Wireshark Lab 6 (IP)

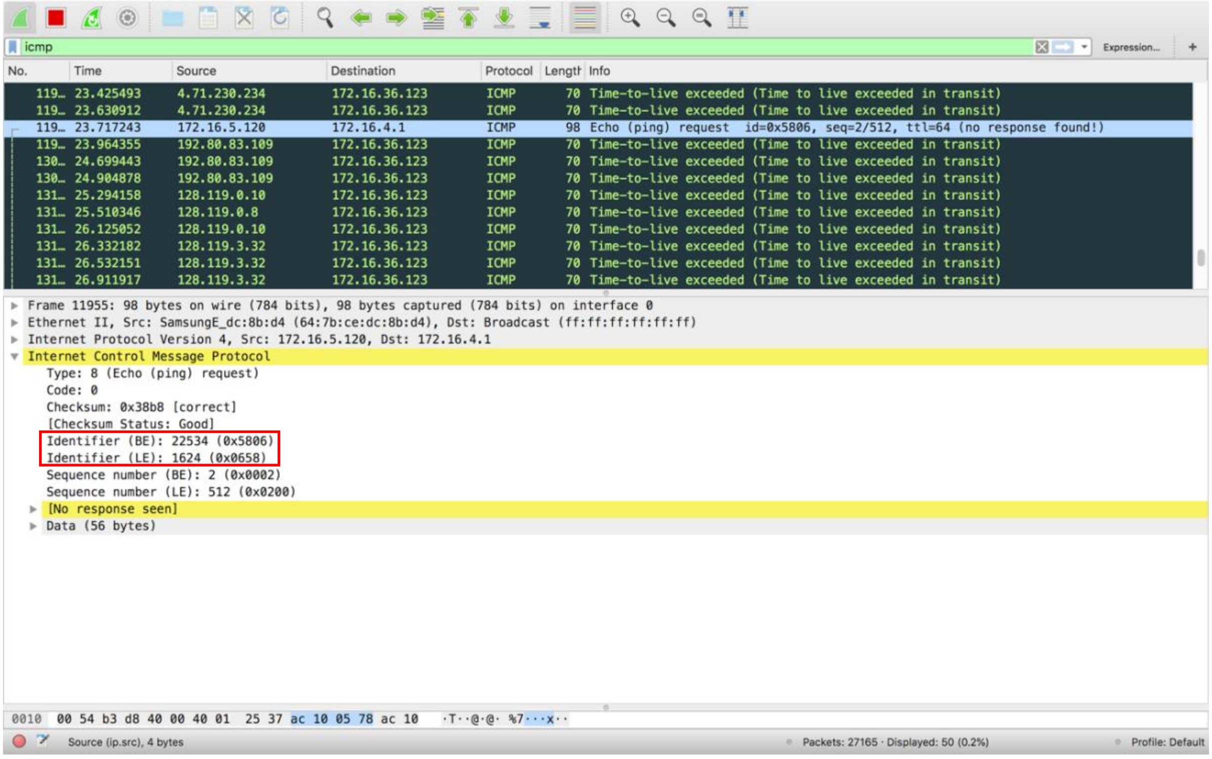
17011599 안정연, 17011588 노하윤

1. What is the IP address of your computer?

The IP address of my computer is 172.16.36.123

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 (0X01)



```
No.    Time       Source          Destination     Protocol Lengtł Info
 119… 23.425493  4.71.230.234    172.16.36.123   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 119… 23.630912  4.71.230.234    172.16.36.123   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 119… 23.717243  172.16.5.120    172.16.4.1      ICMP       98 Echo (ping) request  id=0x5806, seq=2/512, ttl=64 (no response found!)
 119… 23.964355  192.80.83.109   172.16.36.123   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 130… 24.699443  192.80.83.109   172.16.36.123   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 130… 24.904878  192.80.83.109   172.16.36.123   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 131… 25.294158  128.119.0.10    172.16.36.123   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 131… 25.510346  128.119.0.8     172.16.36.123   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 131… 26.125052  128.119.0.10    172.16.36.123   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 131… 26.332182  128.119.3.32    172.16.36.123   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 131… 26.532151  128.119.3.32    172.16.36.123   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 131… 26.911917  128.119.3.32    172.16.36.123   ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
```

