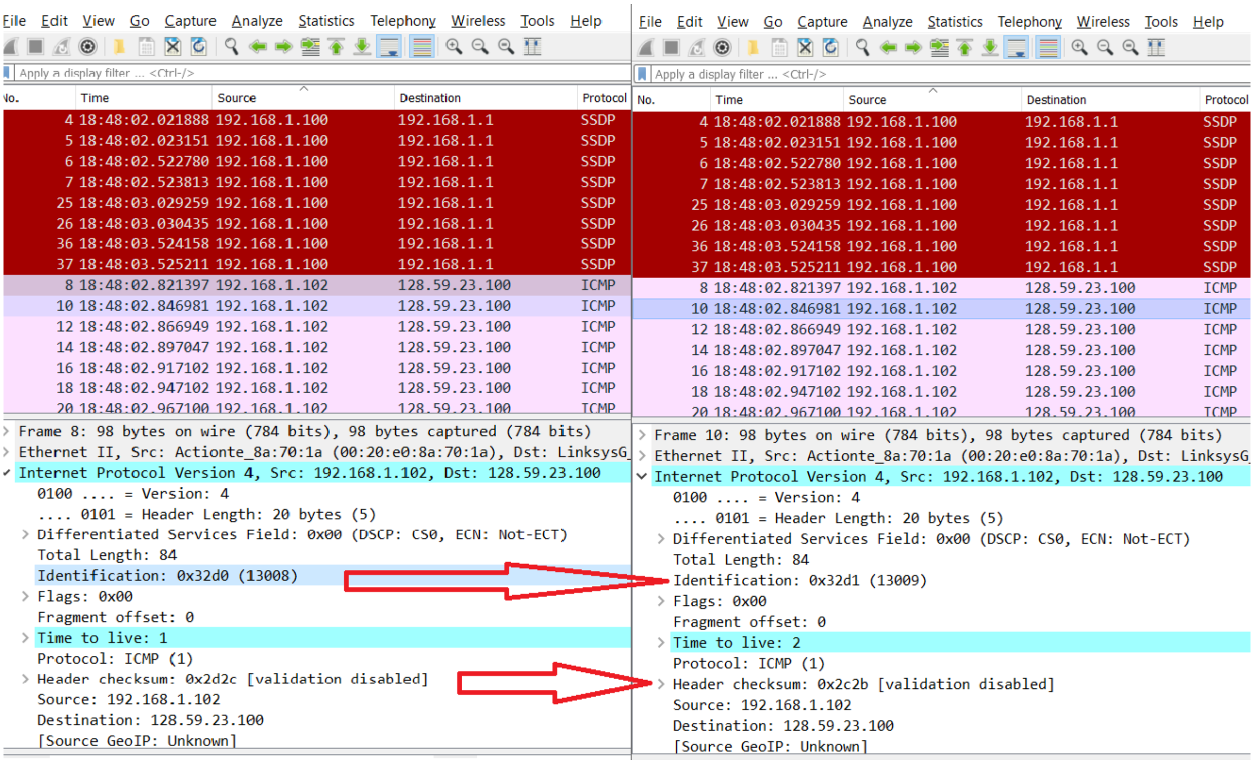
4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

The IP datagram has not been fragmented. You can tell because the flag is not set 0x00 and the fragment offset 0.

Next, sort the traced packets according to IP source address by clicking on the Source column header; a small downward pointing arrow should appear next to the word Source. If the arrow points up, click on the Source column header again. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol portion in the "details of selected packet header" window. In the "listing of captured packets" window, you should see all of the subsequent ICMP messages (perhaps with additional interspersed packets sent by other protocols running on your computer) below this first ICMP. Use the down arrow to move through the ICMP messages sent by your computer.

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?

