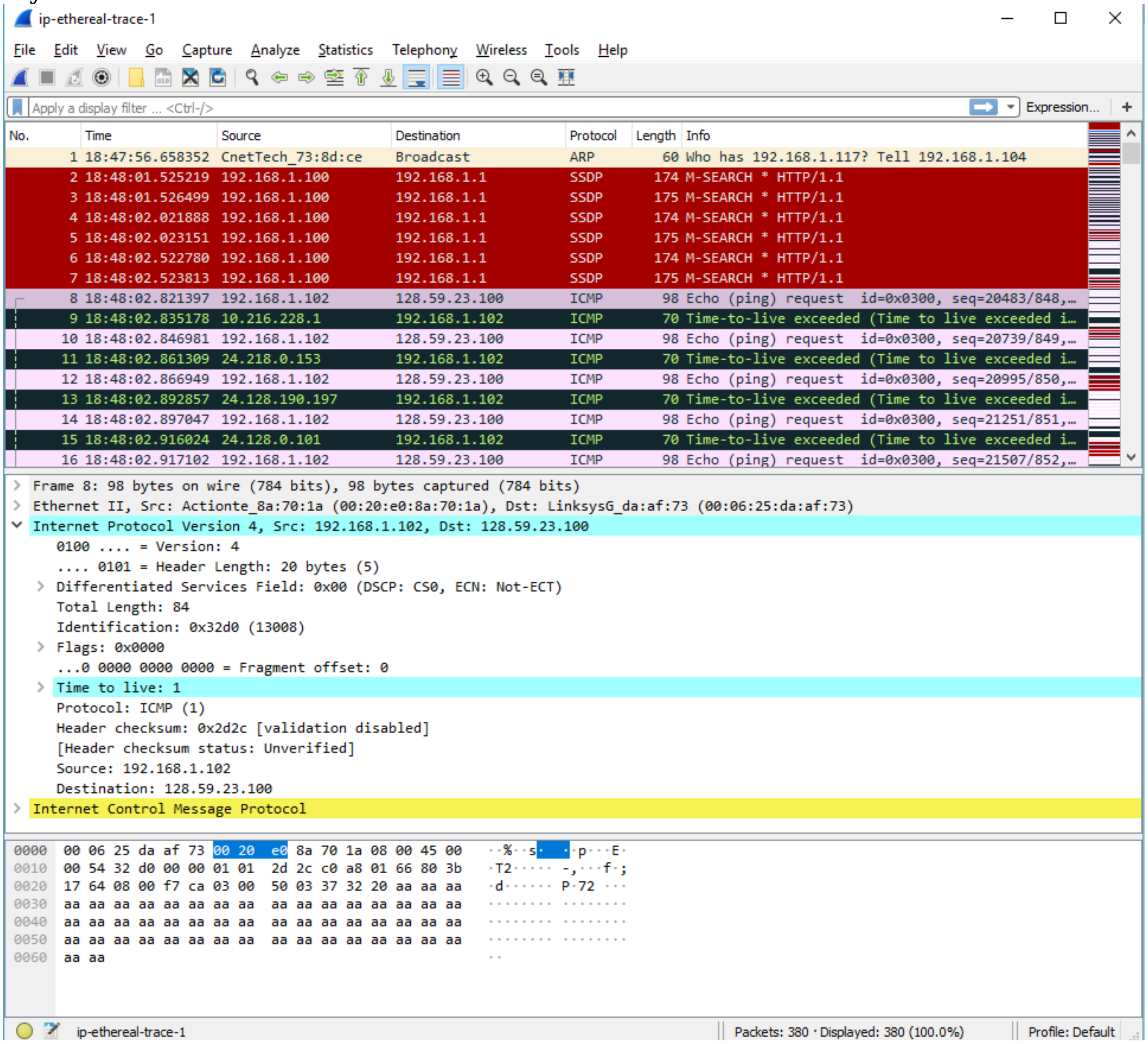
Hao (Jeff) Deng
ID: 932912420

CS 372 – Lab 4

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 IP address is 192.168.1.102