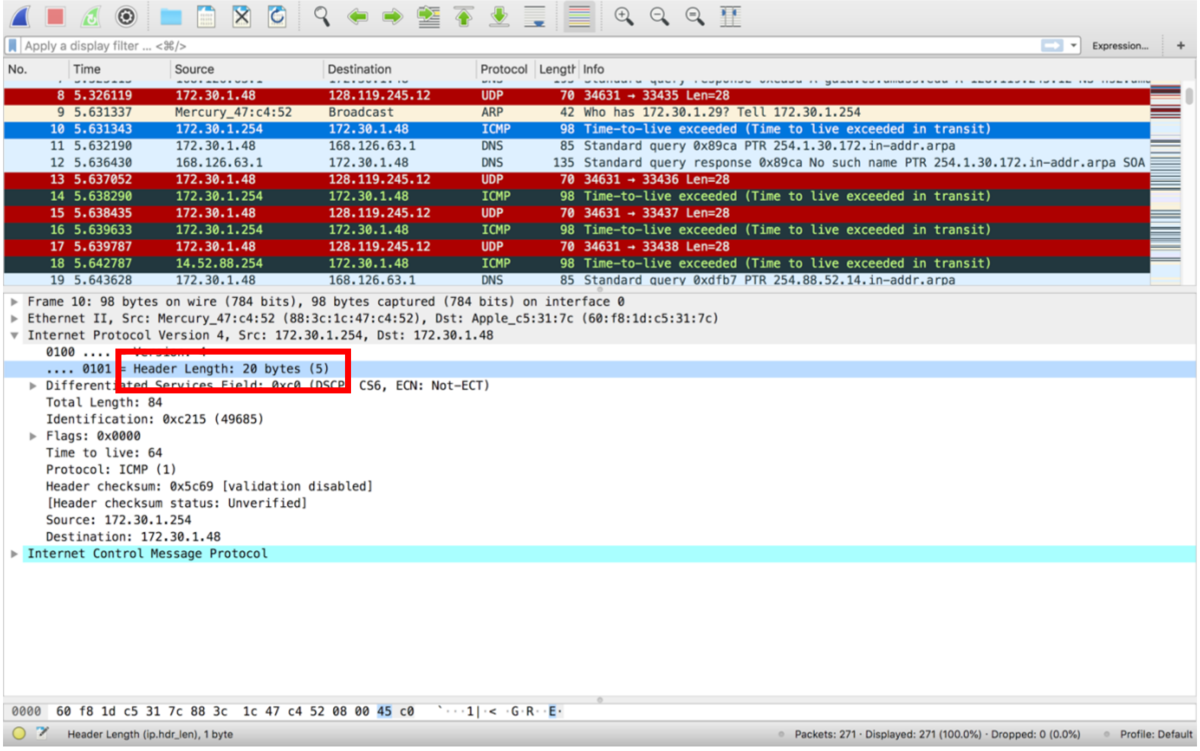
```
▶ Frame 11955: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▶ Ethernet II, Src: SamsungE_dc:8b:d4 (64:7b:ce:dc:8b:d4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Internet Protocol Version 4, Src: 172.16.5.120, Dst: 172.16.4.1
▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x38b8 [correct]
    [Checksum Status: Good]
    Identifier (BE): 22534 (0x5806)
    Identifier (LE): 1624 (0x0658)
    Sequence number (BE): 2 (0x0002)
    Sequence number (LE): 512 (0x0200)
  ▶ [No response seen]
  ▶ Data (56 bytes)
```

```
0010  00 54 b3 d8 40 00 40 01  25 37 ac 10 05 78 ac 10   ·T··@·@· %7···x··
```