Frame number, header checksum, Time to live, and Identification


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time            Source         Destination    Protocol
   4 18:48:02.021888 192.168.1.100  192.168.1.1    SSDP
   5 18:48:02.023151 192.168.1.100  192.168.1.1    SSDP
   6 18:48:02.522780 192.168.1.100  192.168.1.1    SSDP
   7 18:48:02.523813 192.168.1.100  192.168.1.1    SSDP
  25 18:48:03.029259 192.168.1.100  192.168.1.1    SSDP
  26 18:48:03.030435 192.168.1.100  192.168.1.1    SSDP
  36 18:48:03.524158 192.168.1.100  192.168.1.1    SSDP
  37 18:48:03.525211 192.168.1.100  192.168.1.1    SSDP
   8 18:48:02.821397 192.168.1.102  128.59.23.100  ICMP
  10 18:48:02.846981 192.168.1.102  128.59.23.100  ICMP
  12 18:48:02.866949 192.168.1.102  128.59.23.100  ICMP
  14 18:48:02.897047 192.168.1.102  128.59.23.100  ICMP
  16 18:48:02.917102 192.168.1.102  128.59.23.100  ICMP
  18 18:48:02.947102 192.168.1.102  128.59.23.100  ICMP
  20 18:48:02.967100 192.168.1.102  128.59.23.100  ICMP
```

```
> 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_
✓ 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]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time            Source         Destination    Protocol
   4 18:48:02.021888 192.168.1.100  192.168.1.1    SSDP
   5 18:48:02.023151 192.168.1.100  192.168.1.1    SSDP
   6 18:48:02.522780 192.168.1.100  192.168.1.1    SSDP
   7 18:48:02.523813 192.168.1.100  192.168.1.1    SSDP
  25 18:48:03.029259 192.168.1.100  192.168.1.1    SSDP
  26 18:48:03.030435 192.168.1.100  192.168.1.1    SSDP
  36 18:48:03.524158 192.168.1.100  192.168.1.1    SSDP
  37 18:48:03.525211 192.168.1.100  192.168.1.1    SSDP
   8 18:48:02.821397 192.168.1.102  128.59.23.100  ICMP
  10 18:48:02.846981 192.168.1.102  128.59.23.100  ICMP
  12 18:48:02.866949 192.168.1.102  128.59.23.100  ICMP
  14 18:48:02.897047 192.168.1.102  128.59.23.100  ICMP
  16 18:48:02.917102 192.168.1.102  128.59.23.100  ICMP
  18 18:48:02.947102 192.168.1.102  128.59.23.100  ICMP
  20 18:48:02.967100 192.168.1.102  128.59.23.100  ICMP
```