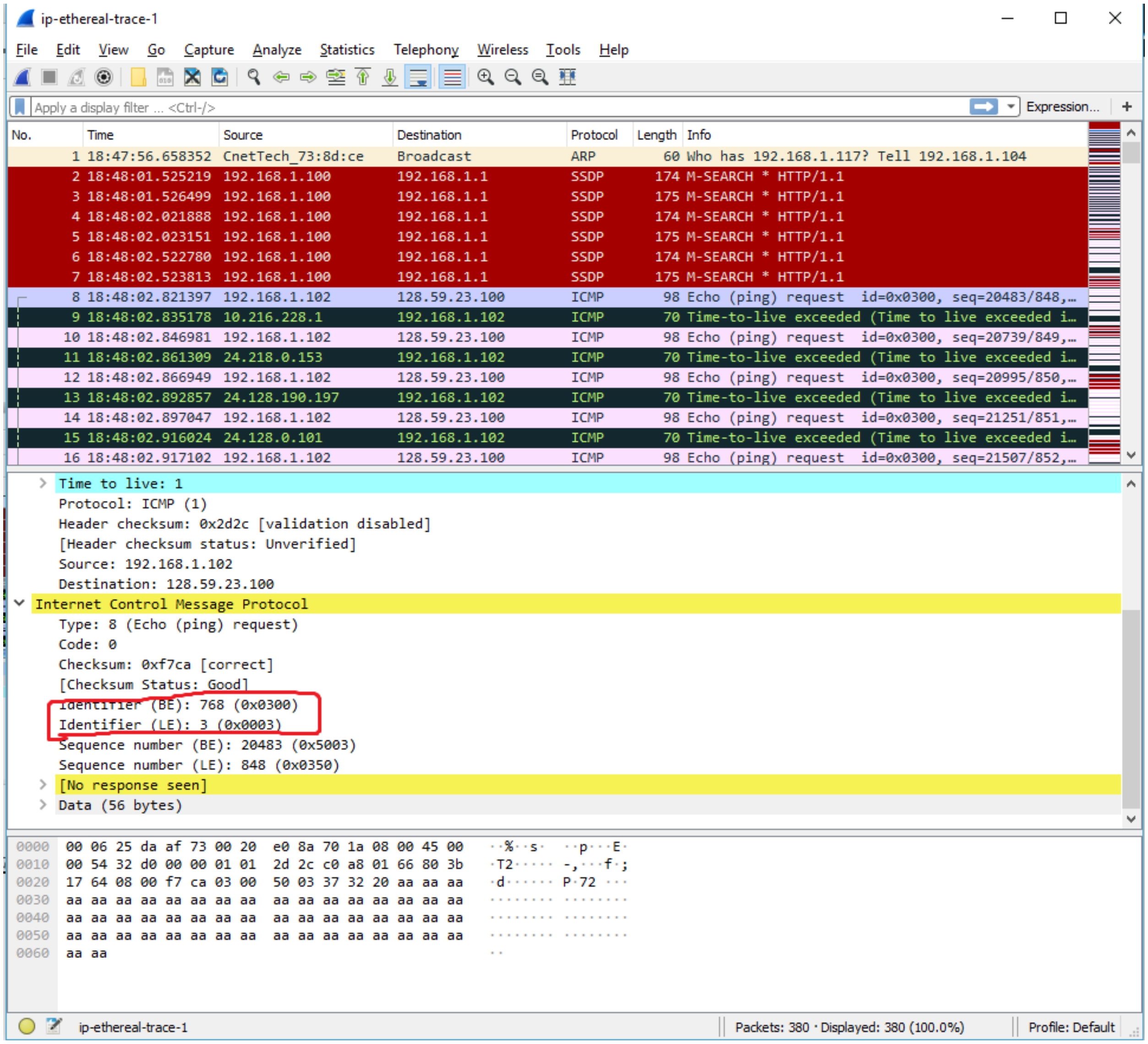


No.	Time	Source	Destination	Protocol	Length	Info
1	18:47:56.658352	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
2	18:48:01.525219	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
3	18:48:01.526499	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
4	18:48:02.021888	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 id=0x0300, seq=20483/848,…
9	18:48:02.835178	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded i…
10	18:48:02.846981	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849,…
11	18:48:02.861309	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded i…
12	18:48:02.866949	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850,…
13	18:48:02.892857	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded i…
14	18:48:02.897047	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851,…
15	18:48:02.916024	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded i…
16	18:48:02.917102	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852,…

```
> 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)
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: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
> Internet Control Message Protocol
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ··%··s· ··p···E·
0010  00 54 32 d0 00 00 01 01  2d 2c c0 a8 01 66 80 3b   ·T2····· -,···f·;
0020  17 64 08 00 f7 ca 03 00  50 03 37 32 20 aa aa aa   ·d······ P·72 ···
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········ ········
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········ ········
0050  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········ ········
0060  aa aa                                              ··
```

2. Within the IP packet header, what is the value in the upper layer protocol field?
   The value of the upper layer protocol field is ICMP (0X03)

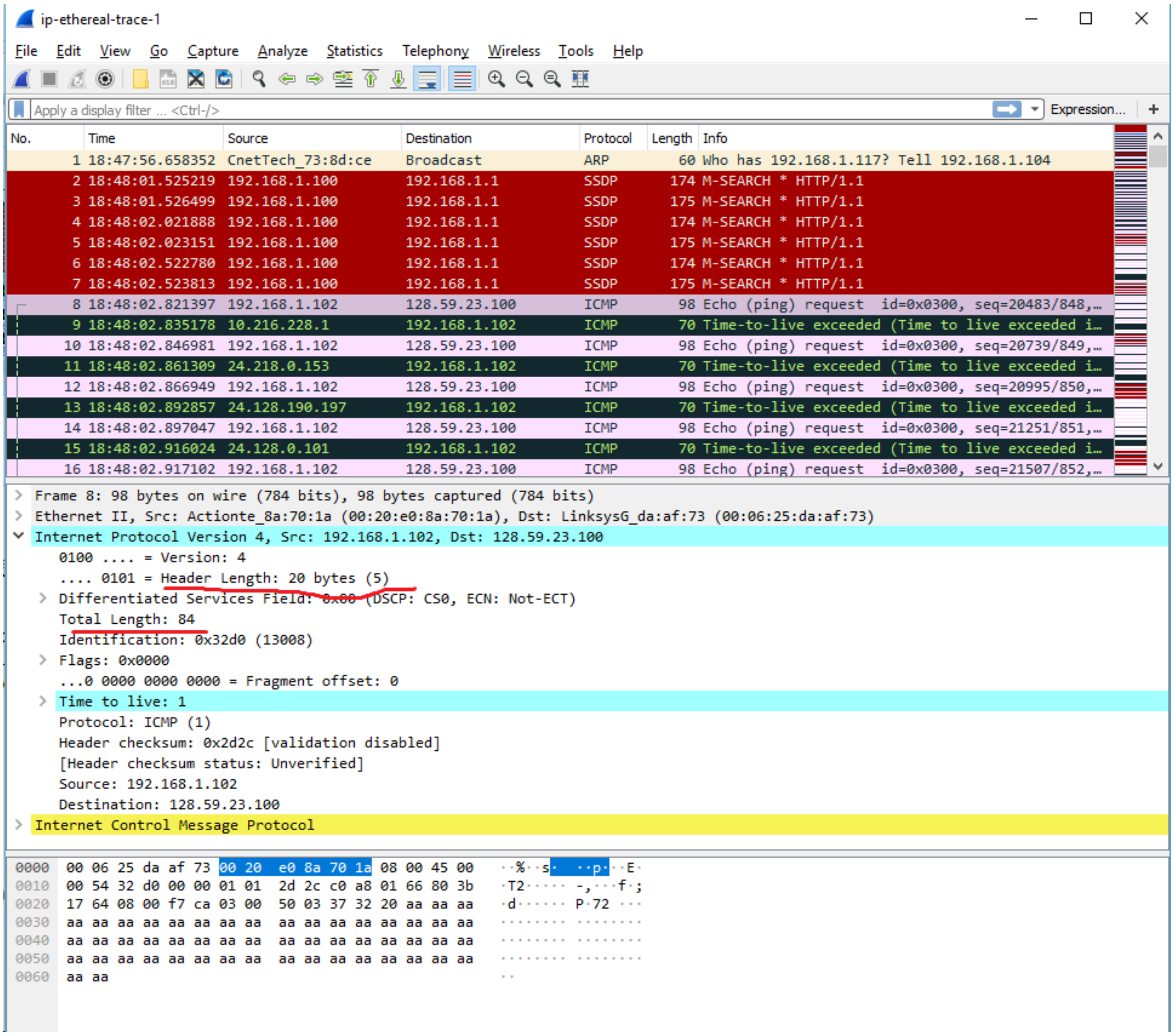

ip-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

```
No.  Time             Source             Destination     Protocol Length Info
   1 18:47:56.658352  CnetTech_73:8d:ce  Broadcast       ARP       60 Who has 192.168.1.117? Tell 192.168.1.104
   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  id=0x0300, seq=20483/848,…
   9 18:48:02.835178  10.216.228.1       192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded i…
  10 18:48:02.846981  192.168.1.102      128.59.23.100   ICMP      98 Echo (ping) request  id=0x0300, seq=20739/849,…
  11 18:48:02.861309  24.218.0.153       192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded i…
  12 18:48:02.866949  192.168.1.102      128.59.23.100   ICMP      98 Echo (ping) request  id=0x0300, seq=20995/850,…
  13 18:48:02.892857  24.128.190.197     192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded i…
  14 18:48:02.897047  192.168.1.102      128.59.23.100   ICMP      98 Echo (ping) request  id=0x0300, seq=21251/851,…
  15 18:48:02.916024  24.128.0.101       192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded i…
  16 18:48:02.917102  192.168.1.102      128.59.23.100   ICMP      98 Echo (ping) request  id=0x0300, seq=21507/852,…
```

```
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7ca [correct]
    [Checksum Status: Good]
    Identifier (BE): 768 (0x0300)
    Identifier (LE): 3 (0x0003)
    Sequence number (BE): 20483 (0x5003)
    Sequence number (LE): 848 (0x0350)
  > [No response seen]
  > Data (56 bytes)
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ··%··s·  ··p···E·
0010  00 54 32 d0 00 00 01 01  2d 2c c0 a8 01 66 80 3b   ·T2·····  -,···f·;
0020  17 64 08 00 f7 ca 03 00  50 03 37 32 20 aa aa aa   ·d······  P·72 ···
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0050  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0060  aa aa                                              ··
```

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.
There are 20 bytes in IP header as shown in the screenshot, and the total length of the packet is 84 bytes.
(84-20=64).
That leaves 64 bytes for the payload of the IP datagram.