Source (ip.src), 4 bytes   Packets: 27165 · Displayed: 50 (0.2%)   Profile: Default

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 the IP header which leaves 36 bytes for the payload of the IP datagram because we were sending a packet of length 56 bytes



```
No.  Time      Source             Destination      Protocol Length Info
  8 5.326119  172.30.1.48        128.119.245.12   UDP       70 34631 → 33435 Len=28
  9 5.631337  Mercury_47:c4:52   Broadcast        ARP       42 Who has 172.30.1.29? Tell 172.30.1.254
 10 5.631343  172.30.1.254       172.30.1.48      ICMP      98 Time-to-live exceeded (Time to live exceeded in transit)
 11 5.632190  172.30.1.48        168.126.63.1     DNS       85 Standard query 0x89ca PTR 254.1.30.172.in-addr.arpa
 12 5.636430  168.126.63.1       172.30.1.48      DNS      135 Standard query response 0x89ca No such name PTR 254.1.30.172.in-addr.arpa SOA
 13 5.637052  172.30.1.48        128.119.245.12   UDP       70 34631 → 33436 Len=28
 14 5.638290  172.30.1.254       172.30.1.48      ICMP      98 Time-to-live exceeded (Time to live exceeded in transit)
 15 5.638435  172.30.1.48        128.119.245.12   UDP       70 34631 → 33437 Len=28
 16 5.639633  172.30.1.254       172.30.1.48      ICMP      98 Time-to-live exceeded (Time to live exceeded in transit)
 17 5.639787  172.30.1.48        128.119.245.12   UDP       70 34631 → 33438 Len=28
 18 5.642787  14.52.88.254       172.30.1.48      ICMP      98 Time-to-live exceeded (Time to live exceeded in transit)
 19 5.643628  172.30.1.48        168.126.63.1     DNS       85 Standard query 0xdfb7 PTR 254.88.52.14.in-addr.arpa
```

```
▶ Frame 10: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▶ Ethernet II, Src: Mercury_47:c4:52 (88:3c:1c:47:c4:52), Dst: Apple_c5:31:7c (60:f8:1d:c5:31:7c)
▼ Internet Protocol Version 4, Src: 172.30.1.254, Dst: 172.30.1.48
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xc215 (49685)
  ▶ Flags: 0x0000
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x5c69 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.30.1.254
    Destination: 172.30.1.48
▶ Internet Control Message Protocol
```

```
0000  60 f8 1d c5 31 7c 88 3c  1c 47 c4 52 08 00 45 c0   `···1|·< ·G·R··E·
```

