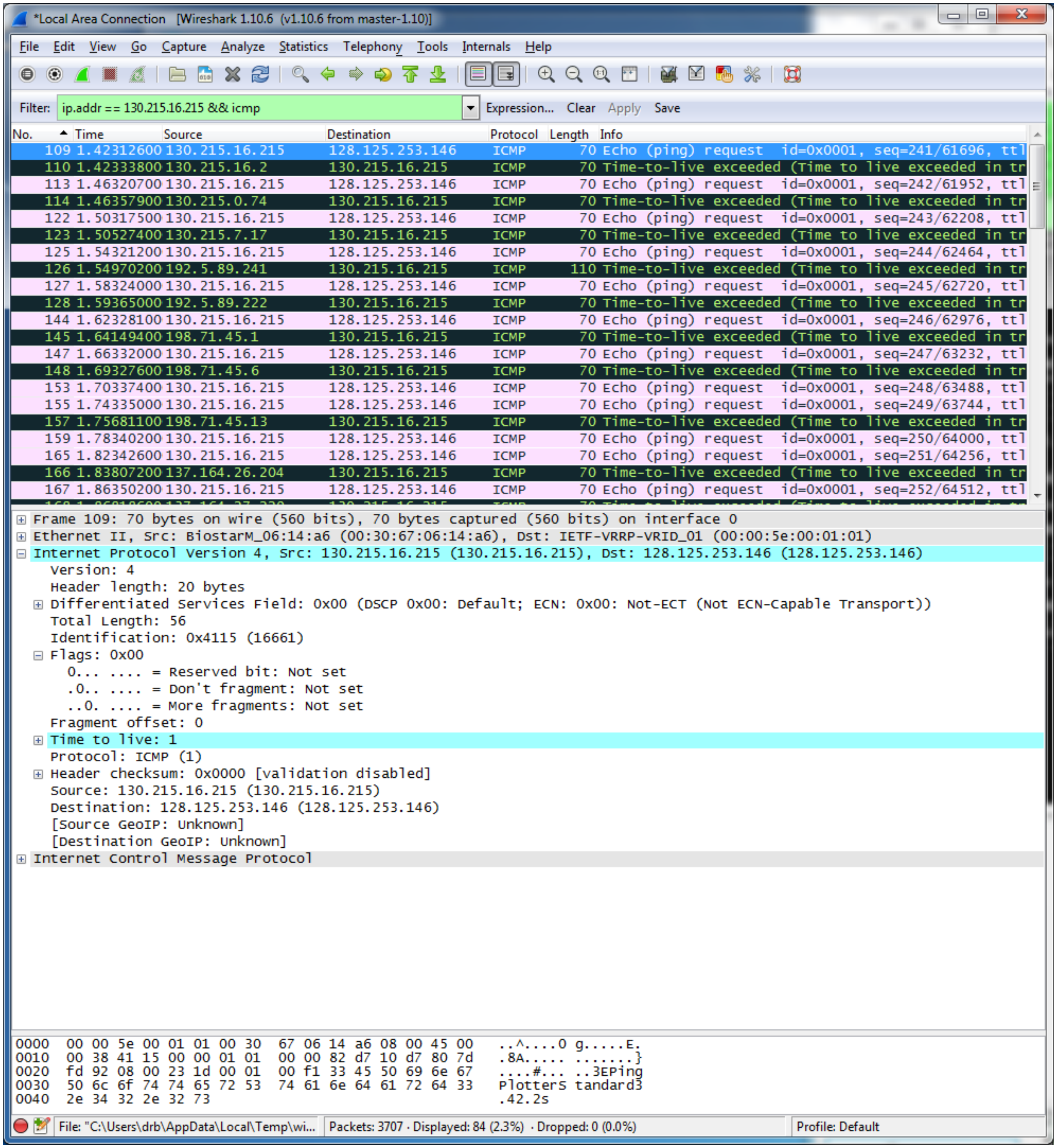
1. Select the first ICMP Echo Request message sent by your computer, expand the Internet Protocol part of the packet in the details window, and print this.


*Local Area Connection [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: ip.addr == 130.215.16.215 && icmp

No.	Time	Source	Destination	Protocol	Length	Info
109	1.42312600	130.215.16.215	128.125.253.146	ICMP	70	Echo (ping) request id=0x0001, seq=241/61696, ttl
110	1.42333800	130.215.16.2	130.215.16.215	ICMP	70	Time-to-live exceeded (Time to live exceeded in tr
113	1.46320700	130.215.16.215	128.125.253.146	ICMP	70	Echo (ping) request id=0x0001, seq=242/61952, ttl
114	1.46357900	130.215.0.74	130.215.16.215	ICMP	70	Time-to-live exceeded (Time to live exceeded in tr
122	1.50317500	130.215.16.215	128.125.253.146	ICMP	70	Echo (ping) request id=0x0001, seq=243/62208, ttl
123	1.50527400	130.215.7.17	130.215.16.215	ICMP	70	Time-to-live exceeded (Time to live exceeded in tr
125	1.54321200	130.215.16.215	128.125.253.146	ICMP	70	Echo (ping) request id=0x0001, seq=244/62464, ttl
126	1.54970200	192.5.89.241	130.215.16.215	ICMP	110	Time-to-live exceeded (Time to live exceeded in tr
127	1.58324000	130.215.16.215	128.125.253.146	ICMP	70	Echo (ping) request id=0x0001, seq=245/62720, ttl
128	1.59365000	192.5.89.222	130.215.16.215	ICMP	70	Time-to-live exceeded (Time to live exceeded in tr
144	1.62328100	130.215.16.215	128.125.253.146	ICMP	70	Echo (ping) request id=0x0001, seq=246/62976, ttl
145	1.64149400	198.71.45.1	130.215.16.215	ICMP	70	Time-to-live exceeded (Time to live exceeded in tr
147	1.66332000	130.215.16.215	128.125.253.146	ICMP	70	Echo (ping) request id=0x0001, seq=247/63232, ttl
148	1.69327600	198.71.45.6	130.215.16.215	ICMP	70	Time-to-live exceeded (Time to live exceeded in tr
153	1.70337400	130.215.16.215	128.125.253.146	ICMP	70	Echo (ping) request id=0x0001, seq=248/63488, ttl
155	1.74335000	130.215.16.215	128.125.253.146	ICMP	70	Echo (ping) request id=0x0001, seq=249/63744, ttl
157	1.75681100	198.71.45.13	130.215.16.215	ICMP	70	Time-to-live exceeded (Time to live exceeded in tr
159	1.78340200	130.215.16.215	128.125.253.146	ICMP	70	Echo (ping) request id=0x0001, seq=250/64000, ttl
165	1.82342600	130.215.16.215	128.125.253.146	ICMP	70	Echo (ping) request id=0x0001, seq=251/64256, ttl
166	1.83807200	137.164.26.204	130.215.16.215	ICMP	70	Time-to-live exceeded (Time to live exceeded in tr
167	1.86350200	130.215.16.215	128.125.253.146	ICMP	70	Echo (ping) request id=0x0001, seq=252/64512, ttl

```
⊞ Frame 109: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
⊞ Ethernet II, Src: BiostarM_06:14:a6 (00:30:67:06:14:a6), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
⊟ Internet Protocol Version 4, Src: 130.215.16.215 (130.215.16.215), Dst: 128.125.253.146 (128.125.253.146)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 56
    Identification: 0x4115 (16661)
  ⊟ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
  ⊞ Time to live: 1
    Protocol: ICMP (1)
  ⊞ Header checksum: 0x0000 [validation disabled]
    Source: 130.215.16.215 (130.215.16.215)
    Destination: 128.125.253.146 (128.125.253.146)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊞ Internet Control Message Protocol
```

```
0000  00 00 5e 00 01 01 00 30  67 06 14 a6 08 00 45 00   ..^....0 g.....E.
0010  00 38 41 15 00 00 01 01  00 00 82 d7 10 d7 80 7d   .8A..... .......}
0020  fd 92 08 00 23 1d 00 01  00 f1 33 45 50 69 6e 67   ....#... ..3EPing
0030  50 6c 6f 74 74 65 72 53  74 61 6e 64 61 72 64 33   PlotterS tandard3
0040  2e 34 32 2e 32 73                                  .42.2s
```

File: "C:\Users\drb\AppData\Local\Temp\wi... Packets: 3707 · Displayed: 84 (2.3%) · Dropped: 0 (0.0%) Profile: Default

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

ICMP (1)

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 bytes: 20 (as seen in screenshot)

Payload bytes: 36 (total length 56 minus the 20 header bytes = 36)

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

   From the previous screenshot, we do not see any IPv4 fragments. We will see these later when we transmit longer ICMP echo requests.