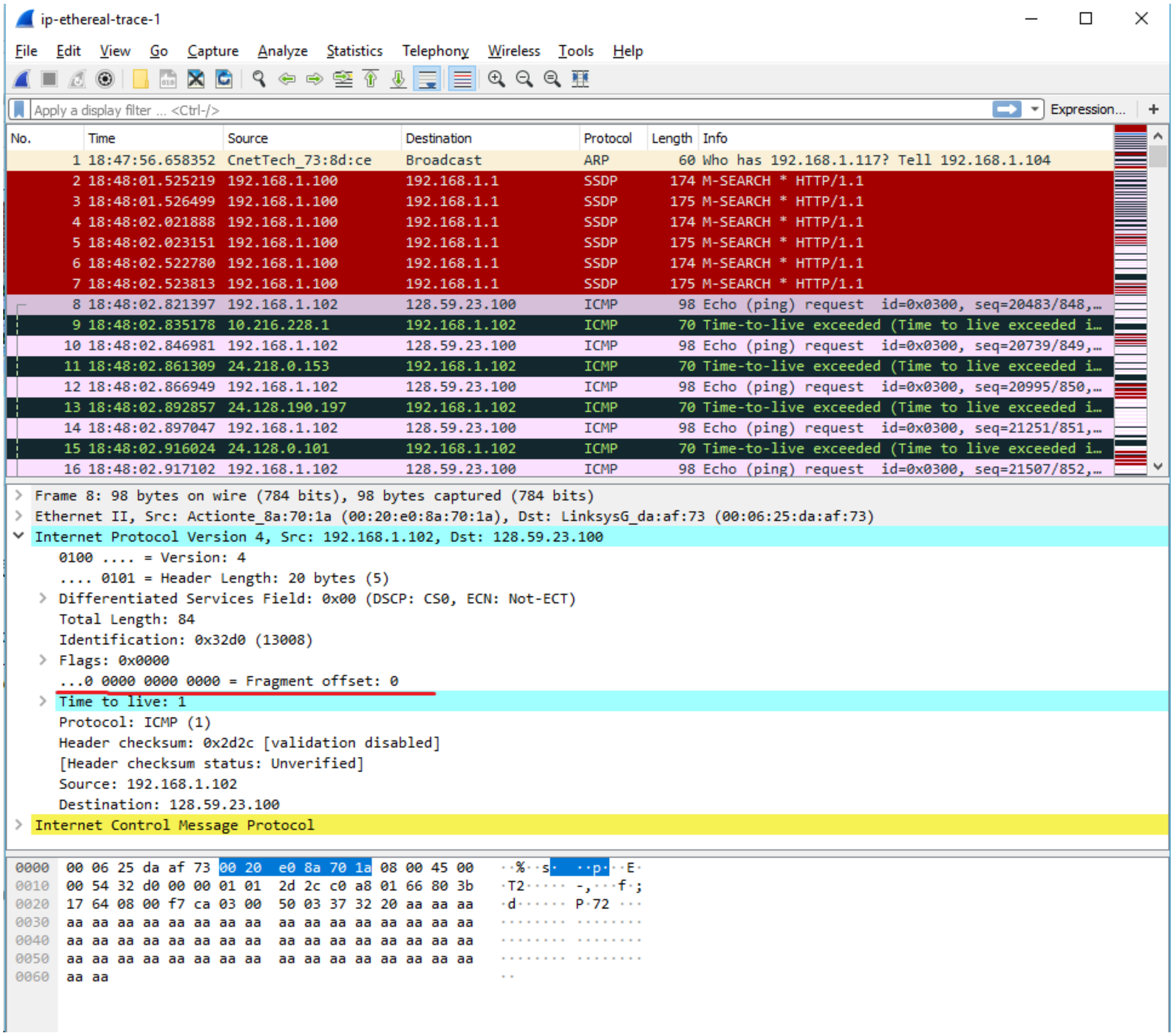

ip-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.    Time             Source             Destination     Protocol  Length Info
     1 18:47:56.658352  CnetTech_73:8d:ce  Broadcast       ARP           60 Who has 192.168.1.117? Tell 192.168.1.104
     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  id=0x0300, seq=20483/848,…
     9 18:48:02.835178  10.216.228.1       192.168.1.102   ICMP          70 Time-to-live exceeded (Time to live exceeded i…
    10 18:48:02.846981  192.168.1.102      128.59.23.100   ICMP          98 Echo (ping) request  id=0x0300, seq=20739/849,…
    11 18:48:02.861309  24.218.0.153       192.168.1.102   ICMP          70 Time-to-live exceeded (Time to live exceeded i…
    12 18:48:02.866949  192.168.1.102      128.59.23.100   ICMP          98 Echo (ping) request  id=0x0300, seq=20995/850,…
    13 18:48:02.892857  24.128.190.197     192.168.1.102   ICMP          70 Time-to-live exceeded (Time to live exceeded i…
    14 18:48:02.897047  192.168.1.102      128.59.23.100   ICMP          98 Echo (ping) request  id=0x0300, seq=21251/851,…
    15 18:48:02.916024  24.128.0.101       192.168.1.102   ICMP          70 Time-to-live exceeded (Time to live exceeded i…
    16 18:48:02.917102  192.168.1.102      128.59.23.100   ICMP          98 Echo (ping) request  id=0x0300, seq=21507/852,…
```

```
> 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)
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: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
> Internet Control Message Protocol
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ··%··s· ··p···E·
0010  00 54 32 d0 00 00 01 01  2d 2c c0 a8 01 66 80 3b   ·T2····· -,···f·;
0020  17 64 08 00 f7 ca 03 00  50 03 37 32 20 aa aa aa   ·d······ P·72 ···
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········ ········
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········ ········
0050  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········ ········
0060  aa aa                                              ··
```

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.
   The fragment offset is set to 0, therefore, the packet has not been fragmented.



ip-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	18:47:56.658352	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
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 id=0x0300, seq=20483/848,…
9	18:48:02.835178	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded i…
10	18:48:02.846981	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849,…
11	18:48:02.861309	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded i…
12	18:48:02.866949	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850,…
13	18:48:02.892857	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded i…
14	18:48:02.897047	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851,…
15	18:48:02.916024	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded i…
16	18:48:02.917102	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852,…