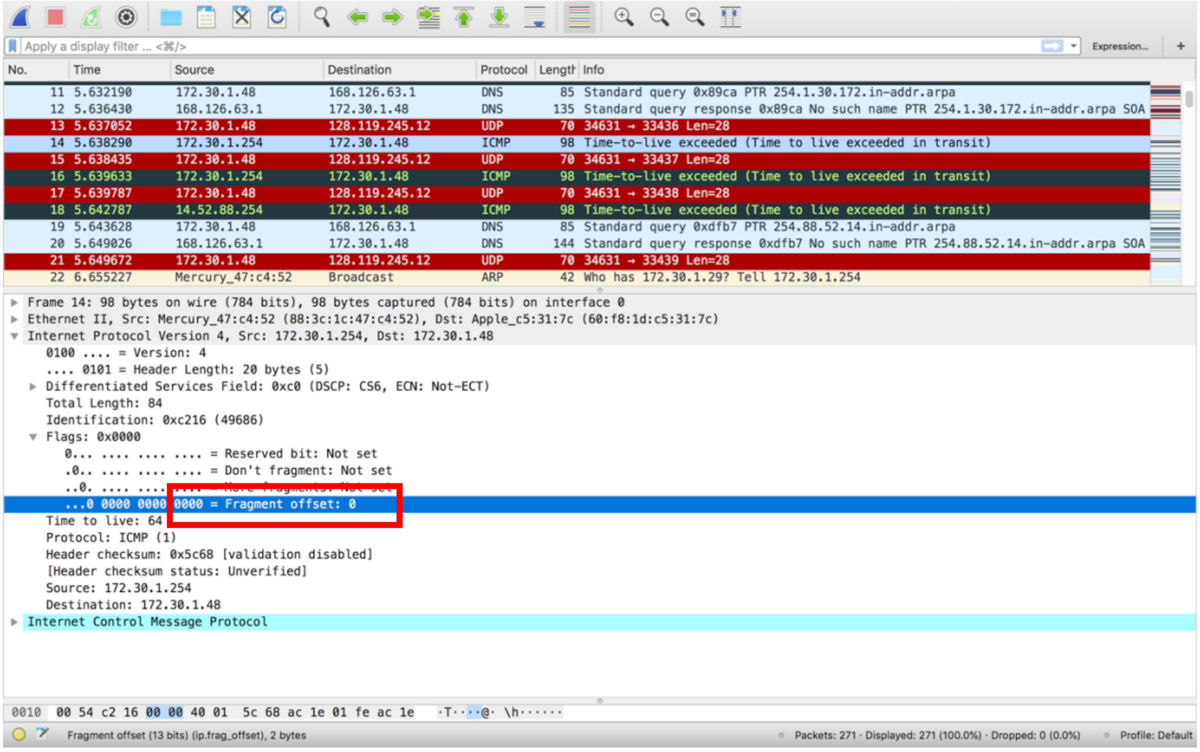
Header Length (ip.hdr_len), 1 byte

Packets: 271 · Displayed: 271 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

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.



```
No.  Time      Source             Destination      Protocol Length Info
 11 5.632190  172.30.1.48        168.126.63.1     DNS       85 Standard query 0x89ca PTR 254.1.30.172.in-addr.arpa
 12 5.636430  168.126.63.1       172.30.1.48      DNS      135 Standard query response 0x89ca No such name PTR 254.1.30.172.in-addr.arpa SOA
 13 5.637052  172.30.1.48        128.119.245.12   UDP       70 34631 → 33436 Len=28
 14 5.638290  172.30.1.254       172.30.1.48      ICMP      98 Time-to-live exceeded (Time to live exceeded in transit)
 15 5.638435  172.30.1.48        128.119.245.12   UDP       70 34631 → 33437 Len=28
 16 5.639633  172.30.1.254       172.30.1.48      ICMP      98 Time-to-live exceeded (Time to live exceeded in transit)
 17 5.639787  172.30.1.48        128.119.245.12   UDP       70 34631 → 33438 Len=28
 18 5.642787  14.52.88.254       172.30.1.48      ICMP      98 Time-to-live exceeded (Time to live exceeded in transit)
 19 5.643628  172.30.1.48        168.126.63.1     DNS       85 Standard query 0xdfb7 PTR 254.88.52.14.in-addr.arpa
 20 5.649026  168.126.63.1       172.30.1.48      DNS      144 Standard query response 0xdfb7 No such name PTR 254.88.52.14.in-addr.arpa SOA
 21 5.649672  172.30.1.48        128.119.245.12   UDP       70 34631 → 33439 Len=28
 22 6.655227  Mercury_47:c4:52   Broadcast        ARP       42 Who has 172.30.1.29? Tell 172.30.1.254
```

```
▶ Frame 14: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▶ Ethernet II, Src: Mercury_47:c4:52 (88:3c:1c:47:c4:52), Dst: Apple_c5:31:7c (60:f8:1d:c5:31:7c)
▼ Internet Protocol Version 4, Src: 172.30.1.254, Dst: 172.30.1.48
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xc216 (49686)
  ▼ Flags: 0x0000
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x5c68 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.30.1.254
    Destination: 172.30.1.48
▶ Internet Control Message Protocol
```

```
0010  00 54 c2 16 00 00 40 01  5c 68 ac 1e 01 fe ac 1e   ·T····@· \h······
```

Fragment offset (13 bits) (ip.frag_offset), 2 bytes

Packets: 271 · Displayed: 271 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

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 and the Identification changes from each datagram to the next.