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?

   Identification field is incrementing.

   Time to live is also incrementing.

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

   The following fields remain 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 (usc.edu's IP address doesn't change)
   - differentiated services (same protocol every time)
   - upper layer protocol (same protocol every time)
   - header checksum (verification disabled in my tests)

   The following fields change:

   - Identification field is incrementing (each IP datagram has a different ID)
   - Time to live is also incrementing (this is how trace route works, as discussed in the assignment)

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

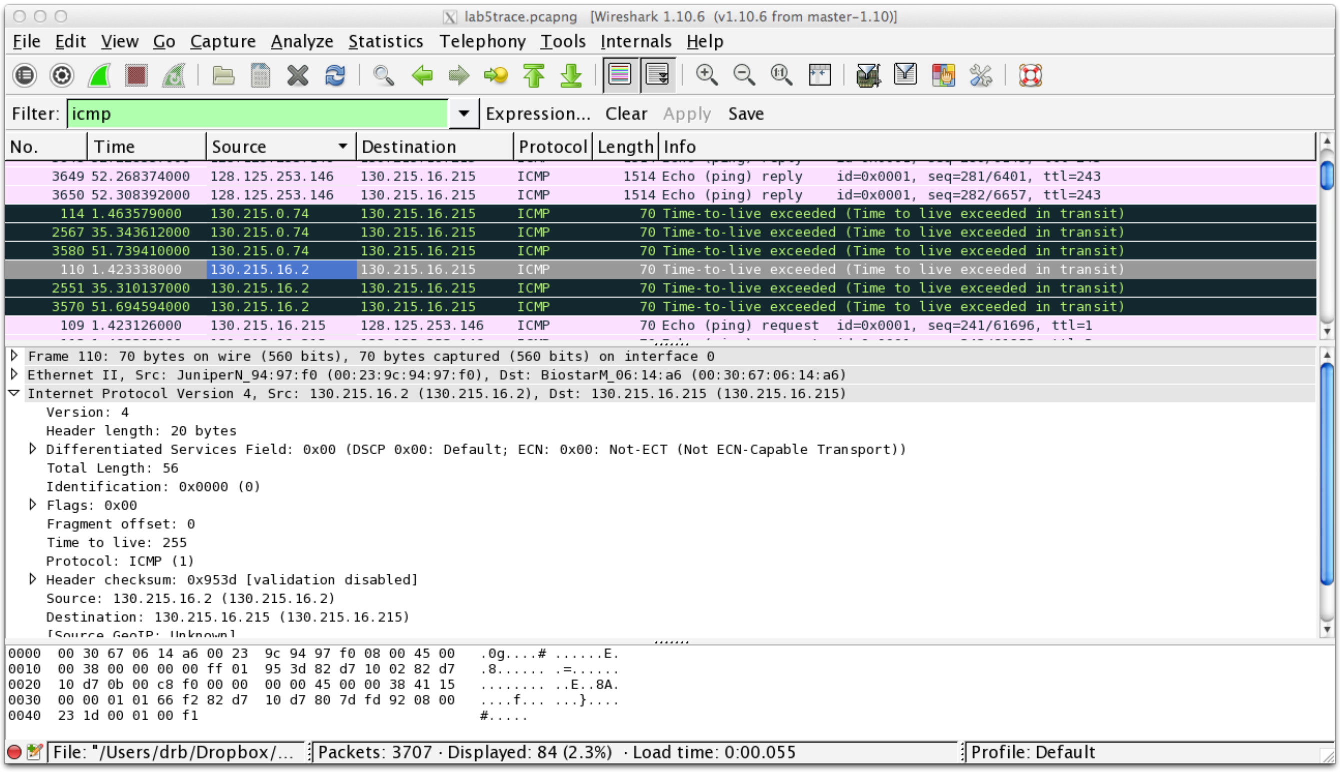
   They are incrementing with each datagram.

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

   My nearest hop router was 130.215.16.32. From the screenshot below, we see that

   - 56 byte pings: Identification = 0 and TTL = 255
   - 2000 byte pings: Identification = 0 and TTL = 255
   - 3500 byte pings: Identification = 0 and TTL = 255

   See three screenshots below.