```
> 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)
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: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
> Internet Control Message Protocol
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ··%··s· ··p···E·
0010  00 54 32 d0 00 00 01 01  2d 2c c0 a8 01 66 80 3b   ·T2····· -,···f·;
0020  17 64 08 00 f7 ca 03 00  50 03 37 32 20 aa aa aa   ·d······ P·72 ···
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········ ········
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········ ········
0050  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········ ········
0060  aa aa                                              ··
```

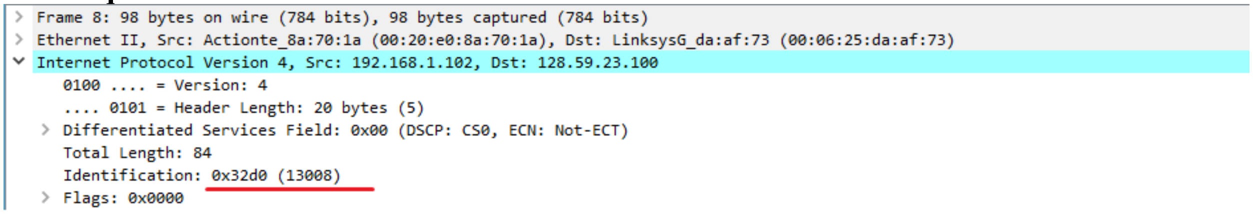
5. Which fields in the IP datagram *always* change from one datagram to the next within this series of ICMP messages sent by your computer?
The header checksum, time to live, and the Identification section change from each datagram to the next.

6. Which fields stay constant? Which of the fields *must* stay constant? Which fields must change? Why?
The following fields stay and must stay constant:
    - **Version (IPv4 always used)**
    - **Header length (doesn't change since we are always using IPv4)**
    - **Source IP (my computer's IP address doesn't change)**
    - **Destination IP (gaia.cs.umass.edu's IP address doesn't change)**
    - **Differentiated services (same protocol every time)**
    - **Upper layer protocol (always use ICMP)**

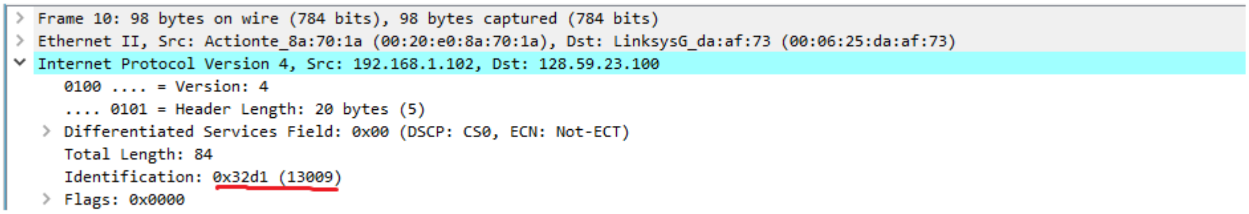
The following fields must change:

- **The header checksum (header changes from each datagram to next)**
- **Identification (incrementing, each IP datagram has a different ID)**
- **Time to live (incrementing, as this is how trace route works)**

7. Describe the pattern you see in the values in the Identification field of the IP datagram
The pattern in the identification field is that the field increases by 1 in each strand of echo requests.

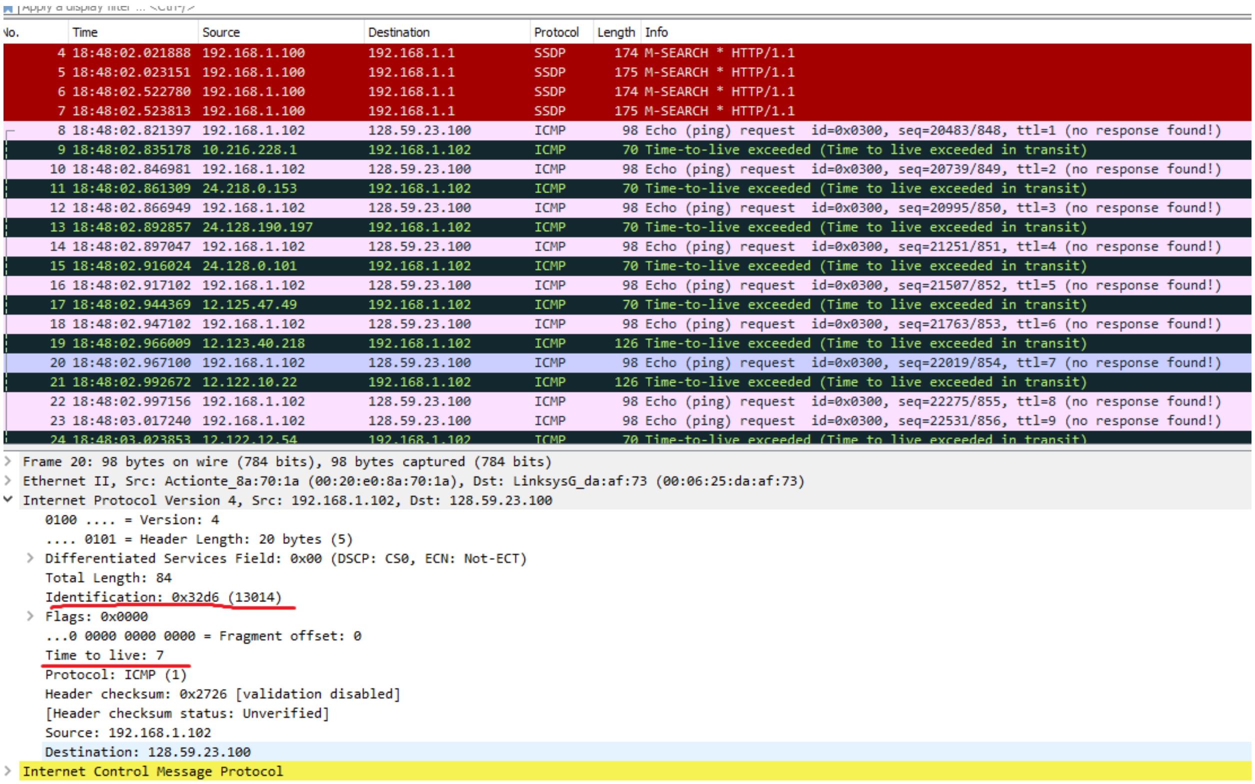


```
> Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d0 (13008)
  > Flags: 0x0000
```