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

Fields that stay constant:

- Version(IPv4)
- Length of header
- Source IP(sending from same place)
- Destination IP(contacting same site)
- Upper layer protocol(always using ICMP)

Fields that must stay constant:

- Same as above

The fields that must change are:

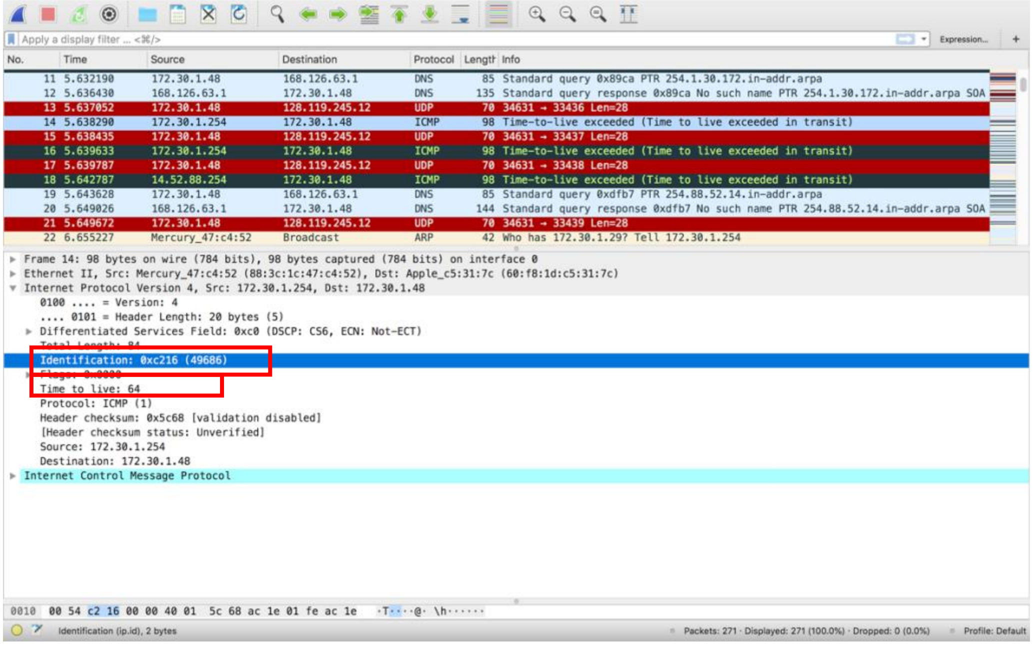
- The header checksum (header changes)
- Identification(to verify packets)

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

The pattern is that the IP header Identification fields increment with each ICMP Echo (ping) request.