```
> Frame 10: 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_
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: 0x32d1 (13009)
  > Flags: 0x00
    Fragment offset: 0
  > Time to live: 2
    Protocol: ICMP (1)
  > Header checksum: 0x2c2b [validation disabled]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
```

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

Constant fields: Version, Header length, source IP(same source), Destination IP(same place), Upper layer protocol,

Fields that change are the checksum because the header changes with each different packet and the Identification which is used to verify each individual packet.

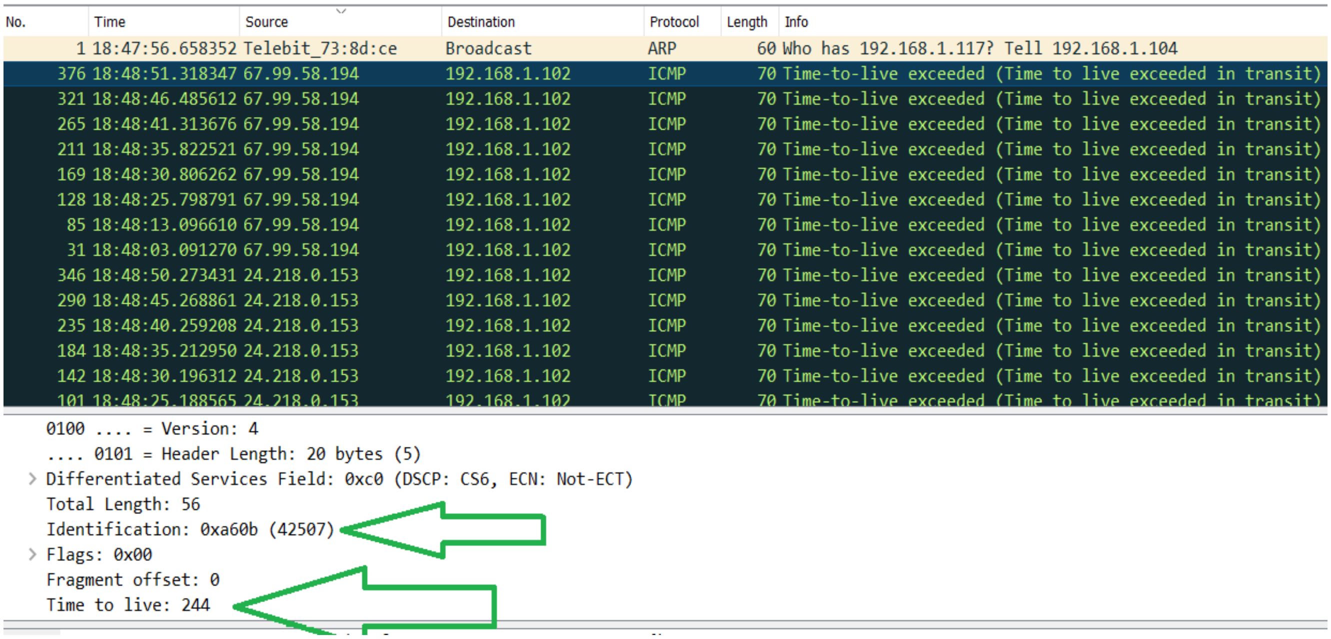
7. Describe the pattern you see in the values in the Identification field of the IP datagram

It goes up by one each time in the echo frames. (As can be seen in the picture above question 6)

Next (with the packets still sorted by source address) find the series of ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router.

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

Identification: 0xa60b (42507
Time to live: 244



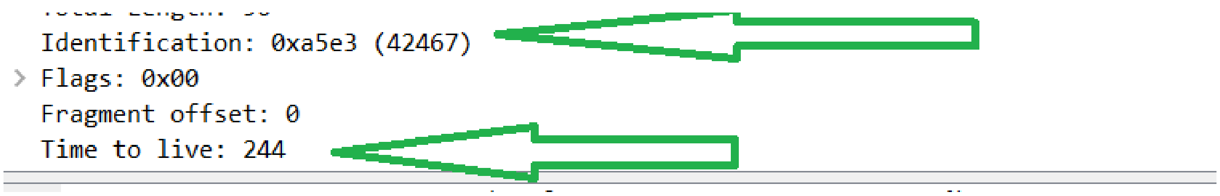
```
No.   Time              Source           Destination    Protocol Length Info
    1 18:47:56.658352 Telebit_73:8d:ce Broadcast      ARP        60 Who has 192.168.1.117? Tell 192.168.1.104
  376 18:48:51.318347 67.99.58.194     192.168.1.102  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  321 18:48:46.485612 67.99.58.194     192.168.1.102  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  265 18:48:41.313676 67.99.58.194     192.168.1.102  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  211 18:48:35.822521 67.99.58.194     192.168.1.102  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  169 18:48:30.806262 67.99.58.194     192.168.1.102  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  128 18:48:25.798791 67.99.58.194     192.168.1.102  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
   85 18:48:13.096610 67.99.58.194     192.168.1.102  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
   31 18:48:03.091270 67.99.58.194     192.168.1.102  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  346 18:48:50.273431 24.218.0.153     192.168.1.102  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  290 18:48:45.268861 24.218.0.153     192.168.1.102  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  235 18:48:40.259208 24.218.0.153     192.168.1.102  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  184 18:48:35.212950 24.218.0.153     192.168.1.102  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  142 18:48:30.196312 24.218.0.153     192.168.1.102  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  101 18:48:25.188565 24.218.0.153     192.168.1.102  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)