lab5trace.pcapng [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

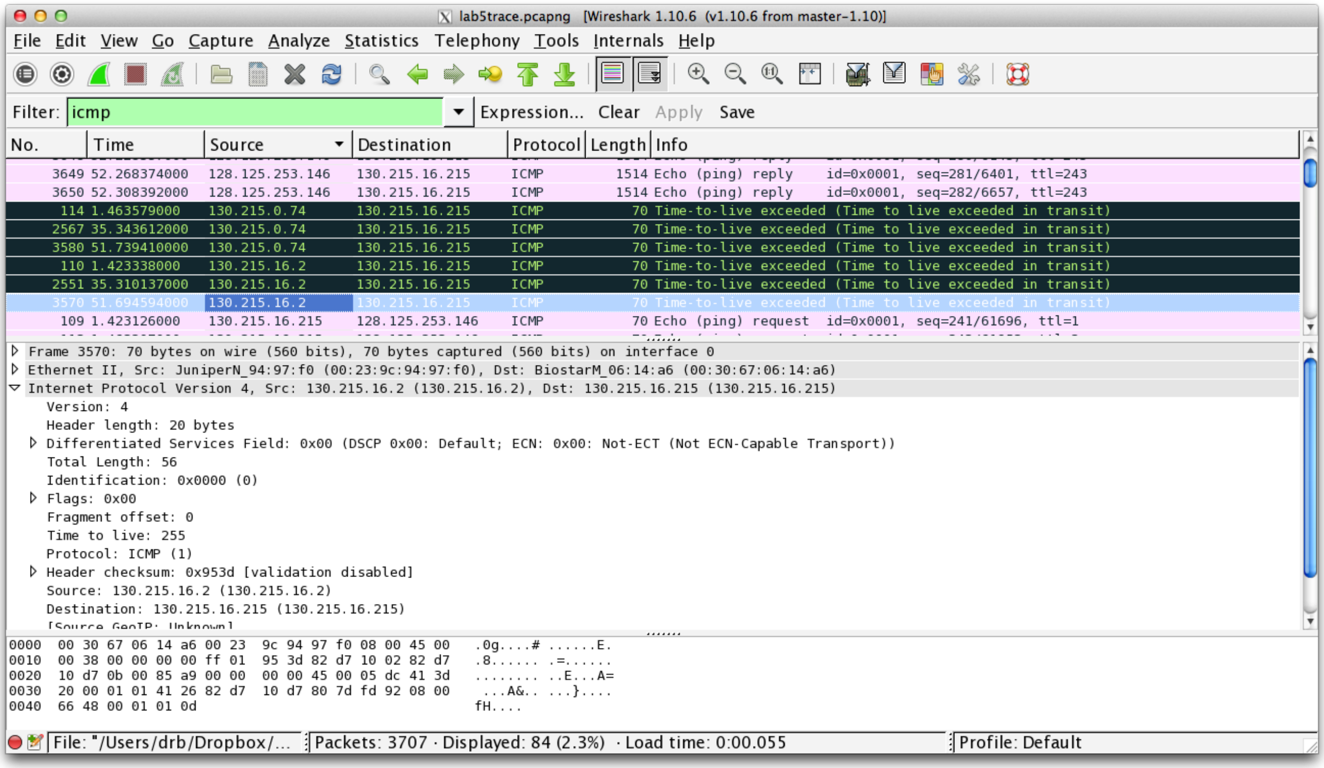
Filter: icmp

```
No.   Time          Source            Destination      Protocol Length Info
 3649 52.268374000  128.125.253.146   130.215.16.215   ICMP     1514 Echo (ping) reply    id=0x0001, seq=281/6401, ttl=243
 3650 52.308392000  128.125.253.146   130.215.16.215   ICMP     1514 Echo (ping) reply    id=0x0001, seq=282/6657, ttl=243
  114 1.463579000   130.215.0.74      130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 2567 35.343612000  130.215.0.74      130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 3580 51.739410000  130.215.0.74      130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  110 1.423338000   130.215.16.2      130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 2551 35.310137000  130.215.16.2      130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 3570 51.694594000  130.215.16.2      130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  109 1.423126000   130.215.16.215    128.125.253.146  ICMP       70 Echo (ping) request  id=0x0001, seq=241/61696, ttl=1
```

```
▷ Frame 110: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▷ Ethernet II, Src: JuniperN_94:97:f0 (00:23:9c:94:97:f0), Dst: BiostarM_06:14:a6 (00:30:67:06:14:a6)
▽ Internet Protocol Version 4, Src: 130.215.16.2 (130.215.16.2), Dst: 130.215.16.215 (130.215.16.215)
    Version: 4
    Header length: 20 bytes
  ▷ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 56
    Identification: 0x0000 (0)
  ▷ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
  ▷ Header checksum: 0x953d [validation disabled]
    Source: 130.215.16.2 (130.215.16.2)
    Destination: 130.215.16.215 (130.215.16.215)
    [Source GeoIP: Unknown]
```

```
0000  00 30 67 06 14 a6 00 23  9c 94 97 f0 08 00 45 00   .0g....# ......E.
0010  00 38 00 00 00 00 ff 01  95 3d 82 d7 10 02 82 d7   .8...... .=......
0020  10 d7 0b 00 c8 f0 00 00  00 00 45 00 00 38 41 15   ........ ..E..8A.
0030  00 00 01 01 66 f2 82 d7  10 d7 80 7d fd 92 08 00   ....f... ...}....
0040  23 1d 00 01 00 f1                                  #.....
```

File: "/Users/drb/Dropbox/... Packets: 3707 · Displayed: 84 (2.3%) · Load time: 0:00.055 Profile: Default


lab5trace.pcapng [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

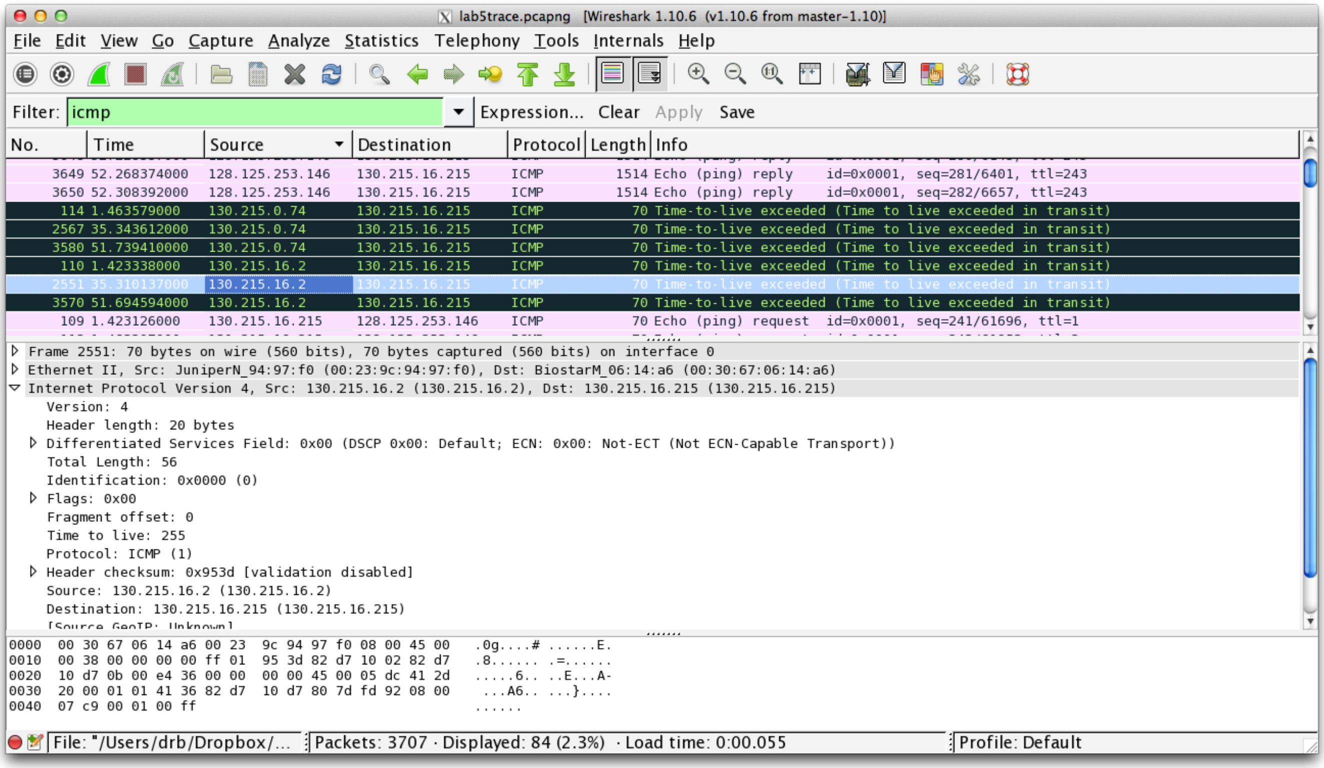
Filter: icmp

```
No.   Time          Source            Destination      Protocol Length Info
 3649 52.268374000  128.125.253.146   130.215.16.215   ICMP     1514 Echo (ping) reply    id=0x0001, seq=281/6401, ttl=243
 3650 52.308392000  128.125.253.146   130.215.16.215   ICMP     1514 Echo (ping) reply    id=0x0001, seq=282/6657, ttl=243
  114 1.463579000   130.215.0.74      130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 2567 35.343612000  130.215.0.74      130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 3580 51.739410000  130.215.0.74      130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  110 1.423338000   130.215.16.2      130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 2551 35.310137000  130.215.16.2      130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 3570 51.694594000  130.215.16.2      130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  109 1.423126000   130.215.16.215    128.125.253.146  ICMP       70 Echo (ping) request  id=0x0001, seq=241/61696, ttl=1
```

```
▷ Frame 3570: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▷ Ethernet II, Src: JuniperN_94:97:f0 (00:23:9c:94:97:f0), Dst: BiostarM_06:14:a6 (00:30:67:06:14:a6)
▽ Internet Protocol Version 4, Src: 130.215.16.2 (130.215.16.2), Dst: 130.215.16.215 (130.215.16.215)
    Version: 4
    Header length: 20 bytes
  ▷ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 56
    Identification: 0x0000 (0)
  ▷ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
  ▷ Header checksum: 0x953d [validation disabled]
    Source: 130.215.16.2 (130.215.16.2)
    Destination: 130.215.16.215 (130.215.16.215)
    [Source GeoIP: Unknown]
```

```
0000  00 30 67 06 14 a6 00 23  9c 94 97 f0 08 00 45 00   .0g....# ......E.
0010  00 38 00 00 00 00 ff 01  95 3d 82 d7 10 02 82 d7   .8...... .=......
0020  10 d7 0b 00 85 a9 00 00  00 00 45 00 05 dc 41 3d   ........ ..E...A=
0030  20 00 01 01 41 26 82 d7  10 d7 80 7d fd 92 08 00    ...A&.. ...}....
0040  66 48 00 01 01 0d                                  fH....
```