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

- Identification: 49686
- TTL: 64



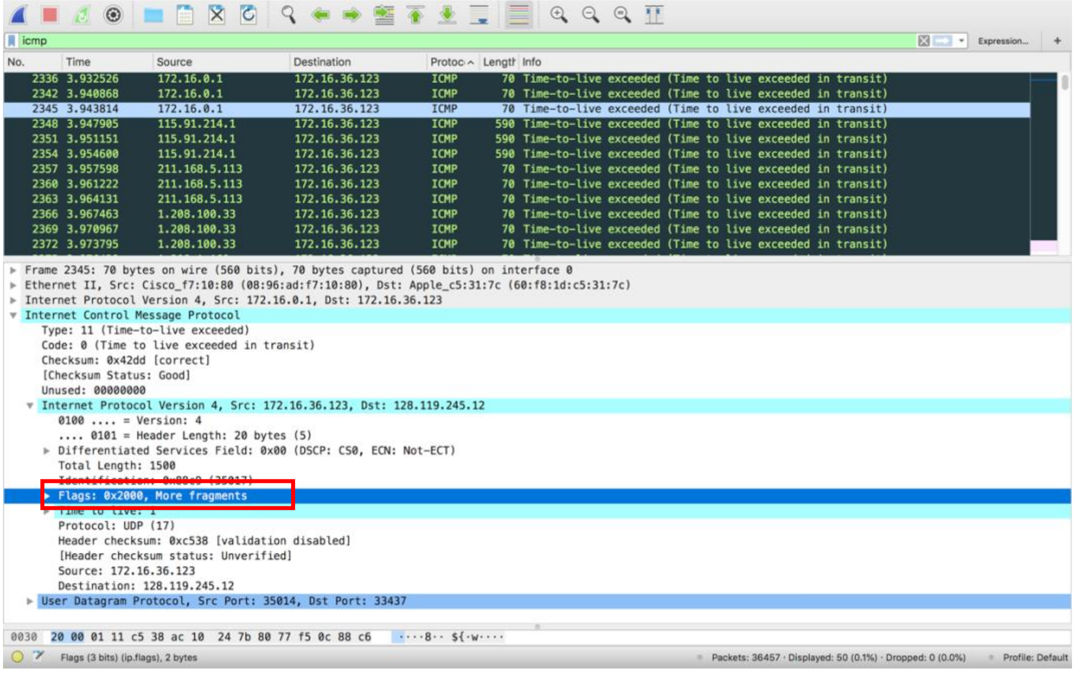
```
Apply a display filter ... <⌘/>                                                        Expression...  +
No.  Time      Source            Destination       Protocol Length Info
  11 5.632190  172.30.1.48       168.126.63.1      DNS        85 Standard query 0x89ca PTR 254.1.30.172.in-addr.arpa
  12 5.636430  168.126.63.1      172.30.1.48       DNS       135 Standard query response 0x89ca No such name PTR 254.1.30.172.in-addr.arpa SOA
  13 5.637052  172.30.1.48       128.119.245.12    UDP        70 34631 → 33436 Len=28
  14 5.638290  172.30.1.254      172.30.1.48       ICMP       98 Time-to-live exceeded (Time to live exceeded in transit)
  15 5.638435  172.30.1.48       128.119.245.12    UDP        70 34631 → 33437 Len=28
  16 5.639633  172.30.1.254      172.30.1.48       ICMP       98 Time-to-live exceeded (Time to live exceeded in transit)
  17 5.639787  172.30.1.48       128.119.245.12    UDP        70 34631 → 33438 Len=28
  18 5.642787  14.52.88.254      172.30.1.48       ICMP       98 Time-to-live exceeded (Time to live exceeded in transit)
  19 5.643628  172.30.1.48       168.126.63.1      DNS        85 Standard query 0xdfb7 PTR 254.88.52.14.in-addr.arpa