    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xa60b (42507)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 244
```

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 identification field is used to separate unique packets. If two were to have the same one, it would suggest they were fragments of the same packet. Therefore, this field continually changes.

However, the TTL field will not change because regardless of the packet number, it will always have to go the same number of steps to reach its destination.

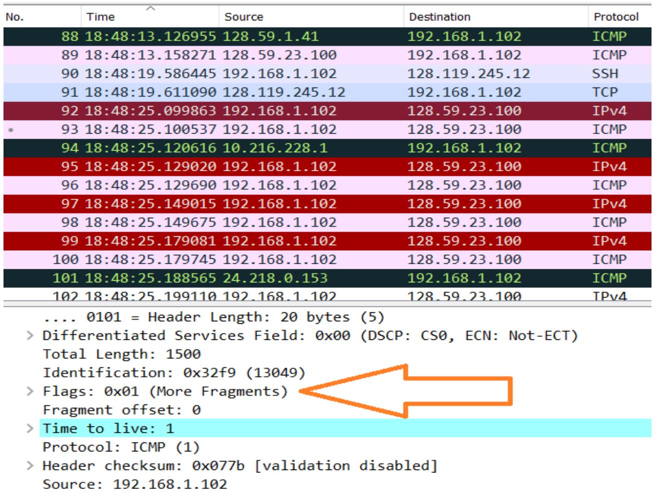


```
    Identification: 0xa5e3 (42467)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 244
```

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? [Note: if you find your packet has not been fragmented, you should download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the *ipethereal-trace-1*packet trace. If your computer has an Ethernet interface, a packet size of 2000 *should* cause fragmentation.[3]]



No.	Time	Source	Destination	Protocol
88	18:48:13.126955	128.59.1.41	192.168.1.102	ICMP
89	18:48:13.158271	128.59.23.100	192.168.1.102	ICMP
90	18:48:19.586445	192.168.1.102	128.119.245.12	SSH
91	18:48:19.611090	128.119.245.12	192.168.1.102	TCP
92	18:48:25.099863	192.168.1.102	128.59.23.100	IPv4
93	18:48:25.100537	192.168.1.102	128.59.23.100	ICMP
94	18:48:25.120616	10.216.228.1	192.168.1.102	ICMP
95	18:48:25.129020	192.168.1.102	128.59.23.100	IPv4
96	18:48:25.129690	192.168.1.102	128.59.23.100	ICMP
97	18:48:25.149015	192.168.1.102	128.59.23.100	IPv4
98	18:48:25.149675	192.168.1.102	128.59.23.100	ICMP
99	18:48:25.179081	192.168.1.102	128.59.23.100	IPv4
100	18:48:25.179745	192.168.1.102	128.59.23.100	ICMP
101	18:48:25.188565	24.218.0.153	192.168.1.102	ICMP
102	18:48:25.199110	192.168.1.102	128.59.23.100	IPv4

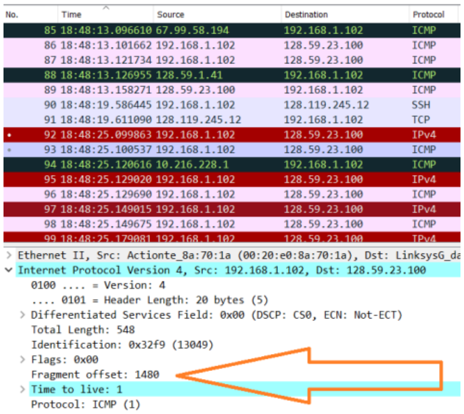
```
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x32f9 (13049)
  > Flags: 0x01 (More Fragments)
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
  > Header checksum: 0x077b [validation disabled]
    Source: 192.168.1.102
```

Yes, that message has been fragmented as noted by the orange arrow.

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?

First fragment is printed out above (under question 10). You can tell it is the first fragment because the flag is set to 0x01 and the offset is set to 0 (which happens when it is the first fragment)

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?