File: "/Users/drb/Dropbox/... Packets: 3707 · Displayed: 84 (2.3%) · Load time: 0:00.055 Profile: Default


labStrace.pcapng [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: icmp

```
No.   Time          Source           Destination    Protocol Length Info
 3649 52.268374000  128.125.253.146  130.215.16.215  ICMP    1514 Echo (ping) reply    id=0x0001, seq=281/6401, ttl=243
 3650 52.308392000  128.125.253.146  130.215.16.215  ICMP    1514 Echo (ping) reply    id=0x0001, seq=282/6657, ttl=243
  114 1.463579000   130.215.0.74     130.215.16.215  ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 2567 35.343612000  130.215.0.74     130.215.16.215  ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 3580 51.739410000  130.215.0.74     130.215.16.215  ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  110 1.423338000   130.215.16.2     130.215.16.215  ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 2551 35.310137000  130.215.16.2     130.215.16.215  ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 3570 51.694594000  130.215.16.2     130.215.16.215  ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  109 1.423126000   130.215.16.215   128.125.253.146 ICMP      70 Echo (ping) request  id=0x0001, seq=241/61696, ttl=1
```

```
▷ Frame 2551: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▷ Ethernet II, Src: JuniperN_94:97:f0 (00:23:9c:94:97:f0), Dst: BiostarM_06:14:a6 (00:30:67:06:14:a6)
▽ Internet Protocol Version 4, Src: 130.215.16.2 (130.215.16.2), Dst: 130.215.16.215 (130.215.16.215)
    Version: 4
    Header length: 20 bytes
  ▷ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 56
    Identification: 0x0000 (0)
  ▷ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
  ▷ Header checksum: 0x953d [validation disabled]
    Source: 130.215.16.2 (130.215.16.2)
    Destination: 130.215.16.215 (130.215.16.215)
```

```
0000  00 30 67 06 14 a6 00 23  9c 94 97 f0 08 00 45 00   .0g....# ......E.
0010  00 38 00 00 00 00 ff 01  95 3d 82 d7 10 02 82 d7   .8...... .=......
0020  10 d7 0b 00 e4 36 00 00  00 00 45 00 05 dc 41 2d   .....6.. ..E...A-
0030  20 00 01 01 41 36 82 d7  10 d7 80 7d fd 92 08 00    ...A6.. ...}....
0040  07 c9 00 01 00 ff                                  ......
```

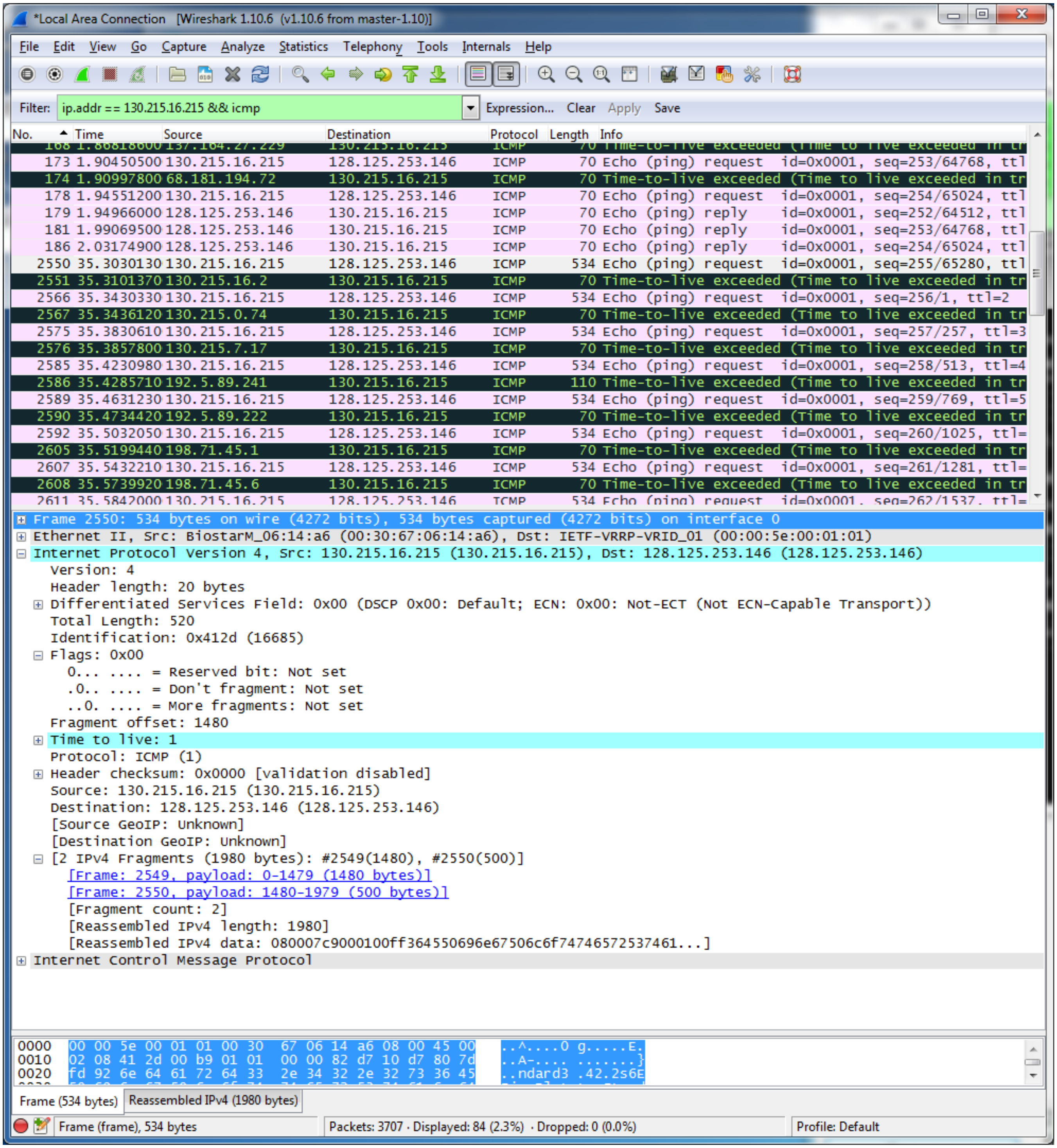
File: "/Users/drb/Dropbox/... Packets: 3707 · Displayed: 84 (2.3%) · Load time: 0:00.055 Profile: Default

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?

   In my test, these fields do not change.

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?