```
> 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_da:af:73 (00:06:25:da:af:73)
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: 0x0000
```

8. What is the value in the Identification field and the TTL field?
Identification: 13014
TTL: 7

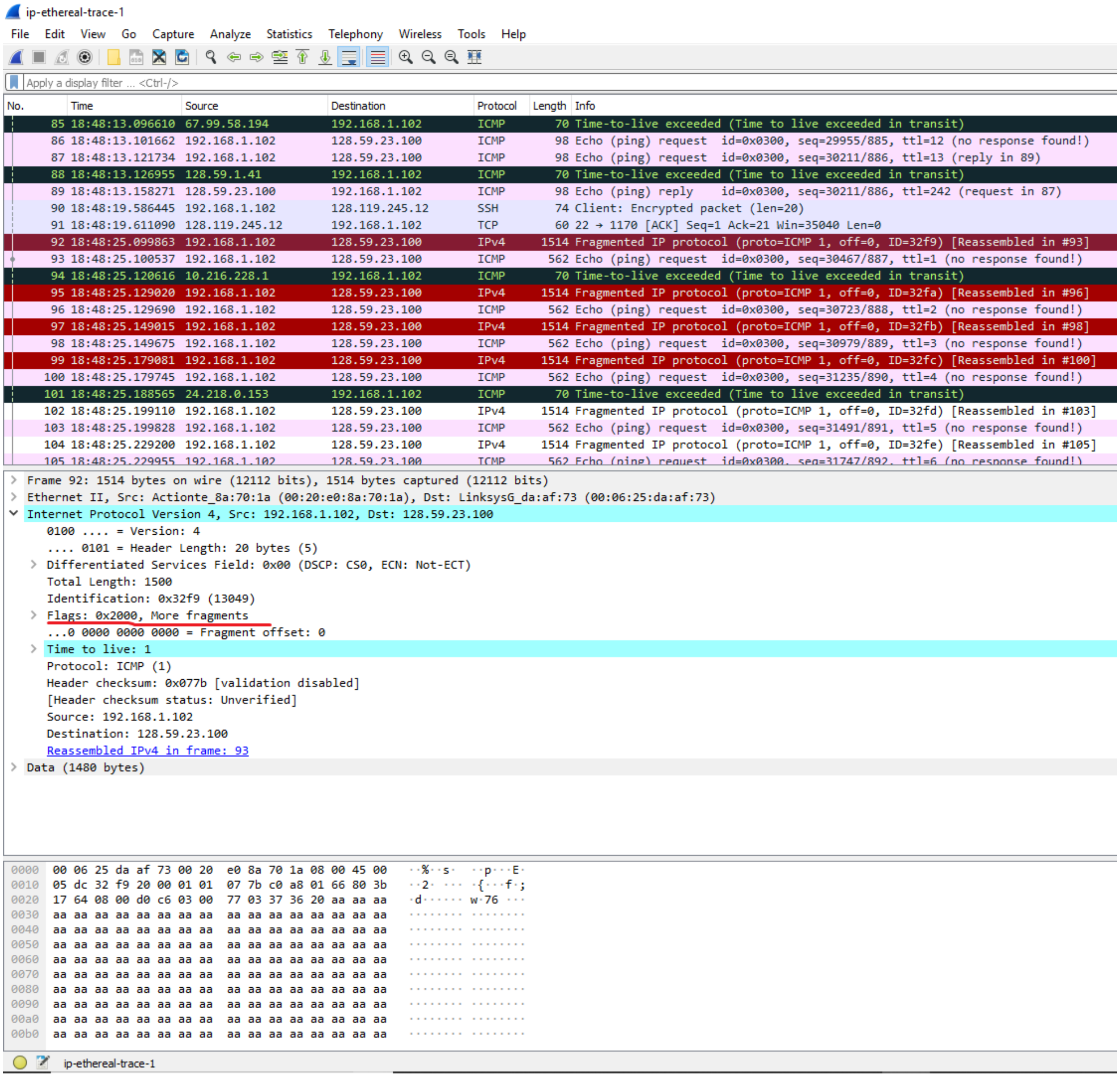


```
Apply a display filter ... <Ctrl-/>
No.  Time             Source          Destination   Protocol Length Info
   4 18:48:02.021888  192.168.1.100   192.168.1.1   SSDP     174 M-SEARCH * HTTP/1.1
   5 18:48:02.023151  192.168.1.100   192.168.1.1   SSDP     175 M-SEARCH * HTTP/1.1
   6 18:48:02.522780  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  id=0x0300, seq=20483/848, ttl=1 (no response found!)
   9 18:48:02.835178  10.216.228.1    192.168.1.102 ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  10 18:48:02.846981  192.168.1.102   128.59.23.100 ICMP      98 Echo (ping) request  id=0x0300, seq=20739/849, ttl=2 (no response found!)
  11 18:48:02.861309  24.218.0.153    192.168.1.102 ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  12 18:48:02.866949  192.168.1.102   128.59.23.100 ICMP      98 Echo (ping) request  id=0x0300, seq=20995/850, ttl=3 (no response found!)
  13 18:48:02.892857  24.128.190.197  192.168.1.102 ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  14 18:48:02.897047  192.168.1.102   128.59.23.100 ICMP      98 Echo (ping) request  id=0x0300, seq=21251/851, ttl=4 (no response found!)
  15 18:48:02.916024  24.128.0.101    192.168.1.102 ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  16 18:48:02.917102  192.168.1.102   128.59.23.100 ICMP      98 Echo (ping) request  id=0x0300, seq=21507/852, ttl=5 (no response found!)
  17 18:48:02.944369  12.125.47.49    192.168.1.102 ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  18 18:48:02.947102  192.168.1.102   128.59.23.100 ICMP      98 Echo (ping) request  id=0x0300, seq=21763/853, ttl=6 (no response found!)
  19 18:48:02.966009  12.123.40.218   192.168.1.102 ICMP     126 Time-to-live exceeded (Time to live exceeded in transit)
  20 18:48:02.967100  192.168.1.102   128.59.23.100 ICMP      98 Echo (ping) request  id=0x0300, seq=22019/854, ttl=7 (no response found!)
  21 18:48:02.992672  12.122.10.22    192.168.1.102 ICMP     126 Time-to-live exceeded (Time to live exceeded in transit)
  22 18:48:02.997156  192.168.1.102   128.59.23.100 ICMP      98 Echo (ping) request  id=0x0300, seq=22275/855, ttl=8 (no response found!)
  23 18:48:03.017240  192.168.1.102   128.59.23.100 ICMP      98 Echo (ping) request  id=0x0300, seq=22531/856, ttl=9 (no response found!)
  24 18:48:03.023853  12.122.12.54    192.168.1.102 ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
```

```
> Frame 20: 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)
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: 0x32d6 (13014)
  > Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 7
    Protocol: ICMP (1)
    Header checksum: 0x2726 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
> Internet Control Message Protocol
```

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 changes from all the replies because this field must have a unique value. If they (2 or more replies) have the same value, then the replies must be fragments of a bigger packet.
   The TLL field does not change because the time to live to the first hop router is always the same.

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



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
 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)
 86 18:48:13.101662 192.168.1.102   128.59.23.100   ICMP       98 Echo (ping) request  id=0x0300, seq=29955/885, ttl=12 (no response found!)
 87 18:48:13.121734 192.168.1.102   128.59.23.100   ICMP       98 Echo (ping) request  id=0x0300, seq=30211/886, ttl=13 (reply in 89)
 88 18:48:13.126955 128.59.1.41     192.168.1.102   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 89 18:48:13.158271 128.59.23.100   192.168.1.102   ICMP       98 Echo (ping) reply    id=0x0300, seq=30211/886, ttl=242 (request in 87)
 90 18:48:19.586445 192.168.1.102   128.119.245.12  SSH        74 Client: Encrypted packet (len=20)
 91 18:48:19.611090 128.119.245.12  192.168.1.102   TCP        60 22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
 92 18:48:25.099863 192.168.1.102   128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
 93 18:48:25.100537 192.168.1.102   128.59.23.100   ICMP      562 Echo (ping) request  id=0x0300, seq=30467/887, ttl=1 (no response found!)
 94 18:48:25.120616 10.216.228.1    192.168.1.102   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 95 18:48:25.129020 192.168.1.102   128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
 96 18:48:25.129690 192.168.1.102   128.59.23.100   ICMP      562 Echo (ping) request  id=0x0300, seq=30723/888, ttl=2 (no response found!)
 97 18:48:25.149015 192.168.1.102   128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]
 98 18:48:25.149675 192.168.1.102   128.59.23.100   ICMP      562 Echo (ping) request  id=0x0300, seq=30979/889, ttl=3 (no response found!)
 99 18:48:25.179081 192.168.1.102   128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc) [Reassembled in #100]
100 18:48:25.179745 192.168.1.102   128.59.23.100   ICMP      562 Echo (ping) request  id=0x0300, seq=31235/890, ttl=4 (no response found!)
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)
102 18:48:25.199110 192.168.1.102   128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fd) [Reassembled in #103]
103 18:48:25.199828 192.168.1.102   128.59.23.100   ICMP      562 Echo (ping) request  id=0x0300, seq=31491/891, ttl=5 (no response found!)
104 18:48:25.229200 192.168.1.102   128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fe) [Reassembled in #105]
105 18:48:25.229955 192.168.1.102   128.59.23.100   ICMP      562 Echo (ping) request  id=0x0300, seq=31747/892, ttl=6 (no response found!)
```