  20 5.649026  168.126.63.1      172.30.1.48       DNS       144 Standard query response 0xdfb7 No such name PTR 254.88.52.14.in-addr.arpa SOA
  21 5.649672  172.30.1.48       128.119.245.12    UDP        70 34631 → 33439 Len=28
  22 6.655227  Mercury_47:c4:52  Broadcast         ARP        42 Who has 172.30.1.29? Tell 172.30.1.254

▶ Frame 14: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▶ Ethernet II, Src: Mercury_47:c4:52 (88:3c:1c:47:c4:52), Dst: Apple_c5:31:7c (60:f8:1d:c5:31:7c)
▼ Internet Protocol Version 4, Src: 172.30.1.254, Dst: 172.30.1.48
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xc216 (49686)
  ▶ Flags: 0x0000
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x5c68 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.30.1.254
    Destination: 172.30.1.48
▶ Internet Control Message Protocol

0010  00 54 c2 16 00 00 40 01  5c 68 ac 1e 01 fe ac 1e   ·T····@· \h······
Identification (ip.id), 2 bytes        Packets: 271 · Displayed: 271 (100.0%) · Dropped: 0 (0.0%)    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?

- The Identification field changes from all of the replies because this field has to 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 pingplotterto be 2000. Has that message been fragmented across more than one IP datagram?

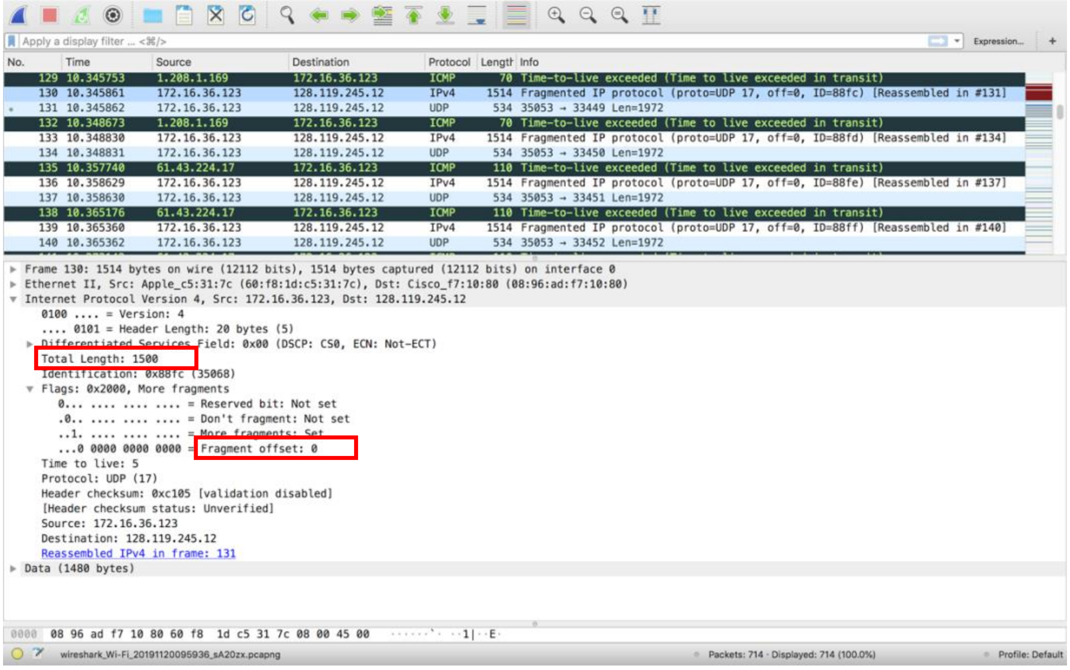
Yes, that message has been fragmented across more than one IP datagram.