```
No.   Time                Source           Destination      Protocol
   85 18:48:13.096610 67.99.58.194      192.168.1.102    ICMP
   86 18:48:13.101662 192.168.1.102     128.59.23.100    ICMP
   87 18:48:13.121734 192.168.1.102     128.59.23.100    ICMP
   88 18:48:13.126955 128.59.1.41       192.168.1.102    ICMP
   89 18:48:13.158271 128.59.23.100     192.168.1.102    ICMP
   90 18:48:19.586445 192.168.1.102     128.119.245.12   SSH
   91 18:48:19.611090 128.119.245.12    192.168.1.102    TCP
   92 18:48:25.099863 192.168.1.102     128.59.23.100    IPv4
   93 18:48:25.100537 192.168.1.102     128.59.23.100    ICMP
   94 18:48:25.120616 10.216.228.1      192.168.1.102    ICMP
   95 18:48:25.129020 192.168.1.102     128.59.23.100    IPv4
   96 18:48:25.129690 192.168.1.102     128.59.23.100    ICMP
   97 18:48:25.149015 192.168.1.102     128.59.23.100    IPv4
   98 18:48:25.149675 192.168.1.102     128.59.23.100    ICMP
   99 18:48:25.179081 192.168.1.102     128.59.23.100    IPv4

> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da
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)
```

Fragment offset is set to 1480. Thi suggests that it is the second part of the fragment. Since the packets were 2000 bytes long and the flag is not set (0x00), This is the second and last fragment.

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

The header checksum, the fragment offset, the flag field, and the legth of the transmitted packet.

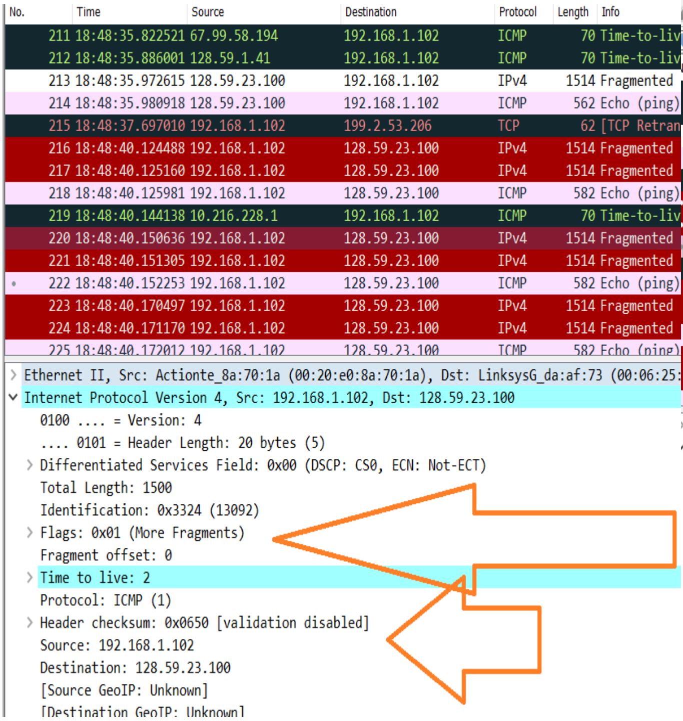
Now find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 3500.

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

3 fragments with offsets 0, 1480, and 2060

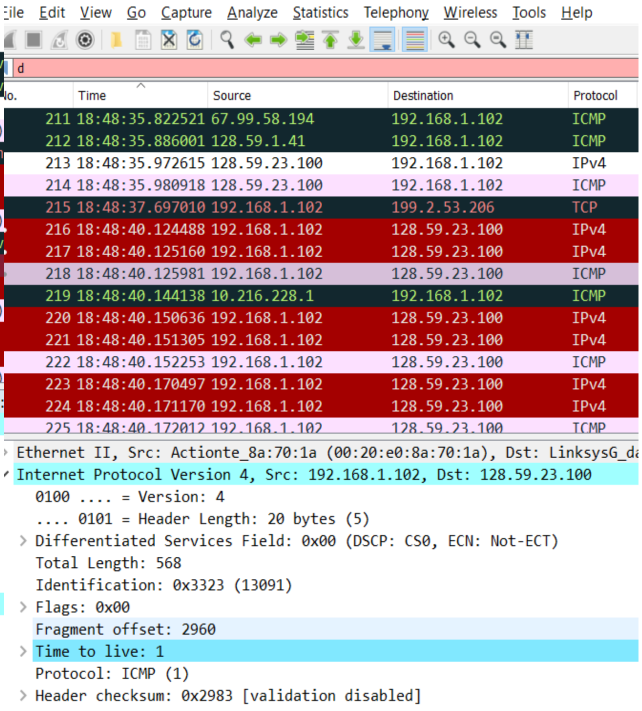
15. What fields change in the IP header among the fragments?

The header checksum, the fragment offset, the flag field, and the legth of the transmitted packet.