    See screenshot below. Note the presence of the IPv4 fragments. I had the setting "Reassemble fragmented IPv4 Datagrams" on for this part, so Wireshark shows the fragments together.



*Local Area Connection [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ip.addr == 130.215.16.215 && icmp
Expression... Clear Apply Save

```
No.   Time       Source          Destination     Protocol Length Info
 168 1.86818600 137.164.27.229  130.215.16.215  ICMP      70 Time-to-live exceeded (Time to live exceeded in tr
 173 1.90450500 130.215.16.215  128.125.253.146 ICMP      70 Echo (ping) request  id=0x0001, seq=253/64768, ttl
 174 1.90997800 68.181.194.72   130.215.16.215  ICMP      70 Time-to-live exceeded (Time to live exceeded in tr
 178 1.94551200 130.215.16.215  128.125.253.146 ICMP      70 Echo (ping) request  id=0x0001, seq=254/65024, ttl
 179 1.94966000 128.125.253.146 130.215.16.215  ICMP      70 Echo (ping) reply    id=0x0001, seq=252/64512, ttl
 181 1.99069500 128.125.253.146 130.215.16.215  ICMP      70 Echo (ping) reply    id=0x0001, seq=253/64768, ttl
 186 2.03174900 128.125.253.146 130.215.16.215  ICMP      70 Echo (ping) reply    id=0x0001, seq=254/65024, ttl
2550 35.3030130 130.215.16.215  128.125.253.146 ICMP     534 Echo (ping) request  id=0x0001, seq=255/65280, ttl
2551 35.3101370 130.215.16.2    130.215.16.215  ICMP      70 Time-to-live exceeded (Time to live exceeded in tr
2566 35.3430330 130.215.16.215  128.125.253.146 ICMP     534 Echo (ping) request  id=0x0001, seq=256/1, ttl=2
2567 35.3436120 130.215.0.74    130.215.16.215  ICMP      70 Time-to-live exceeded (Time to live exceeded in tr
2575 35.3830610 130.215.16.215  128.125.253.146 ICMP     534 Echo (ping) request  id=0x0001, seq=257/257, ttl=3
2576 35.3857800 130.215.7.17    130.215.16.215  ICMP      70 Time-to-live exceeded (Time to live exceeded in tr
2585 35.4230980 130.215.16.215  128.125.253.146 ICMP     534 Echo (ping) request  id=0x0001, seq=258/513, ttl=4
2586 35.4285710 192.5.89.241    130.215.16.215  ICMP     110 Time-to-live exceeded (Time to live exceeded in tr
2589 35.4631230 130.215.16.215  128.125.253.146 ICMP     534 Echo (ping) request  id=0x0001, seq=259/769, ttl=5
2590 35.4734420 192.5.89.222    130.215.16.215  ICMP      70 Time-to-live exceeded (Time to live exceeded in tr
2592 35.5032050 130.215.16.215  128.125.253.146 ICMP     534 Echo (ping) request  id=0x0001, seq=260/1025, ttl=
2605 35.5199440 198.71.45.1     130.215.16.215  ICMP      70 Time-to-live exceeded (Time to live exceeded in tr
2607 35.5432210 130.215.16.215  128.125.253.146 ICMP     534 Echo (ping) request  id=0x0001, seq=261/1281, ttl=
2608 35.5739920 198.71.45.6     130.215.16.215  ICMP      70 Time-to-live exceeded (Time to live exceeded in tr
2611 35.5842000 130.215.16.215  128.125.253.146 ICMP     534 Echo (ping) request  id=0x0001, seq=262/1537, ttl=
```

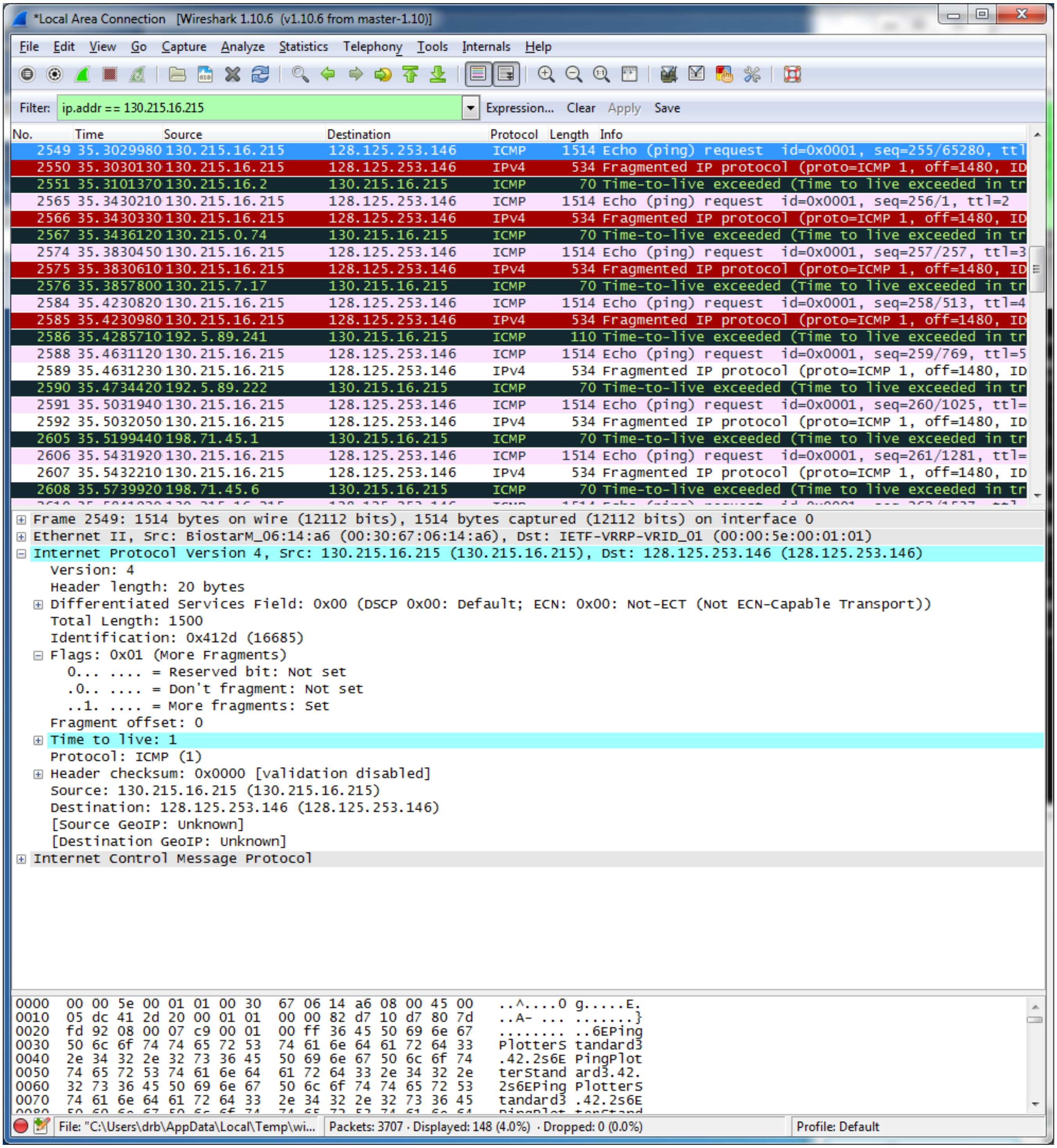
```
⊞ Frame 2550: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface 0
⊞ Ethernet II, Src: BiostarM_06:14:a6 (00:30:67:06:14:a6), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
⊟ Internet Protocol Version 4, Src: 130.215.16.215 (130.215.16.215), Dst: 128.125.253.146 (128.125.253.146)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 520
    Identification: 0x412d (16685)
  ⊟ 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: 0x0000 [validation disabled]
    Source: 130.215.16.215 (130.215.16.215)
    Destination: 128.125.253.146 (128.125.253.146)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ⊟ [2 IPv4 Fragments (1980 bytes): #2549(1480), #2550(500)]
      [Frame: 2549, payload: 0-1479 (1480 bytes)]
      [Frame: 2550, payload: 1480-1979 (500 bytes)]
      [Fragment count: 2]
      [Reassembled IPv4 length: 1980]
      [Reassembled IPv4 data: 080007c9000100ff364550696e67506c6f74746572537461...]
⊞ Internet Control Message Protocol
```

```
0000  00 00 5e 00 01 01 00 30  67 06 14 a6 08 00 45 00   ..^....0 g.....E.
0010  02 08 41 2d 00 b9 01 01  00 00 82 d7 10 d7 80 7d   ..A-.... .......}
0020  fd 92 6e 64 61 72 64 33  2e 34 32 2e 32 73 36 45   ..ndard3 .42.2s6E
```