```
icmp
No.   Time      Source          Destination     Protocol Length Info
 2336 3.932526  172.16.0.1      172.16.36.123   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 2342 3.940868  172.16.0.1      172.16.36.123   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 2345 3.943814  172.16.0.1      172.16.36.123   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 2348 3.947905  115.91.214.1    172.16.36.123   ICMP     590 Time-to-live exceeded (Time to live exceeded in transit)
 2351 3.951151  115.91.214.1    172.16.36.123   ICMP     590 Time-to-live exceeded (Time to live exceeded in transit)
 2354 3.954600  115.91.214.1    172.16.36.123   ICMP     590 Time-to-live exceeded (Time to live exceeded in transit)
 2357 3.957598  211.168.5.113   172.16.36.123   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 2360 3.961222  211.168.5.113   172.16.36.123   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 2363 3.964131  211.168.5.113   172.16.36.123   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 2366 3.967463  1.208.100.33    172.16.36.123   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 2369 3.970967  1.208.100.33    172.16.36.123   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 2372 3.973795  1.208.100.33    172.16.36.123   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)

▸ Frame 2345: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▸ Ethernet II, Src: Cisco_f7:10:80 (08:96:ad:f7:10:80), Dst: Apple_c5:31:7c (60:f8:1d:c5:31:7c)
▸ Internet Protocol Version 4, Src: 172.16.0.1, Dst: 172.16.36.123
▾ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0x42dd [correct]
    [Checksum Status: Good]
    Unused: 00000000
  ▾ Internet Protocol Version 4, Src: 172.16.36.123, Dst: 128.119.245.12
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 1500
      Identification: 0x88c9 (35017)
    ▸ Flags: 0x2000, More fragments
      Time to live: 1
      Protocol: UDP (17)
      Header checksum: 0xc538 [validation disabled]
      [Header checksum status: Unverified]
      Source: 172.16.36.123
      Destination: 128.119.245.12
  ▸ User Datagram Protocol, Src Port: 35014, Dst Port: 33437

0030  20 00 01 11 c5 38 ac 10  24 7b 80 77 f5 0c 88 c6   ····8·· ${·w····
Flags (3 bits) (ip.flags), 2 bytes          Packets: 36457 · Displayed: 50 (0.1%) · 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?

The fact that the flag is set for more segments shows that the datagram has been fragmented (see above). The fragment offset is set to 0 indicating 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.



```
Apply a display filter ... <⌘/>
No.   Time       Source          Destination     Protocol Length Info
  129 10.345753  1.208.1.169     172.16.36.123   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  130 10.345861  172.16.36.123   128.119.245.12  IPv4    1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=88fc) [Reassembled in #131]
  131 10.345862  172.16.36.123   128.119.245.12  UDP      534 35053 → 33449 Len=1972
  132 10.348673  1.208.1.169     172.16.36.123   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  133 10.348830  172.16.36.123   128.119.245.12  IPv4    1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=88fd) [Reassembled in #134]
  134 10.348831  172.16.36.123   128.119.245.12  UDP      534 35053 → 33450 Len=1972
  135 10.357740  61.43.224.17    172.16.36.123   ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
  136 10.358629  172.16.36.123   128.119.245.12  IPv4    1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=88fe) [Reassembled in #137]
  137 10.358630  172.16.36.123   128.119.245.12  UDP      534 35053 → 33451 Len=1972
  138 10.365176  61.43.224.17    172.16.36.123   ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
  139 10.365360  172.16.36.123   128.119.245.12  IPv4    1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=88ff) [Reassembled in #140]
  140 10.365362  172.16.36.123   128.119.245.12  UDP      534 35053 → 33452 Len=1972

▸ Frame 130: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▸ Ethernet II, Src: Apple_c5:31:7c (60:f8:1d:c5:31:7c), Dst: Cisco_f7:10:80 (08:96:ad:f7:10:80)
▾ Internet Protocol Version 4, Src: 172.16.36.123, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x88fc (35068)
  ▾ Flags: 0x2000, More fragments
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..1. .... .... .... = More fragments: Set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 5
    Protocol: UDP (17)
    Header checksum: 0xc105 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.16.36.123
    Destination: 128.119.245.12
    Reassembled IPv4 in frame: 131
▸ Data (1480 bytes)

0000  08 96 ad f7 10 80 60 f8  1d c5 31 7c 08 00 45 00   ······`· ··1|··E·
wireshark_Wi-Fi_20191120095936_sA20zx.pcapng     Packets: 714 · Displayed: 714 (100.0%)     Profile: Default
```

12. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?

The 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.

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

The fields that change are

1. Length
2. Flags Set
3. Fragment offset
4. header checksum

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

After switching to 3500, there are 3 packets created from the original datagram.

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 fragments flags set, while the last fragment is shorter (540) and does not have a flag set.