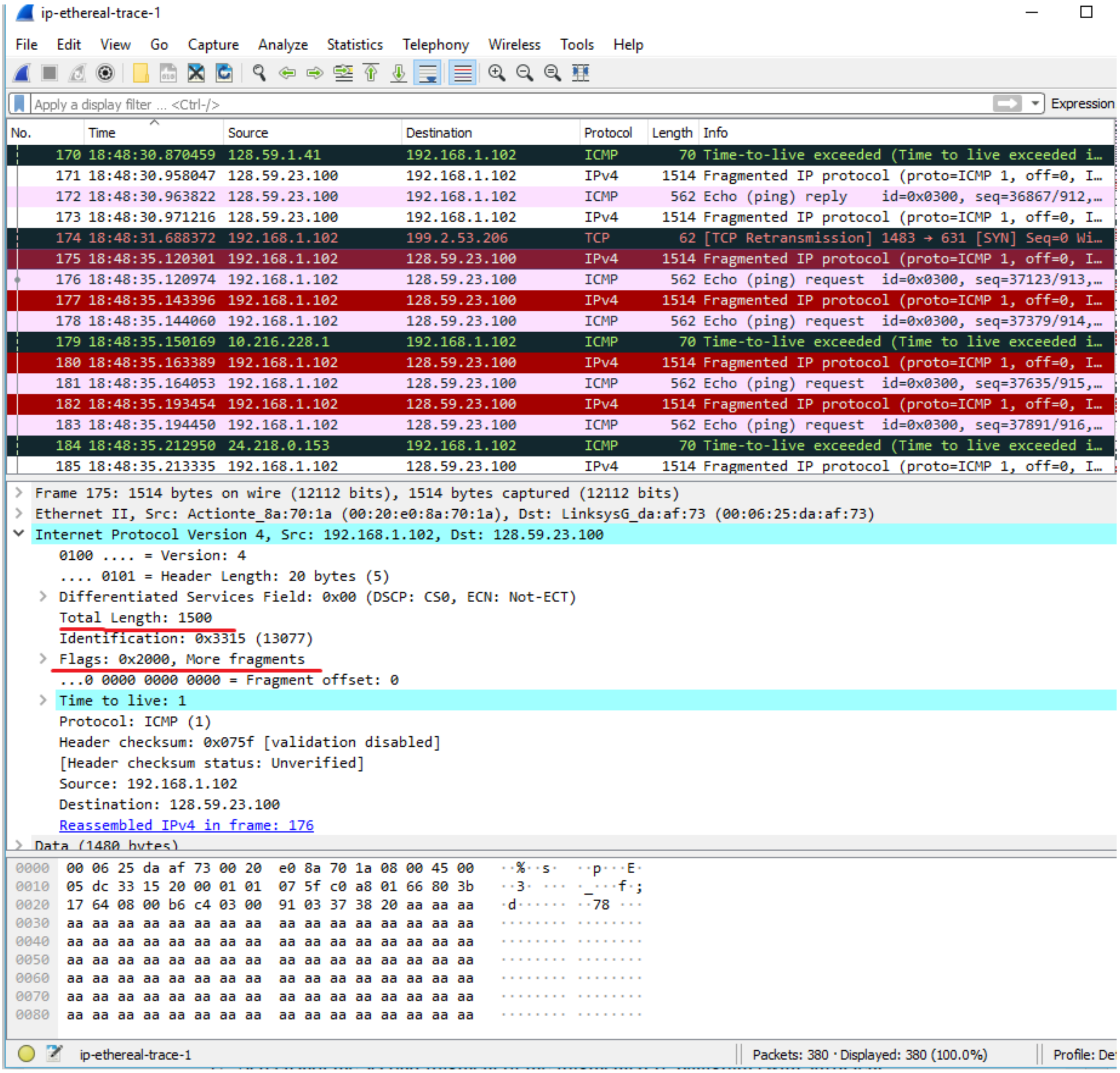
```
> Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x32f9 (13049)
  > Flags: 0x2000, More fragments
    ...0 0000 0000 0000 = Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x077b [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    Reassembled IPv4 in frame: 93
> Data (1480 bytes)
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ··%··s·  ··p···E·
0010  05 dc 32 f9 20 00 01 01  07 7b c0 a8 01 66 80 3b   ··2· ···  ·{···f·;
0020  17 64 08 00 d0 c6 03 00  77 03 37 36 20 aa aa aa   ·d······  w·76 ···
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0050  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0060  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0070  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0080  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0090  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
00a0  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
00b0  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
```

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 fact that the flag is set for more segments shows that the datagram has been fragmented. The fragment offset is set to 0 indicates that this is the first fragment rather than a latter fragment where that value is set to (1480).

    The datagram has a total length of 1500.