Frame (frame), 534 bytes | Packets: 3707 · Displayed: 84 (2.3%) · Dropped: 0 (0.0%) | Profile: Default

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?

    I had to turn off the setting "Reassemble fragmented IPv4 Datagrams" to get this to work. See screenshot below. The "more fragments" bit is set, indicating the datagram been fragmented and there are more fragments coming. The "Fragment offset" is zero, indicating this is the first fragment. The total length of this IP datagram is 1500 bytes.



Filter: ip.addr == 130.215.16.215

```
No.     Time       Source          Destination      Protocol Length Info
   2549 35.3029980 130.215.16.215  128.125.253.146  ICMP     1514 Echo (ping) request  id=0x0001, seq=255/65280, ttl
   2550 35.3030130 130.215.16.215  128.125.253.146  IPv4      534 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
   2551 35.3101370 130.215.16.2    130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in tr
   2565 35.3430210 130.215.16.215  128.125.253.146  ICMP     1514 Echo (ping) request  id=0x0001, seq=256/1, ttl=2
   2566 35.3430330 130.215.16.215  128.125.253.146  IPv4      534 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
   2567 35.3436120 130.215.0.74    130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in tr
   2574 35.3830450 130.215.16.215  128.125.253.146  ICMP     1514 Echo (ping) request  id=0x0001, seq=257/257, ttl=3
   2575 35.3830610 130.215.16.215  128.125.253.146  IPv4      534 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
   2576 35.3857800 130.215.7.17    130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in tr
   2584 35.4230820 130.215.16.215  128.125.253.146  ICMP     1514 Echo (ping) request  id=0x0001, seq=258/513, ttl=4
   2585 35.4230980 130.215.16.215  128.125.253.146  IPv4      534 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
   2586 35.4285710 192.5.89.241    130.215.16.215   ICMP      110 Time-to-live exceeded (Time to live exceeded in tr
   2588 35.4631120 130.215.16.215  128.125.253.146  ICMP     1514 Echo (ping) request  id=0x0001, seq=259/769, ttl=5
   2589 35.4631230 130.215.16.215  128.125.253.146  IPv4      534 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
   2590 35.4734420 192.5.89.222    130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in tr
   2591 35.5031940 130.215.16.215  128.125.253.146  ICMP     1514 Echo (ping) request  id=0x0001, seq=260/1025, ttl=
   2592 35.5032050 130.215.16.215  128.125.253.146  IPv4      534 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
   2605 35.5199440 198.71.45.1     130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in tr
   2606 35.5431920 130.215.16.215  128.125.253.146  ICMP     1514 Echo (ping) request  id=0x0001, seq=261/1281, ttl=
   2607 35.5432210 130.215.16.215  128.125.253.146  IPv4      534 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
   2608 35.5739920 198.71.45.6     130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in tr
```

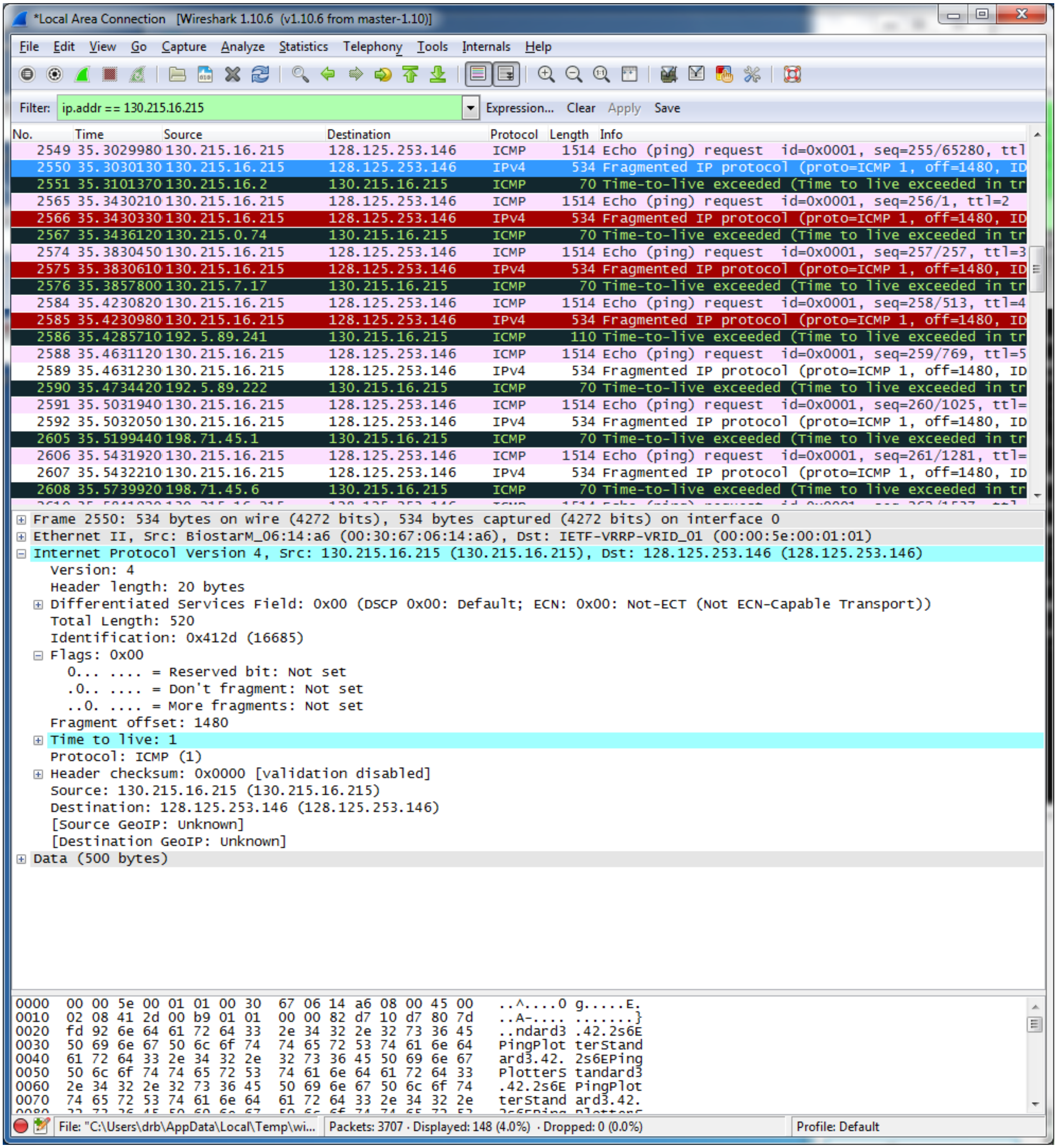
```
⊞ Frame 2549: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
⊞ Ethernet II, Src: BiostarM_06:14:a6 (00:30:67:06:14:a6), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
⊟ Internet Protocol Version 4, Src: 130.215.16.215 (130.215.16.215), Dst: 128.125.253.146 (128.125.253.146)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 1500
    Identification: 0x412d (16685)
  ⊟ Flags: 0x01 (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: 0x0000 [validation disabled]
    Source: 130.215.16.215 (130.215.16.215)
    Destination: 128.125.253.146 (128.125.253.146)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊞ Internet Control Message Protocol
```

```
0000  00 00 5e 00 01 01 00 30  67 06 14 a6 08 00 45 00   ..^....0 g.....E.
0010  05 dc 41 2d 20 00 01 01  00 00 82 d7 10 d7 80 7d   ..A- ... .......}
0020  fd 92 08 00 07 c9 00 01  00 ff 36 45 50 69 6e 67   ........ ..6EPing
0030  50 6c 6f 74 74 65 72 53  74 61 6e 64 61 72 64 33   PlotterS tandard3
0040  2e 34 32 2e 32 73 36 45  50 69 6e 67 50 6c 6f 74   .42.2s6E PingPlot
0050  74 65 72 53 74 61 6e 64  61 72 64 33 2e 34 32 2e   terStand ard3.42.
0060  32 73 36 45 50 69 6e 67  50 6c 6f 74 74 65 72 53   2s6EPing PlotterS
0070  74 61 6e 64 61 72 64 33  2e 34 32 2e 32 73 36 45   tandard3 .42.2s6E
```