```
No.   Time                Source           Destination      Protocol  Length  Info
  211 18:48:35.822521 67.99.58.194      192.168.1.102    ICMP        70 Time-to-liv
  212 18:48:35.886001 128.59.1.41       192.168.1.102    ICMP        70 Time-to-liv
  213 18:48:35.972615 128.59.23.100     192.168.1.102    IPv4      1514 Fragmented
  214 18:48:35.980918 128.59.23.100     192.168.1.102    ICMP       562 Echo (ping)
  215 18:48:37.697010 192.168.1.102     199.2.53.206     TCP         62 [TCP Retran
  216 18:48:40.124488 192.168.1.102     128.59.23.100    IPv4      1514 Fragmented
  217 18:48:40.125160 192.168.1.102     128.59.23.100    IPv4      1514 Fragmented
  218 18:48:40.125981 192.168.1.102     128.59.23.100    ICMP       582 Echo (ping)
  219 18:48:40.144138 10.216.228.1      192.168.1.102    ICMP        70 Time-to-liv
  220 18:48:40.150636 192.168.1.102     128.59.23.100    IPv4      1514 Fragmented
  221 18:48:40.151305 192.168.1.102     128.59.23.100    IPv4      1514 Fragmented
  222 18:48:40.152253 192.168.1.102     128.59.23.100    ICMP       582 Echo (ping)
  223 18:48:40.170497 192.168.1.102     128.59.23.100    IPv4      1514 Fragmented
  224 18:48:40.171170 192.168.1.102     128.59.23.100    IPv4      1514 Fragmented
  225 18:48:40.172012 192.168.1.102     128.59.23.100    ICMP       582 Echo (ping)

> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:
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: 0x3324 (13092)
  > Flags: 0x01 (More Fragments)
    Fragment offset: 0
  > Time to live: 2
    Protocol: ICMP (1)
  > Header checksum: 0x0650 [validation disabled]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
No.   Time                Source           Destination      Protocol
  211 18:48:35.822521 67.99.58.194      192.168.1.102    ICMP
  212 18:48:35.886001 128.59.1.41       192.168.1.102    ICMP
  213 18:48:35.972615 128.59.23.100     192.168.1.102    IPv4
  214 18:48:35.980918 128.59.23.100     192.168.1.102    ICMP
  215 18:48:37.697010 192.168.1.102     199.2.53.206     TCP
  216 18:48:40.124488 192.168.1.102     128.59.23.100    IPv4
  217 18:48:40.125160 192.168.1.102     128.59.23.100    IPv4
  218 18:48:40.125981 192.168.1.102     128.59.23.100    ICMP
  219 18:48:40.144138 10.216.228.1      192.168.1.102    ICMP
  220 18:48:40.150636 192.168.1.102     128.59.23.100    IPv4
  221 18:48:40.151305 192.168.1.102     128.59.23.100    IPv4
  222 18:48:40.152253 192.168.1.102     128.59.23.100    ICMP
  223 18:48:40.170497 192.168.1.102     128.59.23.100    IPv4
  224 18:48:40.171170 192.168.1.102     128.59.23.100    IPv4
  225 18:48:40.172012 192.168.1.102     128.59.23.100    ICMP

> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da
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: 0x3323 (13091)
  > Flags: 0x00
    Fragment offset: 2960
  > Time to live: 1
    Protocol: ICMP (1)
  > Header checksum: 0x2983 [validation disabled]
```