ip-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression

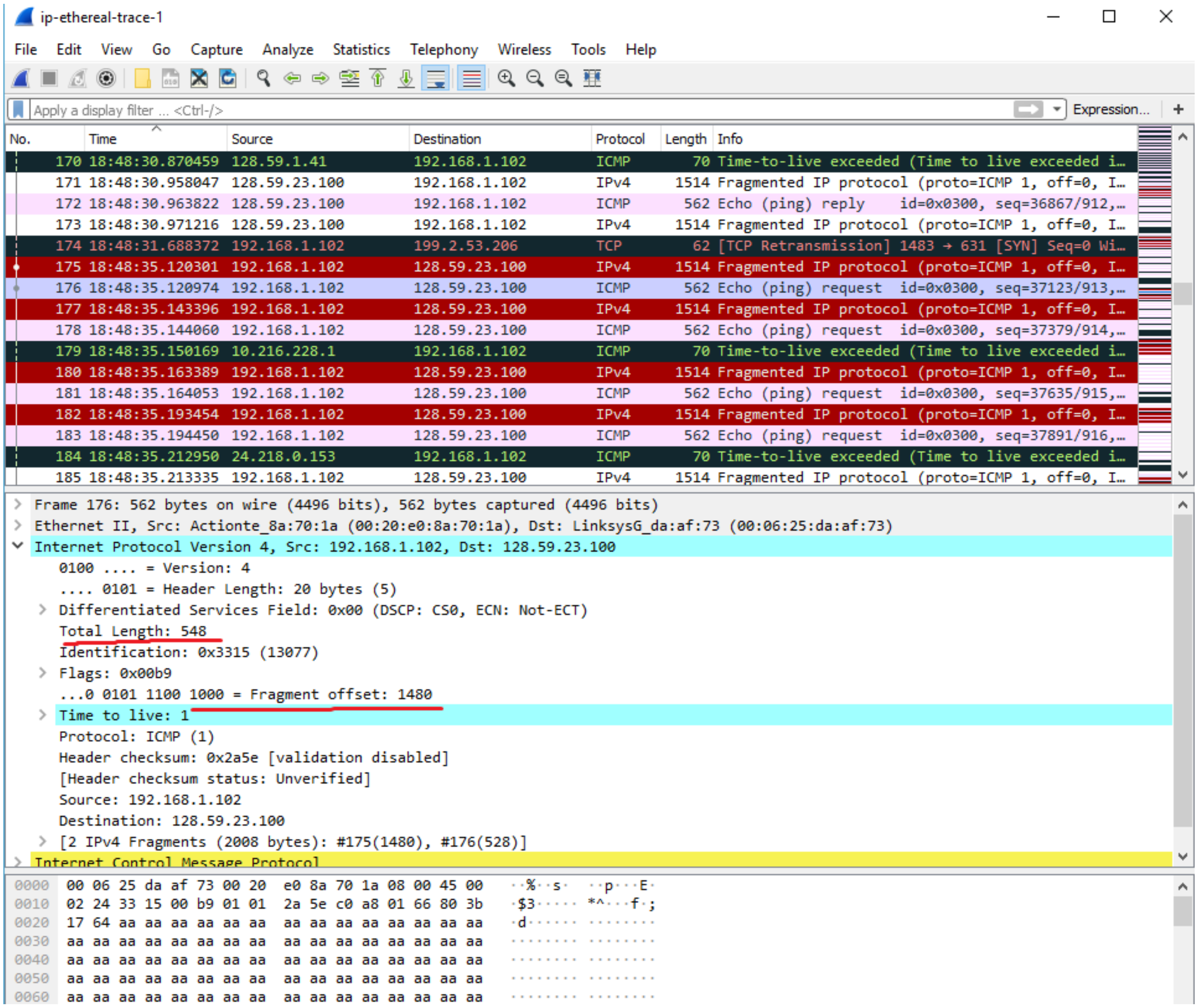
```
No.   Time             Source          Destination     Protocol Length Info
  170 18:48:30.870459  128.59.1.41     192.168.1.102   ICMP       70 Time-to-live exceeded (Time to live exceeded i…
  171 18:48:30.958047  128.59.23.100   192.168.1.102   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, I…
  172 18:48:30.963822  128.59.23.100   192.168.1.102   ICMP      562 Echo (ping) reply    id=0x0300, seq=36867/912,…
  173 18:48:30.971216  128.59.23.100   192.168.1.102   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, I…
  174 18:48:31.688372  192.168.1.102   199.2.53.206    TCP        62 [TCP Retransmission] 1483 → 631 [SYN] Seq=0 Wi…
  175 18:48:35.120301  192.168.1.102   128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, I…
  176 18:48:35.120974  192.168.1.102   128.59.23.100   ICMP      562 Echo (ping) request  id=0x0300, seq=37123/913,…
  177 18:48:35.143396  192.168.1.102   128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, I…
  178 18:48:35.144060  192.168.1.102   128.59.23.100   ICMP      562 Echo (ping) request  id=0x0300, seq=37379/914,…
  179 18:48:35.150169  10.216.228.1    192.168.1.102   ICMP       70 Time-to-live exceeded (Time to live exceeded i…
  180 18:48:35.163389  192.168.1.102   128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, I…
  181 18:48:35.164053  192.168.1.102   128.59.23.100   ICMP      562 Echo (ping) request  id=0x0300, seq=37635/915,…
  182 18:48:35.193454  192.168.1.102   128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, I…
  183 18:48:35.194450  192.168.1.102   128.59.23.100   ICMP      562 Echo (ping) request  id=0x0300, seq=37891/916,…
  184 18:48:35.212950  24.218.0.153    192.168.1.102   ICMP       70 Time-to-live exceeded (Time to live exceeded i…
  185 18:48:35.213335  192.168.1.102   128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, I…

> Frame 175: 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)
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: 0x3315 (13077)
  > Flags: 0x2000, More fragments
    ...0 0000 0000 0000 = Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x075f [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    Reassembled IPv4 in frame: 176
> Data (1480 bytes)

0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ··%··s·  ··p···E·
0010  05 dc 33 15 20 00 01 01  07 5f c0 a8 01 66 80 3b   ··3· ···  ·_···f·;
0020  17 64 08 00 b6 c4 03 00  91 03 37 38 20 aa aa aa   ·d······  ··78 ···
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0050  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0060  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0070  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0080  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········

ip-ethereal-trace-1    Packets: 380 · Displayed: 380 (100.0%)    Profile: De
```

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 second fragment is obvious because it now has a fragment offset of 1480. There are no more fragments because it no longer has a flag set for more fragments.