File: "C:\Users\drb\AppData\Local\Temp\wi... Packets: 3707 · Displayed: 148 (4.0%) · Dropped: 0 (0.0%)

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 there more fragments? How can you tell?

    See screenshot below. The ”Fragment offset” is 1480, indicating this is the second fragment. The “more fragments” bit is clear, indicating this is the last fragment.


*Local Area Connection [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ip.addr == 130.215.16.215
Expression... Clear Apply Save

```
No.     Time       Source          Destination      Protocol Length Info
   2549 35.3029980 130.215.16.215  128.125.253.146  ICMP     1514 Echo (ping) request  id=0x0001, seq=255/65280, ttl
   2550 35.3030130 130.215.16.215  128.125.253.146  IPv4      534 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
   2551 35.3101370 130.215.16.2    130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in tr
   2565 35.3430210 130.215.16.215  128.125.253.146  ICMP     1514 Echo (ping) request  id=0x0001, seq=256/1, ttl=2
   2566 35.3430330 130.215.16.215  128.125.253.146  IPv4      534 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
   2567 35.3436120 130.215.0.74    130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in tr
   2574 35.3830450 130.215.16.215  128.125.253.146  ICMP     1514 Echo (ping) request  id=0x0001, seq=257/257, ttl=3
   2575 35.3830610 130.215.16.215  128.125.253.146  IPv4      534 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
   2576 35.3857800 130.215.7.17    130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in tr
   2584 35.4230820 130.215.16.215  128.125.253.146  ICMP     1514 Echo (ping) request  id=0x0001, seq=258/513, ttl=4
   2585 35.4230980 130.215.16.215  128.125.253.146  IPv4      534 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
   2586 35.4285710 192.5.89.241    130.215.16.215   ICMP      110 Time-to-live exceeded (Time to live exceeded in tr
   2588 35.4631120 130.215.16.215  128.125.253.146  ICMP     1514 Echo (ping) request  id=0x0001, seq=259/769, ttl=5
   2589 35.4631230 130.215.16.215  128.125.253.146  IPv4      534 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
   2590 35.4734420 192.5.89.222    130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in tr
   2591 35.5031940 130.215.16.215  128.125.253.146  ICMP     1514 Echo (ping) request  id=0x0001, seq=260/1025, ttl=
   2592 35.5032050 130.215.16.215  128.125.253.146  IPv4      534 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
   2605 35.5199440 198.71.45.1     130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in tr
   2606 35.5431920 130.215.16.215  128.125.253.146  ICMP     1514 Echo (ping) request  id=0x0001, seq=261/1281, ttl=
   2607 35.5432210 130.215.16.215  128.125.253.146  IPv4      534 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
   2608 35.5739920 198.71.45.6     130.215.16.215   ICMP       70 Time-to-live exceeded (Time to live exceeded in tr
```

```
⊞ Frame 2550: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface 0
⊞ Ethernet II, Src: BiostarM_06:14:a6 (00:30:67:06:14:a6), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
⊟ Internet Protocol Version 4, Src: 130.215.16.215 (130.215.16.215), Dst: 128.125.253.146 (128.125.253.146)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 520
    Identification: 0x412d (16685)
  ⊟ 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: 0x0000 [validation disabled]
    Source: 130.215.16.215 (130.215.16.215)
    Destination: 128.125.253.146 (128.125.253.146)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊞ Data (500 bytes)
```

```
0000  00 00 5e 00 01 01 00 30  67 06 14 a6 08 00 45 00   ..^....0 g.....E.
0010  02 08 41 2d 00 b9 01 01  00 00 82 d7 10 d7 80 7d   ..A-.... .......}
0020  fd 92 6e 64 61 72 64 33  2e 34 32 2e 32 73 36 45   ..ndard3 .42.2s6E
0030  50 69 6e 67 50 6c 6f 74  74 65 72 53 74 61 6e 64   PingPlot terStand
0040  61 72 64 33 2e 34 32 2e  32 73 36 45 50 69 6e 67   ard3.42. 2s6EPing
0050  50 6c 6f 74 74 65 72 53  74 61 6e 64 61 72 64 33   PlotterS tandard3
0060  2e 34 32 2e 32 73 36 45  50 69 6e 67 50 6c 6f 74   .42.2s6E PingPlot
0070  74 65 72 53 74 61 6e 64  61 72 64 33 2e 34 32 2e   terStand ard3.42.
```

File: "C:\Users\drb\AppData\Local\Temp\wi... | Packets: 3707 · Displayed: 148 (4.0%) · Dropped: 0 (0.0%) | Profile: Default