ip-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

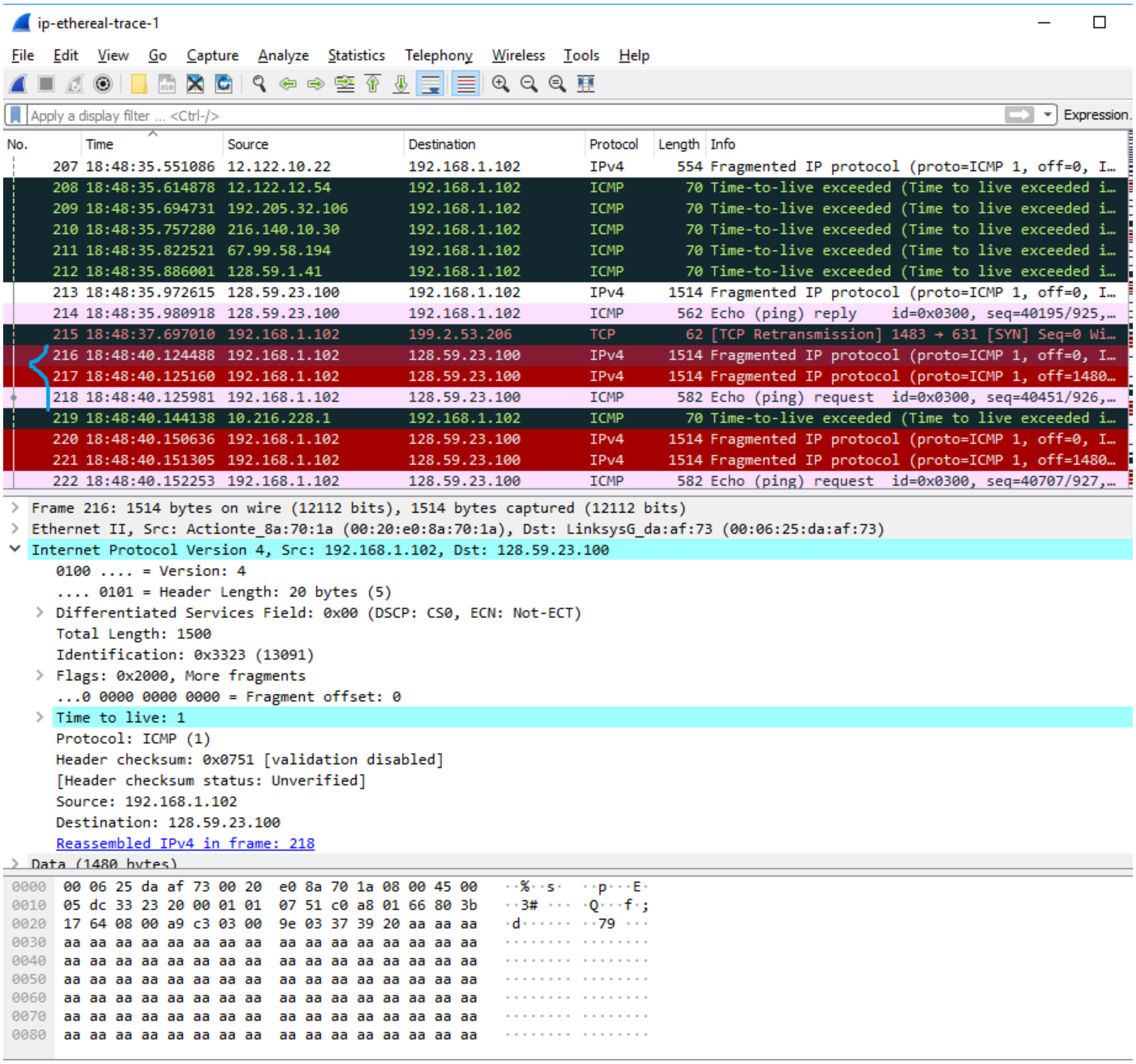
```
No.  Time             Source          Destination     Protocol Length Info
 170 18:48:30.870459  128.59.1.41     192.168.1.102   ICMP       70 Time-to-live exceeded (Time to live exceeded i…
 171 18:48:30.958047  128.59.23.100   192.168.1.102   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, I…
 172 18:48:30.963822  128.59.23.100   192.168.1.102   ICMP      562 Echo (ping) reply    id=0x0300, seq=36867/912,…
 173 18:48:30.971216  128.59.23.100   192.168.1.102   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, I…
 174 18:48:31.688372  192.168.1.102   199.2.53.206    TCP        62 [TCP Retransmission] 1483 → 631 [SYN] Seq=0 Wi…
 175 18:48:35.120301  192.168.1.102   128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, I…
 176 18:48:35.120974  192.168.1.102   128.59.23.100   ICMP      562 Echo (ping) request  id=0x0300, seq=37123/913,…
 177 18:48:35.143396  192.168.1.102   128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, I…
 178 18:48:35.144060  192.168.1.102   128.59.23.100   ICMP      562 Echo (ping) request  id=0x0300, seq=37379/914,…
 179 18:48:35.150169  10.216.228.1    192.168.1.102   ICMP       70 Time-to-live exceeded (Time to live exceeded i…
 180 18:48:35.163389  192.168.1.102   128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, I…
 181 18:48:35.164053  192.168.1.102   128.59.23.100   ICMP      562 Echo (ping) request  id=0x0300, seq=37635/915,…
 182 18:48:35.193454  192.168.1.102   128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, I…
 183 18:48:35.194450  192.168.1.102   128.59.23.100   ICMP      562 Echo (ping) request  id=0x0300, seq=37891/916,…
 184 18:48:35.212950  24.218.0.153    192.168.1.102   ICMP       70 Time-to-live exceeded (Time to live exceeded i…
 185 18:48:35.213335  192.168.1.102   128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, I…
```

```
> Frame 176: 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)
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: 0x3315 (13077)
  > Flags: 0x00b9
    ...0 0101 1100 1000 = Fragment offset: 1480
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x2a5e [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
  > [2 IPv4 Fragments (2008 bytes): #175(1480), #176(528)]
> Internet Control Message Protocol
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ··%··s·  ··p···E·
0010  02 24 33 15 00 b9 01 01  2a 5e c0 a8 01 66 80 3b   ·$3·····  *^···f·;
0020  17 64 aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ·d······  ········
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0050  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0060  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
```

13. What fields change in the IP header between the first and second fragment?
    The fields that changed were:
    - **Length**
    - **Flag set**
    - **Fragment Offset**
    - **Header checksum**

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


ip-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression.

```
No.   Time             Source           Destination     Protocol Length Info
  207 18:48:35.551086  12.122.10.22     192.168.1.102   IPv4      554 Fragmented IP protocol (proto=ICMP 1, off=0, I…
  208 18:48:35.614878  12.122.12.54     192.168.1.102   ICMP       70 Time-to-live exceeded (Time to live exceeded i…
  209 18:48:35.694731  192.205.32.106   192.168.1.102   ICMP       70 Time-to-live exceeded (Time to live exceeded i…
  210 18:48:35.757280  216.140.10.30    192.168.1.102   ICMP       70 Time-to-live exceeded (Time to live exceeded i…
  211 18:48:35.822521  67.99.58.194     192.168.1.102   ICMP       70 Time-to-live exceeded (Time to live exceeded i…
  212 18:48:35.886001  128.59.1.41      192.168.1.102   ICMP       70 Time-to-live exceeded (Time to live exceeded i…
  213 18:48:35.972615  128.59.23.100    192.168.1.102   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, I…
  214 18:48:35.980918  128.59.23.100    192.168.1.102   ICMP      562 Echo (ping) reply    id=0x0300, seq=40195/925,…
  215 18:48:37.697010  192.168.1.102    199.2.53.206    TCP        62 [TCP Retransmission] 1483 → 631 [SYN] Seq=0 Wi…
  216 18:48:40.124488  192.168.1.102    128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, I…
  217 18:48:40.125160  192.168.1.102    128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480…
  218 18:48:40.125981  192.168.1.102    128.59.23.100   ICMP      582 Echo (ping) request  id=0x0300, seq=40451/926,…
  219 18:48:40.144138  10.216.228.1     192.168.1.102   ICMP       70 Time-to-live exceeded (Time to live exceeded i…
  220 18:48:40.150636  192.168.1.102    128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, I…
  221 18:48:40.151305  192.168.1.102    128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480…
  222 18:48:40.152253  192.168.1.102    128.59.23.100   ICMP      582 Echo (ping) request  id=0x0300, seq=40707/927,…
```

```
> Frame 216: 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)
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: 0x3323 (13091)
  > Flags: 0x2000, More fragments
    ...0 0000 0000 0000 = Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x0751 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    Reassembled IPv4 in frame: 218
> Data (1480 bytes)
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ··%··s·  ··p···E·
0010  05 dc 33 23 20 00 01 01  07 51 c0 a8 01 66 80 3b   ··3# ···  ·Q···f·;
0020  17 64 08 00 a9 c3 03 00  9e 03 37 39 20 aa aa aa   ·d······  ··79 ···
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0050  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0060  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0070  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
0080  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········  ········
```

15. What fields change in the IP header among the fragments?
The fields that change are the fragment offset (0, 1480, 2960) and checksum. The first 2 packets also have lengths of 1500 and more fragment flags set, while the last fragment is shorter and does not have a flag set.