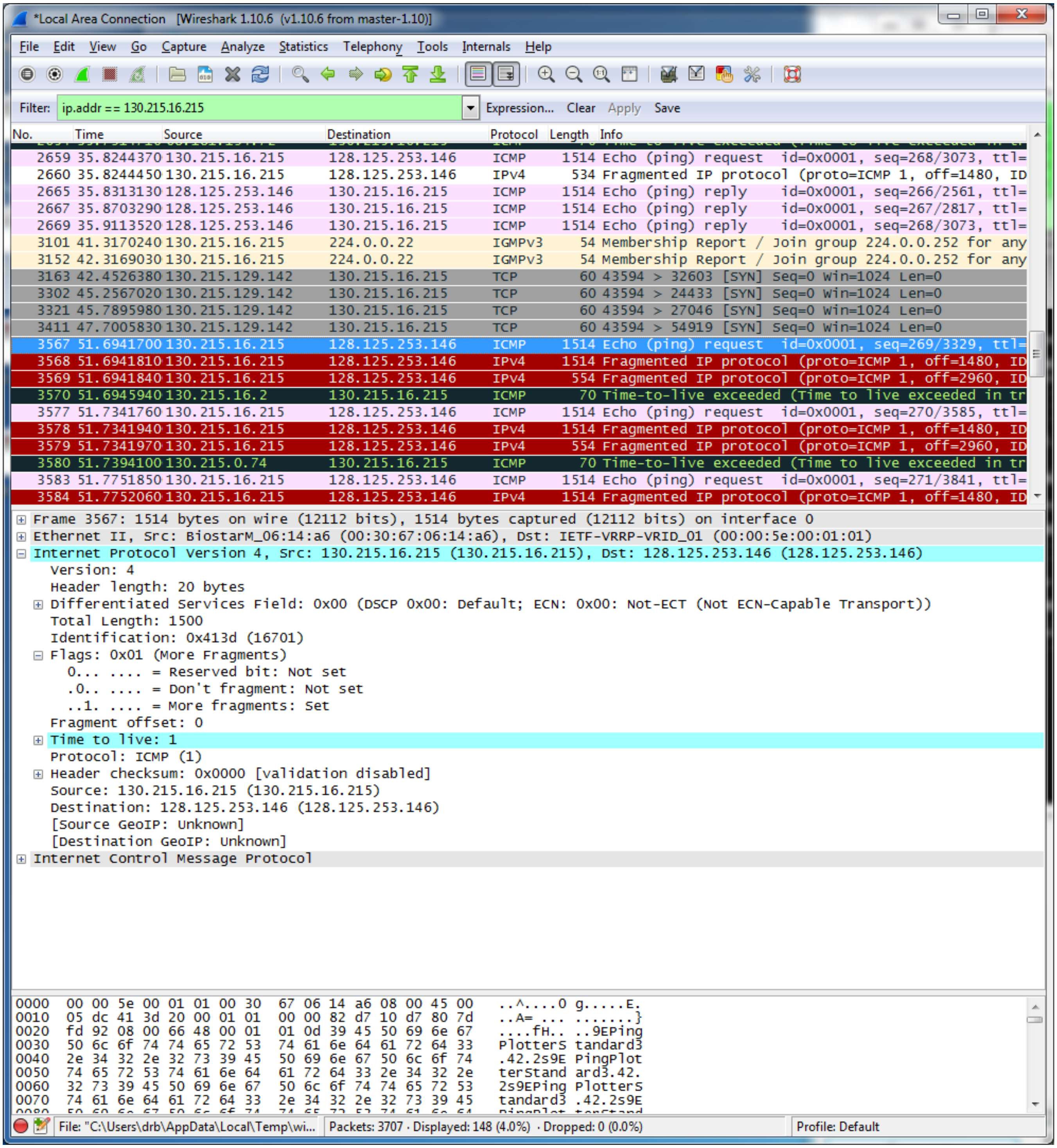
13. What fields change in the IP header between the first and second fragment?

    Total length, the more fragments bit, fragment offset. Note that identification and time to live don't change.

14. 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. How many fragments were created from the original datagram? What fields change in the IP header among the fragments?

See screenshot below. Three fragments were created from the original datagram in this case. The fields that change are:

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


*Local Area Connection [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ip.addr == 130.215.16.215
Expression... Clear Apply Save

```
No.   Time        Source           Destination       Protocol  Length Info
 2659 35.8244370 130.215.16.215   128.125.253.146   ICMP      1514 Echo (ping) request  id=0x0001, seq=268/3073, ttl=
 2660 35.8244450 130.215.16.215   128.125.253.146   IPv4       534 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
 2665 35.8313130 128.125.253.146  130.215.16.215    ICMP      1514 Echo (ping) reply    id=0x0001, seq=266/2561, ttl=
 2667 35.8703290 128.125.253.146  130.215.16.215    ICMP      1514 Echo (ping) reply    id=0x0001, seq=267/2817, ttl=
 2669 35.9113520 128.125.253.146  130.215.16.215    ICMP      1514 Echo (ping) reply    id=0x0001, seq=268/3073, ttl=
 3101 41.3170240 130.215.16.215   224.0.0.22        IGMPv3      54 Membership Report / Join group 224.0.0.252 for any
 3152 42.3169030 130.215.16.215   224.0.0.22        IGMPv3      54 Membership Report / Join group 224.0.0.252 for any
 3163 42.4526380 130.215.129.142  130.215.16.215    TCP         60 43594 > 32603 [SYN] Seq=0 Win=1024 Len=0
 3302 45.2567020 130.215.129.142  130.215.16.215    TCP         60 43594 > 24433 [SYN] Seq=0 Win=1024 Len=0
 3321 45.7895980 130.215.129.142  130.215.16.215    TCP         60 43594 > 27046 [SYN] Seq=0 Win=1024 Len=0
 3411 47.7005830 130.215.129.142  130.215.16.215    TCP         60 43594 > 54919 [SYN] Seq=0 Win=1024 Len=0
 3567 51.6941700 130.215.16.215   128.125.253.146   ICMP      1514 Echo (ping) request  id=0x0001, seq=269/3329, ttl=
 3568 51.6941810 130.215.16.215   128.125.253.146   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
 3569 51.6941840 130.215.16.215   128.125.253.146   IPv4       554 Fragmented IP protocol (proto=ICMP 1, off=2960, ID
 3570 51.6945940 130.215.16.2     130.215.16.215    ICMP        70 Time-to-live exceeded (Time to live exceeded in tr
 3577 51.7341760 130.215.16.215   128.125.253.146   ICMP      1514 Echo (ping) request  id=0x0001, seq=270/3585, ttl=
 3578 51.7341940 130.215.16.215   128.125.253.146   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
 3579 51.7341970 130.215.16.215   128.125.253.146   IPv4       554 Fragmented IP protocol (proto=ICMP 1, off=2960, ID
 3580 51.7394100 130.215.0.74     130.215.16.215    ICMP        70 Time-to-live exceeded (Time to live exceeded in tr
 3583 51.7751850 130.215.16.215   128.125.253.146   ICMP      1514 Echo (ping) request  id=0x0001, seq=271/3841, ttl=
 3584 51.7752060 130.215.16.215   128.125.253.146   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
```

```
⊞ Frame 3567: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
⊞ Ethernet II, Src: BiostarM_06:14:a6 (00:30:67:06:14:a6), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
⊟ Internet Protocol Version 4, Src: 130.215.16.215 (130.215.16.215), Dst: 128.125.253.146 (128.125.253.146)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 1500
    Identification: 0x413d (16701)
  ⊟ Flags: 0x01 (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: 0x0000 [validation disabled]
    Source: 130.215.16.215 (130.215.16.215)
    Destination: 128.125.253.146 (128.125.253.146)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊞ Internet Control Message Protocol
```

```
0000  00 00 5e 00 01 01 00 30  67 06 14 a6 08 00 45 00   ..^....0 g.....E.
0010  05 dc 41 3d 20 00 01 01  00 00 82 d7 10 d7 80 7d   ..A= ... .......}
0020  fd 92 08 00 66 48 00 01  01 0d 39 45 50 69 6e 67   ....fH.. ..9EPing
0030  50 6c 6f 74 74 65 72 53  74 61 6e 64 61 72 64 33   PlotterS tandard3
0040  2e 34 32 2e 32 73 39 45  50 69 6e 67 50 6c 6f 74   .42.2s9E PingPlot
0050  74 65 72 53 74 61 6e 64  61 72 64 33 2e 34 32 2e   terStand ard3.42.
0060  32 73 39 45 50 69 6e 67  50 6c 6f 74 74 65 72 53   2s9EPing PlotterS
0070  74 61 6e 64 61 72 64 33  2e 34 32 2e 32 73 39 45   tandard3 .42.2s9E
```

File: "C:\Users\drb\AppData\Local\Temp\wi... Packets: 3707 · Displayed: 148 (4.0%) · Dropped: 0 (0.0%) Profile: Default